الاتحـــــــاد الـــدولـــــــي للاتصـــــــالات

ITU-T X.1141

(2006/06)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات المعطيات، الاتصال بين الأنظمة المفتوحة والأمن

أمـــن الاتصـــالات

اللغة التأشيرية للتدعيم الأمني (SAML 2.0)

التوصيـــة ITU-T X.1141

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن

الشبكات العمومية للمعطيات	
الخدمات والمرافق	X.1–X.19
السطوح البينية	X.20–X.49
الإرسال والتشوير والتبديل	X.50–X.89
جوانب الشبكة	X.90–X.149
الصيانة	X.150–X.179
الترتيبات الإدارية	X.180–X.199
التوصيل البيني للأنظمة المفتوحة	
النموذج والترميز	X.200–X.209
تعاريف الخدمات	X.210–X.219
مواصفات البروتوكول بأسلوب التوصيل	X.220–X.229
مواصفات البروتوكول بأسلوب غياب التوصيل	X.230–X.239
جداول إعلان المطابقة (PICS)	X.240–X.259
تعرّف هوية البروتوكول	X.260–X.269
بروتوكولات الأمن	X.270–X.279
أشياء مسيرة على الطبقة	X.280–X.289
اختبار المطابقة	X.290–X.299
التشغيل البيني للشبكات	
اعتبارات عامة	X.300–X.349
الأنظمة الساتلية لإرسال البيانات	X.350–X.369
الشبكات القائمة على بروتوكول الإنترنت	X.370–X.379
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التوصيل الشبكي في التوصيل البيني للأنظمة المفتوحة (OSI) وجوانب النظام	
التوصيل الشبكي	X.600–X.629
الفعالية	X.630–X.639
نوعية الخدمة	X.640–X.649
التسمية والعنونة والتسجيل	X.650–X.679
ترميز النظم المجرد واحد (ASN.1)	X.680–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	
الإطار والهيكل المعماري لإدارة الأنظمة	X.700–X.709
خدمة اتصالات الإدارة وبروتوكولاتها	X.710–X.719
هيكل معلومات الإدارة	X.720–X.729
وظائف الإدارة ووظائف الهيكل المعماري للإدارة الموزعة المفتوحة	X.730–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	
الالتزام والتلازم والاستعادة	X.850–X.859
معالجة المعاملات	X.860–X.879
العمليات البُعدية	X.880–X.889
التطبيقات التنوعية لترميز النظم المجرد واحد (ASN.1)	X.890–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن الاتصالات	**X.1000–**

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

اللغة التأشيرية للتدعيم الأمني (SAML 2.0)

الموجـــز

اللغة SAML هي إطار عمل مبني على اللغة التأشيرية التوسيعة (XML) بشأن تبادل المعلومات الأمنية. ويعبر عن هذه المعلومات الأمنية بشكل تأكيدات حول أصحاب، والصاحب هو كيان (بشري أو حاسوبي)، له هوية في ميدان أمني معين. والتأكيد يمكن أن يتضمن عدة إعلانات داخلية مختلفة بشأن الاستيقان والترخيص والنعوت. وتحدد هذه التوصية بروتوكولاً يستطيع الزبائن أن يطلبوا عبره تأكيدات من سلطات في اللغة SAML، وأن يحصلوا على استجابات منها. ويمكن لهذا البروتوكول الذي يكمن في أنساق رسائل طلبات واستجابات مبنية على اللغة XML، أن يكون مرتبطاً ببروتوكولات عديدة تحتية مختلفة للاتصال والنقل. وتحدد اللغة SAML حالياً رابطة إلى بروتوكول مبسط للنفاذ إلى الهدف (SOAP) محمول على بروتوكول نقل نص فائق (HTTP). وتستطيع سلطات اللغة SAML أثناء تحضيرها الاستجابات أن تستخدم مصادر مختلفة للمعلومات مثل ذاكرات وتأكيدات خارجية تخص السياسة قد تكون استلمتها في مدخلات طلبات. وتعرف هذه التوصية عناصر تأكيدات اللغة SAML وأصحابها وشروطها وقواعد معالجتها والإعلانات عنها. وهي تفصل كذلك جانبية (لاحة) لمعطيات شرحية كاملة للغة SAML تتضمن مكان اسم مصاحباً، وأنماط من المعطيات المشتركة، وقواعد المعالجة، ومعالجة التوقيع. كما يوجد فيها عرض مفصل لروابط بروتوكولية عديدة من بينها البروتوكول المبسط للنفاذ إلى الهدف (SOAP) وPAOS (وهو مقلوب SOAP)، وبروتوكول نقل نص فائق (HTTP) معاد التوجيه، وإرسال البروتوكول HTTP بالبريد (HTTP POST)، وتقدم التوصية قائمة شاملة بلاحات اللغة SAML، مثل لاحة التصفح لشبكة الويب باكتتاب وحيد، ولاحة وحيدة لاختتام دورة، حتى تسمح بقبول اللغة SAML 2.0 على نطاق واسع في الصناعة. كما وتقدم التوصية خطوطاً توجيهية لسياق الاستيقان والمطابقة.

وتكافئ هذه التوصية المعيار OASIS SAML 2.0 تقنياً وتتواءم معه. (OASIS: المنظمة المعنية بتقدم معايير المعلومات المهيكلة).

المصدر

وافقت لجنة الدراسات 17 (2005-2008) التابعة لقطاع تقييس الاتصالات بتاريخ 13 يونيو 2006 على التوصية ITU-T X.1141 بموجب الإجراء المحدد في التوصية ITU-T A.8.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA)، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

الصفحة

اللغة التأشيرية للتدعيم الأمني (SAML 2.0)

1 مجال التطبيق

تحدد هذه التوصية اللغة التأشيرية للتدعيم الأمني (SAML 2.0). وهذه اللغة SAML تحدد عِلمي النحو (قواعد التركيب) والدلالات المستعملين في معالجة التأكيدات التي يقدمها كيان من نظام بشأن موضوع ما. وأثناء تقديم هذه التأكيدات، أو أثناء الاعتماد عليها، تستطيع كيانات النظام في اللغة SAML استخدام بروتوكولات أخرى للإفادة عن التأكيد نفسه أو للإفادة عن موضوع التأكيد. وهذه التوصية تحدد بنى تأكيدات اللغة SAML، ومجموعة مصاحبة من البروتوكولات، إضافة إلى قواعد المعالجة المتداخلة في إدارة نظام في اللغة SAML.

وتشفر تأكيدات اللغة SAML ورسائل البروتوكول فيها باللغة التأشيرية التوسّعية (XML)، وتستخدم أماكن الأسماء في هذه اللغة. وتكون مبيتة عادة في بنى أخرى مستخدمة للنقل، مثل طلبات الإرسال بالبريد HTTP POST أو رسائل البروتوكول SOAP المشفرة في اللغة XML. وتحدد هذه التوصية كذلك روابط في اللغة SAML توفر أطر عمل لتبييت ونقل رسائل بروتوكول اللغة SAML. وتقدم هذه التوصية فوق ذلك مجموعة أساسية من الجانبيات (اللاحات)، لاستخدامها في تأكيدات وبروتوكولات اللغة SAML من أجل معالجة حالات استعمال خاصة أو من أجل تحقيق التشغيل البيني عند استخدام ميزات اللغة SAML.

وتعرف هذه التوصية الأمور التالية:

1) متطلبات المطابقة في اللغة SAML؛
2) التأكيدات والبروتوكولات في اللغة SAML:
   - تخطيطة تأكيدات اللغة SAML؛
   - تخطيطة بروتوكولات اللغة SAML؛
3) الروابط في اللغة SAML؛
4) جانبيات اللغة SAML:
   - تخطيطة جانبية الزبون ECP في اللغة SAML؛
   - تخطيطة جانبية النعت X.500/LDAP في اللغة SAML؛
   - تخطيطة جانبية النعت DCE PAC في اللغة SAML؛
   - تخطيطة جانبية النعت XACML في اللغة SAML؛
5) معطيات شرحية للغة SAML؛
6) تخطيطة المعطيات الشرحية للغة SAML:
7) سياق الاستيقان في اللغة SAML.

2 المراجـــع

تتضمن التوصيات التالية وغيرها من المراجع أحكاماً تصبح بمجرد الإحالة إليها في هذا النص، أحكاماً من هذه التوصية. وقد كانت جميع الطبعات المشار إليها بأرقامها صالحة في وقت نشرها. ولما كانت جميع التوصيات والمراجع الأخرى عرضة للمراجعة، فإن الأطراف المشتركة في اتفاقات مبنية على هذه التوصية، مدعوون جميعاً إلى أن يطبقوا، ما أمكنهم، أحدث

طبعات للتوصيات والمراجع الأخرى المعددة أدناه. ويحتفظ مكتب تقييس الاتصالات في الاتحاد الدولي للاتصالات بقائمة مُحَيّنة بتوصيات القطاع ITU-T النافذة. كما يحتفظ فريق المهام الهندسية في الإنترنت (IEFT) بقائمة محينة بطلبات التعليقات (RFC)، وكذلك بالطلبات RFC التي صارت بالية بفعل الطلبات RFC الأحدث منها. كما يحتفظ تجمع شبكة الويب العالمية (W3C) والشفرة الموحدة للتجمع (Unicode Consortium)، واتحاد الحرية (Liberty Alliance) بقائمة مُحَيّنة بأحدث التوصيات والمنشورات الأخرى.

– ITU-T Recommendation X.660 (2004) | ISO/IEC 9834-1:2005, Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree.

– ITU-T Recommendation X.667 (2004) | ISO/IEC 9834-8:2005, Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Generation and Registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components.

– ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.

– ITU-T Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

– ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: authentication framework.

– ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.

– ITU-T Recommendation X.1142 (2006), eXtensible Access Control Markup Language (XACML 2.0).

– IETF RFC 1034 (1987), Domain Names – Concepts and Facilities.

– IETF RFC 1510 (1993), The Kerberos Network Authentication Service (V5).

– IETF RFC 1750 (1994), Randomness Recommendations for Security.

– IETF RFC 1951 (1996), DEFLATE Compressed Data Format Specification Version 1.3.

– IETF RFC 1991 (1996), PGP Message Exchange Formats.

– IETF RFC 2045 (1996), Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.

– IETF RFC 2119 (1997), Keywords for use in RFCs to Indicate Requirement Levels.

– IETF RFC 2246 (1999), The TLS Protocol Version 1.0.

– IETF RFC 2253 (1997), Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names.

– IETF RFC 2396 (1998), Uniform Resource Identifiers (URI): Generic Syntax.

– IETF RFC 2535 (1999), Domain Name System Security Extensions.

– IETF RFC 2616 (1999), Hypertext Transfer Protocol – HTTP/1.1.

– IETF RFC 2617 (1999), HTTP Authentication: Basic and Digest Access Authentication.

– IETF RFC 2798 (2000), Definition of the inetOrgPerson LDAP Object Class.

– IETF RFC 2828 (2000), Internet Security Glossary.

– IETF RFC 2914 (2000), Congestion Control Principles.

– IETF RFC 2915 (2000), The Naming Authority Pointer (NAPTR) DNS Resource Record.

– IETF RFC 2945 (2000), The SRP Authentication and Key Exchange System.

– IETF RFC 2965 (2000), HTTP State Management Mechanism.

– IETF RFC 3023 (2001), *XML Media Types*.

– IETF RFC 3061 (2001), A URN Namespace of Object Identifiers.

– IETF RFC 3075 (2001), XML-Signature Syntax and Processing.

– IETF RFC 3377 (2002), Lightweight Directory Access Protocol (v3): Technical Specification.

– IETF RFC 3403 (2002), Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database.

– IETF RFC 3513 (2003), Internet Protocol Version 6 (IPv6) Addressing Architecture.

– IETF RFC 3546 (2003), Transport Layer Security (TLS) Extensions.

– IETF RFC 3923 (2004), End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP).

– IETF RFC 4122 (2005), A Universally Unique IDentifier (UUID) URN Namespace.

– Liberty Alliance POAS:2003, R. Aarts, Liberty Reverse HTTP Binding for SOAP Specification Version 1.0, Liberty Alliance Project.

– OASIS WSS:2006, WS-Security Core Specification 1.1.

– UNICODE-C, M. Davis; M. J. Dürst: *Unicode Normalization Forms.* UNICODE Consortium, March 2001.

– W3C Canonicalization:2002, *Exclusive XML Canonicalization Version 1.0,* W3C Recommendation, Copyright © [18 July 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xml-exc-c14n/.

– W3C Character Model:2005*, Character Model for the World Wide Web 1.0: Fundamentals,* W3C Recommendation, Copyright © [15 February 2005] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2005/REC-charmod-20050215/.

– W3C Datatypes:2001, *XML Schema Part 2: Datatypes,* W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/.

– W3C Encryption:2002, *XML Encryption Syntax and Processing,* W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

– W3C Web Services Glossary:2004, *Web Services Glossary,* W3C Note, Copyright © [11 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/ws-gloss/.

– W3C HTML:1999, *HTML 4.01 Specification,* W3C Recommendation, Copyright © [24 December 1999] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-html40/.

– W3C Namespaces:1999, *Namespaces in XML,* W3C Recommendation, Copyright © [14 January 1999] World Wide Web Consortium (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml-names/.

– W3C Primer:2005, *SOAP Version 1.2 Part 0: Primer,* W3C Recommendation, Copyright © [24 June 2005] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2003/REC-soap12-part0-20030624/.

– W3C Signature:2002, *XML Signature Syntax and Processing,* W3C Recommendation, Copyright © [12 February 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xmldsigcore/.

– W3C Signature Schema:2001, *XML Signature Schema,* W3C Recommendation, Copyright © [1 March 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd.

– W3C String:1998, *Requirements for String Identity Matching and String Indexing,* W3C Note, Copyright © [10 July 1998] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University, http://www.w3.org/TR/WD-charreq.

– W3C SOAP:2000, *Simple Object Access Protocol (SOAP) 1.1,* W3C Note, Copyright © [08 May 2000] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2000/NOTE-SOAP-20000508.

– W3C XHTML:2002, *The Extensible HyperText Markup Language (Second Edition),* W3C Recommendation, Copyright © [1 August 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University*),* http://www.w3.org/TR/xhtml1/.

– W3C XML 1.0:2004, *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/REC-xml/.

– W3C XML Schema Part 1:2001, *XML Schema Part 1: Structures,* W3C Recommendation, Copyright © [2 May 2001] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/.

ملاحظة – الإحالة إلى وثيقة داخل هذه التوصية، لا يمنحها، كوثيقة مستقلة، الوضع القانوني لتوصية.

3 تعريفـــات

تطبق التعريفات التالية لأغراض هذه التوصية.

1.3 تعريفات مستوردة

1.1.3 تستخدم هذه التوصية المصطلح التالي المعّرف في التوصية ITU-T X.667:

أ) معرف هوية وحيد عالمي (UUID).

2.1.3 تستخدم هذه التوصية المصطلحين التاليين المعّرفين في التوصية ITU-T X.680:

أ) معرف هوية شيء؛

ب) ترميز نمط مفتوح.

3.1.3 تستخدم هذه التوصية المصطلح التالي المعّرف في التوصية ITU-T X.811:

أ) المبدأ.

4.1.3 تستخدم هذه التوصية المصطلحين التاليين المعّرفين في التوصية ITU-T X.812:

أ) معلومات التحكم في النفاذ؛

ب) المستعمل (المستخدم).

5.1.3 تستخدم هذه التوصية المصطلحات التالية المعّرفة في معجم خدمات الويب الصادر عن التجمع W3C:

أ) المرسل الأولي للبروتوكول SOAP؛

ب) مكان اسم؛

ج) المستلم النهائي للبروتوكول SOAP.

6.1.3 تستخدم هذه التوصية المصطلحات التالية المعّرفة في طلب التعليقات 2828 (RFC) الصادر عن فريق المهام الهندسية في الإنترنت (IETF):

أ) نفاذ؛

ب) تحكم في النفاذ؛

ج) الوكيل المفوَّض؛

د) المخدِّم الوكيل المفوَّض؛

ه) يسحب؛

و) يدفع؛

ز) معمارية أمنية؛

ح) سياسة أمنية؛

ط) خدمة أمنية.

7.1.3 تستخدم هذه التوصية المصطلحين التاليين المعّرفين في الطلب RFC 2396 الصادر عن الفريق IETF:

أ) معرف هوية موحد للموارد (URI)؛

ب) مرجع معرف الهوية URI.

2.3 تعريفات إضافية

1.2.3 حقوق النفاذ (access rights): وصف لنمط من التعاملات المرخص لصاحب أن تكون له مع مورد ما، مثل عمليات القراءة والكتابة والتنفيذ والإضافة والتعديل والإلغاء.

2.2.3 حساب (account): اتفاق تجاري رسمي لتقديم معاملات وخدمات بشكل منتظم، بين طرف رئيسي ومزوّد خدمات تجارية.

3.2.3 رابطة حساب (account linkage): طريقة لربط حسابات مزوّدين اثنين مختلفين يمثلان نفس الطرف الرئيسي، بحيث يتمكن المزوّدان من التواصل بشأن الطرف الرئيسي. ويمكن إنشاء رابطة حساب عبر تقاسم النعوت أو اتحاد الهويات.

4.2.3 دور نشيط (فاعل) (active role): الدور الذي يؤديه كيان في نظام عند أدائه عملية ما، عند النفاذ إلى مورد مثلاً.

5.2.3 ميدان إداري (administration domain): بيئة أو سياق تعرفه تجميعة من سياسة إدارية واحدة أو عدة، مع تسجيلات أسماء ميادين في الإنترنت، وكيانات مدنية شرعية (أفراد أو شركات أو كيانات أخرى منظمة بشكل رسمي)، بالإضافة إلى مجموعة من المضيفين وأجهزة الشبكة وشبكات التوصيل البيني (أو غيرها من الملامح المحتملة)، وبالإضافة أيضاً إلى خدمات وتطبيقات شبكة (متنوعة غالباً) تدور حولها. ويمكن أن يحتوي الميدان الإداري على ميدان أمني واحد أو عدة أو أن يعرفها. ويمكن أن يتضمن الميدان الإداري موقعاً واحداً أو عدة. ويمكن أن تتطور الملامح التي تحدد ميداناً إدارياً بتطور الزمن. وأن يحدث ذلك مرات عديدة. ويمكن للميادين الإدارية أن تتعامل مع بعضها، وأن تعقد اتفاقات فيما بينها بشأن تقديم و/أو استعمال خدمات عبر حدودها الإدارية.

6.2.3 مسؤول إداري (administrator): شخص يقيم نظاماً أو يؤمن صيانته أو يستخدمه لإدارة كيانات نظام و/أو مستعمليه و/أو محتوياته. يمكن أن يكون المسؤول الإداري تابعاً لميدان إداري معين، أو أن يكون تابعاً لأكثر من ميدان إداري واحد.

7.2.3 الانتساب، جماعة المنتسبين، الجماعة المنتسبة (affiliation, affiliation group): مجموعة من كيانات نظام تتقاسم مكان اسم واحد (بالمعنى التوحيدي) لمعرفات هوية الأطراف الرئيسية.

8.2.3 إغفال الاسم (anonymity): صفة أو حالة كون الشيء مغفل الاسم، وهو الظرف الذي يكون فيه للشيء اسم هوية مجهولان أو مخفيان.

9.2.3 الطرف المؤكِّد (asserting party): رسمياً، هو الميدان الإداري الذي يستضيف سلطة واحدة من سلطات اللغة SAML أو أكثر، وبصورة غير رسمية، هو مرحلة (درجة) من سلطة في اللغة SAML.

10.2.3 تأكيد (assertion): جزء من المعطيات تنتجه سلطة في اللغة SAML، ويخص فعل استيقان يتعلق بصاحب، أو معلومات نعت بشأن صاحب، أو معطيات ترخيص تنطبق على صاحب، بالنسبة إلى مورد معين.

11.2.3 نعت (attribute): خاصية مميزة لشيء. وفيما يخص الأشياء الحقيقية، يعبر عن النعوت غالباً بمصطلحات الملامح الفيزيائية، مثل القد والشكل والوزن واللون. أما فيما يخص أشياء الفضاء السيبري (الافتراضي) فيمكن أن تكون لها نعوت تصف القد، ومنط التشفير وعنوان الشبكة وغيرها. وتتمثل النعوت غالباً بأزواج من "اسم النعت" و"قيمة النعت"، مثل "foo" تكون له قيمة 'bar'، و"count" تكون له قيمة 1، و"gizmo" تكون له القيمتان "frob" و"2".

12.2.3 تأكيد نعت (attribute assertion): تأكيد يحمل معلومات عن نعوت صاحب.

13.2.3 سلطة نعت (attribute authority): كيان في نظام ينتج تأكيدات نعت.

14.2.3 استيقان (authentication): عملية تحديد ما إذا كان شخص أو شيء هو في الواقع ما يدّعي كونه، وذلك بدرجة معينة من الثقة.

15.2.3 تأكيد استيقان (authentication assertion): تأكيد يحمل معلومات عن عملية استيقان ناجحة أجريت حول صاحب معين.

16.2.3 سلطة استيقان (authentication authority): كيان في نظام ينتج تأكيدات استيقان.

17.2.3 ترخيص (authorization): عملية تحدد، بعد تقويم المعلومات المطبقة للتحكم في النفاذ، ما إذا كان صاحب ما مسموحاً له بالحصول على أنماط نفاذ محددة إلى مورد معين. ويكون الترخيص عادة موجوداً في سياق الاستيقان. فما أن يستيقن صاحب، حتى يمكن أن يرخص له بالقيام بأنماط مختلفة من النفاذ.

18.2.3 قرار ترخيص (authorization decision): نتيجة فعل الترخيص. وقد تكون النتيجة سلبية، أي يمكن أن تشير إلى أن الصاحب غير مرخص له بالنفاذ إلى المورد.

19.2.3 تأكيد قرار ترخيص (authorization decision assertion): تأكيد يحمل معلومات عن قرار ترخيص.

20.2.3 قناة خلفية (back channel): تحيل القناة الخلفية إلى الاتصالات المباشرة بين كيانين في نظام دون رسالة "إعادة توجيه" عبر كيان آخر في النظام، مثل زبون بروتوكول نقل نص فائق (HTTP) (مثل وكيل المستعمل).

21.2.3 رابطة، رابطة بروتوكول (binding; protocol binding): بصورة عامة، هي توصيف لوضع بعض الرسائل المعينة من بروتوكول، أو ربما تخطيطات تبادل الرسائل، على تقابل بصورة ملموسة في بروتوكول آخر. فمثلاً وضع رسالة اللغة SAML <AuthnRequest> على تقابل في بروتوكول HTTP هو رابطة. ووضع نفس رسالة اللغة SAML على تقابل في بروتوكول مبسط للنفاذ إلى الهدف (SOAP) هو رابطة أخرى. ويعطى لكل رابطة اسم في سياق اللغة SAML من التخطيطة "SAML xxx binding".

22.2.3 ثبوتيات (credentials): معطيات تنقل من أجل تنظيم هوية مطلوبة لطرف رئيسي.

23.2.3 مستعمل نهائي (end user): شخص طبيعي يستخدم موارد لأغراض تطبيقية.

24.2.3 كيان (entity): انظر "كيان نظام".

25.2.3 يوحّد (federate): يقيم وصلة أو رابطة بين كيانين أو أكثر.

26.2.3 اتحاد (federation): يستعمل هذا المصطلح في معنيين.

1) فعل إقامة علاقة بين كيانين؛
2) جمعية تضم أي عدد من مزوّدي الخدمات ومزوّدي الهويات.

27.2.3 هوية موحَّدة (federated identity): يقال عن هوية طرف رئيسي إنها موحَّدة بين مجموعة من المزوّدين، عندما يكون هناك اتفاق بين المزوّدين حول مجموعة من معرفات الهوية و/أو النعوت لاستعمالها في الإحالة إلى الطرف الرئيسي.

28.2.3 قناة جبهية (front channel): تعود القناة الجبهية إلى "قناة اتصالات" يمكن أن تقام بين مخدّمين يتكلمان بالبروتوكول HTTP، مستخدمين رسائل "البروتوكول HTTP المعاد توجيهه" وبالتالي فهما يمرران الرسائل من أحدهما إلى الآخر عبر وكيل مستعمل، أي عبر متصفح لشبكة الويب أو أي زبون آخر للبروتوكول HTTP.

29.2.3 معرف هوية (identifier): شيء من المعطيات (سلسلة مثلاً) يوضع على تقابل مع كيان من نظام، يحيل إلى هذا الكيان من النظام بطريقة وحيدة. ويمكن أن يكون لكيان في نظام عدة معرفات هوية متمايزة تحيل إليه. ومعرف الهوية هو من حيث الجوهر "نعت مميز" للكيان.

30.2.3 هوية (identity): جوهر كيان وماهيته. ويجري عادة وصف هوية الشخص بخصائصه، التي يمكن أن يكون من بينها عدد من معرفات الهوية.

31.2.3 التخلي عن توحيد الهوية (identity defederation): العمل الذي يحدث عندما يتفق المزودون على إيقاف الإحالة إلى الطرف الرئيسي عبر مجموعة من معرفات الهوية و/أو النعوت.

32.2.3 توحيد الهوية (identity federation): فعل إحداث هوية موحدّة باسم طرف رئيسي.

33.2.3 مزوّد هوية (identity provider): نوع من مزوّدي الخدمة ينشئ معلومات الهوية للأطراف الرئيسية ويؤمن صيانتها ويديرها، كما يقدم استيقان الطرف الرئيسي إلى غيره من مزوّدي الخدمة داخل اتحاد، كما في حالة جانبيات (لاحات) متصفح شبكة الويب.

34.2.3 مزوّد هوية خفيف (identity provider lite): نوع من مزوّدي الخدمة ينشئ معلومات الهوية للأطراف الرئيسية ويؤمن صيانتها ويديرها، كما يقدم استيقان الطرف الرئيسي إلى غيره من مزوّدي الخدمة داخل اتحاد، مستخدماً فقط الأجزاء اللازمة من اللغة SAML.

35.2.3 افتتاح دورة، اكتتاب (login, logon, sign-on): العملية التي يقدم فيها مستخدم ثبوتيات إلى سلطة استيقان، ويقيم دورة بسيطة أو اخيتارياً يقيم دورة غنية.

36.2.3 اختتام دورة، انسحاب (logout, logoff, sign-off): العملية التي يعبّر فيها مستخدم عن رغبته في إنهاء دورة بسيطة أو دورة غنية.

37.2.3 لغة إرشادية (markup language): مجموعة من عناصر ونعوت اللغة الإرشادية التوسّعية (XML)، مطلوب تطبيقها على بنية وثيقة باللغة XML لغرض محدّد. وتعرّف عادة اللغة الإرشادية عن طريق مجموعة من تخطيطات اللغة XML مع التوثيق المرافق.

38.2.3 واصف اسم (name qualifier): سلسلة توضح بلا لبس معرف هوية يمكن استخدامة في أكثر من مكان اسم (بالمعنى التوحيدي) من أجل تمثيل أطراف رئيسية مختلفة.

39.2.3 طرف (party): هو بصورة غير رسمية طرف رئيسي واحد أو عدة أطراف رئيسية مشتركة في عملية أو في اتصال، كاستلام تأكيد أو النفاذ إلى مورد.

40.2.3 اسم مستعار دائم (persistent pseudonym): معرف هوية اسم محتفظ بسريته، يعيّنه مزوّد هوية للتعريف بهوية طرف رئيسي لدى طرف واثق معين، لفترة طويلة تمتد على عدة دورات. ويمكن أن يستخدم لتمثيل توحيد هوية.

41.2.3 نقطة قرار سياسي (policy decision point) (PDP): كيان في نظام يتخذ قرارات الترخيص لذاته ولغيره من كيانات النظام التي تطلب مثل تلك القرارات. فنقطة PDP في اللغة SAMl مثلاً تستهلك طلبات قرار بالترخيص رداً على ذلك. ونقطة قرار السياسة (PDP) هي "سلطة قرار الترخيص".

42.2.3 نقطة وضع سياسة موضع التنفيذ (policy enforcement point) (PEP): كيان في نظام يطلب قرارات بالترخيص، ويضعها بالتالي موضع التنفيذ. فنقطة PEP في اللغة SAML مثلاً ترسل طلبات قرار بالترخيص إلى نقطة PDP، وتستهلك تأكيدات قرار الترخيص ا لمرسلة استجابة لها.

43.2.3 هوية رئيسية (principal identity): تمثيل لهوية طرف رئيسي، ويكون عادة معرّف هوية.

44.2.3 جانبية (لاحَة) (profile): مجموعة من القواعد تختص بغرض أو بعدة أغراض. ويعطى لكل مجموعة اسم في التخطيطة "جانبية xxx في اللغة SAML" أو التخطيطة "جانبية في اللغة SAML xxx":

1) قواعد بشأن كيفية تبييت التأكيدات في بروتوكو أو في أي سياق استعمال آخر، وكيفية استخراجها منه.
2) قواعد بشأن استخدام رسائل بروتوكول اللغة SAML في سياق استخدام خاص
3) قواعد بشأن وضع نعوت معبّر عنها في اللغة SAML على تقابل في أنظمة أخرى لتمثيل النعوت. وتدعى مثل هذه المجموعة من القواعد "جانبية نعوت".

45.2.3 رابطة بروتوكول (protocol binding): انظر "رابطة" (الفقرة 21.2.3).

46.2.3 مزوّد (pfovider): تعبير عام يشير بنفس الوقت إلى مزوّدي الهوية وإلى مزوّدي الخدمة.

47.2.3 طرف واثق (relying party): كيان في نظام يقرر اتخاذ إجراء استناداً إلى معلومات واردة من كيان آخر في النظام. فالطرف الواثق في اللغة SAML يعتمد على استلام تأكيدات واردة من طرف مؤكّد (سلطة في اللغة SAML) حول موضوع.

48.2.3 طالب (requester): كيان في نظام يستعمل بروتوكول اللغة SAML لكي يطلب خدمات من كيان آخر في النظام (هو سلطة في اللغة SAML، مستجيب). ولا يستعمل مصطلح "الزبون" لهذا المفهوم لأن العديد من كيانات النظام تعمل على التآون أو على التوالي كزبائن وكمخدمات معاً. وفي الحالات التي تستعمل فيها رابطة البروتوكول SOAP في اللغة SAML، يكون الطالب في اللغة SAML يتميز معمارياً عن المرسل الأولي في البروتوكول SOAP.

49.2.3 مورد (resource): معطيات موجودة في نظام معلوماتي (على شكل ملفات أو معلومات في الذاكرة إلخ)، وكذلك:

1) خدمة يقدمها نظام.
2) بند في تجهيزات نظام (وبعبارة أخرى إحدى مكوّنات نظام مثل العتاديات أو البرمجيات أو البرمجيات الراسخة أو الوثائقيات).

50.2.3 مستجيب (responder): كيان في نظام (سلطة في اللغة SAML) يستخدم بروتوكول اللغة SAML لكي يستجيب لطلب خدمات وارد من كيان آخر في نظام (طالب). ولا يستعمل مصطلح "مخدّم" لهذا المفهوم لأن العديد من كيانات النظام تعمل على التآون أو على التوالي كزبائن وكمخدّمات معاً. وفي الحالات التي تستعمل فيها رابطة البروتوكول SOAP في اللغة SAML، يكون المستجيب في اللغة SAML يتميز معمارياً عن المستقبل الأخير في البروتوكول SOAP.

51.2.3 دور (role): تعرف القواميس الدور بأنه "الشخصية أو النص الذي يؤديه ممثل" أو "هو الوظيفة أو الوضع". وتلعب كيانات النظام أدواراً مختلفة على التوالي أو على التآون، مثل الأدور النشيطة (الفاعلة) والأدوار المنفعلة. ويعتبر مفهوم المسؤول الإداري دوراً على الغالب.

52.2.3 شيء مصطنع في اللغة SAML (SAML artifact): شيء صغير من معطيات مهيكلة، ثابت القد يستهدف رسالة بروتوكول في اللغة SAML متغيرة القد، تكون أكبر منه في العادة. وتصمم مصطفات اللغة SAML لكي تبيّت في محدات المواقع الموحدة للموارد (URL)، وتُحمل في رسائل البروتوكول HTTP، مثل رسائل الاستجابة في البروتوكول HTTP مع شفرات الحالة "3xx Redirection" والرسائل اللاحقة HTTP GET. وبهذا الشكل يستطيع مزوّد الخدمة أن يحمل بصورة غير مباشرة، عبر وكيل مستعمل، شيئاً مصطنعاً في اللغة SAML إلى مزوّد آخر يستطيع هو الآخر لاحقاً أن يغيّر إحالة الشيء المصطنع، عن طريق التعامل المباشر مع المزوّد الفعلي، والحصول على رسالة البروتوكول في اللغة SAML.

53.2.3 سلطة في اللغة SAML (SAML authority): كيان مجرّد في نظام داخل نموذج ميدان اللغة SAML، وهو يصدر التأكيدات. انظر أيضاً سلطة نعت، وسلطة استيقان، ونقطة قرار سياسي (PDP).

54.2.3 أمن (security): تجميعة من إجراءات الحفظ تضمن سرية المعلومات، وتحمي الأنظمة أو الشبكات المستعملة في معالجة المعلومات، وتتحكم في النفاذ إليها. ويشمل الأمن عادة مفاهيم السرية والائتمانية والسلامة والتيسر. ويهدف الأمن إلى أن يضمن للنظام كونه قادراً على مقاومة التهجمات.

55.2.3 تدعيم أمني (security assertion): تدعيم يدرس في سياق معمارية أمنية.

56.2.3 سياق أمني (security context): السياق الأمني لرسالة، فيما يتعلق برسالة فردية في بروتوكول اللغة SAML، هو الاتحاد الدلالي بين فدرات الرأسية الأمنية إلى مستلم. وفي هذا الشأن الأخير، يكون من أمثلة الآلية الأمنية المستعملةفي الطبقات السفلية من كُدْسة الشبكة، البروتوكولات التالية: HTTP وأمن طبقة النقل (TLS)، وأمن بروتوكول الإنترنت (IPSec).

57.2.3 ميدان أمني (security domain): بيئة أو سياق تحدده نماذج أمنية ومعمارية أمنية، بما في ذلك مجموعة من الموارد مع مجموعة من كيانات النظام مرخص لها بالنفاذ إلى الموارد. ويمكن أن تكون إقامة ميدان أمني أو عدة ميادين في ميدان إداري واحد. والملامح التي تحدد ميداناً أمنياً معيناً تتطور عادة مع الزمن.

58.2.3 تعبير عن سياسة أمنية (security policy expression): وضع هويات رئيسية و/أو نعوت على تقابل مع أعمال جائزة. وتكون تعبيرات السياسة الأمنية غالباً قوائم تحكم في النفاذ بشكل أساسي.

59.2.3 مزوّد خدمة (service provider): الدور الذي يؤديه كيان في نظام بأن يقدّم خدمات إلى أطراف رئيسية أو إلى كيانات نظام أخرى.

60.2.3 مزوّد خدمة خفيف (service provider lite): الدور الذي يؤديه كيان في نظام بأن يقدم خدمات إلى أطراف رئيسية أو إلى كيانات نظام أخرى، مستخدماً فقط الجزء اللازم من بروتوكول اللغة SAML.

61.2.3 دورة (session): تفاعل يدوم بين كيانات نظام، يشترك فيها طرف رئيسي غالباً، ويتّسم بالحفاظ على حالة ما من التفاعل أثناء مدة التفاعل.

62.2.3 سلطة دورة (session authority): دور يؤديه كيان في نظام عند حفاظه على الحالة المتعلقة بالدورات.

63.2.3 مشترك في دورة (session participant): دور يؤديه كيان في نظام عند اشتراكه في دورة مع سلطة دورة واحدة على الأقل.

64.2.3 انسحاب (sign-off): انظر "اختتام دورة" (الفقرة 36.2.3).

65.2.3 اكتتاب (sign-on): انظر "افتتاح دورة" (الفقرة 35.2.3).

66.2.3 موقع (site): مصطلح غير رسمي للدلالة على ميدان إداري بالمعنى الجغرافي أو بمعنى الاسم في نظام أسماء الميدان (DNS). وقد يكون يميل إلى منطقة جغرافية أو طوبولوجية معينة من ميدان إداري، أو قد يكون يغطي عدة ميادين إداريةن كما هي الحال بشأن موقع مزوّد خدمة تطبيقية (ASP).

67.2.3 صاحب (subject): طرف رئيسي في سياق ميدان أمني. وتقدّم تأكيدات اللغة SAML إعلانات عن الأصحاب.

68.2.3 كيان نظام (أو في نظام)، كيان (system entity, entity): عنصر نشيط من نظام حاسوب أو شبكة. مثل عملية مؤتمتة أو مجموعة من العمليات، أو نظام فرعي، أو شخص أو مجموعة من الأشخاص تجسّد مجموعة متميزة من الوظائفيات.

69.2.3 انقضاء الإمهال (time-out): فترة زمنية تصبح بعض الشروط صائبة عند انتهائها، إن لم تحدث بعض الأحداث. مثل الدورة التي تنتهي لأن حالتها ظلت غير نشيطة أثناء فترة محددة تدعى "بلوغ نهاية المهلة".

70.2.3 اسم مستعار عابر (transient pseudonym): معرف هوية اسم محتفظ بسريته، يعينة مزوّد هوية للتعريف بهوية طرف رئيسي لدى طرف واثق معين، لفترة قصيرة نسبياً لا تمتد على عدة دورات.

71.2.3 نعت في اللغة XML (XML attribute): بنية من معطيات اللغة XML مبيّنة في واسم البداية من عنصر اللغة XML، لها اسم ولها قيمة.

72.2.3 عنصر من اللغة XML (XML element): بنية من معطيات اللغة XML مرتبة تراتبياً بين غيرها، مثل البنى في وثيقة في اللغة XML، يدل عليها واسم بداية وواسم نهاية أو واسم فارغ.

4 المختصرات

تطبق المختصرات التالية لأغراض هذه التوصية | هذا المعيار الدولي:

AA	سلطة نعت	*(Attribute Authority)*
ASN.1	ترميز قواعد التركيب (النحو) المجرّد 1	*(Abstract Syntax Notation One)*
ASP	مزوّد خدمة تطبيقية	*(Application Service Provider)*

CA	سلطة إصدار الشهادة	*(Certification Authority)*
CMP	بروتوكول إدارة الشهادة	*(Certificate Management Protocol)*
CRL	قائمة إبطال الشهادات	*(Certificate Revocation List)*
DCE	نظام تحريكي لاكتشاف التفويضات	*(Distributed Computing Environment)*
DDDS	بيئة الحساب الموزَّع	*(Dynamic Delegation Discovery System)*
DNS	نظام أسماء الميدان	*(Domain Name System)*
ECP	زبون أو وكيل مفوّض معزّز	*(Enhanced Client/Proxy)*
HTTP	بروتوكول نقل نص فائق	*(HyperText Transfer Protocol)*
HTTPS	بروتوكول مأمون لنقل نص فائق	*(Secure HyperText Transfer Protocol)*
IdP	مزوّد هوية	*(Identity Provider)*
IdP Lite	مزوّد هوية خفيف	*(Identity Provider Lite)*
IP	بروتوكول إنترنت	*(Internet Protocol)*
IPSec	أمن بروتوكول الإنترنت	*(Internet Protocol Security)*
MD5	الخوارزمية 5 لموجز الرسالة	*(Message Digest algorithm 5)*
MIME	توسّعات متعددة الأغراض في بريد الإنترنت	*(Multipurpose Internet Mail Extensions)*
NAPTR	مسدِّد سلطة التسمية	*(Naming Authority PoinTeR)*
OID	معرف هوية شيء	*(Object IDentifier)*
PAC	شهادات نعت مميز	*(Privilege Attribute Certificates)*
PAOS	البروتوكول SOAP مقلوباً	*(Reverse SOAP)*
PDP	نقطة قرار سياسي	*(Policy Decision Point)*
PEP	نقطة وضع سياسة موضع التنفيذ	*(Policy Enforcement Point)*
PGP	سرية جيدة نوعاً ما	*(Pretty Good Privacy)*
PKI	بنية تحتية للمفتاح العمومي	*(Public-Key Infrastructure)*
POP	برهان التملك	*(Proof of Possession)*
RA	سلطة تسجيل	*(Registration Authority)*
RSA	خوارزمية رايفست وشمير وأدليمان العمومية	*(Rivest, Shamir, Adleman (public key algorithm)*
SHA-1	خوارزمية الفرم المأمون–1	*(Secure Hash Algorithm 1)*
SP	مزوّد خدمة	*(Service Provider)*
SPKI	بنية تحتية بسيطة للمفتاح العمومي	*(Simple Public Key Infrastructure)*
SP Lite	مزوّد خدمة خفيف	*(Service Provider Lite)*
SSO	اكتتاب بالتوقيع الوحيد	*(Single Sign On)*
TLS	بروتوكول أمن طبقة النقل	*(Transport Layer Security protocol)*
URI	معرّف هوية موحّد للموارد	*(Uniform Resource Identifier)*
UTC	التوقيت العالمي المنسّق	*(Coordinated Universal Time)*
UUID	معرف هوية وحيد عالمي	*(Universal Unique IDentifier)*
XACML	لغة تأشيرية توسّعية للتحكم في النفاذ	*(eXtensible Access Control Markup Language)*
XML	لغة تأشيرية توسّعية	*(eXtensible Markup Language)*

5 اصطلاحات

تستعمل هذه التوصية الكلمات الحاكمة التالية "يتعين" و"يتعين ألا" و"يتطلب" و"يجب" و"يجب ألا" و"ينبغي ألا" و"يمكن" و"اختياري". وتفسر هذه المصطلحات الواردة في هذه التوصية على النحو المشروح في طلب التعليقات RFC 2119 الصادر عن فريق المهام الهندسية في الإنترنت (IETF).

وتستعمل هذه التوصية وثائق التخطيطة في اللغة XML المطابقة للجزء 1 من تخطيطة اللغة XML الصادرة عن التجمع W3C، وللجزء 2 من تخطيطة اللغة XML الصادرة عن التجمع W3C، وللنص المعياري لتلك المواصفات التي تشرح قواعد التركيب وعلم الدلالات لتأكيدات اللغة SAML ولرسائل البروتوكول فيها المشفرة في اللغة XML. وفي حالات عدم التوافق بين وثائق التخطيطة في اللغة XML وقوائم التخطيطة في هذه التوصية، تسود وثائق التخطيطة. ويلاحظ أن هذه التوصية تفرض في بعض الحالات قيوداً تذهب إلى أبعد من القيود التي تفرضها وثائق التخطيطة.

6 نظرة شاملة

ترمي هذه التوصية إلى تحديد الصيغة 2 من اللغة الإرشادية للتدعيم الأمني (SAML). وهي تحدد على النحو (قواعد التركيب) والدلالات المستعملين في معالجة التأكيدات التي يقدمها كيان من نظام بشأن موضوع ما. وأثناء تقديم هذه التأكيدات، أو أثناء الاعتماد عليها، تستيطع كيانات النظام في اللغة SAML استخدام بروتوكولات أخرى للإفادة عن التأكيد نفسه أو عن موضوع التأكيد. وهذه التوصية تحدد بنى تأكيدات اللغة SAML، ومجموعة مصاحبة من البروتوكولات إضافة إلى قواعد المعالجة المتدخلة في إدارة نظام في اللغة SAML.

وتشفر تأكيدات اللغة SAML ورسال البروتوكول منها باللغة التأشيرية التوسّعية (XML)، وتستخدم أماكن الأسماء في هذه اللغة. وتكون مبيتة عادة في بنى أخرى مستخدمة للنقل، مثل طلبات الإرسال بالبريد HTTP POST أو رسائل البروتوكول SOAP المشفرة في اللغة XML. ويحدد البند 7 أنماط المعطيات المشتركة في استعمالات اللغة SAML. ويقدم البند 8 إطار عمل للتأكيدات والبروتوكولات في اللغة SAML. ويشرح البند 9 نموذج المعطيات الشرحية للغة SAML. ويفصل البند 10 أطر العمل لدمج ونقل رسائل بروتوكول اللغة SAML. كما يقدم البند 11 مجموعة أساسية من الجانبيات لاستخدامها في تأكيدات وبروتوكولات اللغة SAML من أجل معالجة حالات استعمال خاصة أو من أجل تحقيق التشغيل البيني عند استخدام ميزات اللغة SAML. ويعرض البند 12 سياق الاستيقان في اللغة SAML. وتحدد فيها السياقات التالية خصوصاً:

- تخطيطة سياق الاستيقان في اللغة SAML؛
- أنماط التخطيطات لسياق الاستيقان SAML؛
- تخطيطة صنف السياق في اللغة SAML من أجل بروتوكولات الإنترنت؛
- تخطيطة صنف السياق في اللغة SAML من أجل كلمة سر في بروتوكول الإنترنت؛
- تخطيطة صنف السياق في اللغة SAML من أجل البروتوكول كيربروس؛
- تخطيطة صنف السياق في اللغة SAML من أجل المتنقل بعامل واحد غير مسجل؛
- تخطيطة صنف السياق في اللغة SAML من أجل المتنقل بعاملين اثنين غير مسجل؛
- تخطيطة صنف السياق في اللغة SAML من أجل المتنقل بعامل واحد مع عقد؛
- تخطيطة صنف السياق في اللغة SAML من أجل المتنقل بعاملين اثنين مع عقد؛
- تخطيطة صنف السياق في اللغة SAML من أجل كلمة السر؛
- تخطيطة صنف السياق في اللغة SAML من أجل نقل مَحْمي بكلمة سر؛
- تخطيطة صنف السياق في اللغة SAML من أجل دورة سابقة؛
- تخطيطة صنف السياق في اللغة SAML من أجل مفتاح عمومي–التوصية X.509؛
- تخطيطة صنف السياق في اللغة SAML من أجل مفتاح عمومي–سرية جيدة نوعاً ما (PGP)؛

- تخطيطة صنف السياق في اللغة SAML من أجل مفتاح عمومي–بنية تحتية بسيطة للمفتاح العمومي (SPKI) ؛
- تخطيطة صنف السياق في اللغة SAML من أجل مفتاح عمومي–توقيع في اللغة XML؛
- تخطيطة صنف السياق في اللغة SAML من أجل بطاقة ذكية؛
- تخطيطة صنف السياق في اللغة SAML من أجل بنية تحتية للمفتاح العمومي (PKI) ببطاقة ذكية؛
- تخطيطة صنف السياق في اللغة SAML من أجل برمجية بنية تحتية للمفتاح العمومي؛
- تخطيطة صنف السياق في اللغة SAML من أجل المهاتفة؛
- تخطيطة صنف السياق في اللغة SAML من أجل المهاتفة (الرحّالة)؛
- تخطيطة صنف السياق في اللغة SAML من أجل المهاتفة (الشخصانية)؛
- تخطيطة صنف السياق في اللغة SAML من أجل المهاتفة (المستيقنة)؛
- تخطيطة صنف السياق في اللغة SAML من أجل كلمة سر بعيدة مأمونة؛
- تخطيطة صنف السياق في اللغة SAML من أجل استيقان زبون مبني على شهادة SL/TLS؛
- تخطيطة صنف السياق في اللغة SAML من أجل إذنة متزامنة.

ويوفر البند 13 إطار عمل لتنفيذ اللغة SAML يلزم اتباعه بغية تأمين المطابقة. وفي البند 13 تناقش متطلبات المطابقة من أساليب سير العمل والنماذج الأمنية. وأخيراً يتضمن الملحق A قائمة بجميع تخطيطات اللغة SAML المرافقة.

7 أنماط المعطيات المشتركة

تعرف الفقرات التالية استعمال وتفسير أنماط المعطيات المشتركة الورادة في تخطيطات اللغة SAML.

1.7 قيم السلاسل

يكون نمط جميع قيم السلاسل في اللغة SAML هو النمط **xs:string** المكوّن من أنماط المعطيات في اللغة XML التابعة للتجمع W3C. ويجب أن تكون جميع سلاسل الرسائل في اللغة SAML الواردة في هذه التوصية مكونة على الأقل من سمة ليست فرغاً أبيض، ما لم ينص على غير ذلك.

يجب أن تقارن، ما لم ينص على غير ذلك في هذه التوصية أو في جانبية خاصة، جميع عناصر وثائق اللغة SAML التي تخطيطتها من النمط **xs:string** في اللغة XML، أو من نمط مشتق من هذا النمط، باستخدام مقارنة اثنينية مضبوطة. وبصورة خاصة يجب ألا تكون تطبيقات وتطويرات اللغة SAML متوقفة على مقارنات سلاسل لا تتحسس بصندوق حروف الطباعة، ولا على تقييس أو تشذيب الفراغات البيضاء، أو على تحويل الأنساق المحلية الخاصة مثل الأعداد أو العملات. ويرمي هذا المتطلب إلى التطابق مع سلسلة التجمع W3C.

وإذا كان أحد التطبيقات يقارن قيماً ممثلة باستخدام تشفيرات مختلفة للسمات، يجب على هذا التطبيق أن يستخدم طريقة للمقارنة تعيد نفس النتيجة التي يعيدها تحويل قيمتين في تشفير السمات بالشفرة الموحّدة، بشكل التقييس C، ثم إجراء مقارنة بعد ذلك تكون اثنينية مضبوطة. ويرمي هذا المتطلب إلى التطابق مع نموذج السمات للتجمع W3C، وخاصة مع القواعد المتعلقة بالنص المقيس في الشفرة الموحّدة.

أما التطبيقات التي تقارن المعطيات المستلمة في وثائق اللغة SAML بالمعطيات الواردة في مصادر خارجية، فيجب عليها أن تأخذ بالحسبان قواعد التقييس المحددة للغة XML. والنص الوارد في العناصر يكون مقيساً بحيث تتمثل نهايات السطور باستخدام سمات الرجوع إلى أول السطر (ASCII CODE $10_{Decimal}$). بينما يتم تقييس قيم النعت في اللغة XML المعرفة بشكل سلاسل (أو أنماط مشتقة من سلاسل)، كما هو مشروح في الفقرة 3.3.3 من اللغة XML 1.0 التابعة للتجمع W3C. ويستعاض عن جميع سمات الفراغات البيضاء ببياضات (ASCII CODE $32_{Decimeal}$).

لا تحدد هذه التوصية أي ترتيب لمقارنة قيم النعت أو محتويات العنصر في اللغة XML، ولا لفرز هذه القيم أو المحتويات. ويجب ألا تتوقف تطبيقات اللغة SAML على ترتيب الفرز الخاص بالقيم، لأنها قد تختلف باختلاف عمليات الضبط المحلية التي يقوم بها الضيوف المتدخلون.

2.7 قيم معرّفات الهوية الموحّدة للموارد (URI)

يكون نمط جميع القيم المرجعية للمعرف URI في اللغة SAML هو النمط **xs:anyURI**، المكوّن من أنماط المعطيات في اللغة XML التابعة للتجمع W3C.

يجب أن تكون جميع القيم المرجعية للمعرف URI الواردة داخل العناصر أو النعوت المعرفة في اللغة SAML، مكونة على الأقل من سمة واحدة ليست فراغاً أبيض، ويطلب أن تكون مطلقة، ما لم ينص على غير ذلك في هذه المواصفة.

تستخدم هذه التوصية بصورة موسّعة مراجع المعرف URI كمعرفات هوية، مثل شفرات الحالة، وأنماط الأنساق، وأسماء النعوت، وكيانات النظام وغيرها. لذلك يجب من حيث الأساس أن تكون القيم بنفس الوقت وحيدة ومتماسكة، حتى لا يستخدم أبداً نفس المعّرف URI في أوقات مختلفة، ليمثل معلومات تحتية مختلفة.

3.7 قيم زمنية

يكون لجميع القيم الزمنية في اللغة SAML النمط **xs:dateTime**، المكوّن من أنماط المعطيات في اللغة XML التابعة للتجمع W3C، ويتعين أن يعبر عنها بالتوقيت المنسّق (UTC)، دون أي مركبة من مناطق التوقيت.

وينبغي ألا تعتمد كيانات النظام على استبانة زمنية أدق من الميلي ثانية. ويتعين ألا تولد التطبيقات لحظات زمنية تحدد الثواني المفوّتة.

4.7 معرفات الهوية والقيم المرجعية لمعرفات الهوية (ID)

يستخدم النمط البسيط **xs:ID** للإعلان عن معرفات الهوية في اللغة SAML من أجل التأكيدات والطلبات والاستجابات. ويتعين على القيم المعلن عنها في هذه التوصية أنها من النمط **xs:ID** أن تفي بالصفات التالية إضافة إلى الصفات التي يفرضها تعريف النمط **xs:ID** بالذات:

- على كل جزء يسند معرف هوية، أن يتأكد من أن الاحتمال مهمل في أن يسند هذا الجزء أو أي جزء آخر معرف الهوية ذاته عن غير قصد إلى موضوع معطيات مختلف.
- وعندما يعلن موضوع معطيات أن له معرف هوية خاصاً، يتعين ألا يكون هناك بالضبط سوى مثل هذا الإعلان الوحيد.

والآلية التي يتأكد بها كيان في نظام في اللغة SAML من وحدانية معرف الهوية، تعود إلى تنفيذ التطبيق. وعند استخدام تقنية ما عشوائية أو شبه عشوائية، يتعين ألا يكون احتمال تطابق معرفي هوية اثنين مختارين، يساوي أو يقل عن 2^{-128}، وينبغي ألا يساوي الاحتمال أو يقل عن 2^{-160}. ويستوفى هذا المطلب بتشفير قيمة مختارة عشوائياً بطول من البتات محصور بين 128 بتة و160 بتة. ويتعين أن يكون التشفير مطابقاً للقواعد التي تحدد نمط المعطيات **xs:ID**. ويجب تغذية أي مولد شبه عشوائي بمواد وحيدة حتى تضمن صفات الوحدانية المطلوبة بين الأنظمة المختلفة.

ويستخدم النمط البسيط **xs:NCName** في اللغة SAML لمرجعية معرفات الهوية من النمط **xs:ID**، لأن النمط **xs:IDREF** لا يمكن استخدامه لهذا الغرض. ففي اللغة SAML، يمكن للعنصر الذي يسميه مرجع معرف هوية في اللغة SAML، أن يُعرف في وثيقة منفصلة عن الوثيقة المستعمل فيها مرجع معرف الهوية. فاستخدام النمط **xs:IDREF** قد ينتهك مطلب كون هذه القيمة تقابل قيمة نعت لمعرف الهوية على عنصر ما من نفس وثيقة اللغة XML.

8 التأكيدات والبروتوكولات في اللغة SAML

تحدد اللغة SAML على قواعد التركيب والدلالات المستعملين في معالجة التأكيدات التي يقدمها كيان من نظام بشأن موضوع ما. وأثناء تقديم هذه التأكيدات، أو أثناء الاعتماد عليها، تستطيع كيانات النظام في اللغة SAML استخدام بروتوكولات أخرى للإفادة عن التأكيد نفسه، أو عن موضوع التأكيد. وتحدد هذه التوصية بنى تأكيدات اللغة SAML، ومجموعة مصاحبة من البروتوكولات إضافة إلى قواعد المعالجة المتداخلة في إدارة نظام في اللغة SAML.

وتشفر تأكيدات اللغة SAML ورسائل البروتوكول فيها باللغة التأشيرية التوسّعية (XML) (انظر صيغة اللغة XML 1.0 التابعة للتجمع W3C)، وتستخدم أماكن الأسماء في هذه اللغة (انظر أماكن الأسماء التابعة للتجمع W3C). وتكون مبيّتة عادة في بنى أخرى مستخدمة للنقل، مثل طلبات إرسال HTTP بالبريد (HTTP POST) أو رسائل البروتوكول SOAP المشفرة في اللغة XML. ويقدم البند 10 أطر عمل لتبييت ونقل رسائل البروتوكول في اللغة SAML. أما البند 11 فيقدم مجموعة أساسية من الجانبيات لاستخدام تأكيدات وبروتوكولات اللغة SAML من أجل أداء حالات استعمال خاصة أو من أجل تحقيق التشغيل البيني عند استخدام ميزات اللغة SAML.

1.8 تأكيدات اللغة SAML

التأكيد هو ترزيم من المعلومات تنطوي على صفر أو عدد من الإعلانات تقدمها **سلطة في اللغة SAML**. وتسمى سلطات اللغة SAML أطرافاً مؤكِّدة في المناقشات حول توليد التأكيدات وتبادلها، كما تسمى كيانات النظام التي تستخدم هذه التأكيدات **الأطراف الواثقة**. (ويختلف هذان المصطلحان عن **الطالب** و**المستجيب** اللذين يحتفظ بهما لمناقشات تبادل رسائل البروتوكول في اللغة SAML).

وتقدم تأكيدات اللغة SAML عادة حول **صاحب**، يمثله العنصر <subject>. ومع ذلك فاستخدام العنصر <subject> اختياري، إذ تستطيع مواصفات وجانبيات أخرى أن يستخدم بنية تأكيد اللغة SAML لتقديم إعلانات مشابهة دون تحديد صاحب، أو بتحديد الصاحب بكيفية أخرى. ويوجد في العادة عدد من **مزوّدي الخدمة** الذين يمكنهم استخدام التأكيدات حول صاحب من أجل التحكم في النفاذ وتقديم خدمة حسب طلب الزبون، فيصبحون بالتالي هم الأطراف الواثقة بطرف مؤكِّد يدعى **مزوّد الخدمة**.

تعرف هذه التوصية ثلاثة أنواع من إعلانات التأكيد التي يمكن أن تصدرها سلطة في اللغة SAML. وجميع الإعلانات المحددة على أنها في اللغة SAML تكون مرتبطة بصاحب. وأنواع الإعلانات الثلاثة المعّرفة في هذه التوصية هي:

- **الاستيقان**: جرى الاستيقان من صاحب التأكيد بوسيلة خاصة في لحظة معينة.
- **النعت**: يترافق صاحب التأكيد مع نعوت معتمدة.
- **قرار الترخيص**: جاء طلب الترخيص لصاحب التأكيد بالنفاذ إلى الموارد المعينة ممنوحاً أو مرفوضاً.

ملاحظة (للاطّلاع) – يقترح PE13 (انظر OASIS PE:2006) إضافة "أو غير محدد" إلى الفقرة السابقة.

تكون البنية الخارجية للتأكيد عمومية، تقدم المعلومات المشتركة لجميع الإعلانات التي تحتويها. ويوجد داخل التأكيد سلسلة من العناصر الداخلية توصف الاستيقان أو النعت أو قرار الترخيص أو الإعلانات التي يحددها المستعمل والتي تحتوي على العناصر المعينة.

وتسمح تخطيطة التأكيدات في اللغة SAML بالتوسّعات، كما هو مشروح في الفقرة 11.8، التي تسمح بالتوسّعات التي يحددها المستعمل للتأكيدات والإعلانات، كما تسمح بتعريف أنواع جديدة من التأكيدات والإعلانات.

1.1.8 رأسية التخطيطة والإعلانات عن أمكنة الأسماء

القطعة التالية من التخطيطة تعرف أمكنة الأسماء في اللغة XML، والمعلومات الأخرى الخاصة برأسية تخطيطة التأكيد.

```
<schema targetNamespace="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
```

```
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <import namespace="http://www.w3.org/2001/04/xmlenc#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-
20021210/xenc-schema.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-assertion-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V1.0 (November, 2002):
              Initial Standard Schema.
            V1.1 (September, 2003):
              Updates within the same V1.0 namespace.
            V2.0 (March, 2005):
              New assertion schema for SAML V2.0 namespace.
        </documentation>
    </annotation>
…
</schema>
```

2.1.8 معرفات هوية الاسم

تحدد الفقرات التالية تركيب اللغة SAML الذي يحتوي على معرفات الهوية التوصيفية للأصحاب ومصدري التأكيدات (الأطراف المؤكدة) ورسائل البروتوكول.

هناك عدة مناسبات تكون مفيدة في اللغة SAML لكي يتواصل كيانان في نظام بشأن طرف ثالث، فمثلاً يتيح بروتوكول طلب الاستيقان في اللغة SAML استيقان صاحب بواسطة طرف ثالث. إذاً من المفيد وضع وسيلة يمكن بواسطتها مصاحبة الأطراف لمعرفات هوية تكون دلالية لكل واحد من الأطراف. وقد يلزم في بعض الأحيان قصر الميدان الذي يمكن فيه استخدام معرف هوية على مجموعة صغيرة من كيانات النظام (للحفاظ على سرية صاحب مثلاً). ويمكن أيضاً استعمال معرفات هوية مشابهة للإشارة إلى مصدر رسالة بروتوكول أو تأكيد في اللغة SAML.

ويستطيع كيانا نظام أو أكثر استعمال نفس قيمة معرف هوية الاسم عند الإحالة إلى هويات مختلفة. وعليه يمكن أن يكون لكل كيان فهم مختلف لنفس هذا الاسم. وتوفر اللغة SAML **واصفات أسماء** لكي تزيل كل لبس عن معرف هوية اسم، فتضعه مثلاً في مكان اسم (**namespace**) موحّد يعود إلى واصفات الاسم. وتتيح صيغة اللغة SAML v2.0 لمعرف الهوية أن يوصف بنفس الوقت بعبارتي الطرف المؤكِّد أو الطرف الواثق أو المنتسب الخاص، وبذلك تفسح المجال أمام معرفات الهوية لكي تعرض عند اللزوم علم دلالات تزاوجياً.

ويمكن أيضاً تجفير معرفات الهوية من أجل تحسين خصائصها المتعلقة بالحفاظ على السرية، وخصوصاً عندما يكون معرف الهوية سيرسل عبر وسيط.

ملاحظة – لاجتناب استخدام تركيبات معقدة نسبياً لتخطيطة اللغة XML، لا تتقاسم مختلف أنماط العناصر معرفات الهوية تراتبية مشتركة.

1.2.1.8 العنصر <BaseID>

العنصر <BaseID> هو نقطة توسّع تتيح للتطبيقات أن تضيف أنواعاً جديدة من معرفات الهوية. ونمطه المعقد **BaseIDAbstractTyupe** هو نمط مجرد، فلا يمكن استعماله بالتالي إلا أساساً لنمط مشتق. وهو ينطوي على النعتين التاليين المطلوب استخدامهما في التمثيلات التوسّعية لمعرف الهوية:

- NameQualifier [اختياري]
ميدان أمني أو إداري يصف معرف الهوية. ويوفر هذا النعت وسيلة لتوحيد معرفات الهوية الواردة من ذاكرات مستعملين مختلفة، من دون تضارب.

- SPNameQualifier [اختياري]
يضيف إلى توصيف معرف الهوية اسم مزوّد الخدمة أو جماعة المزوّدين المنتسبين. ويوفر هذا النعت وسيلة إضافية لتوحيد معرفات الهوية على أساس الطرف الواثق أو الأطراف الواثقة.

وينبغي حذف النعتين NameQualifier وSPNameQualifier، إلا إذا كان تعريف نمط معرف الهوية يعرف صراحة استخدامها وعلم دلالاتهما.

والقطعة التالية من التخطيطة تعرف العنصر <BaseID> ونمطه المعقد **BaseIDAbstracType**:

```
<attributeGroup name="IDNameQualifiers">
    <attribute name="NameQualifier" type="string" use="optional"/>
    <attribute name="SPNameQualifier" type="string" use="optional"/>
</attributeGroup>
<element name="BaseID" type="saml:BaseIDAbstractType"/>
<complexType name="BaseIDAbstractType" abstract="true">
    <attributeGroup ref="saml:IDNameQualifiers"/>
</complexType>
```

2.2.1.8 النمط المعقّد NameIDType

يستخدم النمط المعقّد **NameIDType** عندما يستخدم عنصر لتمثيل كيان باسم تُقَيّمه سلسلة. إنه شكل من معّرفات الهوية أشد تقييداً من العنصر <BaseID>، وهو نمط ينطوي في نفس الوقت على العنصرين <NameID> و<Issuer>. وهو يوفر النعوت التالية الاختيارية إضافة إلى محتوى السلسلة المتضمنة معرف الهوية الحقيقي:

- NameQualifier [اختياري]
الميدان الأمني أو الإداري الذي يصف الاسم. ويوفر هذا النعت وسيلة لتوحيد الأسماء الواردة من ذاكرات مستعملين مختلفة، من دون تضارب.

- SPNameQualifier [اختياري]
يضيف إلى توصيف الاسم اسم مزوّد الخدمة أو جماعة المزوّدين المنتسبين. ويوفر هذا النعت وسيلة إضافية لتوحيد الأسماء على أساس الطرف الواثق أو الأطراف الواثقة.

- Format [اختياري]
مرجع إلى معرف URI، يمثل تصنيف معلومات معرف الهوية المبنية على سلسلة. انظر الفقرة الفرعية 3.7.8 تعريفات اللغة SAML لمرجع المعرف URI التي يمكن استعمالها كقيم للنعت Format، مع أوصافها وقواعد معالجتها المصاحبة. وما لم توجد مواصفة مغايرة يقدمها عنصر على أساس هذا النمط، وإذا لم تقدم أي قيمة للنعت Format، فإن القيمة: Urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified (انظر الفقرة الفرعية 1.3.7.8) تبقى نافذة المفعول.

وعند استخدام النعت Format بقيمة هي غير القيمة المحددة في الفقرة الفرعية 3.7.8، يجب تفسير محتوى عنصر من هذا النمط طبقاً لتعريف هذا النسق المتوفر خارج هذه التوصية. وما لم توجد دلالة مغايرة يقدمها تعريف النسق، فإن قضايا إغفال الاسم، والاسم المستعار، وديمومة معرف الهوية بالنسبة إلى الأطراف المؤكدة والواثقة تعود إلى مسؤولية التنفيذ.

- SPProvidedID [اختياري]
معرف هوية لاسم يقدمه مزوّد الخدمة أو جماعة المزوّدين المنتسبين بشأن الكيان، إن كان هذا المعرف يختلف عن معرف هوية الاسم الرئيسي المعطى في محتوى العنصر. ويوفر هذا النعت وسيلة لدمج استخدام اللغة SAML مع معرفات الهوية الموجودة والتي سبق أن استخدمها مزوّد خدمة. فيمكن مثلاً أن يكون معرف الخدمة الموجود "مرتبطاً" بالكيان عن طريق استخدام بروتوكول إدارة معرفات هوية الأسماء المحدد في الفقرة الفرعية 8.2.8.

ويمكن إضافة قواعد تخص محتوى هذه النعوت (أو حذفها) تحددها عناصر تستخدم هذا النمط، وبواسطة تعريفات نسق معينة. وينبغي حذف النعتين NameQualifier وSPNameQualifier، إلا إذا كان العنصر أو النسق يعرف صراحة استخدامهما وعلم دلالتهما.

والقطعة التالية من التخطيطة تعرف النمط المعقد **NameIDType**:

```
<complexType name="NameIDType">
    <simpleContent>
        <extension base="string">
            <attributeGroup ref="saml:IDNameQualifiers"/>
            <attribute name="Format" type="anyURI" use="optional"/>
            <attribute name="SPProvidedID" type="string" use="optional"/>
        </extension>
    </simpleContent>
</complexType>
```

3.2.1.8 العنصر <NameID>

يكون العنصر <NameID> من النمط **NameIDType** (انظر الفقرة الفرعية 2.2.1.8) ويستخدم في تركيبات مختلفة لتأكيدات اللغة SAML، كما في العنصرين <Subject> و<SubjectConfirmation> وفي رسائل بروتوكول مختلفة (انظر الفقرة 2.8).

```
<element name="NameID" type="saml:NameIDType"/>
```

4.2.1.8 العنصر <EncryptedID>

يكون العنصر <EncryptedID> من النمط **EncryptedElementType**، ويحمل محتوى عنصر معرف هوية غير مجفر، بأسلوب مجفر، كما هو معرف في تجفير التجمع W3C. ويحتوي العنصر <EncryptedID> العنصرين التاليين:

- <xenc:EncryptedData> [مطلوب]
المحتوى المجفر وتفصيلات التجفير المصاحبة كما هو معرف في تجفير التجمع W3C. وينبغي أن يكون النعت Type موجوداً، وإذا كان موجوداً، يجب أن يحتوي على قيمة من http://www.w3.org/2001/04/xmlenc#Element.

والعنصر المجفر يجب أن يحتوي على عنصر من النمط **NameIDType** أو **AssertionType** أو على نمط مشتق من **BaseIDAbstractType** أو **NameIDType** أو **AssertionType**.

- <xenc:EncryptedKey> [صفر أو أكثر]
مفاتيح فك تجفير مغلفة، كما هو معرف في تجفير التجمع W3C. وينبغي أن يحتوي كل مفتاح مغلف على نعت Recipient يحدد الكيان الذي جفر المفتاح من أجله. ويجب أن تكون قيمة النعت Recipient هي معرف الهوية للمعرف URI لكيان نظام في اللغة SAML، كما هو محدد في الفقرة 4.8.

ومعرفات الهوية المجفرة مهيأة لكي تلعب دور آلية تحمي السرية، عندما تكون قيمة النص الواضح ستمر عبر وسيط. وفي مثل هذه الحالة، يجب أن يكون النص المشفر وحيداً في كل عملية تجفير معينة. ولمزيد من التوضيح حول هذه المسألة انظر الفقرة 3.6 من تجفير اللغة XML التابع للتجمع W3C.

يمكن تجفير تأكيد بكامله في هذه العنصر، واستخدامة كمعرف هوية. وفي هذه الحالة، يقدم العنصر <Subject> من التأكيد المجفر "معرف الهوية" لصاحب التأكيد التغليفي. وعليه إذا كان التأكيد المعرف للهوية غير صالح، كذلك يكون التأكيد التغليفي.

والقطعة التالية من التخطيطة تعرف العنصر <EncryptedID> ونمطه المعقد EncryptedElementType:

```
<complexType name="EncryptedElementType">
    <sequence>
         <element ref="xenc:EncryptedData"/>
         <element ref="xenc:EncryptedKey" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
</complexType>
<element name="EncryptedID" type="saml:EncryptedElementType"/>
```

5.2.1.8 العنصر <Issuer>

يعطي العنصر <Issuer> مع النمط المعقد **NameIDType** معلومات عن مصدر تأكيد أو رسالة بروتوكول في اللغة SAML. ويتطلب العنصر استخدام سلسلة لكي تحمل اسم المصدر، ولكنه يسمح بقطع مختلفة من المعطيات الوصفية (انظر الفقرة الفرعية 2.2.1.8) مع تجاوز القاعدة الدارجة لهذا النمط من العناصر، وإذا لم تقدم أي قيمة للنعت Format مع هذا العنصر، تبقى القيمة urn : oasis : names : tc : SAML : 2 : 0 : nameid-format : entity سارية المفعول (انظر الفقرة الفرعية 2.2.1.8).

والقطعة التالية من التخطيطية تعرف العنصر <Issuer>:

```
<element name="Issuer" type="saml:NameIDType"/>
```

3.1.8 التأكيـــدات

تحدد الفقرة التالية تركيبات اللغة SAML التي تحتوي على معلومات التأكيد أو التي تقدم رسائل للرجوع إلى تأكيد موجود.

1.3.1.8 العنصر <AssertionIDRef>

العنصر <AssertionIDRef> يميل إلى تأكيد في اللغة SAML بمعرف هويته الوحيد. والسلطة الخاصة التي تصدر التأكيد أو السلطة التي يمكن الحصول على التأكيد لديها، ليست محددة كجزء من الإحالة. انظر الفقرة الفرعية 3.2.8 عنصر البروتوكول الذي يستخدم مثل هذه الإحالة لكي يطلب التأكيد المقابل.

والقطعة التالية من التخطيطة تعرف العنصر <AssertionIDRef>:

```
<element name="AssertionIDRef" type="NCName"/>
```

2.3.1.8 العنصر <AssertionURIRef>

العنصر <AssertionURIRef> يحيل إلى تأكيد في اللغة SAML بمرجع للمعرف URI. ويمكن استخدام مرجع المعرف URI لاسترجاع التأكيد المقابل بكيفية معينة من مرجع المعرف URI. انظر الفقرة 3.7 معلومات عن كيفية استعمال هذا العنصر في رابطة بروتوكول للقيام بذلك.

والقطعة التالية من التخطيطة تعرف العنصر <AssertionURIRef>:

```
<element name="AssertionURIRef" type="anyURI"/>
```

3.3.1.8 العنصر <Assertion>

يكون العنصر <Assertion> من النمط المعقد **AssertionType**. ويحدد هذا النمط المعلومات الأساسية التي هي مشتركة بين جميع التأكيدات، بما فيها العناصر والنعوت التالية:

- Version [مطلوب]

  صيغة هذا التأكيد. ومعرف الهوية لصيغة اللغة SAML في هذه التوصية هو "2.0". والصيغ في اللغة SAML، تناقش في الفقرة 3.8.

- ID [مطلوب]
معرف هوية هذا التأكيد. إنه من النمط **xs:ID**. ويتعين أن يتبع المتطلبات المحددة في الفقرة 3.7 من أجل وحدانية معرف الهوية.

- <IssueInstant> [مطلوب]
لحظة وقت الإصدار، مقدرة بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- <Issuer> [مطلوب]

سلطة في اللغة SAML التي تعتمد التأكيد. وينبغي أن يكون المصدر لا لبس فيه عند الأطراف الواثقة المقصودة.

ولا تحدد هذه التوصية أي علاقات خاصة بين الكيان الذي يمثله هذا العنصر وبين الموقع على التأكيد (إن وُجد). وإن مثل هذه المتطلبات التي يفرضها طرف واثق يستخدم التأكيد أو تفرضها جانبيات معينة هي من اختصاص التطبيق.

- <ds:Signature> [اختياري]
توقيع في اللغة XML يحمي سلامة التأكيد، ويستيقن مُصدره، كما هو مشروح أدناه في الفقرة 4.8.

- <Subject> [اختياري]

صاحب الإعلان أو الإعلانات الواردة في التأكيد.

- <Conditions> [اختياري]
الشروط الواجب تقديرها عند التوثق من صلاحية التأكيد و/أو عند استعماله. انظر الفقرة الفرعية 5.18 لمزيد من المعلومات حول كيفية تقدير هذه الشروط.

- <Advice> [اختياري]
معلومات إضافية تتعلق بالتأكيد، تساعد على المعالجة في بعض الحالات، ولكن التطبيقات تتجاهلها لأنها لا تفهم النصيحة أو أنها لا ترغب في استعمالها.

صفر أو أكثر من عناصر الإعلان التالية:

- <Statement>
إعلان عن نمط معين في تخطيطة توسّعية. ويجب استعمال النعت **xs:type** للدلالة على النمط الحقيقي للإعلان.

- <AuthnStatement>
إعلان عن استيقان.

- <AuthzDecisionStatement>
إعلان عن قرار ترخيص.

- <AttributeStatement>
إعلان عن نعت.

وكل تأكيد بلا إعلانات، يجب أن يحتوي على العنصر <Subject>. ومثل هذا التأكيد يعرف هوية طرف رئيسي بطريقة يمكن إحالتها أو إثباتها باستعمال طرائق اللغة SAML، ولكنه لا يؤكد أي معلومات إضافية تصحب هذا الطرف الرئيسي.

وإلا فإذا كان <Subject> موجوداً، فهو يعرف هوية صاحب جميع الإعلانات الواردة في التأكيد. أما إذا كان <Subject> محذوفاً، فإن الإعلانات الواردة في التأكيد تنطبق على صاحب أو أصحاب تعرف هوياتهم بكيفية معينة في التطبيق أو في الجانبية. واللغة SAML نفسها لا تعرف مثل هذه الإعلانات، والتأكيد الذي لا صاحب له لا يكون له أي معنى محدد في هذه التوصية.

وحسب متطلبات البروتوكولات أو الجانبيات الخاصة، قد يحتاج مُصدر تأكيد اللغة SAML إلى أن يجري استيقانه، كما قد يتطلب الأمر غالباً حماية السلامة. ويمكن أن يتوفر الاستيقان وسلامة الرسالة عن طريق آليات توفرها رابطة بروتوكول أثناء تسليم تأكيد (انظر البند 10). والتأكيد في اللغة SAML يمكن أن يكون موقعاً، مما يضمن استيقان المُصْدر وحماية السلامة في نفس الوقت.

وإذا كان مثل هذا التوقيع مستعملاً، إذاً يجب أن يكون العنصر <ds : Signature> موجوداً، ويجب على طرف واثق أن يتحقق من صلاحية التوقيع (مما يعني أن التأكيد لم يمس) من حيث مطابقته لتوقع اللغة XML التابع للتجمع W3C. وإذا وجد التوقيع غير صالح، يجب على الطرف الوايق ألا يعتمد على محتويات التأكيد. أما إذا كان التوقيع صالحاً، فينبغي للطرف الواثق أن يقيّم التوقيع لكي يحدد هوية المُصْدر ومناسبة صلته، يمكنه متابعة معالجة التأكيد وفقاً لهذه التوصية ولما يبدو له مناسباً (مثل تقدير الشروط وإبداء الرأي واتّباع القواعد الخاصة بالجانبيات وغير ذلك).

وسواء كانت الإعلانات موقعة أو غير موقعة، فإن إدراج العديد منها داخل تأكيد واحد هو مكافئ من حيث الدلالات لمجموعة من التأكيدات تحتوي على هذه الإعلانات بصورة فردية (شريطة أن يكون الصاحب والشروط وما إليها هي ذاتها).

والقطعة التالية من التخطيطة تُعرف العنصر <Assertion> ونمطه المعقد **AssertionType**:

```
<element name="Assertion" type="saml:AssertionType"/>
<complexType name="AssertionType">
      <sequence>
            <element ref="saml:Issuer"/>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="saml:Subject" minOccurs="0"/>
            <element ref="saml:Conditions" minOccurs="0"/>
            <element ref="saml:Advice" minOccurs="0"/>
            <choice minOccurs="0" maxOccurs="unbounded">
                  <element ref="saml:Statement"/>
                  <element ref="saml:AuthnStatement"/>
                  <element ref="saml:AuthzDecisionStatement"/>
                  <element ref="saml:AttributeStatement"/>
            </choice>
      </sequence>
      <attribute name="Version" type="string" use="required"/>
      <attribute name="ID" type="ID" use="required"/>
      <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```

4.3.1.8 العنصر <EncryptedAssertion>

يمثل العنصر <EncyptedAssertion> تأكيداً بالأسلوب المجفر، كما هو معرف في تجفير التجمع W3C. ويحتوي العنصر <EncryptedAssertion> على العنصرين التاليين:

- <xenc:EncryptedData> [مطلوب]
المحتوى المجفر وتفصيلات التجفير المصاحبة، كما هو معروف في تجفير التجمع W3C. وينبغي أن يكون النعت Type موجوداً، وإذا كان موجوداً، يجب أن يحتوي على قيمة من http://www.w3.org/2001/04/xm1enc#Element. ويجب أن يحتوي المحتوى المجفر على عنصر يكون نمطه **AssertionType** أو نمطاً مشتقاً منه.

- <xenc:EncryptedKey> [صفر أو أكثر]
مفاتيح فك تجفير مغلفة، كما هو معرف في تجفير التجمع W3C. وينبغي أن يحتوي كل مفتاح مغلف على نعت Recipient يحدد الكيان الذي جفّر المفتاح من أجله. ويجب أن تكون قيمة النعت Recipient هي معرف الهوية للمعرف URI لكيان في نظام في اللغة SAML، كما هو محدد في الفقرة 7.8.

والتأكيدات المجفرة مهيأة لتكون آلية تحمي السرية، عندما تكون قيمة النص الواحد ستمر عب وسيط.

والقطعة التالية من التخطيطة تعرف العنصر <EncryptedAssertion>:

```
<element name="EncryptedAssertion" type="saml:EncryptedElementType"/>
```

4.1.8 الأصحاب

تحدد هذه الفقرة تركيبة اللغة SAML المستعملة لوصف صاحب تأكيد. والعنصر الاختياري <Subject> يحدد الطرف الرئيسي الذي هو صاحب جميع الإعلانات (صفر أو أكثر) المحتواة في التأكيد. وهو يحتوي على معرف هوية واحد، أو على سلسلة مؤلفة من تأكيد واحد للصاحب أو من عدة تأكيدات، أو على كليهما:

- معرفات الهوية <BaseID> و<NameID> أو <EncryptedID> [اختياري]
تعرف هوية الصاحب.

- <SubjectConfirmation> [صفر أو أكثر]
معلومات تتيح إثبات الصاحب. فإذا قدم أكثر من إثبات للصاحب، يكفي استيفاء واحد منها فقط لإثبات الصاحب لأغراض تطبيق التأكيد.

يمكن أن يحتوي العنصر <Subject> بنفس الوقت على معرف هوية وعلى صفر أو أكثر من إثباتات الصاحب يستطيع طرف واثق أن يتحقق منها عند معالجة التأكيد. فإذا تحقق أي واحد من إثباتات الصاحب المتضمنة، يستيطع الطرف الواثق أن يعالج الكيان الذي يقدم التأكيد كواحدة من الإثباتات التي جعلها الطرف المؤكِّد تصاحب الطرف الرئيسي المعرفة هويته في معرف هوية الاسم. وهي تصاحب الإعلانات الواردة في التأكيد. ويمكن أن يكون هذا الكيان الشاهد و الصاحب الحقيقي هما نفس الكيان، كما يمكن ألا يكونا كذلك.

وإذا لم يكن هناك إثبات صاحب متضمن، لن تكون هناك أي علاقة محددة بين مقدّم التأكيد والصاحب الحقيقي.

ولا يجوز للعنصر <Subject> أن يعرف هوية أكثر من طرف رئيسي واحد.

والقطعة التالية من التخطيطة تعرف العنصر <Subject> ونمطه المعقد <SubjectType>:

```
<element name="Subject" type="saml:SubjectType"/>
<complexType name="SubjectType">
      <choice>
        <sequence>
              <choice>
                    <element ref="saml:BaseID"/>
                    <element ref="saml:NameID"/>
                    <element ref="saml:EncryptedID"/>
              </choice>
              <element ref="saml:SubjectConfirmation" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <element ref="saml:SubjectConfirmation" maxOccurs="unbounded"/>
      </choice>
</complexType>
```

1.4.1.8 العنصر <SubjectConfirmation>

يقدم العنصر <SubjectConfirmation> الوسائل إلى طرف واثق لكي يتحقق من التقابل بين صاحب التأكيد والطرف الذي يجري الطرف الوائق التواصل معه. وهو يحتوي على النعوت والعناصر التالية:

- <Method> [مطلوب]
مرجع للمعرف URI يعرف هوية بروتوكول أو آلية يطلب استعمالها لإثبات الصاحب. ومراجع المعرف URI التي تعرف هويات طرائق الإثبات المعرفة في اللغة SAML، هي معرفة في البند 11. ويمكن إضافة طرائق إضافية بعد تعريف معرفات URI وجانبيات جديدة أو باتفاق خاص.

- <BaseID> أو <NameID> أو <EncryptedID> [اختياري]
يعرف هوية الكيان المتوقع منه أن يستوفي المتطلبات المتضمنة لإثبات الصاحب.

- <SubjectConfirmationData> [اختياري]
معلومات إثبات إضافية لاستعمالها في طريقة إثبات خاصة. فقد يكون مثلاً المحتوى العاد لهذا العنصر عنصراً من <ds:KeyInfo> كما هو معرف في تجفير التجمع W3C، يعرف هوية مفتاح تجفير (انظر أيضاً الفقرة 3.4.1.8). ويمكن لطرائق إثبات خاصة أن تعرف نمطاً من تخطيطة يصف العناصر أو النعوت أو المحتويات التي قد تظهر في العنصر <SubjectConfirmationData>.

والقطعة التالية من التخطيطة تعرف العنصر <SubjectConfirmation> ونمطه المعقد **SubjectConfirmationType**:

```
<element name="SubjectConfirmation" type="saml:SubjectConfirmationType"/>
<complexType name="SubjectConfirmationType">
      <sequence>
            <choice minOccurs="0">
                  <element ref="saml:BaseID"/>
                  <element ref="saml:NameID"/>
                  <element ref="saml:EncryptedID"/>
            </choice>
            <element ref="saml:SubjectConfirmationData" minOccurs="0"/>
      </sequence>
      <attribute name="Method" type="anyURI" use="required"/>
</complexType>
```

2.4.1.8 العنصر <SubjectConfirmationData>

يكون العنصر <SubjectConfirmationData> من النمط المعقد **SubjectConfirmationDataType**. وهو يحدد المعطيات الإضافية على إثبات الصاحب، أو التي تحدد الظروف التي يمكن لفعل إثبات الصاحب أن يتم فيها. ويقع إثبات الصاحب عندما يسعى طرف مؤكِّد إلى التحقق من العلاقات القائمة بين الكيان الذي قدّم التأكيد (أي الكيان الشاهد) وبين الصاحب المطالب بالتأكيد.

- <NotBefore> [اختياري]
لحظة زمنية لا يمكن إثبات الصاحب قبلها. وتشفر القيمة الزمنية بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- <NotOnOrAfter> [اختياري]
لحظة زمنية لا يمكن إثبات الصاحب بعدها أبداً. وتشفر القيمة الزمنية بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- <Recipient> [اختياري]
معرف الهوية URI الذي يحدد الكيان أو الموقع الذي يمكن لكيان شاهد أن يقدم التأكيد له أو فيه. فقد يدل هذا النعت مثلاً على أن التأكيد يجب تسليمه إلى نقطة انتهائية خاصة من الشبكة، بغية منع أي وسيط من إعادة توجيهه إلى مكان آخر.

- <InResponseTo> [اختياري]
معرف هوية رسالة بروتوكول في اللغة SAML، يمكن لكيان شاهد أن يقدم التأكيد استجابة لها. فهذا النعت يمكن استعماله لربط التأكيد بطلب في اللغة SAML أدى إلى تقديمه.

- <Address> [اختياري]
عنوان أو مجلة في الشبكة، يمكن لكيان شاهد أن يقدم منهما التأكيد. فهذا النعت يمكن استعماله مثلاً لربط التأكيد التأكيد بعناوين زبون خاصة، لكي يمنع أي معتدٍ من سرقة التأكيد بسهولة وتقديمه اعتباراً من أي مجلة أخرى. وينبغي تقديم عناوين بروتوكول الإنترنت من الصيغة 4 (IPv4) بالنسق المعتاد من الأرقام العشرية تفصل بينها نقاط

(مثل 4.3.2.1)، بينما ينبغي تقديم العناوين IPv6 كما هو معرف في الفقرة من طلب التعليقات RFC 3513 الصادر عن الفريق IETF (مثل "FEDC:BA98:7654:3210:FEDC:BA98:7654:3210").

- نعـــوت اعتباطية

يستعمل هذا النمط المعقّد نقطة توسّع <xs:anyAttribute>، لكي يسمح بإضافة نعوت اعتباطية في اللغة XML، موصوفة في مكان اسم للتركيبات <SubjectConfirmationData>، دون الحاجة إلى توسّع صريح في التخطيطة. وهذا يتيح إضافة ما يلزم من المجالات الإضافية لتقديم معلومات إضافية تفيد الإثبات. ويتعين على توسّعات اللغة SAML ألا تضيف نعوتاً محلية من اللغة XML (غير موصوفة في مكان اسم) أو نعوتاً من اللغة XML موصوفة في مكان اسم موصوف في اللغة XML للنمط المعقد **SubjectConfirmationDataType** أو إلى نمط مشتق منه، إن مثل هذه النعوت محجوزة لصيانة وتحسين اللغة SAML بالذات في المستقبل.

- عناصر اعتباطية

يستعمل هذا النمط المعقّد نقطة توسّع <xs:any>، لكي يسمح بإضافة عناصر اعتباطية في اللغة XML إلى التركيبات <SubjectConfirmationData>، دون الحاجة إلى توسّع صريح في التخطيطة. وهذا يتيح إضافة ما يلزم من العناصر الإضافية لتقديم معلومات إضافية تفيد في الإثبات.

إن طرائق وجانبيات الإثبات الخاصة التي تستعمل هذه الطرائق يمكنها أن تطالب باستعمال نعت واحد أو أكثر من هذه النعوت المعرفة في هذا النمط المعقد. فما هو عدد هذه النعوت (وإثباتات الصاحب عامة) التي يمكن استعمالها، انظر البند 13.

إن المدة الزمنية المحددة للنعتين الاختياريين NotBefore وNotOnOrAfter، إن كانا موجودين، ينبغي أن تقع في الفترة الكلية لصلاحية التأكيد، مثلما هي محددة في النعتين NotBefore وNotOnOrAfter للعنصر <Conditions>. وإذا كان النعتان موجودين، يتعين أن تكون قيمة NotBefore أقل من (أبكر من) قيمة NotOnOrAfter.

والقطعة التالية من التخطيطة تعرف العنصر <SubjectConfirmationData> ونمطه المعقد **SubjectConfirmationDataType**:

```
<element name="SubjectConfirmationData"
type="saml:SubjectConfirmationDataType"/>
<complexType name="SubjectConfirmationDataType" mixed="true">
       <complexContent>
              <restriction base="anyType">
                     <sequence>
                            <any namespace="##any" processContents="lax"
minOccurs="0" maxOccurs="unbounded"/>
                   </sequence>
                     <attribute name="NotBefore" type="dateTime"
use="optional"/>
                     <attribute name="NotOnOrAfter" type="dateTime"
use="optional"/>
                     <attribute name="Recipient" type="anyURI"
use="optional"/>
                     <attribute name="InResponseTo" type="NCName"
use="optional"/>
                     <attribute name="Address" type="string"
use="optional"/>
                     <anyAttribute namespace="##other"
processContents="lax"/>
              </restriction>
       </complexContent>
</complexType>
```

3.4.1.8 النمط المعقد KeyInfoConfirmationDataType

يفرض النمط المعقد **KeyInfoConfirmationDataType** على العنصر <SubjectConfirmationData> أن يحتوي على عنصر واحد أو أكثر من العناصر <ds:KeyInfo> التي تعرف هويات مفاتيح التجفير التي تُستخدم بطريقة ما

لاستيقان كيان شاهد. وطريقة الإثبات الخاصة يجب أن تحدد الآلية الصحيحة التي يمكن بها استعمال معطيات الإثبات. ويمكن أن تظهر أيضاً النعوت الاختيارية التي يعرفها النمط المعقد **SubjectConfirmationDataType**.

وينبغي لهذا النمط المعقد، أو لأي نمط مشتق منه، أن تستعمله كل طريقة إثبات تعرف معطيات إثباتها بمصطلحات العنصر <ds:KeyInfo>.

وطبقاً لتجفير التجمع W3C، على كل عنصر <ds:KeyInfo> أن يعرف هوية مفتاح واحد تجفيري. ويمكن لعناصر متميزة <ds:KeyInfo> أن تعرف هويات عدة مفاتيح، تماماً كما يحدث لطرف رئيسي.

حين يستخدم مفاتيح مختلفة لكي يثبت نفسه لدى أطراف واثقة مختلفة.

والقطعة التالية من التخطيطة تعرف النمط المعقد **KeyInfoConfirmationDataType**:

```
<complexType name="KeyInfoConfirmationDataType" mixed="false">
       <complexContent>
              <restriction base="saml:SubjectConfirmationDataType">
                     <sequence>
                            <element ref="ds:KeyInfo"
maxOccurs="unbounded"/>
                     </sequence>
            </restriction>
       </complexContent>
</complexType>
```

4.4.1.8 مثال على <Subject> يثبته مفتاح

لشرح الكيفية التي تتفق بها عناصر وأنماط مختلفة، يرد أدناه مثال على عنصر <Subject> يحتوي على معرف هوية اسم وعلى إثبات صاحب مبنيين على برهان التملك لمفتاح. ويكون هنا استخدام النمط **KeyInfoConfirmationDataType** للتعريف بهوية قواعد التركيب لمعطيات الإثبات، هو عنصر <ds:KeyInfo>:

```
<Subject>
       <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
       scott@example.org
       </NameID>
       <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-
of-key">
              <SubjectConfirmationData
xsi:type="saml:KeyInfoConfirmationDataType">
                     <ds:KeyInfo>
                            <ds:KeyName>Scott's Key</ds:KeyName>
                     </ds:KeyInfo>
              </SubjectConfirmationData>
       </SubjectConfirmation>
</Subject>
```

5.1.8 Conditions

تحدد هذه الفقرة تركيبة اللغة SAML التي تضع القيود على الاستعمال المقبول لتأكيدات اللغة SAML. ويمكن أن يحتوي العنصر <Conditions> على العناصر والنعوت التالية:

- NotBefore [اختياري]

يحدد أبكر لحظة يكون التأكيد صالحاً عندها. وتشفر القيمة الزمنية بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- NotOnOrAfter [اختياري]

يحدد اللحظة التي يصل فيها التأكيد إلى انقضاء صلاحيته. وتشفر القيمة الزمنية بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- <Condition> [أي عدد]
شرط نمط معرف في تخطيطة توسّعية. فيتعين استخدام النعت xsi:type للدلالة على الشرط الحقيقي.

- <AudienceRestriction> [أي عدد]
يحدد أن التأكيد موجّه إلى جمهور خاص.

- <OneTimeUse> [اختياري]
يحدد أن التأكيد ينبغي أن يستعمل فوراً، ويتعين ألا يحتفظ به لاستعمال لاحق. وعلى الرغم من أن التخطيطة تتيح عدة مناسبات، إلا أنه يتعين أن تكون لهذا العنصر فرصة واحدة على الأكثر.

- <ProxyRestriction> [اختياري]
يعين التحديدات التي يفرضها الطرف المؤكِّد على الأطراف الواثقة التي ترغب في أن تعمل لاحقاً كأطراف مؤكَّدة، فتصدر تأكيدات خاصة بها، استناداً إلى المعلومات الواردة في التأكيد الأصلي. وعلى الرغم من أن التخطيطة تتيح عدة مناسبات، إلا أنه يتعين أن تكون لهذا العنصر فرصة واحدة على الأكثر.

ولما كان استخدام النعت xsi:type يتيح لتأكيد أن يحتوي على أكثر من فرصة واحدة من نمط فرعي تحدده اللغة SAML من **ConditionsType** (مثل **OneTimeType**)، فإن التخطيطة لا تحدّ صراحة عدد المرات التي يمكن فيها تضمين شروط خاصة. ويمكن لنمط خاص من الشروط أن يضع حداً لمثل هذا الاستعمال، كما هو مبين أعلاه.

والقطعة التالية من التخطيطة تعرف العنصر <Conditions> ونمطه المعقد **ConditionsType**:

```
<element name="Conditions" type="saml:ConditionsType"/>
<complexType name="ConditionsType">
       <choice minOccurs="0" maxOccurs="unbounded">
              <element ref="saml:Condition"/>
              <element ref="saml:AudienceRestriction"/>
              <element ref="saml:OneTimeUse"/>
              <element ref="saml:ProxyRestriction"/>
     </choice>
       <attribute name="NotBefore" type="dateTime" use="optional"/>
       <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
</complexType>
```

1.5.1.8 القواعد العامة للمعالجة

إذا كان تأكيد يحتوي على العنصر <Conditions>، تكون صلاحية التأكيد متوقفة عندئذ على العناصر الفرعية والنعوت المقدمة، باستعمال القواعد التالية بالترتيب المبين أدناه.

كل تأكيد يحدد الشرط Valid حالة صلاحيته، يمكن مع ذلك أن يكون غير جدير بالثقة أو غير صالح لأسباب مختلفة، منها أنه غير مكوّن بشكل جيد أو تخطيطة غير صالحة، أو أنه غير صادر عن سلطة في اللغة SAML جديرة بالثقة، أو أنه غير مستيقن بوسائل جديرة بالثقة.

وقد لا تؤثر بعض الشروط مباشرة في صلاحيته التأكيد المحتوى (إنها تقيم دوماً بالصالح (Valid))، ولكنها تقيّد سلوك الأطراف الواثقة من حيث استخدامها للتأكيد:

- إذا لم يكن أي عنصر فرعي أو نعت مقدماً في العنصر <Condition>، يعتبر التأكيد صالحاً (Valid) بالنسبة إلى معالجة الشرط.
- إذا تحدد أي عنصر فرعي أو نعت من العنصر <Conditions> أنه غير صالح، يعتبر التأكيد عندئذ غير صالح.

- إذا كان لا يمكن تقييم أي عنصر فرعي أو نعت من العنصر <Conditions>، أو إذا كان أي عنصر مصادف غير مفهوم، لا يمكن عندئذ تحديد صلاحية التأكيد، فيعتبر غير محدّد.
- إذا كانت جميع العناصر الفرعية والنعوت من العنصر <Conditions> محددة بأنها صالحة، يعتبر التأكيد عندئذ صالحاً بالنسبة إلى معالجة الشرط.

وأول قاعدة تُطبّق تنهي معالجة الشروط، وبالتالي يكون تحديد كون التأكيد غير صالح يتقدم على كون التأكيد غير محدد.

وكل تأكيد يتحدد أنه غير صالح أو غير محدّد، يتعين على الطرف الواثق أن ينبذه (مهما يكن سياق المعالجة أو جانبيتها)، كما لو كان التأكيد سيئ التكوين أو غير قابل للاستعمال.

2.5.1.8 النعتان NotBefore وNotOnOrAfter

يحدد النعتان NotBefore وNotOnOrAfter حدّين زمنيين لصلاحية التأكيد داخل سياق جانبية استعماله أو جانبيتي استعمالهما. إنهما لا يضمنان بقاء كون الإعلانات في التأكيد صحيحة أو دقيقة أثناء فترة الصلاحية.

يعين النعت NotBefore اللحظة الزمنية التي تبدأ فيها فترة الصلاحية. بينما يعين النعت NotOnOrAfter محذوفة، تعتبر عندئذ غير معيّنة.

فإذا كان النعت NotBefore غير معين (وإذا كانت جميع الشروط الأخرى المقدمة مقيّمة على أنها صالحة "Valid")، يكون التأكيد صالحاً بالنسبة إلى الشروط في أي لحظة قبل اللحظة الزمنية التي يعينها النعت NotOnOrAfter. وإذا كان النعت NotOnOrAfter غير معين (وإذا كانت جميع الشروط الأخرى المقدّمة مقيّمة على أنها صالحة "Valid")، يكون التأكيد صالحاً بالنسبة إلى الشروط في أي لحظة بدءاً من اللحظة الزمنية التي يعينها النعت NotBefore ومن دون أي مهلة انقضاء. وإذا لم يكن أي واحد من النعتين معيناً (وإذا كانت جميع الشروط الأخرى المقدمة مقيّمة على أنها صالحة "Valid"، يكون التأكيد صالحاً بالنسبة إلى الشروط في أي لحظة كانت.

وإذا كان كلا النعتين موجودين، يتعين أن تكون قيمة NoBefore أقل من (أبكر من) قيمة النعت NotOnOrAfter.

3.5.1.8 العنصر <Conditions>

يعمل العنصر <Conditions> نقطة توسّعية لشروط جديدة. ونمطه المعقد **ConditionAbstractType** هو نمط مجرد، ولا يمكن استعماله بالتالي إلا كأساس لنمط مشتق.

والقطعة التالية من التخطيطة تعرف العنصر <Condition> ونمطه المعقد **ConditionAbstractTypee**:

```
<element name="Condition" type="saml:ConditionAbstractType"/>
<complexType name="ConditionAbstractType" abstract="true"/>
```

4.5.1.8 العنصران <AudienceRestriction> و<Audience>

يحدد العنصر <AudienceRestriction> أن التأكيد موجه إلى جمهور واحد معين أو إلى عدة جماهير تعرف هوياتها عناصر <Audience>. وعلى الرغم من أن الطرف الواثق في اللغة SAML يستطيع استخلاص النتائج من تأكيد، إلا أن الطرف المؤكِّد في اللغة SAML لا يقدم أي تمثيل صريح بشأن وثاقة الصلة أو الجدارة بالثقة لمثل هذا الطرف. إنه يحتوي على العنصر التالي:

- <Audience>

  مرجع لمعرف الهوية URI يعرف هوية جمهور مقصود. يمكن لمرجع المعرف URI أن يعرف هوية وثيقة تشرح بنود وشروط العضوية في جمهور. ويمكنه أيضاً أن يحتوي على معرف الهوية الوحيد URI من معرف هوية اسم في اللغة SAML يشرح كياناً في نظام.

عضواً في واحد من الجماهير المحددة أو في أكثر من جمهور.

لا يستطيع الطرف المؤكّد في اللغة SAML أن يمنع طرفاً مكشوفاً له التأكيد، من اتخذ أي عمل استناداً إلى المعلومات المقدمة لديه. ومع ذلك فإن العنصر <AudienceRestriction> يتيح للطرف المؤكد في اللغة SAML الإعلان صراحة عن عدم توفر أي ضمانة لمثل هذا الطرف بالشكل المقروء من الإنسان ومن الآلة. وبينما لا توجد أي ضمانة من أن تتمسك أي محكمة بمثل هذا الاستبعاد للضمانة في كل مناسبة، إلا أن احتمال التمسك باستبعاد الضمانة قد تحسّن كثيراً.

ويمكن للعديد من العناصر <AudienceRestriction> أن ترد في تأكيد واحد، ويتعين في ظرف واحد معين مجموعات منفصلة (أو "OR" المنطقية)، وتشكل في ظروف عديدة مجموعات معطوفة (و "AND" المنطقية).

والقطعة التالية من التخطيطة تعرف العنصر <AudienceRestriction> ونمطه المعقد **AudienceRestriction**:

```
<element name="AudienceRestriction"
       type="saml:AudienceRestrictionType"/>
<complexType name="AudienceRestrictionType">
       <complexContent>
              <extension base="saml:ConditionAbstractType">
                     <sequence>
                            <element ref="saml:Audience"
maxOccurs="unbounded"/>
                     </sequence>
              </extension>
       </complexContent>
</complexType>
<element name="Audience" type="anyURI"/>
```

5.5.1.8 العنصر <OneTimeUse>

يمكن للأطراف الواثقة أن تختار بصورة عامة الاحتفاظ بالتأكيدات، أو بالمعلومات التي تحتويها، بشكل آخر. ويتيح عنصر الشرط <OneTimeUse> لسلطة ما أن تبين أن المعلومات الواردة في التأكيد غالباً ما تتغير قريباً جداً، فينبغي الحصول على معلومات حديثة لدى كل استعمال. ومن أمثلة ذلك تأكيد يحتوي على <AuthzDecisionStatement> هو نتيجة لسياسة تحدد التحكم في النفاذ في كل ساعة من اليوم.

وإذا كانت ميقاتيات النظام متزامنة تزامناً دقيقاً في بيئة متناثرة، يمكن استيفاء هذا المطلب عند استخدام فترة الصلاحية بكل عناية. ومع ذلك لما كان لابد من وجود بعض الحيدان بين ميقاتيات الأنظمة، وأن هذا الحيدان يختلط مع بعض التأخير المحتمل في الإرسال، فلا يوجد أي سبيل مناسب لكي يحد المُصْدر تحديداً مناسباً من عمر التأكيد، دون المخاطرة بمجازفة كبيرة في انقضاء صلاحية التأكيد قبل وصوله.

ويدل العنصر <OneTimeUse> على أن التأكيد ينبغي أن يستعمله الطرف الواثق فوراً، ويتعين علدم الاحتفاظ به لاستعمال لاحق. وتكون الأطراف الواثقة حرة دائماً في أن تطلب لكل استعمال تأكيداً حديثاً. ومع ذلك فالتطبيقات التي تختار أن تحتفظ بالتأكيدات لاستعمال لاحق، يتعين عليها أن تتقيد بالعنصر <OneTimeUse>. وهذا الشرط مستقل عن معلومات الشرط <NotBefore> و<NotOnOrAfter>.

ولكي يأخذ الطرف الواثق قيد الاستعمال الوحيد على عاتقه، ينبغي له أن يحتفظ بذاكرة مَخْبأ للتأكيدات التي عالجها وتحتوي مثل هذا الشرط. وفي كل مرة يعالج فيها تأكيد يحتوي على هذا الشرط، ينبغي التحقق من المخبأ للتأكد من أن هذا التأكيد بالذات لم يسبق للطرف الواثق أن استلمه وعالجه.

ويتعين على سلطة اللغة SAML ألا تورد أكثر من عنصر واحد <OneTimeUse> داخل العنصر <Condition> من تأكيد.

ولأغراض تحديد صلاحية العنصر <Conditions>، يعتبر العنصر <OneTimeUse> صالحاً دائماً. وهذا يعني أن هذا الشرط لا يؤثر في الصلاحية ولكنه شرط للاستعمال.

والقطعة التالية من التخطيطة تعرف العنصر <OneTimeUse> ونمطه المعقد **OneTimeUseType**:

```
<element name="OneTimeUse" type="saml:OneTimeUseType"/>
```

```
<complexType name="OneTimeUseType">
       <complexContent>
              <extension base="saml:ConditionAbstractType"/>
</complexContent>
</complexType>
```

6.5.1.8 العنصر <ProxyRestriction>

يعين التحديدات التي يفرضها الطرف المؤكد على الأطراف الواثقة التي ترغب في أن تعمل بدورها كأطراف مؤكدة، فتصدر لاحقاً تأكيدات خاصة بها، استناداً إلى المعلومات الواردة في التأكيد الأصلي. ويتعين على الطرف الواثق الذي يعمل كطرف مؤكّد ألا يصدر تأكيداً ينتهك هو نفسه التقييدات المحددة في هذا الشرط باعتباره تأكيداً يحتوي على مثل هذا الشرط.

ويحتوي العنصر <ProxyRestriction> على العنصر والنعت التاليين:

- Count [اختياري]
يحدد العدد الأعظم من الوسطاء الذي يسمح الطرف المؤكِّد بوجودهم ما بين هذا التأكيد وتأكيد آخر كان قد صدر في آخر المطاف اعتماداً على هذا التأكيد.

- <Audience> [صفر أو أكثر]
يحدد مجموعة الجماهير التي يسمح الطرف المؤكّد أن تصدر لها تأكيدات جديدة اعتماداً على هذا التأكيد.

وإذا كانت قيمة Count تساوي الصفر، فهي تدل على أنه يتعين على طرف واثق ألا يصدر تأكيداً إلى طرف واثق آخر اعتماداً على هذا التأكيد. أما إذا كانت قيمته أكبر من الصفر، فيتعين على كل تأكيد صادر على هذا النحو أن يحتوي هو نفسه على عنصر <ProxyRestriction> مع قيمة للحساب Count تكون أصغر من هذه القيمة بواحد على الأكثر.

وإذا كانت لا توجد عناصر <Audience> محددة، عندئذ لا تكون هناك تقييدات على الجمهور مفروضة على الأطراف الواثقة التي يمكن أن تقدم لها تأكيدات لاحقاً. وإلا فيتعين على كل تأكيد صادر على هذا النحو أن يحتوي هو نفسه على عنصر <AudienceRestriction> مع عنصر واحد <Audience> على الأقل كان موجوداً في العنصر السابق <ProxyRestriction>، ولن يوجد أي عنصر <Audience> لم يكن موجوداً في العنصر السابق <ProxyRestriction>.

ويتعين على سلطة اللغة SAML ألا تورد أكثر من عنصر واحد <ProxyRestriction> داخل العنصر <Conditions> من تأكيد.

ولأغراض تحديد صلاحية العصنر <Conditions>، يعتبر العنصر <ProxyRestriction> صالحاً دائماً. وهذا يعني أن هذا الشرط لا يؤثر في الصلاحية، ولكنه شرط للاستعمال.

والقطعة التالية من التخطيطة تعرف العنصر <ProxyRestriction> ونمطه المعقد **ProxyRestrictionType**:

```
<element name="ProxyRestriction" type="saml:ProxyRestrictionType"/>
<complexType name="ProxyRestrictionType">
       <complexContent>
              <extension base="saml:ConditionAbstractType">
                     <sequence>
                            <element ref="saml:Audience" minOccurs="0"
maxOccurs="unbounded"/>
                     </sequence>
                     <attribute name="Count" type="nonNegativeInteger"
use="optional"/>
              </extension>
       </complexContent>
</complexType>
```

6.1.8 Advice

تعرف هذه الفقرة تركيبات اللغة SAML التي تحتوي على المعلومات الإضافية عن تأكيد، يرغب الطرف المؤكِّد في إعطائها إلى الطرف الواثق.

ويحتوي العنصر <Advice> على أي معلومات إضافية ترغب في توفيرها سلطة في اللغة SAML. ويمكن للتطبيقات أن تتجاهل هذه المعلومات دون أن يؤثر ذلك لا في دلالات التأكيد ولا في صلاحيته.

يحتوي العنصر <Advice> على خليط من العناصر <Assertion> و<EncryptedAssertion> و<AssertionIDRef> و<AssertionURIRef> عددها صفر أو أكثر، والعناصر الموصوفة بمكان اسم في أمكنة أسماء أخرى ليست في اللغة SAML.

وفيما يلي بعض الاستعمالات المحتملة للعنصر <Advice>:

- إيراد براهين واضحة تدعم مطالبات التأكيد المذكور، سواء مباشرة (عبر دمج المطالبات) أو بصورة غير مباشرة (بالإحالة إلى التأكيدات المذكورة للدعم).
- إقامة البرهان على مطالبات التأكيد.
- تحديد التوقيت ونقاط التوزيع لتحيينات التأكيد.

والقطعة التالية من التخطيطة تعرف العنصر <Advice> ونمطه المعقد **AdvideType**:

```
<element name="Advice" type="saml:AdviceType"/>
<complexType name="AdviceType">
       <choice minOccurs="0" maxOccurs="unbounded">
              <element ref="saml:AssertionIDRef"/>
              <element ref="saml:AssertionURIRef"/>
              <element ref="saml:Assertion"/>
              <element ref="saml:EncryptedAssertion"/>
              <any namespace="##other" processContents="lax"/>
       </choice>
</complexType>
```

7.1.8 الإعلانات (Statements)

جميع الإعلانات المعرفة في اللغة SAML تكون مرفقة بصاحب. وتكون تأكيدات اللغة SAML صادرة حول **صاحب**، يمثله العنصر <Subject>. ومع ذلك فالعنصر <Subject> اختياري، ويمكن للمواصفات والجانبيات الأخرى أن تستعمل بنية تأكيد اللغة SAML، لكي تصنع تأكيدات مشابهة من دون أن تحدد صاحباً، أو ربما تحدد الصاحب بأسلوب آخر. وتعرّف الفقرات الفرعية التالية تركيبات اللغة SAML التي تحتوي على معلومات الإعلان.

1.7.1.8 العنصر (Statement)

العنصر <Statement> هو نقطة توسّع تتيح للتطبيقات الأخرى المستندة إلى التأكيد أن تعيد استعمال إطار العمل لتأكيد اللغة SAML. واللغة SAML هي نفسها تشتق إعلاناتها المركزية من هذه النقطة التوسّعية. ونمطها المعقد **StatementAbstractType** هو نمط مجرد، ولذلك فهو يستعمل فقط كأساس لنمط مشتق.

والقطعة التالية من التخطيطة تعرف العنص <Statement> ونمطه المعقد **StatementAbstractType**:

```
<element name="Statement" type="saml:StatementAbstractType"/>
<complexType name="StatementAbstractType" abstract="true"/>
```

2.7.1.8 العنصر <AuthnStatement>

يصف العنصر <AuthnStatement> إعلاناً من سلطة اللغة SAML يؤكد أن صاحب التأكيد قد جرى استيقانه بأسلوب خاص في وقت معين. والتأكيدات التي تحتوي على العناصر <AuthnStatement> يتعين عليها أن تحتوي على العنصر <Subject>.

ونمط هذا العنصر هو **AuthnStatementType** الذي يوسع **StatementAbstractType** بإضافة العناصر والنعوت التالية:

ملاحظة – أزيل العنصر <AuthorityBinding> ونمطه المقابل من العنصر <AuthnStatement> من الصيغة التالية V2.0 للغة SAML.

- AuthnInstant [مطلوب]
يحدد اللحظة التي جرى فيها الاستيقان. وتشفر القيمة الزمنية بالتوقيت UTC كما هو مشروح في الفقرة 3.7.

- SessioinIndex [اختياري]
يحدد دليل دورة خاصة ما بين الطرف الرئيسي الذي يعرف الصاحب هويته وبين السلطة الاستيقانية.

- SessionNotOnOrAfter [اختياري]
يحدد اللحظة التي تعتبر فيها الدورة بين الطرف الرئيسي الذي يعرف الصاحب هويته وبين سلطة اللغة SAML التي تصدر هذا الإعلان، قد انتهت. وتشفر القيمة الزمنية بالتوقيت UTC كما هو مشروح في الفقرة 3.7. وليست هناك علاقة لازمة بين هذا النعت ونعت الشرط NotOnOrAfter الذي قد يكون موجوداً في التأكيد.

- SubjectLocality [اختياري]
يحدد اسم الميدان في النظام DNS والعنوان في البروتوكول IP للنظام الذي جرى فيه ظاهرياً استيقان صاحب التأكيد.

- AuthnContext [مطلوب]
السياق الذي استخدمته السلطة الاستيقانية حتى وأثناء الحدث الاستيقاني الذي أدى إلى هذا الإعلان. ويحتوي على مرجع إلى صنف سياق الاستيقان، أو إلى إعلان عن سياق الاستيقان أو مرجع عن الإعلان، أو إلى كليهما. انظر البند 12 (سياق الاستيقان) للحصول على وصف كامل للمعلومات عن سياق الاستيقان.

ويمكن بصورة عامة استعمال أي قيمة سلسلة كقيمة للنعت SessionIndex. ومع ذلك عندما تكون السرية مطلوبة، يجب الاهتمام بألا تحول قيمة SessionIndex دون صلاحية آليات السرية الأخرى. وعليه ينبغي ألا يمكن استعمال هذه القيمة لكي يتابع طرف رئيسي النشاط عبر مشتركين مختلفين في الدورة. وهناك فيما يلي حلان يحققان هذا الهدف ويوصى بهما:

- تستخدم أعداد صحيحية موجبة (أو تكرر ثوابت واردة في قائمة) للنعت SessionIndex. وينبغي لسلطة اللغة SAML أن تختار مجالاً من قيم الأعداد الأصلية بحيث يكون أي عدد صحيح كبيراً بما يكفي حتى يمنع أن تجرى أعمال طرف رئيسي معين عبر مشتركين عديدين في الدورة. وينبغي لسلطة اللغة SAML أن تختار عشوائياً قيماً للنعت SessionIndex من داخل هذا المجال (إلا عندما يطلب تأمين قيم وحيدة للإعلانات اللاحقة المعطاة لنفس المشترك في الدورة، ولكن كجزء من دورة متميزة).
- تستخدم قيمة معرف الهوية للتأكيد المغلف في النعت SessionIndex.

والقطعة التالية من التخطيطة تعرف العنصر <AuthnStatement> ونمطه المعقد **AuthnStatementType**:

```
<element name="AuthnStatement" type="saml:AuthnStatementType"/>
<complexType name="AuthnStatementType">
       <complexContent>
              <extension base="saml:StatementAbstractType">
                     <sequence>
                            <element ref="saml:SubjectLocality"
minOccurs="0"/>
                            <element ref="saml:AuthnContext"/>
                     </sequence>
                     <attribute name="AuthnInstant" type="dateTime"
use="required"/>
                     <attribute name="SessionIndex" type="string"
use="optional"/>
                     <attribute name="SessionNotOnOrAfter" type="dateTime"
use="optional"/>
              </extension>
       </complexContent>
</complexType>
```

1.2.7.1.8 العنصر <SubjectLocality>

يحدد العنصر <SubjectLocality> اسم الميدان في النظام DNS والعنوان في البروتوكول IP للنظام الذي جرى منه استيقان صاحب التأكيد. وله النعتان التاليان:

- Address [اختياري]
عنوان الشبكة للنظام الذي جرى منه استيقان الطرف الرئيسي الذي عرف الصاحب هويته. وعناوين الصيغة 4 لبروتوكول الإنترنت (IPv4) ينبغي أن تتمثل بالنسق العشري المنقط (مثل "4.3.2.1"). وعناوين الصيغة 6 لبروتوكول الإنترنت (IPv6) ينبغي أن تتمثل ما هو محدد في طلب التعليقات RFC 3513, 2.2 الصادر عن فريق المهام IETF (مثل "FEDC:BA98:7654:3210:FEDC:BA98:7654:3210").

- DNSName [اختياري]
اسم الميدان في النظام DNS للنظام الذي جرى منه استيقان الطرف الرئيسي الذي عرّف الصاحب هويته. هذا العنصر استشاري بالكامل، طالما أن هذين المجالين عرضة بسهولة "للتحريف الساخر"، غير أنهما قد يشكلان معلومات مفيدة في بعض التطبيقات.

والقطعة التالية من التخطيطة تعرف العنصر <SubjectLocality> ونمطه المعقد **SubjectLocalityType**:

```
<element name="SubjectLocality" type="saml:SubjectLocalityType"/>
<complexType name="SubjectLocalityType">
       <attribute name="Address" type="string" use="optional"/>
       <attribute name="DNSName" type="string" use="optional"/>
</complexType>
```

2.2.7.1.8 العنصر <SubjectLocality>

يحدد العنصر <AuthnContext> سياق حدث استيقاني. ويمكن أن يحتوي العنصر على مرجع إلى صنف سياق الاستيقان، أو إلى إعلان عن سياق الاستيقان أو مرجع إلى الإعلان، أو إلى كليهما. ولنمطه المعقد **AuthnContextType** العناصر التالية:

- <AuthnContextClassRef> [اختياري]
مرجع إلى معرف URI يعرف هوية صنف سياق الاستيقان الذي يشرح الإعلان عن سياق الاستيقان التالي.

- <AuthnContextDecl> أو <AuthnContextDeclRef> [اختياري]
إما إعلان عن سياق استيقان توفره قيمة، وإما مرجع إلى معرف URI يعرف هوية مثل هذا الإعلان. ويمكن أن ينحل المرجع إلى المعرف URI مباشرة في وثيقة للغة XML تحتوي على الإعلان المحال إليه.

- <AuthenticatingAuthority> [صفر أو أكثر]
صفر أو أكثر من معرفات الهوية الوحيدة لسلطات الاستيقان التي اشتركت في استيقان الطرف الرئيسي (ولا تشمل مُصْدر التأكيد ا لذي يفترض فيه أن يكون مشتركاً من دون أن يسمى هنا صراحة).

انظر البند 12 للشرح الكامل عن معلومات سياق الاستيقان.

والقطعة التالية من التخطيطة تعرف العنصر <AuthnContext> ونمطه المعقد **AuthnContextType**:

```
<element name="AuthnContext" type="saml:AuthnContextType"/>
<complexType name="AuthnContextType">
       <sequence>
              <choice>
                     <sequence>
                            <element ref="saml:AuthnContextClassRef"/>
                            <choice minOccurs="0">
                                   <element ref="saml:AuthnContextDecl"/>
                                   <element
ref="saml:AuthnContextDeclRef"/>
```

```
                        </choice>
                    </sequence>
                    <choice>
                        <element ref="saml:AuthnContextDecl"/>
                        <element ref="saml:AuthnContextDeclRef"/>
                    </choice>
                </choice>
                <element ref="saml:AuthenticatingAuthority" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
</complexType>
<element name="AuthnContextClassRef" type="anyURI"/>
<element name="AuthnContextDeclRef" type="anyURI"/>
<element name="AuthnContextDecl" type="anyType"/>
<element name="AuthenticatingAuthority" type="anyURI"/>
```

3.7.1.8 العنصر <AttributeStatement>

يشرح العنصر <AttributeStatement> إعلان سلطة اللغة SAML الذي يؤكد أن صاحب التأكيد هو المصاحب للنعوت المحددة. ويتعين على التأكيدات التي تحتوي على العناصر <AttributeStatement> أن تحتوي على العنصر <Subject>.

إنه من النمط **AttributeStatementType** الذي يوسّع النمط **StatementAbstractType** بإضافة العنصر التالي إليه:

- <Attribute> أو <EncryptedAttribute> [واحد أو أكثر]

يحدد العنصر <Attribute> نعتاً لصاحب التأكيد. ويمكن لنعت مجفر في اللغة SAML أن يكون متضمناً في العنصر <EncryptedAttribute>.

والقطعة التالية من التخطيطة تعرف العنصر <AttributeStatement> ونمطه المعقد **AttributeStatementType**:

```
<element name="AttributeStatement" type="saml:AttributeStatementType"/>
<complexType name="AttributeStatementType">
        <complexContent>
                <extension base="saml:StatementAbstractType">
                        <choice maxOccurs="unbounded">
                                <element ref="saml:Attribute"/>
                                <element ref="saml:EncryptedAttribute"/>
                        </choice>
                </extension>
      </complexContent>
</complexType>
```

1.3.7.1.8 العنصر <Attribute>

يعرف العنصر <Attribute> هوية النعت باسمه، ويتضمن اختيارياً قيمته أو قيمه. وهو من النمط المعقد **AttributeType**. ويستخدم داخل إعلان نعت ليعبر عن نعوت وقيم خاصة مصاحبة لصاحب تأكيد، كما هو مشروح في الفقرة السابقة. وهو يستخدم أيضاً في استفهام عن نعت لكي يطالب بأن تعاد قيم اللغة SAML المحددة. ويحتوي العنصر <Attribute> على نعوت اللغة XML التالية:

- <Name> [مطلوب]
  اسم النعت.

- NameFormat [اختياري]
  مرجع المعرف URI لتمثيل تصنيف أسماء النعت لأغراض تفسير الاسم. انظر الفقرة الفرعية 2.7.8 بعض مراجع المعرف URI التي يمكن استخدامها كقيمة للنعت NameFormat، وشروحاتها وقواعد معالجتها المصاحبة. وإذا

كانت لا تتوفر أي قيمة NameFormat، يكون معرف الهوية التالي urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified نافذ المفعول.

- FriendlyName [اختياري]

سلسلة توفر شكلاً لاسم النعت مقروءاً من الإنسان، يمكمن أن يفيد في حالات فيها الاسم (Name) الفعلي معقداً أو عائماً، كما هي الحال مع معرف هوية الشيء (OID) (كما تعرفه التوصية ITU-T X.660) أو مع معرف الهوية الوحيد العالمي (UUID) (كما تعرفه التوصية ITU-T X.667). ويتعين استخدام قيمة النعت هذه كأساس لتعريف رسمي لهوية نعوت اللغة SAML.

- نعوت اعتباطية

يستعمل هذا النمط المعقد نقطة توسّع <xs:Attribute>، لكي يسمح بإضافة نعوت اعتباطية في اللغة XML إلى التركيبات <Attribute>، دون الحاجة إلى توسّع صريح في التخطيطة. وهذا يتيح إضافة ما يلزم من المجالات الإضافية لتقديم معلمات إضافية تستعمل مثلاً في الاستفهام عن النعت. ويتعين على توسّعات اللغة SAML ألا تضيف نعوتاً محلية من اللغة XML (غير موصوفة في مكان اسم) أو نعوتاً من اللغة XML موصوفة في مكان اسم موصوف في اللغة SAML للنمط المعقد **AttributeType** أو إلى نمط مشتق منه. إن مثل هذه النعوت محجوزة لصيانة وتحسين اللغة SAML بالذات في المستقبل.

- <AttributeValue> [أي عدد]

يحتوي على قيمة للنعت. وإذا كان أي نعت يحتوي على أكثر من قيمة واحدة منفصلة، يوصى بأن تظهر كل قيمة في عنصرها الخاص <AttributeValue>. وإذا عزى أكثر من عنصر واحد <AttributeValue> إلى نعت ما، وكان لأي واحد من العناصر نمط معطيات (datatype) مسند عبر xsi:type، يتعين عندئذ على جميع العناصر <AttributeValue> أن يكون لها نمط معطيات مطابق مسند.

ويتوقف معنى العنصر <AttributeValue> الذي لا يحتوي على العناصر <AttributeValue>، على السياق الموجود فيه. ففي داخل <AttributeStatement>، إذا وجد نعت اللغة SAML و لم تكن له قيم، يتعين عندئذ حذف العنصر <AttributeValue>. وفي داخل <Sample:AttributeQuery>، يدل غياب القيم على أن الطالب مهتم بأي واحدة من قيم النعت المسمى أو بجميعها (انظر أيضاً الفقرة 2.8).

وأي استعمالات أخرى للعنصر <Attribute> من قبل جانبيات أو مواصفات أخرى، يتعين عليها أن تعرف دلالات مواصفة أو حذف العناصر <AttributeValue>.

والقطعة التالية من التخطيطة تعرف العنصر <Attribute> ونمطه المعقد **AttributeType**:

```
<element name="Attribute" type="saml:AttributeType"/>
<complexType name="AttributeType">
       <sequence>
              <element ref="saml:AttributeValue" minOccurs="0"
maxOccurs="unbounded"/>
       </sequence>
       <attribute name="Name" type="string" use="required"/>
       <attribute name="NameFormat" type="anyURI" use="optional"/>
       <attribute name="FriendlyName" type="string" use="optional"/>
       <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

يوفر العنصر <AttributeValue> قيمة النعت المحدد في اللغة SAML. إنه من النمط **xs: anyType** الذي يتيح لكل لغة XML جيدة التركيب أن تظهر كمحتوى للعنصر.

وإذا كان محتوى المعطيات الواردة في عنصر <AttributeValue> من نمط بسيط في تخطيطة اللغة XML (مثل **xs:integer** أو **xs:string**)، يمكن الإعلان صراحة عن نمط المعطيات (datatype) بواسطة إعلان xsi:type في العنصر

<AttributeVlue>. وإذا كانت قيمة النعت تحتوي على معطيات مُبنينة، يمكن تعريف المعطيات اللازمة في تخطيطة توسّعية.

ملاحظة – إن تحديد نمط معطيات غير النمط البسيط في تخطيطة اللغة XML عن <AttributeValue> باستخدام xsi:type، يتطلب وجود تخطيطة توسّعية تعرف نمط المعطيات (datatype) بغية السماح بمتابعة معالجة التخطيطة.

وإذا كان أي نعت في اللغة SAML يتضمن قيمة خالية، مثل السلسلة الخالية، يتعين على العنصر <AttributeValue> المقابل أن يكون خالياً (ويُعرض ذلك بصورة عامة بالشكل <AttributeValue>). ويتقدم هذا في الأسبقية على المتطلب الموجود في الفقرة 1.7 القائل بأن قيم السلسلة الواردة في محتوى اللغة SAML يحتوي على الأقل سمة واحدة ليست فراغاً أبيض.

وإذا كان نعت اللغة SAML يتضمن قيمة "معدوم"، يتعين على العنصر المقابل <AttributeValue> أن يكون خالياً، وأن يحتوي على نعت اللغة XML xsi:nil مع قيمة "صائب" أو "1".

والقيمة التالية من التخطيطة تعرف العنصر <AttributeValue>.

```
<element name="AttributeValue" type="anyType" nillable="true"/>
```

2.3.7.1.8 العنصر <EncryptedAttribute>

يمثل العنصر <EncryptedAttribute> نعتاً في اللغة SAML مصوغاً بأسلوب مجفر كما هو مشروح في تجفير التجمع W3C. ويحتوي العنصر <EncryptedAttribute> على العناصر التالية:

- <xenc:EncryptedData> [مطلوب]
المحتوى المجفر وتفصيلات التجفير المصاحبة كما هوي معرف في تجفير التجمع W3C. وينبغي لنعت النمط أن يكون موجوداً، وإذا كان موجوداً يتعين عليه أن يحتوي على قيمة من: http://www.w3.org/2001/04/xmlenc#Element. ويتعين على المحتوى المجفر أن يحتوي على عنصر يكون نمطه **AttributeType**، أو يكون نمطاً مشتقاً منه.
- <xenc:EncryptedKey> [صفر أو أكثر]
مفاتيح فك تجفير مغلفة، كما هو معرف في تجفير التجمع W3C, وينبغي لكل مفتاح مغلف أن يحتوي على نعت Recipient (مستلم) يحدد الكيان الذي جرى تجفير المفتاح من أجله. وينبغي لقيمة المستلم أن تكون المعرف URI لكيان في نظام مع معرف هوية اسم في اللغة SAML، كما هو معرف في الفقرة 7.8.

والنعوت المجفرة معدّة لتأمين حماية السرية عندما تكون قيمة النص الصريح ستمر عبر وسيط.

والقطعة التالية من التخطيطة تعرف العنصر <EncryptedAttribute>:

```
<element name="EncryptedAttribute" type="saml:EncryptedElementType"/>
```

4.7.1.8 العنصر <AuthzDecisionStatement>

يشرح العنصر <AuthzDecisionStatement> إعلاناً تصدره سلطة في اللغة SAML يؤكد أن طلباً للنفاذ إلى المورد المعين قدمه صاحب تأكيد، قد أنتج قرار ترخيص استناداً إلى برهان معين بصورة اختيارية. ويتعين على التأكيدات التي تحتوي على العناصر <AuthzDecisionStatement> أن تحتوي على العنصر <Subject>.

وتعرف هوية المورد عن طريق مرجع إلى المعرف URI. وبغية الحصول على تفسير صحيح للتأكيد والحرص على سلامته، يتعين على سلطة اللغة SAML وعلى الطرف الواثق فيها أن يفسرا كل مرجع إلى المعرف URI بطريقة منسقة. والفشل في

التفسير المتسق للمرجع إلى المعرف URI تنتج عنه قرارات ترخيص مختلفة، حسب تشفير المرجع إلى المعرف URI للمورد. وتوجد قواعد تقييس المراجع إلى المعرف URI في البند 6 من طلب التعليقات REC 2396 التابع لفريق المهام IETF.

ولتحاشي أي غموض ناتج عن اختلاف تشفير المعرف URI، ينبغي لكيانات النظام في اللغة SAML أن تستخدم الشكل المقيس للمعرف URI حيثما أمكن ذلك كما يلي:

- ينبغي لسلطات اللغة SAML أن تشفر جميع المراجع إلى المعرف URI للمورد وفقاً للشكل المقيس.
- ينبغي للأطراف الواثقة أن تحول المراجع إلى المعرف URI للمورد إلى الشكل المقيس قبل معالجتها.

وقد ينتج التفسير غير المتسق للمرجع إلى المعرف URI عن اختلافات بين قواعد التركيب للمرجع إلى المعرف URI ودلالات نظام ملفات تحتي. ويتطلب الأمر مزيداً من الاهتمام، إذا كانت المراجع إلى المعرف URI مستعملة لتحديد لغة سياسية من أجل التحكم في النفاذ. وينبغي للنظام الذي يستخدم تأكيدات اللغة SAML أن يستوفي الشرطين الأمنيين التاليين:

- إن بعض أجزاء قواعد التركيب للمرجع إلى المعرف URI تكون حساسة لصندوق حروف الطباعة. فإذا كان نظام الملفات التحتي غير حساس لهذا الصندوق، ينبغي للطالب ألا يكون قادراً على كسب النفاذ إلى مورد مرفوض، بتغييره الموقع الصندوقي لجزء من المرجع إلى المعرف URI للمورد.
- تتوفر لدى العديد من أنظمة الملفات آليات مثل المسيرات المنطقية والوصلات الرمزية، مما يتيح للمستعملين إقامة تكافؤات منطقية بين مداخل نظام الملفات. وينبغي للطالب الا يكون قادراً على كسب النفاذ إلى مورد مرفوض بإحداثه مثل هذا التكافؤ.

يكون العنصر <AuthzDecisionStatement> من النمط **AuthzDecisionStatementType**، الذي يوسع النمط **StatementAbstractType** بإضافة العناصر والنعوت التالية:

– Resource [مطلوب]
المرجع إلى المعرف URI الذي يعرف هويته المورد المطلوب ترخيص النفاذ إليه. ويمكن أن يكون لهذا النعت قيمة خالية ("") للمرجع إلى المعرف URI، ويكون معناه هو "بداية الوثيقة الحالية"ن كما هو محدد في طلب التعليقات RFC 2396, 4.2 التابع لفريق المهام IETF.

– Decision [مطلوب]
القرار الذي تصدره سلطة اللغة SAML بشأن المورد المحدد. وتكون القيمة من النمط البسيط **DecisionType**.

– <Action> [واحد أو أكثر]
مجموعة الأعمال المرخص القيام بها على المورد المعين.

– <Evidence> [اختياري]
مجموعة التأكيدات التي تعتمد عليها سلطة اللغة SAML لدى إصدارها القرار.

والقطعة التالية من التخطيطة تعرف العنصر <AuthzDecisionStatement> ونمطه المعقد **AuthDecisionStatementType**:

```
<element name="AuthzDecisionStatement"
type="saml:AuthzDecisionStatementType"/>
<complexType name="AuthzDecisionStatementType">
     <complexContent>
            <extension base="saml:StatementAbstractType">
                  <sequence>
                        <element ref="saml:Action"
maxOccurs="unbounded"/>
                        <element ref="saml:Evidence" minOccurs="0"/>
                  </sequence>
```

```
                    <attribute name="Resource" type="anyURI"
use="required"/>
                    <attribute name="Decision" type="saml:DecisionType"
use="required"/>
            </extension>
     </complexContent>
</complexType>
```

1.4.7.1.8 النمط البسيط DecisionType

النمط البسيط **DecisionType** يعرف القيم المحتمل إيرادها كحالة من الإعلان عن قرار الترخيص.

- `Permit`
  العمل المعين مسموح.
- `Deny`
  العمل المعين مرفوض.
- `Indeterminate`
  لا تستطيع سلطة اللغة SAML أن تحدد إن كان العمل المعين مسموعاً أو مرفوضاً.

تستعمل قيمة القرار `Indeterminate` في الحالات التي تتطلب فيها سلطة اللغة SAML القدرة على توفير إعلان إيجابي، ولكنها غير قادرة على إصدار قرار. ويمكن أن تعاد معلومات إضافية بشأن أسباب الرفض أو عدم القدرة على إصدار القرار، بشكل عناصر <StatusDential> ضمن <Rsponse> المغلفة.

والقطعة التالية من التخطيطة تعرف العنصر البسيط من **DecisionType**:

```
<simpleType name="DecisionType">
       <restriction base="string">
              <enumeration value="Permit"/>
              <enumeration value="Deny"/>
              <enumeration value="Indeterminate"/>
       </restriction>
</simpleType>
```

2.4.7.1.8 العنصر <Action>

العنصر <Action> يحدد عملاً يمكن القيام به على المورد المعين والإذن مطلوب له. ومحتوى سلسلة المعطيات يقدم اسم العمل المطلوب القيام به على المورد المعين، وله النعت التالي:

- `NameSpace` [اختياري]
  مرجع إلى المعرف URI يمثل مكان الاسم الذي يُطلب أن يُشرح فيه العمل المعين. فإذا كان العنصر غائباً، يكون مكان الاسم `urn:oasis:names:tc:SAML:1.0:action:rwedc-negation` المحدد في الفقرة 7.8 نافذ المفعول.

  ملاحظة (للاطّلاع) – يقترح PE36 (انظر OASIS PE:2006) أن يستعاض عن النص السابق بما يلي:

- `NameSpace` [مطلوب]
  مرجع إلى المعرف URI يمثل مكان الاسم الذي يُطلب أن يُشرح فيه العمل المعين.

والقطعة التالية من التخطيطة تعرف العنصر <Action> ونمطه المعقد **ActionType**:

```
<element name="Action" type="saml:ActionType"/>
<complexType name="ActionType">
       <simpleContent>
```

```
                <extension base="string">
                        <attribute name="Namespace" type="anyURI"
use="required"/>
                </extension>
        </simpleContent>
</complexType>
```

3.4.7.1.8 العنصر <Evidence>

يحتوي العنصر <Evidence> على تأكيد واحد أو عدة تأكيدات أو إحالات إلى تأكيدات تعتمد عليها سلطة اللغة SAML لدى اتخاذها قرار الترخيص. ونمطه المعقد هو **EvidenceType**:

- <AssertionIDRef> [أي عدد]
يحدد تأكيداً بالإحالة إلى قيمة النعت لمعرف هوية التأكيد.

- <AssertionURIRef> [أي عدد]
يحدد تأكيداً عن طريق مرجع إلى المعرف URI.

- <Assertion> [أي عدد]
يحدد تأكيداً عن طريق قيمة.

- <EncryptedAssertion> [أي عدد]
يحدد تأكيداً مجفراً عن طريق قيمة.

إن تقديم تأكيد كبرهان قد يؤثر على اتفاق الثقة بين الطرف الواثق في اللغة SAML وسلطة اللغة SAML التي تتخذ قرار الترخيص. فمثلاً عندما يقدم طرف واثق في اللغة SAML تأكيداً في طلب إلى سلطة اللغة SAML، قد تستعمل سطلة اللغة SAML هذا التأكيد كبرهان لدى اتخاذها قرار الترخيص، دون التصديق على صلاحية تأكيد العنصر <Evidence> لا حيال الطرف الواثق، ولا حيال أي طرف ثالث.

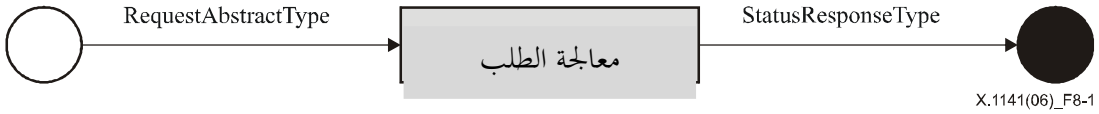
والقطعة التالية من التخطيطة تعرف العنصر <Evidence> ونمطه المعقد EvidenceType:

```
<element name="Evidence" type="saml:EvidenceType"/>
<complexType name="EvidenceType">
        <choice maxOccurs="unbounded">
                <element ref="saml:AssertionIDRef"/>
                <element ref="saml:AssertionURIRef"/>
                <element ref="saml:Assertion"/>
                <element ref="saml:EncryptedAssertion"/>
        </choice>
</complexType>
```

2.8 بروتوكولات اللغة SAML

يمكن توليد وتبادل رسائل وبروتوكولات اللغة SAML باستخدام بروتوكولات متنوعة. وروابط اللغة SAML الواردة في البند 10 تشرح وسائل معينة لنقل رسائل البروتوكول باستخدام بروتوكولات النقل الحالية المنتشرة على نطاق واسع. وجانبية اللغة SAML الواردة في البند 11 تشرح عدداً معنياً من تطبيقات البروتوكولات المعرفة في هذه الفقرة، كما تشرح قواعد المعالجة والتقييدات والمتطلبات الإضافية التي تسهل التشغيل البيني.

ورسائل الطلب والاستجابة المعنية في اللغة SAML مشتقة من أنماط مشتركة، فيرسل الطالب عنصراً مشتقاً من **RequestAbstractType** إلى مستجيب في اللغة SAML، فيولد المستجيب عنصراً مطابقاً للنمط **StatusResponseType** أو مشتقاً منه، كما هو مبين في الشكل 1.8.



الشكل X.1141/1-8 – بروتوكول الطلب والاستجابة في اللغة SAML

وفي بعض الحالات التي تسمح بها الجانبيات، يمكن توليد استجابة في اللغة SAML وإرسالها، من دون أن يكون المستجيب قد استلم طلباً مقابلاً لها.

وتؤدي البروتوكولات المعرفة في اللغة SAML الأعمال التالية:

- ترجح أحد التأكيدات المطلوبة أو عدة منها. ويمكن أن يحدث هذا استجابة إما لطلب مباشر لتأكيدات معينة وإما لاستفهام عن تأكيدات تستوفي معايير خاصة.
- تؤدي الاستيقان بناء على الطلب، وترجع التأكيد المقابل.
- تسجل معرف الهوية لاسم أو تنهي تسجيل اسم، بناءً على الطلب.
- تسحب رسالة بروتوكول كانت قد طلبت عن طريق شيء مصطنع.
- تؤدي انسحاباً شبه متزامن من مجموعة دورات مترابطة ("انسحاب وحيد")، بناءً على الطلب.
- توفر وضعاً على تقابل لمعرف هوية اسم، بناء على الطلب.

ولا تظهر في هذه الفقرة التوصيفات النصية للعناصر والأنماط في مكان الاسم من بروتوكول اللغة SAML، مع السابقة التقليدية لمكان الاسم التي هي: `samlp`، وللتوضيح فإن التوصيفات النصية للعناصر والأنماط في مكان الاسم لتأكيد في اللغة SAML تظهر مع السابقة التقليدية لمكان الاسم التي هي: `saml`.

1.2.8 رأسية التخطيطة وإعلانات مكان الاسم

القطعة التالية من التخطيطة تعرف أماكن الأسماء وغيرها من معلومات الرأسية من أجل تخطيطة البروتوكول:

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-protocol-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V1.0 (November, 2002):
              Initial Standard Schema.
            V1.1 (September, 2003):
              Updates within the same V1.0 namespace.
            V2.0 (March, 2005):
              New protocol schema based in a SAML V2.0 namespace.
     </documentation>
    </annotation>
…
</schema>
```

2.2.8 الطلبات والاستجابات

تحدد الفقرات الفرعية التالية تركيبات اللغة SAML والمتطلبات الأساسية التي تستند إليها رسائل الطلبات والاستجابات التي تستعملها بروتوكولات اللغة SAML.

1.2.2.8 النمط المعقّد RequestAbstractType

جميع الطلبات في اللغة SAML تكون أنماطها مشتقة من النمط المعقد المجرد **RequestAbstractType** . ويعرف هذا النمط نعوتاً وعناصر مشتركة تصاحب جميع الطلبات في اللغة SAML:

ملاحظة – أزيل العنصر <RespondWith> من الصيغة الثانية للنمط **RequestAbstractType** في اللغة SAML.

- ID [مطلوب]

معرف هوية الطلب. إنه من النمط **xs:ID**، ويجب أن يتقيد بالمتطلبات المحددة في الفقرة 4.7 من أجل وحدانية معرفة الهوية. ويجب أن تتواءم قيم النعت ID في طلب مع قيم النعت InResponseTo في الاستجابة المقابلة للطلب.

- Version [مطلوب]

صيغة هذا الطلب. فمعرف هوية صيغة اللغة SAML في هذه التوصية هو "2.0".

- IssueInstant [مطلوب]

اللحظة الزمنية التي صدر الطلب فيها. وتشفر القيمة الزمنية بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- Destination [اختياري]

مرجع المعرف URI الذي يبين العنوان الذي أرسل هذا الطلب إليه. وهذا يفيد في اتقاء إعادة الإرسال الخبيثة للطلبات إلى مقاصد غير مقصودة، وهذه الحماية مطلوبة في بعض روابط البروتوكول. فإذا كان المستلم الحقيقي موجوداً، يتعين عليه أن يتحقق من أن المرجع إلى المعرف URI يعرف هوية الموقع الذي جرى فيه استلام الرسالة. وإلا فيتعين استبعاد الطلب. ويمكن أن تتطلب بعض روابط البروتوكول استعمال هذا النعت (انظر البند 10).

- Consent [اختياري]

يبين ما إذا كانت موافقة الطرف الرئيسي على إرسال هذا الطلب قد حصلت أم لا (ووفق أي شروط). انظر الفقرة الفرعية 4.7.8 ما هي المراجع إلى المعرف URI التي يمكن استعمالها كقيمة للنعت Consent وتوصيفاتها المصاحبة. فإذا لم تتوفر أي قيمة للنعت Consent، يكون معرف الهوية urn:oasis:names:tc:SAML:2.0:consent:unspecified نافذ المفعول.

- saml:Issuer [اختياري]

يعرف هوية الكيان الذي ولّد رسالة الطلب.

- ds:Signature [اختياري]

توقيع في اللغة XML يستيقن الطالب ويوفر سلامة الرسالة، كما هو مشروح أدناه في الفقرة 4.8.

- <Extensions> [اختياري]

تحتوي نقطة التوسّع هذه على عناصر توسّع اختيارية لرسالة البروتوكول، جرى الاتفاق بشأنها بين الأطراف المتواصلة. ولا تطلب أي تخطيطة للتوسّع من أجل استعمال نقطة التوسّع هذه، وحتى إذا كانت قد قدمت تخطيطة ما، فإن ضبط الصلاحية غير الدقيق لا يفرض أي متطلب على كون التوسّع صالحاً. وعناصر التوسّع في اللغة SAML يجب أن تكون موصّفة بمكان اسم، في مكان اسم غير موصّف في اللغة SAML.

قد يحتاج الطالب في اللغة SAML، حسب متطلبات بعض البروتوكولات أو الجانبيات، أن يستيقن نفسه، كما تُطْلب غالباً سلامة الرسالة. ويمكن تأمين سلامة الاستيقان والرسالة بآليات توفرها رابطة البروتوكول (انظر البند 10). ويمكن أن يكون الطلب في اللغة SAML موقّعاً، الأمر الذي يوفر استيقان الطالب وسلامة الرسالة معاً.

وعند استعمال مثل هذا التوقيع، يتعين وجود العنصر <ds:Signature>، ويتعين على المستجيب في اللغة SAML أن يتحقق من صلاحية هذا التوقيع (وهذا يعني أن الرسالة ليس فيها تلاعب) طبقاً للتوقيع في التجمع W3C. فإذا كان غير صالح، يتعين على المستجيب عندئذ ألا يعتمد على محتويات الطلب وينبغي أن يجيب بوجود خطأ. أما إذا كان صالحاً، ينبغي للمستجيب عندئذ أن يقيّم التوقيع لكي يحدد هوية الموقع ووثاقة صلته، ويمكنه أن يتابع معالجة الطلب أو يجيب بوجود خطأ (إن كان الطلب غير صالح لسبب آخر).

إذا كان النعت Consent وارداً، وكانت القيمة تدل على حصول موافقة الطرف الرئيسي بشكل ما، ينبغي عندئذ توقيع الطلب.

إذا بدا للمستجيب في اللغة SAML أن طلباً ما غير صالح، وفقاً لقواعد التركيب في اللغة SAML أو لقواعد المعالجة فيها، يتعين عليه عندما يجيب أن يرجع رسالة استجابة في اللغة SAML مع العنصر <StatusCode> ومع القيمة urn:oasis:names:tc:SAML:2.0:status:Requester. وقد يكون من الأسلم في بعض الحالات عدم الإجابة أطلاقاً، كما في حالة وجود شك بتوقع هجمة لرفض الخدمة.

والقطعة التالية من التخطيطة تعرف النمط المعقد **RequestAbstractType**:

```
<complexType name="RequestAbstractType" abstract="true">
       <sequence>
              <element ref="saml:Issuer" minOccurs="0"/>
              <element ref="ds:Signature" minOccurs="0"/>
              <element ref="samlp:Extensions" minOccurs="0"/>
       </sequence>
       <attribute name="ID" type="ID" use="required"/>
       <attribute name="Version" type="string" use="required"/>
       <attribute name="IssueInstant" type="dateTime" use="required"/>
       <attribute name="Destination" type="anyURI" use="optional"/>
       <attribute name="Consent" type="anyURI" use="optional"/>
</complexType>
<element name="Extensions" type="samlp:ExtensionsType"/>
<complexType name="ExtensionsType">
       <sequence>
              <any namespace="##other" processContents="lax"
maxOccurs="unbounded"/>
       </sequence>
</complexType>
```

2.2.8.2 النمط المعقّد StatusResponseType

جميع الاستجابات في اللغة SAML أنماطها مشتقة من النمط المعقد **StatusResponseType**. ويعرف هذا النمط نعوتاً وعناصر مشتركة تصاحب جميع الاستجابات في اللغة SAML.

- ID [مطلوب]

معرف هوية الاستجابة. إنه من النمط **xs:ID**، ويجب أن يتقيد بالمتطلبات المحددة في الفقرة 4.7 من أجل وحدانية معرف الهوية.

- InResponseTo [اختياري]

إحالة إلى معرف هوية الطلب الذي تقابله الاستجابة، إن وجد. وإذا كانت الاستجابة ليست مولدة استجابة لطلب، أو إذا كانت قيمة النعت ID الموافق للطلب لا يمكن تحديدها (كأن يكون الطلب سيئ التكوين)، يتعين أن

يكون هذا النعت غير موجود. وإلا يتعين أن يكون موجوداً، وأن تتواءم قيمته مع قيمة النعت ID الموافق للطلب المقابل.

- `Version` [مطلوب]
صيغة هذه الاستجابة. فمعرف هوية صيغة اللغة SAML في هذه التوصية هو "2.0".

- `IssueInstant` [مطلوب]
اللحظة الزمنية التي صدرت الاستجابة فيها. وتشفر القيمة الزمنية بالتوقيت UTC كما هو مشروح في الفقرة 3.7.

- `Destination` [اختياري]
مرجع المعرف URI الذي يبين العنوان الذي أرسلت هذه الاستجابة إليه. وهذا يفيد في اتقاء إعادة الإرسال الخبيثة للاستجابات إلى مقاصد غير مقصودة، وهذه الحماية مطلوبة في بعض روابط البروتوكول. فإذا كان المستلم الحقيقي موجوداً، يتعين عليه أن يتحقق من أن المرجع إلى المعرف URI يعرّف هوية الموقع الذي جرى فيه استلام الرسالة. وإلا فيتعين استبعاد الاستجابة. ويمكن أن تتطلب بعض روابط البروتوكول استعمال هذا النعت (انظر البند 10).

- `Consent` [اختياري]
يبين ما إذا كانت موافقة الطرف الرئيسي على إرسال الاستجابة قد حصلت أم لا (ووفق أي شروط). انظر الفقرة الفرعية 4.7.8 ما هي المراجع إلى المعرف URI التي يمكن استعمالها كقيمة للنعت Consent وتوصيفاته المصاحبة. فإذا لم تتوفر أي قيمة للنعت Consent، يكون معرف الهوية `urn:oasis:names:tc:SAML:2.0:consent:unspecified` (انظر الفقرة الفرعية 4.7.8) نافذ المفعول.

- `saml:Issuer` [اختياري]
يعرف هوية الكيان الذي ولّد رسالة الاستجابة. (لمزيد من المعلومات عن هذا العنصر، انظر الفقرة الفرعية 5.2.1.8).

- `<ds:Signature>` [اختياري]
توقيع في اللغة XML يستيقن المستجيب ويوفر سلامة الرسالة، كما هو مشروح أدناه في الفقرة 4.8.

- `<Extentions>` [اختياري]
تحتوي نقطة التوسّع هذه على عناصر توسّع اختيارية لرسالة البروتوكول، جرى الاتفاق بشأنها بين الأطراف المتواصلة. ولا تطلب أي تخطيطة للتوسّع من أجل استعمال نقطة التوسّع هذه، وحتى إذا كانت قد قدمت تخطيطة ما، فإن ضبط الصلاحية غير الدقيق لا يفرض أي متطلب على كون التوسّع صالحاً. وعناصر التوسّع في اللغة SAML يجب أن تكون موصّفة بمكان اسم، في مكان اسم غير موصّف في اللغة SAML.

- `<Status>` [مطلوب]
شفرة تمثل حالة الطلب المقابل.

قد يحتاج المستجيب في اللغة SAML، حسب متطلبات بعض البروتوكولات أو الجانبيات، أن يستيقن نفسه، وقد تُطْلب غالباً سلامة الرسالة. ويمكن تأمين سلامة الاستيقان والرسالة بآليات توفرها رابطة البروتوكول. ويمكن أن تكون الرسالة في اللغة SAML موقّعة، الأمر الذي يوفر استيقان المستجيب وسلامة الرسالة معاً.

وعند استعمال مثل هذا التوقيع، يتعين وجود العنصر `<ds:Signature>`، ويتعين على الطالب في اللغة SAML أن يتحقق من صلاحية هذا التوقيع (وهذا يعني أن الرسالة ليس فيها تلاعب) طبقاً للتوقيع في اللغة XML للتجمع W3C. فإذا كان غير صالح، يتعين على الطالب عندئذ ألا يعتمد على محتويات الاستجابة، وينبغي له أن يعالجها على أنها خطأ. أما إذا كان صالحاً،

فينبغي للطالب عندئذ أن يقيّم التوقيع لكي يحدد هوية الموقّع ووثاقة صلته، ويمكنه أن يتابع معالجة الاستجابة على النحو الذي يبدو مناسباً.

وإذا كان النعت Consent وارداً، وكانت القيمة تدل على حصول موافقة الطرف الرئيسي بشكل ما، ينبغي عندئذ توقيع الاستجابة.

والقطعة التالية من التخطيطة تعرّف النمط المعقد **StatusResponseType**:

```
<complexType name="StatusResponseType">
      <sequence>
            <element ref="saml:Issuer" minOccurs="0"/>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="samlp:Extensions" minOccurs="0"/>
            <element ref="samlp:Status"/>
      </sequence>
      <attribute name="ID" type="ID" use="required"/>
      <attribute name="InResponseTo" type="NCName" use="optional"/>
      <attribute name="Version" type="string" use="required"/>
      <attribute name="IssueInstant" type="dateTime" use="required"/>
      <attribute name="Destination" type="anyURI" use="optional"/>
      <attribute name="Consent" type="anyURI" use="optional"/>
</complexType>
```

1) العنصر <Status>

يحتوي العنصر <Status> على العناصر التالية:

- <StatusCode> [مطلوب]
  شفرة تمثل حالة النشاط الجاري استجابة للطلب المقابل.
- <StatusMessage> [اختياري]
  رسالة يمكن ترجيعها إلى مشغِّل.
- <StatusDetail> [اختياري]
  معلومات إضافية تخص حالة الطلب.

والقطعة التالية من التخطيطة تعرّف العنصر <Status> ونمطه المعقد StatusType:

```
<element name="Status" type="samlp:StatusType"/>
<complexType name="StatusType">
   <sequence>
        <element ref="samlp:StatusCode"/>
        <element ref="samlp:StatusMessage" minOccurs="0"/>
        <element ref="samlp:StatusDetail" minOccurs="0"/>
   </sequence>
</complexType>
```

2) العنصر <StatusCode>

يحدد العنصر <StatusCode> شفرة أو مجموعة من الشفرات المبيتة، تمثل حالة الطلب المقابل. وللعنصر <StatusCode> العنصر والنعت التاليان:

- Value [مطلوب]
  قيمة شفرة الحالة. ويحتوي هذا النعت على مرجع إلى المعرف URI. والقيمة العليا للعنصر <StatusCode> يتعين أخذها من القائمة العالية المستوى المتوفرة في هذه الفقرة.

- <StatusCode> [اختياري]
شفرة حالة تابعة، تقدم مزيداً من المعلومات الخاصة عن ظرف الخطأ. ويمكن أن يحذف المستجيب شفرات الحالة التابعة بغية اتقاء الهجمات التي تسعى إلى اختبار معلومات إضافية عن طريق تقديم طلبات خاطئة عن قصد.

قيم <StatusCode> العالية المستوى المسموحة هي التالية:

```
urn:oasis:names:tc:SAML:2.0:status:Success
```

الطلب نجح. يمكن ترجيع معلومات إضافية في العنصرين <StatusMessage> و/أو <StatusDetail>.

```
urn:oasis:names:tc:SAML:2.0:status:Requester
```

لم يمكن إجراء الطلب، بسبب خطأ من جانب الطالب.

```
urn:oasis:names:tc:SAML:2.0:status:Responder
```

لم يكن إجراء الطلب، بسبب خطأ من جانب المستجيب في اللغة SAML أو من جانب السلطة في اللغة SAML.

```
urn:oasis:names:tc:SAML:2.0:status:VersionMismatch
```

لم يستطع المستجيب في اللغة SAML أن يعالج الطلب، لأن صيغة إرسال الطلب كانت غير صحيحة. أحيل إلى شفرات الحالة التالية من المستوى الثاني في مواضع مختلفة من هذه التوصية. ويمكن أن تعرّف شفرات حالة إضافية من المستوى الثاني في الصيغ المستقبلية لتوصية اللغة SAML. وكيانات النظام حرة في أن تعرّف مزيداً من شفرات الحالة الخاصة بتعريفها مراجع مناسبة إلى المعرف URI.

```
urn:oasis:names:tc:SAML:2.0:status:AuthnFailed
```

لم يكن المزوّد المستجيب قادراً على استيقان الطرف الرئيسي بنجاح.

```
urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue
```

صودف محتوى غير متوقع أو غير صالح داخل العنصر.<saml:Attribute>.أو العنصر.<saml:AttributeValue>.

```
urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy
```

المزوّد المستجيب لا يقدر أو لا يريد دعم سياسة معرف هوية الاسم المطلوبة.

```
urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext
```

لا يستطيع المستجيب تلبية متطلبات سياق الاستيقان المحددة.

```
urn:oasis:names:tc:SAML:2.0:status:NoAvailableIDP
```

يستخدمه وسيط ليشير إلى أنه لا يوجد أي واحد من العناصر <Loc> لدى مزود هوية مقبول في <IDPList> يمكن حله أو لا يوجد أي واحد من مزودي الهويات المقبولين متيسراً.

```
urn:oasis:names:tc:SAML:2.0:status:NoPassive
```

يدل على أن المزوّد المستجيب لا يستطيع استيقان الطرف الرئيسي بصورة منفعلة، كما كان مطلوباً.

```
urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP
```

يستخدمه وسيط ليشير إلى أنه لا يوجد أي واحد من مزوّدي الهوية في <IDPList> يعتمده الوسيط.

```
urn:oasis:names:tc:SAML:2.0:status:PartialLogout
```

تستخدمه سلطة دورة لتشير إلى مشترك في دورة على أنه لم يكن قادراً على نشر افتتاح الدورة إلى جميع المشتركين الآخرين في الدورة.

```
urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded
```

يشير إلى أن المزوّد المستجيب لا يستطيع استيقان الطرف الرئيسي مباشرة، وغير مسموح له أن يعيد التفويض بالطلب.

```
urn:oasis:names:tc:SAML:2.0:status:RequestDenied
```

أي من المستجيب في اللغة SAML أو من السلطة في اللغة SAML قادر على معالجة الطلب، إلا أنه اختار عدم الاستجابة. ويمكن استعمال شفرة الحالة هذه حيث يوجد داعٍ بشأن السياق الأمني لرسالة الطلب أو بشأن تتابع رسائل الطلب المستلمة من طالب خاص.

```
urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported
```

لا يعتمد الطلب أي من المستجيب في اللغة SAML أو السلطة في اللغة SAML.

```
urn:oasis:names:tc:SAML:2.0:status:RequestVersionDeprecated
```

لا يستطيع المستجيب في اللغة SAML معالجة أي طلبات بصيغة البروتوكول التي ترد في الطلب.

```
urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooHigh
```

لا يستطيع المستجيب في اللغة SAML معالجة الطلب لأن صيغة البروتوكول المحددة في رسالة الطلب هي ارتقاء جسيم بأعلى صيغة للبروتوكول يعتمدها المستجيب.

```
urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooLow
```

لا يستطيع المستجيب في اللغة SAML معالجة الطلب لأن صيغة البروتوكول المحددة في رسالة الطلب قديمة جداً.

```
urn:oasis:names:tc:SAML:2.0:status:ResourceNotRecognized
```

إن قيمة المورد الواردة في رسالة الطلب هي غير صالحة أو غير معترف بها.

```
urn:oasis:names:tc:SAML:2.0:status:TooManyResponses
```

يمكن أن تحتوي رسالة الاستجابة عدداً من العناصر أكبر مما يستطيع ترجيعه المستجيب في اللغة SAML.

```
urn:oasis:names:tc:SAML:2.0:status:UnknownAttrProfile
```

قُدّم كيان لا معرفة له بجانبية نعت خاص، مع نعت مسحوب من هذه الجانبية.

```
urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal
```

المزوّد المستجيب لا يتعرف إلى الطرف الرئيسي الذي يحدده الطلب أو ينطوي عليه.

```
urn:oasis:names:tc:SAML:2.0:status:UnsupportedBinding
```

لا يستطيع المستجيب في اللغة SAML تلبية الطلب بالضبط، باستخدام رابطة البروتوكول المحددة في الطلب. والقطعة التالية من التخطيطة تعرّف العنصر <StatusCode> ونمطه المعقد **StatusCodeType**.

```
<element name="StatusCode" type="samlp:StatusCodeType"/>
<complexType name="StatusCodeType">
    <sequence>
      <element ref="samlp:StatusCode" minOccurs="0"/>
    </sequence>
    <attribute name="Value" type="anyURI" use="required"/>
</complexType>
```

3) العنصر <StatusMessage>

يحدد العنصر <StatusMessage> رسالة يمكن ترجيعها إلى مشغّل:

والقطعة التالية من التخطيطة تعرّف العنصر <StatusMessage>:

```
<element name="StatusMessage" type="string"/>
```

4) العنصر <StatusDetail>

يمكن استعمال العنصر <StatusDetail> لتحديد معلومات إضافية تخص حالة الطلب. وتتكون المعلومات الإضافية من عنصر أو أكثر مأخوذة من أي مكان اسم، دون تطلب وجود تخطيطة أو إقرار صلاحية تخطيطة لمحتويات العنصر <StatusDetail>.

والقطعة التالية من التخطيطة تعرّف العنصر <StatusDetail> ونمطه المعقد **StatusDetailType**:

```
<element name="StatusDetail" type="samlp:StatusDetailType"/>
<complexType name="StatusDetailType">
    <sequence>
        <any namespace="##any" processContents="lax" minOccurs="0"
        maxOccurs="unbounded"/>
    </sequence>
</complexType>
```

3.2.8 الاستفهام عن تأكيد وبروتوكول الطلب

تحدد هذه الفقرة الفرعية الرسائل وقواعد المعالجة عند طلب التأكيدات الموجودة بواسطة المرجع أو الاستفهام عنها بواسطة الصاحب أو نمط الإعلان.

1.3.2.8 العنصر <AssertionIDRequest>

إذا كان الطالب يعرف معرّف الهوية الوحيد لتأكيد واحد أو لتأكيدات، يمكن استخدام عنصر الرسالة <AssertionIDRequest> من أجل طلب ترجيعها في رسالة <Response>. ويستخدم العنصر <saml:AssertionIDRequest> لتحديد كل تأكيد مطلوب ترجيعه.

والقطعة التالية من التخطيطة تعرّف العنصر <AssertionIDRequest>:

```
<element name="AssertionIDRequest" type="samlp:AssertionIDRequestType"/>
<complexType name="AssertionIDRequestType">
      <complexContent>
            <extension base="samlp:RequestAbstractType">
                  <sequence>
                        <element ref="saml:AssertionIDRef"
maxOccurs="unbounded"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
```

2.3.2.8 الاستفهامات

تعرف الفقرات الفرعية التالية رسائل طلب الاستفهام في اللغة SAML.

1.2.3.2.8 العنصر <SubjectQuery>

عنصر الرسالة <SubjectQuery> هو نقطة توسّع تسمح بتعريف استفهامات جديدة في اللغة SAML لكي تحدد صباحاً واحداً في اللغة SAML. ونمطه المعقد **SubjectQueryAbstractType** هو نمط مجرد فهو بالتالي لا يستعمل إلا كأساس لنمط مشتق. إن النمط **SubjectQueryAbstractType** يضيف العنصر <saml:Subject> (المعرف في الفقرة الفرعية 4.1.8) إلى النمط **RequestAbstractType**.

والقطعة التالية من التخطيطة تعرف العنصر <SubjectQuery> ونمطه المعقد **SubjectQueryAbstractType**:

```
<element name="SubjectQuery" type="samlp:SubjectQueryAbstractType"/>
<complexType name="SubjectQueryAbstractType" abstract="true">
      <complexContent>
            <extension base="samlp:RequestAbstractType">
                  <sequence>
                        <element ref="saml:Subject"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
```

2.2.3.2.8 العنصر <AuthnQuery>

يستعمل عنصر الرسالة <AuthnQuery> لطرح الاستفهام "أي التأكيدات التي تتضمن إعلانات الاستيقان هي متيسرة لهذا الصاحب؟" والاستجابة <Response> الناجحة سوف تحتوي على تأكيد واحد أو أكثر، تتضمن إعلانات الاستيقان.

ويتعين ألا تستعمل الرسالة <AuthnQuery> كطلب لاستيقان جديد باستخدام الثبوتات المقدمة في الطلب. إن العنصر <AuthnQuery> هو طلب إعلانات عن أعمال استيقان كانت قد جرت في تعامل سابق بين الصاحب المشار إليه وسلطة الاستيقان.

هذا العنصر هو النمط **AuthnQueryType** الذي يوسّع النمط **SubjectQueryAbstractType** بإضافة العنصر والنعت التاليين:

- SessionIndex [اختياري]

  يشكل عند وجوده مرشاحاً لاستجابات محتملة. ومثل هذا الاستفهام يطرح السؤال التالي "ما هي التأكيدات الموجودة بحوزتك وتتضمن إعلانات استيقان خاصة بهذا الصاحب داخل سياق المعلومات المقدمة عن الدورة؟"

- <RequestAuthnContext> [اختياري]

  يشكل عند وجوده مرشاحاً لاستجابات محتملة. ومثل هذا الاستفهام يطرح السؤال التالي "ما هي التأكيدات الموجودة بحوزتك وتتضمن إعلانات استيقان خاصة بهذا الصاحب وتلبي المتطلبات الواردة في سياق الاستيقان داخل هذا العنصر؟"

وعندما تستجيب سلطة اللغة SAML لاستفهام استيقاني، ترجع التأكيدات مع إعلانات الاستيقان على النحو التالي:

- إن القواعد المعطاة في الفقرة الفرعية 4.3.2.8 بشأن التواؤم مع العنصر <Subject> في الاستفهام هي التي تعرّف هوية التأكيدات التي يمكن ترجعيها.

- إذا كان النعت SessionIndex موجوداً في الاستفهام، يتعين على واحد على الأقل من العناصر <AuthnStatement> الموجودة في مجموعة التأكيدات المرجعة، أن يحتوي على نعت SessionIndex يتواءم مع النعت SessionIndex الموجود في الاستفهام. وترجيع المجموعة الكاملة من جميع التأكيدات الموائمة داخل الاستجابة هو أمر اختياري.
- إذا كان العنصر <RequestAuthnContext> موجوداً في الاستفهام، يتعين على واحد على الأقل من العناصر <AuthnStatement> الموجودة في مجموعة التأكيدات المرجّعة، أن يحتوي على عنصر <AuthnContext> يستوفي العنصر الموجود في الاستفهام. وترجيع المجموعة الكاملة من جميع التأكيدات الموائمة داخل الاستجابة هو أمر اختياري.

والقطعة التالية من التخطيطة تعرّف العنصر <AuthnQuery> ونمطه المعقد **AuthnQuery**:

```
<element name="AuthnQuery" type="samlp:AuthnQueryType"/>
<complexType name="AuthnQueryType">
       <complexContent>
              <extension base="samlp:SubjectQueryAbstractType">
                     <sequence>
                            <element ref="samlp:RequestedAuthnContext"
minOccurs="0"/>
                     </sequence>
                     <attribute name="SessionIndex" type="string"
use="optional"/>
              </extension>
       </complexContent>
</complexType>
```

1) العنصر <RequestAuthnContext>

يحدد العنصر <RequestAuthnContext> متطلبات سياق الاستيقان في إعلانات الاستيقان المرجّعة، استجابة لطلب أو لاستفهام. ويعرّف نمطه المعقد **RequestAuthnContextType** العنصر والنعت التاليين:

– <saml:AuthnContextClassRef> أو <saml:AuthnContextDeclRef> [واحد أو أكثر]

يحدد مرجعاً واحداً إلى المعرّف URI لتعريف هوية أصناف سياق الاستيقان أو إعلاناته. وهذان العنصران معرفان في الفقرة الفرعية 2.2.7.1.8. انظر البند 12 لمزيد من المعلومات حول أصناف سياق الاستيقان.

– Comparison [اختياري]

يحدد طريقة المقارنة المستعملة لتقييم الأصناف أو الإعلانات المطلوبة للسياق، واحدة مما يلي "exact" أو "minimum" أو "maximum" أو "better". وقيمة التغيب هي "exact".

ويمكن استعمال مجموعة من مراجع الأصناف أو من مراجع الإعلانات. ويتعين على مجموعة المراجع العتمدة أن تكون مقيّمة كمجموعة مرتبة، يكون العنصر الأول فيها هو الصنف أو الإعلان الأكثر تفضيلاً في سياق الاستيقان. وإذا لم يكن أي واحد من الأصناف أو الإعلانات المحددة يمكن تلبيته طبقاً للقواعد الواردة أدناه، يجب أن المستجيب أن يرجع رسالة <Response> مع <StatusCode> من المستوى الثاني من: urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext.

إذا كان النعت Comparison موضوعاً على "exact" أو كان محذوفاً، يتعين عندئذ على سياق الاستيقان الناتج في إعلان الاستيقان أن يكون متوائماً تماماً مع واحد على الأقل من سياقات الاستيقان المحددة.

وإذا كان النعت Comparison موضوعاً على "minimum"، يتعين عندئذ على سياق الاستيقان الناتج في إعلان الاستيقان، أن يكون على الأقل بقوة (كما يبدو للمستجيب) واحد من سياقات الاستيقان المحددة.

وإذا كان النعت Comparison موضوعاً على "better"، يتعين عندئذ على سياق الاستيقان الناتج في إعلان الاستيقان، أن يكون أقوى (كما يبدو للمستجيب) من أي واحد من سياقات الاستيقان المحددة.

وإذا كان النعت Comparison موضوعاً على "maximum"، يتعين عندئذ على سياق الاستيقان الناتج في إعلان الاستيقان، أن يكون أقوى ما يمكن (كما يبدو للمستجيب)، دون أن يتجاوز على الأقل قوة واحد من سياقات الاستيقان المحددة.

والقطعة التالية من التخطيطة تعرّف العنصر <RequestedAuthnContext> ونمطه المعقد **RequestAuthnContextType**:

```
<element name="RequestedAuthnContext" type="samlp:RequestedAuthnContextType"/>
<complexType name="RequestedAuthnContextType">
  <choice>
         <element ref="saml:AuthnContextClassRef" maxOccurs="unbounded"/>
         <element ref="saml:AuthnContextDeclRef" maxOccurs="unbounded"/>
  </choice>
  <attribute name="Comparison" type="samlp:AuthnContextComparisonType"
use="optional"/>
</complexType>
<simpleType name="AuthnContextComparisonType">
  <restriction base="string">
         <enumeration value="exact"/>
         <enumeration value="minimum"/>
         <enumeration value="maximum"/>
         <enumeration value="better"/>
  </restriction>
</simpleType>
```

3.2.3.2.8 العنصر <AttributeQuery>

يستخدم العنصر <AttributeQuery> لوضع الاستفهام "ترجيع النعوت المطلوبة لهذا الصاحب". وتكون الاستجابة الناجحة بشكل تأكيدات تحتوي على إعلانات نعوت، إلى الحد الذي تسمح به السياسة. ويكون هذا العنصر من النمط **AttributeQueryType** الذي يوسّع **SubjectQueryAbstractType** بإضافة العنصر التالي:

- <saml:Attribute> [أي عدد]

يحدد كل عنصر <saml:Attribute> نعتاً تكون قيمته (أو قيمه) مطلوباً ترجيعها. فإذا لم يتحدد أي نعت، فإن ذلك يدل على أن جميع النعوت التي تسمح بها السياسة هي مطلوبة. فإذا كان عنصر معين <saml:Attribure> يحتوي على عنصر واحد أو أكثر من العناصر <saml:AttributeValues>، وإذا تم ترجيع هذا العنصر في الاستجابة، يتعين عليه ألا يحتوي على قيم ليست مساوية للقيم المحددة في الاستفهام. وفي غياب قواعد التساوي التي تحددها جانبيات أو نعوت معينة، يعرّف التساوي على أنه تمثيل مطابق في اللغة XML للقيمة. ولمزيد من المعلومات عن العنصر <saml:Attribute>، انظر الفقرة الفرعية 1.3.7.1.8.

ويتعين على استفهام وحيد ألا يحتوي على عنصرين <saml:Attribute> مع نفس قيمتي الاسم (Name) ونسق الاسم (NameFormat) (وهذا يعني أن نعتاً معيناً يجب أن يسمى مرة واحدة فقط في الاستفهام).

عندما تستجيب سلطة في اللغة SAML لاستفهام عن نعت، فإنها ترجع تأكيدات مع إعلانات عن نعت على النحو التالي:

- إن القواعد المعطاة في الفقرة الفرعية 4.3.2.8 بشأن التواؤم مع العنصر <Subject> في الاستفهام هي التي تعرّف هوية التأكيدات التي يمكن ترجيعها.
- إذا كان أي عنصر <Attribute> موجوداً في الاستفهام، فإنه يقيّد/يرشّح النعوت، واختيارياً يقيّد/يرشّح القيم المرجّعة كما هو مذكور أعلاه.

- إن النعوت والقيم المرجّعة يمكن أيضاً أن تقيدها اعتبارات خاصة بسياسة التطبيق.

ويمكن استعمال شفرتي الحالة من المستوى الثاني التاليتين urn:oasis:names:tc:SAML:2.0:status:UnknownAttrProfile مع urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue للدلالة على إشكالات حاصلة في تفسير معلومات النعت أو القيمة في الاستفهام.

والقطعة التالية من التخطيطة تعرّف العنصر <AttributeQuery> ونمطه المعقد **AttributeQueryType**:

```
<element name="AttributeQuery" type="samlp:AttributeQueryType"/>
<complexType name="AttributeQueryType">
       <complexContent>
              <extension base="samlp:SubjectQueryAbstractType">
                     <sequence>
                            <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
                     </sequence>
              </extension>
       </complexContent>
</complexType>
```

4.2.3.2.8 العنصر <AuthzDecisionQuery>

يستخدم العنصر <AuthzDecisionQuery> لوضع الاستفهام "هل ينبغي أن يسمح لهذا الصاحب بهذه الأعمال على هذا المورد، اعتماداً على هذا البرهان؟". وتكون الاستجابة الناجحة بشكل تأكيدات تحتوي على إعلانات قرار الترخيص.

ملاحظة – جمدت الميزة <AuthzDecisionQuery> في الصيغة V2.0 للغة SAML، من دون أي تخطيط لتحسين مستقبلي. والمستعملون الذين يطلبون وظائفية إضافية يمكنهم العودة إلى اللغة الإرشادية التوسّعية للتحكم في النفاذ (XACML) (انظر التوصية ITU-T X.1142) التي تقدم ميزات محسنة لقرار الترخيص.

وهذا العنصر هو من النمط **AuthzDecisionQuery** الذي يوسّع **SubjectQueryAbstractType** بإضافة العناصر والنعوت التالية:

– Resource [مطلوب]

مرجع إلى المعرّف URI يدل على المورد الذي يطلب الترخيص له.

– <Saml:Action> [واحد أو أكثر]

الأعمال التي يطلب الترخيص لها. انظر الفقرة الفرعية 2.4.7.1.8، لمزيد من المعلومات عن هذا العنصر.

– <Saml:Evidence> [اختياري]

مجموعة من التأكيدات يمكن أن تعتمد عليها سلطة اللغة SAML لدى اتخاذها قرار الترخيص. انظر الفقرة الفرعية 3.4.7.1.8، لمزيد من المعلومات عن هذا العنصر.

عندما تستجيب سلطة في اللغة SAML لاستفهام عن قرار ترخيص، فإنها ترجع تأكيدات مع إعلانات عن قرار الترخيص كما يلي:

- إن القواعد المعطاة في الفقرة الفرعية 4.3.2.8 بشأن التواؤم مع العنصر <Subject> في الاستفهام هي التي تعرف هوية التأكيدات التي يمكن ترجيعها.

والقطعة التالية من التخطيطة تعرّف العنصر <AuthzDecisionQuery> ونمطه المعقد **AuthzDecisionQueryType**:

```
<element name="AuthzDecisionQuery" type="samlp:AuthzDecisionQueryType"/>
<complexType name="AuthzDecisionQueryType">
  <complexContent>
```

```
        <extension base="samlp:SubjectQueryAbstractType">
                <sequence>
                        <element ref="saml:Action" maxOccurs="unbounded"/>
                        <element ref="saml:Evidence" minOccurs="0"/>
                </sequence>
                <attribute name="Resource" type="anyURI" use="required"/>
        </extension>
  </complexContent>
</complexType>
```

3.3.2.8 العنصر <Response>

يستخدم عنصر الرسالة <Response> عندما تتكون الاستجابة من قائمة تتضمن صفراً من التأكيدات أو عدة منها تلبي الطلب. وهو من النمط المعقد **ResponseType** الذي يوسّع **StatusResponseType** بإضافة العنصر التالي:

- <saml:Assertion> أو <saml:EncryptedAssertion> [أي عدد]

يحدد تأكيداً بقيمة، أو اختيارياً يحدد تأكيداً مجفراً بقيمة. انظر الفقرة الفرعية 3.3.1.8 لمزيد من المعلومات عن هذا العنصر.

والقطعة التالية من التخطيطة تعرّف العنصر <Response> ونمطه المعقد **ResponseType**:

```
<element name="Response" type="samlp:ResponseType"/>
<complexType name="ResponseType">
        <complexContent>
                <extension base="samlp:StatusResponseType">
                        <choice minOccurs="0" maxOccurs="unbounded">
                                <element ref="saml:Assertion"/>
                                <element ref="saml:EncryptedAssertion"/>
                        </choice>
                </extension>
        </complexContent>
</complexType>
```

4.3.2.8 العنصر <Response>

عند الاستجابة لرسالة معرفة في اللغة SAML، يتعين على كل تأكيد ترجعه سلطة في اللغة SAML أن يحتوي على عنصر <Saml:Subject> شديد التواؤم مع العنصر <Saml:Subject> الموجود في الاستفهام وعنصر S1 <Saml:Subject> يتواءم بشدة مع عنصر S2 إذا، وفقط إذا، تحقق الشرطان التاليان معاً:

- إذا كان العنصر S2 يتضمن عنصراً معرفاً للهوية (<BaseID> أو <NameID> أو <EncryptedID>)، يتعين على العنصر S1 أن يتضمن عنصراً معرفاً للهوية مطابقاً، ولكن معرّف الهوية يمكن أن يكون مجفراً (أم لا) في أي واحد من العنصرين S1 أو S2. وبعبارة أخرى، يتعين أن يكون شكل معرّف الهوية المفكوك تجفيره متطابقاً في العنصرين S1 وS2 كليهما. ويعني "التطابق" أن تكون محتويات العنصر المعرّف للهوية وقيم النعت هي نفسها. ومعرّف الهوية المجفّر سيكون مطابقاً للأصلي وفق هذا التعريف، بعد فك تجفيره.
- إذا كان العنصر S2 يتضمن عنصراً واحداً أو أكثر من العناصر <saml:SubjectConfirmation>، يتعين على العنصر S1 أن يتضمن على الأقل عنصراً واحداً <saml:SubjectConfirmation>، بحيث يمكن إثبات العنصر S1 بنفس الكيفية التي يشرحها على الأقل عنصر واحد <saml:SubjectConfirmation> في العنصر S2.

وإليك مثالاً على ما هو مسموح وما هو غير مسموح، فالعنصر S1 يمكنه أن يحتوي على <saml:NameID> مع قيمة خاصة للنسق (Format)، كما أن العنصر S2 يمكنه أن يحتوي على عنصر <saml:EncryptedID> هو نتيجة تجفير

العنصر <saml:NameID> في العنصر S1. وفي كل الأحوال لا يمكن للعنصرين S1 وS2 أن يحتويا على عنصر <saml:NameID> تختلف فيه قيم النسق (Format) ومحتوى العنصر، حتى لو كان معرّفا الهوية الاثنان يحيلان إلى نفس الطرف الرئيسي.

إذا كانت سلطة في اللغة SAML لا تستطيع تقديم تأكيد مع إعلان يتقيد بالتقييدات التي يعبّر عنها استفهام أو مرجع تأكيد، يتعين على العنصر <Response> ألا يحتوي على عنصر <Assertion>، وأن يحتوي على عنصر <StatusCode> له القيمة التالية urn:oasis:names:tc:SAML:2.0:status:Success.

ويتعين التقيد بجميع قواعد المعالجة الأخرى المصاحبة لرسائل الطلب والاستجابة التحتية.

4.2.8 بروتوكول طلب استيقان

عندما يرغب طرف رئيسي (أو وكيل يعمل باسم الطرف الرئيسي) في الحصول على تأكيدات تحتوي على إعلانات استيقان، لكي يضع سياقاً أمنياً عند طرف واثق واحد أو أكثر، يمكنه استعمال بروتوكول طلب استيقان، لكي يرسل عنصر رسالة <AuthnRequest> إلى سلطة في اللغة SAML، ويطلب منها ترجيع رسالة <Response> تحتوي على واحد أو أكثر من مثل هذه التأكيدات. ومثل هذه التأكيدات يمكن أن تحتوي على إعلانات إضافية من أي نمط، ولكن تأكيداً واحداً على الأقل يجب أن يحتوي على الأقل على تأكيد استيقان. وسلطة في اللغة SAML التي تعتمد هذا البروتوكول تدعى أيضاً مزوّد هوية.

وبغض النظر عن هذا المطلب، فإن المحتويات المعينة في التأكيدات المرجّعة تتوقف على جانبية أو سياق الاستعمال. وكذلك فإن الوسائل الصحيحة التي يستيقن بها الطرف الرئيسي أو الوكيل نفسه لدى مزوّد الهوية ليست محددة، لذلك فإن وسائل الاستيقان يمكن أن تؤثر على محتوى الاستجابة. والقضايا الأخرى ذات العلاقة بإقرار صلاحية ثبوتيات الاستيقان من قبل مزوّد الهوية أو أي تواصلات بين مزوّد الهوية وأي كيانات أخرى مشتركة في عملية الاستيقان، تقع كلها خارج نطاق هذا البروتوكول.

والتوصيفات وقواعد المعالجة الواردة في الفقرات الفرعية التالية تستخدم مراجع إلى العناصر الفاعلة التالية التي يمكن أن يكون العديد منها نفس الكيان الموجود في جانبية استعمال خاصة:

- الطالب
  الكيان الذي ينشئ طلب الاستيقان، والذي يجب ترجيع الاستجابة إليه.
- المقّدم
  الكيان الذي يقدّم الطلب إلى مزوّد الهوية، وهو إما أن يستيقن نفسه أثناء إرسال الرسالة، وإما أن يعتمد على سياق أمني موجود ليعرّف عن هويته. إذا لم يقم الطالب بالعمل، فإن المقدم يعمل كوسيط بين الطالب ومزوّد الهوية المستجيب.
- الصاحب المطلوب
  الكيان الذي يجري طلب تأكيد أو تاكيدات عنه.
- الكيان الشاهد
  الكيان أو الكيانات المتوقع منها أن تكون قادرة على تلبية واحد من العناصر <SubjectConfirmation> الموجودة في التأكيد أو التأكيدات الناتجة.
- الطرف الواثق
  الكيان أو الكيانات المتوقع منها أن تستهلك التأكيد أو التأكيدات، لكي تحقق غرضاً تعرفه جانبية الاستعمال أو سياقه، وبصورة عامة لوضع سياق أمني.
- مزوّد هوية
  الكيان الذي يسلمه المقدّم الطلب، والذي يستلم منه المقدّم الاستجابة.

العنصر <AuthnRequest>

لكي يطلب مقدّم من مزوّد هوية إصدار تأكيد مع إعلان استيقان، عليه أن يستيقن نفسه لدى مزوّد الهوية هذا (أو يعتمد على سياق أمني موجود)، ويرسل له رسالة <AuthnRequest> تشرح الصفات التي يحتاج أن يتمتع بها التأكيد الناتج، حتى يلبي الغرض. ومن بين هذه الصفات، قد توجد معلومات تتعلق بمحتوى التأكيد و/أو معلومات تتعلق بكيفية تسليم رسالة <Response> الناتجة إلى الطالب. وعملية استيقان المقدّم يمكن أن تجري قبل أو أثناء أو بعد التسليم الأولي للرسالة <AuthnRequest>.

يمكن ألا يكون الطالب هو نفس مقدّم الطلب، إذا كان الطالب مثلاً طرفاً واثقاً ينوي استعمال التأكيد الناتج لاستيقان الصاحب المطلوب أو الترخيص له، بحيث يتمكن الطرف الواثق من أن يقرر إن كان سيقدم الخدمة.

ينبغي أن تكون الرسالة <AuthnRequest> موقَّعة وإلا فمستيقنة وسلامتها محميّة بواسطة رابطة البروتوكول المستعملة لتسليم الرسالة.

هذه الرسالة هي من النمط المعقد **AuthnRequest** الذي يوسّع **RequestAbstractType** بإضافة العناصر والنعوت التالية، التي هي جميعها اختيارية عادة، إلا أنها قد تكون مطلوبة في بعض الجانبيات:

- <Saml:subject> [اختياري]

  يحدد الصاحب المطلوب للتأكيد أو التأكيدات الناتجة، وهو قد تحتوي على عنصر واحد أو أكثر من العناصر <saml:SubjectConfirmation>، لكي يبين كيف تثبت التأكيدات الناتجة، ومن يثبتها. انظر الفقرة الفرعية 4.1.8 لمزيد من المعلومات عن هذا العنصر.

  وإذا كان محذوفاً بالكامل أو إذا لم يكن مدرجاً فيه أي معرف هوية، يفترض في مقدّم الرسالة أن يكون هو الصاحب المطلوب. وإذا لم تكن مدرجة العناصر <saml:SubjectConfirmation>، يفترض في المقدّم أن يكون هو الكيان الشاهد الوحيد المطلوب، كما يفترض أن تكون الطريقة متضمنة في جانبية الاستعمال و/أو في سياسات مزوّد الهوية.

- <NameIDPolicy> [اختياري]

  يحدّد القيود على معرف هوية الاسم المطلوب استعمالها لتمثيل الصاحب المطلوب. وإذا كان محذوفاً، يمكن عندئذ استعمال أي نمط من معرفات الهوية التي يقبلها مزود الهوية للصاحب المطلوب، ضمن الحدود التي تعينها أي سياسة خاصة ذات صلة بالانتشار، فيما يتعلق بالسرية مثلاً.

- <saml:Conditions> [اختياري]

  يحدد شروط اللغة SAML التي يتوقع الطالب أن يلاقيها للحد من الصلاحية و/أو استعمال التأكيد أو التأكيدات الناتجة. ويمكن للمستجيب أن يعدّل هذه المجموعة أو أن يزيدها، حسبما يراه لازماً. وتستعمل المعلومة الموجودة في هذا العنصر كمدخل إلى عملية تركيب التأكيد، بدلاً من كونها شروطاً لاستعمال الطلب بالذات. (انظر الفقرة الفرعية 5.1.8 لمزيد من المعلومات عن هذا العنصر).

- <RequestAuthnContext> [اختياري]

  يحدد المتطلبات، إن وجدت، التي يفرضها الطالب على سياق الاستيقان الذي ينطبق على استيقان مقدّم المزوّد المستجيب.

- <Scoping> [اختياري]

  يحدد مجموعة من مزوّدي الهوية الذي يثق بهم الطالب لاستيقان المقدّم، وكذلك التحديدات والسياق المتعلقة بالتوكيل التفويضي بالرسالة <AuthnRequest> من المستجيب إلى مزوّدي الهوية التالين.

- ForceAuthn [اختياري]

قيمة بولانية. إن كانت "صائبة"، يتعين على مزوّد الهوية أن يستيقن المقدّم مباشرة، بدلاً من أن يعتمد على سياق أمني سابق. وإذا لم تكن هناك قيمة مقدمة، تكون القيمة بالتغيب هي "خاطئة". وفي كل الأحوال، إذا كانت كلتا القيمتين ForceAuthn وIsPassive "صائبتين"، يتعين على مزوّد الهوية ألا يستيقن المقدّم حديثاً، إلا إذا كانت قيود IsPassive يمكن استيفاؤها.

- IsPassive [اختياري]

قيمة بولانية. إن كانت "صائبة"، يتعين على مزوّد الهوية وعلى وكيل المستعمل بالذات ألا يتحكما تحكماً مؤثياً في السطح البيني للمستعمل انطلاقاً من الطالب، وأن يتعاملا مع المقدّم بكيفية محسوسة. وإذا لم تكن هناك قيمة مقدمة، تكون القيمة بالتغيب هي "خاطئة".

- AssertionConsumerServiceIndex [اختياري]

يعرف بصورة غير مباشرة هوية المكان الذي ينبغي فيه ترجيع الرسالة <Response> إلى الطالب. وهو ينطبق فقط على الجانبيات التي يكون فيها الطالب مختلفاً عن المقدّم، كما في حالة جانبية الاكتتاب الوحيد (SSO) لمتصفح شبكة الويب في هذه التوصية. ويتعين على مزوّد الهوية أن يمتلك وسيلة موثوقة لكي يضع قيمة الدليل في النعت على تقابل مع المكان المصاحب للطالب. ويقدم البند 9 آلية محتملة واحدة. وإذا كان مخدوماً، يتعين على مزود الهوية أن يرجع الرسالة <Response> إلى المكان المصاحب بالتغيب للطالب من أجل جانبية الاستعمال. وإذا كان الدليل المحدد غير صالح، يمكن عندئذ لمزوّد الهوية أن يرجع الرسالة <Response> مع خطأ أو يمكنه استعمال المكان بالتغيب. ويستبعد هذا النعت بالتبادل مع النعتين AssertionConsumerServiceURL وProtocolBinding.

- AssertionConsumerServiceURL [اختياري]

يحدد بالقيمة المكان الذي يتعين فيه ترجيع الرسالة <Response> إلى الطالب. ويتعين على المستجيب أن يضمن بوسيلة ما أن القيمة المحددة هي في الواقع مصاحبة للطالب. ويقدم البند 9 آلية محتملة واحدة، أما التوقيع على الرسالة المتضمنة <AuthnRequest> فهو أمر آخر. ويستبعد هذا النعت بالتبادل مع النعت AssertionConsumerServiceIndex، وهو يترافق عادة مع النعت ProtocolBinding.

- ProtocolBinding [اختياري]

مرجع إلى المعرّف URI يعرّف هوية رابطة البروتوكول في اللغة SAML المطلوب استعمالها عند ترجيع الرسالة <Response>. انظر البند 10 لمزيد من المعلومات عن روابط البروتوكول والمراجع إلى المعرّف URI المعرِّفة لها. ويستبعد هذا النعت بالتبادل مع النعت AssertionConsumerServiceIndex، وهو يترافق عادة مع النعت AssertionConsumerServiceURL.

- AttributeConsumingServiceIndex [اختياري]

يعرف بصورة غير مباشرة هوية المعلومات المصاحبة للطالب التي تشرح نعوت اللغة SAML التي يرغب الطالب من مزوّد الهوية أو يطلب منه أن تتضمنها الرسالة <Response>. ويتعين على مزوّد الهوية أن يمتلك وسيلة موثوقة لكي يضع قيمة الدليل في النعت على تقابل مع المعلومات المصاحبة للطالب. ويقدم البند 9 آلية محتملة واحدة. ويمكن لمزوّد الهوية أن يستخدم هذه المعلومات لملء عنصر واحد أو أكثر من العناصر <Saml:AttributeStatement> الواردة في التأكيد أو التأكيدات التي يرجعها.

- ProviderName [اختياري]

يحدد اسم الطالب بشكل مقروء من الإنسان، لكي يستعمله وكيل مستعمل المقدّم أو مزوّد الهوية. انظر الفقرة الفرعية 4.4.2.8 من أجل القواعد العامة للمعالجة الخاصة بهذه الرسالة.

والقطعة التالية من التخطيطة تعرّف العنصر <AuthnRequest> ونمطه المعقد **AuthnRequestType**:

```
<element name="AuthnRequest" type="samlp:AuthnRequestType"/>
<complexType name="AuthnRequestType">
       <complexContent>
              <extension base="samlp:RequestAbstractType">
                     <sequence>
                            <element ref="saml:Subject" minOccurs="0"/>
                            <element ref="samlp:NameIDPolicy"
minOccurs="0"/>
                            <element ref="saml:Conditions"
minOccurs="0"/>
                            <element ref="samlp:RequestedAuthnContext"
minOccurs="0"/>
                            <element ref="samlp:Scoping" minOccurs="0"/>
                     </sequence>
                     <attribute name="ForceAuthn" type="boolean"
use="optional"/>
                     <attribute name="IsPassive" type="boolean"
use="optional"/>
                     <attribute name="ProtocolBinding" type="anyURI"
use="optional"/>
                     <attribute name="AssertionConsumerServiceIndex"
type="unsignedShort" use="optional"/>
                     <attribute name="AssertionConsumerServiceURL"
type="anyURI" use="optional"/>
                     <attribute name="AttributeConsumingServiceIndex"
type="unsignedShort" use="optional"/>
                     <attribute name="ProviderName" type="string"
use="optional"/>
              </extension>
       </complexContent>
</complexType>
```

1.4.2.8 العنصر <NameIDPolicy>

يضبط العنصر <NameIDPolicy> معرّف هوية الاسم في أصحاب التأكيدات الناتجة من العنصر <AuthnRequest>. ويعرّف نمطه المعقد NameIDPolicyType النعوت التالية:

- Format [اختياري]

يحدد المرجع إلى المعرف URI المقابل لنسق معرف هوية الاسم المعرف في هذه التوصية أو في غيرها (انظر أمثلة في الفقرة الفرعية 3.7.8). وتعرّف القيم الإضافية من urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted خصوصاً لكي تستعمل داخل هذا النعت حتى تبين لطلب ما أن معرف الهوية الناتج هو مجفر.

- SPNameQualifier [اختياري]

يحدد اختيارياً أن يرجع معرف هوية صاحب التأكيد (أو أن يتم إحداثه) في مكان الاسم لمزوّد الخدمة الذي هو غير الطالب، أو في مكان الاسم لجماعة المنتسبين مزوّدي الخدمة. انظر في هذه التوصية على سبيل المثال التعريف urn:oasis:names:tc:SAML:2.0:nameid-format:persistent.

- AllowCreate [اختياري]

قيمة بولانية تستعمل للدلالة عما إذا كان مسموحاً لمزوّد الهوية، أثناء استيفاء الطلب، أن يحدث معرف هوية جديداً لكي يمثل الطرف الرئيسي. وقيمة التغيب هي "خاطئة". وعندما تكون القيمة "خاطئة"، فإن الطالب يقيّد مزوّد الهوية ألا يصدر تأكيداً إلا له، إن كان قد سبق ووضع معرف هوية مقبول للطرف الرئيسي. وهذا لا يمنع

مزوّد الهوية من إحداث معرفات هوية على هذا الشكل خارج سياق هذا الطلب الخاص (إقامته لعدد كبير من الأطراف الرئيسية مسبقاً، مثلاً).

الملاحظة 1 (للاطّلاع) – يوضح PE14 (انظر OASIS PE:2006) أدناه التعريف العلوي:

قيمة بولانية مستعملة للدلالة عما إذا كان الطالب يضمن لمزوّد الهوية، أثناء استيفاء الطلب، الإذن بإحداث معرف هوية جديد أو بمصاحبة معرف هوية موجود يمثل الطرف الرئيسي لطرف واثق. وقيمة التغيب هي "خاطئة" إذا لم يكن النعت موجوداً أو إذا كان العنصر بكامله محذوفاً.

الملاحظة 2 (للاطّلاع) – يقترح PE14 (انظر OASIS PE:2006) أن يضاف النص التالي إلى الفقرة أعلاه:

يمكن استعمال النعت AllowCreate من قبل بعض التطورات للتأثير في إحداث حالات يدعمها مزوّد الهوية تتصل باستعمال معرف هوية الاسم (أو أي نعت دائم يعرّف الهوية بطريقة وحيدة) من قبل طرف واثق خاص لأغراض مختلفة منها إحداث دينامي لمعرف هوية أو نعت أو سعي للحصول على موافقة أو استعمال لاحق لبروتوكول إدارة معرف هوية الاسم أو أغراض أخرى ذات صلة.

وعندما تكون القيمة "خاطئة"، يحاول الطالب تقييد مزوّد الهوية، لكي لا يصدر تأكيداً إلا إذا كان بالفعل إنشاء مثل هذه الحالة او كان لا يبدو لمزوّد الهوية أن من الممكن تطبيق استعمال معرف هوية. وهذا لا يمنع مزوّد الهوية من الافتراض أن مثل هذه المعلومات موجودة خارج سياق هذا الطلب الخاص (مثل إقامته لعدد كبير من الأطراف الرئيسي).

بينما تتيح القيمة "صائبة" لمزوّد الهوية اتخاذ أي إجراء ذي صلة يرغب فيه هو لتلبية الطلب، مع التحفظ لأي قيود أخرى يفرضها الطلب أو تفرضها السياسة (مثل النعت IsPassive).

ولا يستطيع الطالبون افتراض سلوك معين من مزوّدي الهوية حيال الإحداث الأولي أو من رابطة معرفي الهوية باسمهم، نظراً إلى أن هذه التفضيلات متروكة للتطبيقات أو للتطورات. وإذا كان غائباً من الجانبيات الخاصة التي تحكم استعمال هذا النعت، يمكن استعماله كنصيحة لمزودي الهوية بشأن نية الطالب اختزان معرف الهوية أو ربطه بقيمة محلية.

وقد تكون القيمة "خاطئة" مستعملة للدلالة على أن الطالب ليس مستعداً أن يقوم بذلك أو ليس قادراً على ذلك، ويوفر على مزوّد الهوية بذل جهود لا طائل فيها.

والطالبون الذين لا يستعملون هذا النعت استعمالاً خاصاً ينبغي لهم أن يضعوا القيمة على "صائبة" لاستمثال التشغيل البيني. ويتعين ألا يستعمل النعت AllowCreate، وينبغي تجاهله في الطلبات أو التأكيدات الصادرة عن معرفات هوية الأسماء مع النسق: urn:oasis:names:tc:SAML:2.0:nameid-format:transient (فهم يمنعون أي حالة من هذا الشكل في ذواتهم أو انطلاقاً منهم).

عندما يستعمل هذا العنصر، ويكون محتواه غير مفهوم أو غير مقبول بالنسبة إلى مزوّد الهوية، يتعين على عنصر الرسالة <Response> أن يتم ترجيعه مع حالة <Status> خطأ، ويمكنه أن يحتوي على <StatusCode> من المستوى الثاني من urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy.

وإذا كانت قيمة النسق (Format) محذوفة أو كانت موضوعة على urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified، يكون مزوّد الهوية حراً في ترجيع أي نوع من معرفات الهوية، مع التحفظ لأي تقييدات إضافية وتدل قيمة النسق الخاصة urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted على أن التأكيد (أو التأكيدات) الناتج يجب أن يحتوي على العناصر <EncryptedID> بدلاً من النص الواضح.

إن الشكل غير المجفر التحتي لمعرف هوية الاسم يمكن أن يكون من أي نمط يعتمده مزوّد الهوية للصاحب المطلوب.

الملاحظة 3 (للاطّلاع) – يقترح PE6 (انظر OASIS PE:2003) أن يضاف النص التالي إلى نهاية الفقرة أعلاه:

لا يستطيع مزوّد الخدمة أن يطلب بصفة خاصة أن يتم ترجيع نوع خاص من معرفات الهوية، إن كان يطلب التجفير. إن عنصر المعطيات الشرحية <md:NameIDFormat> الوارد في البند 9 أو أي وسيلة أخرى خارج النطاق، يمكن استعمالها لتحديد نوع معرف الهوية الواجب تجفيره وترجعيه.

الملاحظة 4 (للاطّلاع) – يقترح PE15 (انظر OASIS PE:2006) أن تضاف الفقرة التالية:

عندما يستعمل نسق (Format) معرف في الفقرة الفرعية 7.3.7.8 هو غير urn:oasis:names:TC:SAML:2.0:nameid-format:unspecified أو غير urn:oasis:names:TC:SAML:2.0:nameid-format:encrypted، وإذا كان مزوّد الهوية يعيد أي تأكيد، يكون عندئذ:

- يتعين على قيمة النسق للعنصر <NameID> داخل <Subject> لأي <Assertion> أن تكون مطابقة لقيمة النسق المعتمد في <NameIDPolicy>.
- وإذا كان SPNameQualifier غير محذوف في <NameIDPolicy>، يتعين على القيمة SPnameQualifier للعنصر <NameID> داخل <Subject> لأي <Assertion> أن تكون مطابقة لقيمة SPNameQualifier المعتمدة في <NameIDPolicy>.

وبغض النظر عن النسق (Format) في <NameIDPolicy>، يستطيع مزوّد الهوية أن يرجع <EncryptedID> في صاحب التأكيد الناتج، إن كانت السياسات النافذة لدى مزوّد الهوية (الذي يمكن أن يكون خاصاً بمزوّد الخدمة) تتطلب أن يستعمل معرف هوية مجفراً.

وإذا كان الطالب يرغب في أن يسمح لمزوّد الهوية أن يضع معرف هوية جديداً للطرف الرئيسي، إن لم يكن يوجد له أي معرف هوية، يتعين عليه أن يورد هذا العنصر مع النعت AllowCreate الموضوع على "صائب". وإلا فلا يعود يمكن إلا للطرف الرئيسي الذي سبق لمزوّد هوية أن وضع له معرف هوية يمكن أن يستعمله الطالب، أن يتم استيقانه بنجاح. وهذا مفيد خاصة بالاشتراك مع القيمة urn:oasis:names:tc:SAML:2.0:nameid-format:persistent (انظر البند 12).

الملاحظة 5 (للاطّلاع) – يقترح PE14 (انظر OASIS PE:2006) تجاهل الفقرة العلوية.

والقطعة التالية من التخطيطة تعرف العنصر <NameIDPolicy> ونمطه المعقد **NameIDPolicyType**:

```
<element name="NameIDPolicy" type="samlp:NameIDPolicyType"/>
<complexType name="NameIDPolicyType">
       <attribute name="Format" type="anyURI" use="optional"/>
       <attribute name="SPNameQualifier" type="string" use="optional"/>
       <attribute name="AllowCreate" type="boolean" use="optional"/>
</complexType>
```

2.4.2.8 العنصر <Scoping>

يحدد العنصر <Scoping> مزوّدي الهوية الذين يثق الطالب بهم من أجل استيقان المقدم، وكذلك الحدود والسياق المتعلقة بالتوكيل التفويضي الذي يجريه المستجيب بالرسالة <AuthnRequest> إلى مزوّدي الهوية اللاحقين. ونمطه المعقد **ScopingType** يعرّف العناصر والنعوت التالية:

– ProxyCount [اختياري]
يحدد عدد العنونات غير المباشرة للتوكيل التفويضي المسموح بها بين مزوّد الهوية الذي يستلم هذه الرسالة <AuthnRequest> وبين مزوّد الهوية الذي سيستيقن الطرف الرئيسي أخيراً. والحساب المساوي صفراً لا يسمح بأي توكيل تفويضي، بينما يعبر حذف هذا النعت غياب أي تقييد من هذا النوع.

– IDPList [اختياري]
قائمة اطّلاعية بمزودي الهوية والمعلومات المصاحبة لهان يعتقد الطالب أنها مقبولة لاستجابة الطلب.

- RequesterID [صفر أو أكثر]

يعرف هوية مجموعة الكيانات الطالبة التي يعمل الطالب باسمها. يستعمل لتواصل سلسلة الطالبين عندما يحدث توكيل تفويضي، كما هو مشروح في الفقرة الفرعية 5.4.2.8 انظر الفقرة الفرعية 6.3.7.8 توصيف معرّفات هوية الكيان.

في الجانبيات التي تحدد وسيطاً نشيطاً، يمكن للوسيط أن يتفحص القائمة وأن يرجع رسالة <Response> مع حالة <Status> خطأ و<StatusCode> من المستوى الثاني من urn:oasis:names:tc:SAML:2.0:status:NoAvailableIDP أو من urn:oasis:names:tc:SAML:2.0:status:NoSupportedIDP إن كان لا يستطيع الاتصال بأي واحد من مزوّدي الهوية المحددين أو كان لا يعتمد أياً منهم.

والقطعة التالية من التخطيطة تعرّف العنصر <Scoping> ونمطه المعقد **ScopingType**:

```
<element name="Scoping" type="samlp:ScopingType"/>
<complexType name="ScopingType">
       <sequence>
              <element ref="samlp:IDPList" minOccurs="0"/>
              <element ref="samlp:RequesterID" minOccurs="0"
maxOccurs="unbounded"/>
       </sequence>
       <attribute name="ProxyCount" type="nonNegativeInteger"
use="optional"/>
</complexType>
<element name="RequesterID" type="anyURI"/>
```

3.4.2.8 العنصر <IDPList>

يحدد العنصر <IDPList> مزوّدي الهوية الذين يثق الطالب بهم من أجل استيقان المقدّم. ونمطه المعقد IDPListType يعرف العناصر التالية:

- <IDPEntry> [واحد أو أكثر]

معلومات عن مزوّد هوية وحيد.

- <GetComplete> [اختياري]

إذا كانت القامة <IDPList> ليست مكتملة، فإن استعمال هذا العنصر يحدد مرجعاً إلى المعرف URI يمكن استعماله لاسترجاع القائمة المكتملة. ويجب أن ينتج عن استرجاع الموارد المصاحبة للمعرف URI مرحلة من اللغة XML، ويكون عنصرها الجذري هو <IDPList> الذي لا يحتوي هو نفسه على العنصر <GetComplete>.

والقطعة التالية من التخطيطة تعرّف العنصر <IDPList> ونمطه المعقد **IDPListType**:

```
<element name="IDPList" type="samlp:IDPListType"/>
<complexType name="IDPListType">
       <sequence>
              <element ref="samlp:IDPEntry" maxOccurs="unbounded"/>
              <element ref="samlp:GetComplete" minOccurs="0"/>
       </sequence>
</complexType>
<element name="GetComplete" type="anyURI"/>
```

ويحدد العنصر <IDPEntry> معرف هوية وحيداً يثق الطالب به من أجل استيقان المقدّم. ويعرّف نمطه المعقد **IDPEntryType** النعوت التالية:

- <ProviderID> [مطلوب]

معرف الهوية الوحيد لمزوّد الهوية. انظر الفقرة الفرعية 6.3.7.8 لتوصيف مثل هذه المعرفات للهوية.

- Name [اختياري]

اسم لمزوّد الهوية مقروء من الإنسان.

- Loc [اختياري]

مرجع إلى المعرف URI يمثل موقع نقطة انتهائية خاصة بجانبية، تعتمد بروتوكول طلب الاستيقان. ويتعين على الرابطة المطلوب استعمالها أن تكون مفهومة من جانبية الاستعمال.

والقطعة التالية من التخطيطة تعرف العنصر <IDPEntry> ونمطه المعقد IDPEntry:

```
<element name="IDPEntry" type="samlp:IDPEntryType"/>
<complexType name="IDPEntryType">
       <attribute name="ProviderID" type="anyURI" use="required"/>
       <attribute name="Name" type="string" use="optional"/>
       <attribute name="Loc" type="anyURI" use="optional"/>
</complexType>
```

4.4.2.8 قواعد المعالجة

يعتمد تبادل الرسائل <AuthnRequest> و<Response> على سيناريوهات استعمال متنوعة، وهو بالتالي مصمم لاستعماله في سياق خاص يحدّ من هذه الإمكانية، وتكون فيه أنواع محددة من الدخل والخرج مطلوبة أو محظورة. وتنطبق قواعد المعالجة التالية كسلوك لا يتغير عبر أي جانبية من هذا التبادل في البروتوكول. ويتعين أيضاً التقيد بجميع قواعد المعالجة الأخرى التي تصحب الرسائل التحتية الخاصة بالطلب والاستجابة.

ويتعين على المستجيب أن يجيب في النهاية على رسالة <AuthnRequest> برسالة <Response> تتضمن تأكيداً واحداً أو أكثر يستوفي المواصفات التي يحددها الطلب، أو برسالة <Response> تتضمن <Status> يشرح الخطأ الذي حدث. وقد يقوم المستجيب بتبادلات رسائل إضافية مع المقدّم، حسب الحاجة للمبادرة إلى عملية الاستيقان أو لإكمالها، مع التحفظ لطبيعة رابطة البروتوكول وآلية الاستيقان. وكما هو مشروح في الفقرة الفرعية التالية، فهذا يتضمن تفويض الطلب بتوجيه المقدّم إلى مزوّد هوية آخر عن طريق إصداره رسالته الخاصة <AuthnRequest>، حتى يمكن استعمال التأكيد الناتج لاستيقان المقدّم لدى المستجيب الأصلي، باستخدام اللغة SAML بالفعل كآلية استيقان.

وإذا كان المتسجيب غير قادر على استيقان المقدّم، أو كان لا يعترف بالصاحب المطلوب، أو كان ممنوعاً من تقديم تأكيد بفعل سياسات نافذة المفعول لدى مزوّد الهوية (كأن يكون الصاحب المقصود قد حظر على مزوّد الهوية تقديم تأكيدات إلى

الطرف الواثق)، يتعين على المستجيب عندئذ أن يرجع <Response> مع <Status> بالخطأ، ويمكنه ترجيع <StatusCode> من المستوى الثاني من:

urn:oasis:names:tc:SAML:2.0:status:AuthnFailed

أو من urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal

وإذا كان العنصر <Saml:Subject> موجوداً في الطلب، يتعين على العنصر <Saml:Subject> في التأكيد الناتج أن **يتواءم بشدة** مع الطلب <Saml:Subject>، كما هو مشروح في الفقرة الفرعية 4.3.2.8، ما عدا أن معرف الهوية يمكن أن يكون المحتوى الفيزيائي لمعرف الهوية مختلفاً، ولكنه يتعين أن يحيل إلى نفس الطرف الرئيسي.

وكل المحتوى المعرّف خاصة داخل <AuthnRequest> يكون اختيارياً، على الرغم من كون بعض المحتوى مطلوباً من بعض الجانبيات. وغياب أي محتوى خاص إطلاقاً، يقتضي اتباع السلوك التالي:

- يتعين على التأكيد (أو التأكيدات) المرجّعة أن تحتوي على العنصر <Saml:Subject> الذي يمثل المقدّم. ومزوّد الهوية هو الذي يحدد نمط معرّف الهوية ونسقه. ويتعين أن يكون إعلان واحد على الأقل في تأكيد واحد على الأقل هو <Saml:AuthnStatement> الذي يشرح الاستيقان الذي يقوم به المستجيب أو خدمة الاستيقان التي تصحبه.
- ينبغي لمقدّم الطلب أن يكون إلى أقصى ما يمكن، هو الشاهد الوحيد القادر على تلبية <Saml:SubjectConfirmation> في التأكيد (أو التأكيدات). وفي حالة كون طرائق الإثبات ضعيفة، يجب استعمال آليات خاصة بالرابطة أو غيرها للمساعدة على تلبية هذا المطلب.
- يتعين على التأكيد (أو التأكيدات) الناتج أن يحتوي على العنصر <Saml:AudienceRestriction> الذي يحيل إلى الطالب باعتباره طرفاً واثقاً مقبولاً. ويمكن إيراد جماهير أخرى، حسبما يبدو مناسباً لمزوّد الهوية.

5.4.2.8 التوكيل التفويضي

إذا استلم مزوّد هوية <AuthnRequest> وكان لم يستيقن المقدّم بَعْدُ، أو كان لا يستطيع استيقان المقدّم مباشرة، ولكنه يعتقد أن المقدّم قد تم استيقانة بالفعل لدى مزوّد هوية آخر أو أي مكافئ آخر ليس في اللغة SAML، يمكنه الاستجابة للطلب بإصداره <AuthnRequest> يكون جديداً باسمه الخاص، ليجري تقديمه إلى مزوّد الهوية الآخر، أو بإصداره طلباً من أي نسق آخر ليس في اللغة SAML، يعترف الكيان به. ويسمى مزوّد الهوية الأصلي مزوّد الهوية الموكِّل المفوِّض.

بعد نجاح ترجيع <Response> (أو المكافئ الذي ليس من اللغة SAML) إلى المزوّد الموكِّل المفوِّض، يمكن استعمال التأكيد الذي تتضمنه الاستجابة أو المكافئ الذي ليس من اللغة SAML، لاستيقان المقدِّم، وبذلك يستطيع المزوّد الموكِّل المفوِّض إصدار تأكيد من خاصته استجابة للطلب الأصلي <AuthnRequest>، مكملاً تبادل الرسائل الكلي. ويمكن لمزوّدي الهوية، الموكِّل المفوِّض والمستيقن كليهما، أن يتضمنا تقييدات على نشاط التوكيل التفويضي في الرسائل والتأكيدات التي يصدرانها، كما هو مشروح في الفقرات الفرعية السابقة والتالية.

يستطيع الطالب أن يؤثر في سلوك الوكيل المفوّض بإدراجه عنصر <Scoping> حيث يضع المزوّد قيمة مرغوبة للنعت ProxyCount و/أو يشير إلى قائمة من مزوّدي الهوية المفضّلين الذين يمكن أن يكونوا وكلاء مفوضين بإدراج قائمة مرتبة <IDPList> من المزوّدين المفضّلين.

يستطيع مزوّد الهوية أن يراقب الاستعمال الثانوي لتأكيداته بواسطة مزوّدي الهوية الموكّلين المفوّضين باستخدام العنصر <ProxyRestriction> في التأكيدات التي يصدرها الموكّلين المفوّضين باستخدام العنصر <ProxyRestriction> في التأكيدات التي يصدرها.

يمكن لمزوّد هوية أن يفوّض <AuthnRequest> إن كان النعت ProxyCount محذوفاً أو كان أكبر من الصفر. واختياري القيام بالتوكيل التفويضي أم لا هو أمر تابع للسياسة المحلية. يمكن أن يختار مزود الهوية التفويض إلى مزوّد مذكور في القائمة <IDPList> إن كانت متوفرة، ولكنه غير ملزم بفعل ذلك.

ويتعين على مزوّد الهوية ألا يقوم بأي توكيل تفويضي، حيث يكون النعت ProxyCount موضوعاً على الصفر. ويتعين على مزوّد الهوية أن يرجع حالة <Status> خطأ، تحتوي، على قيمة <StatusCode> من المستوى الثاني من urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded إلا إذا كان يمكنه أن يستيقن المقدّم مباشرة.

إذا اختار مزوّد الهوية الموكل المفوض أن يفوض هوية من اللغة SAML عندما يحدث طلباً جديداً <AuthnRequest>، يتعين عليه أن يدرج أشكالاً مكافئة أو أكثر صرامة لجميع المعلومات الواردة في الطلب الأصلي (مثل سياسة سياق الاستيقان). ومع ذلك فطالما أن المزوّد الموكّل المفوض حر في تحديد العنصر <NameIDPolicy> الذي يرغب فيه، فهذا يزيد فرص الاستجابة الناجحة إلى أقصى حد.

وإذا كان مزوّد الهوية القائم بالاستيقان ليس مزوّد هوية من اللغة SAML، يتعين على المزوّد الموكّل أن تكون لديه وسيلة أخرى تضمن للعناصر التي تحكم تفاعل وكيل المستعمل (مثلاً <IsPassive>) أن تفتخر بالمزوّد القائم بالاستيقان.

يتعين أن يحتوي الطلب الجديد <AuthnRequest> نعتاً هو <ProxyCount> له قيمة تقل بواحد على الأكثر عن القيمة الأصلية. وإذا كان الطلب الأصلي لا يحتوي على نعت <ProxyCount>، ينبغي للطلب الجديد أن يحتوي على نعت <ProxyCount>.

وإذا كانت القائمة <IDPList> محددة في الطلب الأصلي، يتعين أن يحتوي الطلب الجديد أيضاً على قائمة <IDPList>. ويستطيع مزوّد الهوية الموكّل المفوِّض أن يضيف مزوّدي هوية إضافيين إلى آخر القائمة <IDPList>، ولكنه يجب ألا يزيل أي واحد من القائمة.

ويعالج طلب الاستيقان واستجابته بالطريقة العادية، وفقاً للقواعد المعطاة في هذا البند وفي جانبية الاستعمال. وبمجرد أن يتم استيقان المقدّم لدى مزوّد الهوية الموكّل المفوِّض (في حالة اللغة SAML عند تسليم <Response>)، تُتَّبع الخطوات التالية:

- يحضر مزوّد الهوية الموكّل المفوّض تأكيداً جديداً باسمه الخاص، بأن ينسخ المعلومات ذات الصلة من التأكيد الأصلي أو من المكافئ في اللغة SAML.
- يتعين على العنصر <Saml:Subject> من التأكيد الجديد أن يحتوي معرف هوية يلبي أفضليات الطالب الأصلي، كما هي معرفة في عنصره <NameIDPolicy>.
- يتعين على <Saml:AuthnStatement> في التأكيد الجديد أن يحتوي على العنصر <Saml:AuthnContext> الذي يحتوي على العنصر <Saml:AuthnticatingAuthority> الذي يحيل إلى مزوّد الهوية المحال إليه المقدم من مزوّد الهوية الموكّل المفوّض. وإذا كان التأكيد الأصلي يحتوي على المعلومة <Saml:AuthnContext> التي تحتوي على عنصر واحد أو أكثر من العناصر <Saml:AuthnticatingAuthority>، ينبغي لهذه العناصر أن تكون واردة في التأكيد الجديد، على أن يوضع العنصر الجديد في آخرها.
- إذا لم يكن مزوّد الهوية القائم بالاستيقان هو مزوّد في اللغة SAML، يتعين على مزوّد الهوية الموكّل المفوّض أن يولد قيمة وحيدة لمعرف الهوية من أجل المزوّد القائم بالاستيقان. وينبغي أن تبقى هذه القيمة متماسكة مع الزمن عبر الطلبات المختلفة. ويتعين ألا تتعارض هذه القيمة مع القيم التي يستعملها أو يولدها مزوّدون آخرون في اللغة SAML.

- يمكن نسخ جميع المعلومات الأخرى <Saml:AuthnContext> أو ترجمتها أو حذفها، وفقاً لسياسات مزوّد الهوية الموكّل المفوِّض، شريطة أن تتم تلبية المتطلبات الأصلية التي يفرضها الطالب.

وإذا جرى في المستقبل أن طُلب من مزوّد الهوية أن يستيقن نفس المقدّم لطالب ثانٍ، وكان هذا الطلب صارماً بقدر الطلب الأصلي أو أقل منه (حسبما يحدد ذلك مزوّد الهوية الموكّل المفوِّض)، يستطيع مزوّد الهوية أن يفوّت إحداث طلب جديد <AuthnRequest> إلى مزوّد الهوية القائم بالاستيقان، وأن يصدر فوراً تأكيداً آخر (بافتراض أن التأكيد الأصلي أو المكافئ الذي ليس من اللغة SAML الذي استلمه مازال صالحاً).

5.2.8 بروتوكول استبانة الشيء المصطنع

يوفر بروتوكول استبانة الشيء المصطنع آلية يمكن بواسطتها نقل رسائل بروتوكول اللغة SAML في رابطة اللغة SAML عن طريق الإحالة بدلاً من القيمة. ويمكن الحصول على الطلبات وعلى الاستجابات معاً بالإحالة عند استخدام هذا البروتوكول المتخصص. فيقوم مرسل الرسالة، بدلاً من أن يربط رسالة ببروتوكول نقل، بإرسال قطعة صغيرة من المعطيات تدعى الشيء المصطنع باستخدامه الرابطة. ويمكن أن يأخذ الشيء المصطنع أشكالاً مختلفة، لكنه يجب أن يعتمد وسيلة يتمكن المستلم بواسطتها من تحديد من هو المرسل. وعندئذ يستخدم المستلم، إذا رغب في ذلك، هذا البروتوكول بالاشتراك مع بروتوكول ربط مختلف في اللغة SAML (متزامن في العادة) لكي يستبين الشيء المصطنع في رسالة البروتوكول الأصلية.

والاستعمال الأكثر شيوعاً لهذه الآلية يكون بوجود روابط لا تستطيع بسهولة حمل الرسالة بسبب قدّها، أو لإيصال رسالة عبر قناة مأمونة ما بين الطالب والمستجيب في اللغة SAML، وتحاشي الحاجة إلى توقيع.

وقد يتطلب بروتوكول استبانة الشيء المصطنع حمايات، وذلك يتوقف على خصائص الرسالة التحتية التي تمرر بالإحالة، ومن هذه الحمايات الاستيقان المتبادل وحماية السلامة والسرية إلخ التي تطلب من رابطة البروتوكول المستعملة لاستبانة الشيء المصطنع. وفي كل الأحوال يتعين على الشيء المصطنع أن يظهر دلالات وحيدة الاستعمال بحيث لا يمكن أن يستعملها أي طرف آخر، بمجرد استبانة الشيء المصطنع بنجاح.

وبغض النظر عن رسالة البروتوكول الحاصلة، يتعين معالجة نتيجة استبانة الشيء المصطنع تماماً كما لو كانت الرسالة الحاصلة قد أرسلت أصلاً حمل الشيء المصطنع.

1.5.2.8 العنصر <ArtifactResolve>

تستخدم الرسالة <ArtifactResolve> لكي تطلب ترجيع رسالة البروتوكول في اللغة SAML في رسالة <ArtifactResponse>، بعد تحديد شيء مصطنع يمثل رسالة البروتوكول في اللغة SAML.

وينبغي أن تكون الرسالة <ArtifactResolve> موقّعة وإلا فمستيقنة وسلامتها محمية من رابطة البروتوكول المستعملة في تسليم الرسالة.

وهذه الرسالة من النمط المعقد **ArtifactResolveType** الذي يوسع **RequestAbstractType** ويضيف العنصر التالي:

- Artifact [مطلوب]

  قيمة الشيء المصطنع التي يستلمها الطالب، ويرغب الآن في ترجمتها إلى رسالة البروتوكول التي يمثلها.

والقطعة التالية من التخطيطة تعرّف العنصر <ArtifactResolve> ونمطه المعقد **ArtifactResolveType**:

```
<element name="ArtifactResolve" type="samlp:ArtifactResolveType"/>
<complexType name="ArtifactResolveType">
      <complexContent>
            <extension base="samlp:RequestAbstractType">
                  <sequence>
                        <element ref="samlp:Artifact"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
<element name="Artifact" type="string"/>
```

2.5.2.8 العنصر <ArtifactResponse>

يتعين على مستلم الرسالة <ArtifactResolve> أن يستجيب بعنصر الرسالة <ArtifactResponse>. وهذا العنصر من النمط المعقد **ArtifactResponseType** الذي يوسّع **StatusResponseType** بعنصر وحيد اختياري استبدالي يقابل رسالة البروتوكول في اللغة SAML المرجّعة. ويمكن أن يكون هذا العنصر المغلف طلباً او استجابة.

وينبغي للرسالة <ArtifactResponse> أن تكون موقّعة وإلا فمُستيقنة وسلامتها محمية من رابطة البروتوكول المستعملة لتسليم الرسالة.

والقطعة التالية من التخطيطة تعرّف العنصر <ArtifactResponse> ونمطه المعقد **ArtifactResponseType**:

```
<element name="ArtifactResponse" type="samlp:ArtifactResponseType"/>
<complexType name="ArtifactResponseType">
      <complexContent>
            <extension base="samlp:StatusResponseType">
                  <sequence>
                        <any namespace="##any" processContents="lax"
minOccurs="0"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
```

3.5.2.8 قواعد المعالجة

إذا كان المستجيب يعترف بأن الشيء المصطنع صالح، يجيب برسالة البروتوكول المصاحبة في عنصر الرسالة <ArtifactResponse>. وإلا فإنه يجيب بالعنصر <ArtifactResponse> من دون رسالة مبيتة فيه. وفي كلتا الحالتين، يتعين أن يتضمن العنصر <Status> عنصراً <StatusCode> مع قيمة للشفرة urn:oasis:names:tc:SAML:2.0:status:Success. ورسالة استجابة من دون رسالة مبيتة داخلها تسمى استجابة خالية في بقية هذه الفقرة.

ويتعين على المستجيب أن ينفذ صفة الاستعمال مرة واحدة على الشيء المصطنع، مع التأكد من أن كل طلب لاحق مع نفس الشيء المصطنع يقدمه أي طالب، ستنتج له استجابة خالية كما شرح آنفاً.

ويمكن لبعض رسائل البروتوكول في اللغة SAML، وبصورة خاصة الرسالة <AuthnRequest> في بعض الجانبيات، أن تكون معدّة لكي يستهلكها أي طرف يستلمها، ويقدر أن يستجيب لها بشكل مناسب. وفي كثير من الحالات الأخرى تكون الرسالة معدّة لكيان معين. لذلك يتعين في هذه الحالات على الشيء المصطنع أن يكون عند إصداره مصحوباً بالمستلم المقصود للرسالة التي يمثلها الشيء المصطنع. فإذا استلم مُصْدر الشيء المصطنع رسالة <ArtifactResolve> من الطالب تبين أنه لا يستطيع استيقان ذاته كمستلم أصلي مقصود، يتعين على مُصدر الشيء أن يرجع استجابة خالية.

وينبغي لمصدر الشيء المصطنع أن ينفذ أقصر حدّ زمني عملي لقابلية استعمال الشيء المصطنع، بحيث تتوفر نسخة زمنية مقبولة (ولكن ليس أكثر) أمام مستلم الشيء المصطنع لكي يحصل على الشيء المصطنع ويرجعه في رسالة <ArtifactResolve> إلى مُصْدره.

يتعين أن يتضمن النعت InResponseTo في الرسالة <ArtifactResponse> قيمة للنعت معرف الهوية المقابل في الرسالة <ArtifactResolve>، ولكن رسالة البروتوكول المبيتة ستحتوي على معرف هوية الرسالة الخاص بها، وفي حالة استجابة مبيّتة فإنها قد تحتوي على قيمة مختلفة للنعت InResponseTo تقابل رسالة الطلب الأصلي التي تجيب عليها الرسالة المبيّتة.

ويجب التقيد بجميع قواعد المعالجة الأخرى المصاحبة لرسائل الطلب والاستجابة التحتية.

6.2.8 بروتوكول إدارة معرف هوية الاسم

بعد أن يوضع معرف هوية الاسم لطرف رئيسي، ويرغب مزوّد هوية في تغيير قيمة و/أو نسق معرف الهوية الذي سوف يستخدمه للإحالة إلى الطرف الرئيسي أو ليبين أن معرف هوية الاسم لم يعد يستعمل للإحالة إلى الطرف الرئيسي، فإنه يخبر مزوّدي الخدمة بالتغيير، بأن يرسل لهم رسالة <ManageNameIDRequest>.

الملاحظة 1 (للاطّلاع) – يعرف PE12 (OASIS PE:2006) النية المقصودة من الفقرة أعلاه، بأن يعيد كتابتها على النحو التالي:

بعد أن يوضع معرف هوية الاسم لطرف رئيسي، ويرغب مزوّد هوية في تغيير قيمة معرف الهوية الذي سوف يستخدمه للإحالة إلى الطرف الرئيسي أو ليبين أن معرف هوية الاسم لم يعد يستعمل للإحالة إلى الطرف الرئيسي، فإنه يخبر مزوّدي الخدمة بالتغيير، بأن يرسل لهم رسالة <ManageNameIDRequest>.

ويستعمل مزوّد الخدمة هذه الرسالة أيضاً لكي يسجل أو يغير قيمة SPProvidedID المطلوب إيرادها عندما يستعمل معرف هوية الاسم التحتي للاتصال به، أو لكي ينهي استعمال معرف هوية الاسم بينه وبين مزوّد الهوية.

لا يستعمل هذا البروتوكول عادة مع معرفات هوية الأسماء "العابرة"، لأن قيمها ليست مهيأة لكي تدار على أساس أمد طويل.

الملاحظة 2 (للاطّلاع) – يوضّح PE14 (OASIS PE:2006) النص العلوي كما يلي:

يتعين ألا يستعمل هذا البروتوكول بالاشتراك مع النسق

.urn:oasis:names:tc:SAML:2.0:nameidformat:transient <NameID> Format

1.6.2.8 العنصر <ManageNameIDRequest>

يرسل المزوّد رسالة <ManageNameIDRequest> لكي يخبر المستلم بتغيير معرف هوية الاسم أو ليدل على انتهاء معرف هوية اسم.

وينبغي أن تكون الرسالة <ManageNameIDRequest> موقّعة وإلا فمستيقنة وسلامتها محمية من قبل رابطة البروتوكول المستعملة لتسليم الرسالة.

وهذه الرسالة هي من النمط المعقد **ManageNameIDRequestType** الذي يوسّع **RequestAbstractType** ويضيف العنصرين التاليين:

– <Saml:NameID> أو <Saml:EncryptedID> [مطلوب]

معرف هوية الاسم ومعطيات التوصيف المصاحبة له (بنص واضح أو بشكل مجفر) الذي يحدد الطرف الرئيسي كما هو معترف به بالهوية وبمزوّد الخدمة قبل هذا الطلب (انظر الفقرة الفرعية 2.1.8 لمزيد من المعلومات عن هذه العناصر).

– <NewID> أو <NewEncryptedID> أو <Terminate> [مطلوب]

قيمة معرف هوية الاسم الجديدة (بنص واضح أو بشكل مجفر) يطلب استعمالها عند الاتصال بالمزوّد الطالب فيما يخص هذا الطرف الرئيسي، أو دلالة على أن استعمال معرف الهوية القديم قد انتهى. ففي الحالة الأولى، إن كان الطالب هو مزود الخدمة، يتعين أن يظهر معرف الهوية الجديد في العناصر <NewID> التالية في النعت SPProvidedID. أما إذا كان الطالب هو مزوّد الهوية، ينبغي أن تظهر القيمة الجديدة في العناصر <NameID> التالية كمحتويات العنصر.

ملاحظة (للاطّلاع) – يقترح PE12 (انظر OASIS PE:2006) أن يذيّل الفقرة أعلاه بما يلي:

وفي كل من الحالتين، إذا كان <NewEncryptedID> هو المستعمل، يكون محتواه المجفر هو فقط العنصر <NewID> الذي يحتوي فقط القيمة الجديدة لمعرف الهوية (لا يمكن تغيير النسق والواصفات بمجرد وضعها).

القطعة التالية من التخطيطة تعرّف العنصر <ManageNameIDRequest> ونمطه المعقد **ManageNameIDRequestType**:

```
<element name="ManageNameIDRequest" type="samlp:ManageNameIDRequestType"/>
<complexType name="ManageNameIDRequestType">
       <complexContent>
              <extension base="samlp:RequestAbstractType">
                     <sequence>
                            <choice>
                                   <element ref="saml:NameID"/>
                                   <element ref="saml:EncryptedID"/>
                            </choice>
                            <choice>
                                   <element ref="samlp:NewID"/>
                                   <element ref="samlp:NewEncryptedID"/>
                                   <element ref="samlp:Terminate"/>
                            </choice>
                     </sequence>
              </extension>
       </complexContent>
</complexType>
<element name="NewID" type="string"/>
<element name="NewEncryptedID" type="saml:EncryptedElementType"/>
<element name="Terminate" type="samlp:TerminateType"/>
<complexType name="TerminateType"/>
```

2.6.2.8 العنصر <ManageNameIDResponse>

يتعين على مستلم الرسالة <ManageNameIDRequest> أن يجيب بالرسالة <ManageNameIDResponse> التي هي من النمط **StatusResponseType** من دون محتوى إضافي.

وينبغي أن تكون الرسالة <ManageNameIDResponse> موقّعة وإلا فمستيقنة وسلامتها محمية من قبل رابطة البروتوكول المستعملة لتسليم الرسالة.

والقطعة التالية من التخطيطة تعرف العنصر <ManageNameIDResponse>:

```
<element name="ManageNameIDResponse" type="samlp:StatusResponseType"/>
```

3.6.2.8 قواعد المعالجـــة

إذا كان الطلب يتضمن العنصر <Saml:NameID> (أو صيغته المجفّرة) الذي لا يعترف به المستلم، يتعين على المزوّد المستجيب أن يجيب بالحالة <Status> خطأ، أو يمكنه أن يجيب بالعنصر <StatusCode> من: urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal.

الملاحظة 1 (للاطّلاع) – يوضّح PE14 (انظر OASIS PE:2006) الفقرة أدناه. يرجى الرجوع إلى التذييل VIII لمزيد من التفاصيل.

وإذا كان الطلب يتضمن العنصر <Terminate>، يكون المزوّد الطالب يشير إلى (في حالة مزود خدمة) أنه لن يقبل تأكيدات بعد الآن من هذا المزوّد للخدمة حول الطرف الرئيسي. ويستطيع المزوّد المستلم أن يقوم بأي عملية صيانة مع معرفته أن العلاقة المتمثلة مع معرف هوية الاسم قد انتهت. ويمكنه أن يختار وقف صلاحية الدورة (الدورات) النشيطة لطرف رئيسي أنهيت العلاقة معه.

الملاحظة 2 (للاطّلاع) – يقترح PE8 (انظر OASIS PE:2006) أن يستعاض عن الجملة الأخيرة في هذه الفقرة بالتالي:

ينبغي له عامة ألا يوقف صلاحية أي دورة (دورات) نشيطة للطرف الرئيسي الذي أنهيت العلاقة معه. فإذا كان المزوّد المستلم هو مزوّد هوية، ينبغي له ألا يوقف صلاحية أي دورة (دورات) نشيطة للطرف الرئيسي مقامة مع مزوّدي خدمة آخرين. يمكن أن يرسل المزوّد الطالب رسالة <LogoutRequest>، قبل المبادرة إلى إنهاء معرف هوية الاسم بإرسالة رسالة <ManageNameIDRequest> إن كانت هذه هي نية المزوّد الطالب (مثلاً تتم المبادرة إلى إنهاء معرف هوية الاسم عبر مسؤول إداري يرغب في إنهاء جميع أنشطة المستعمل). ويجب على المزود الطالب ألا يرسل رسالة <LogoutRequest> بعد إرسال الرسالة <ManageNameIDRequest>.

إذا طلب مزوّد الخدمة تغيير معرفة لهوية الطرف الرئيسي، بإدراجه العنصر <NewID> أو <NewEncryptedID>، يتعين على مزوّد الهوية أن يورد محتوى العنصر باعتباره SPProvidedID، عندما يتصل لاحقاً بمزود الخدمة فيما يخص هذا الطرف الرئيسي.

وإذا طلب مزوّد الهوية تغيير معرفه لهوية الطرف الرئيسي بإدراجه العنصر <NewID> أو <NewEncryptedID>، يتعين على مزوّد الخدمة ألا يستعمل محتوى العنصر باعتباره محتوى العنصر <Saml:NameID>، عندما يتصل لاحقاً بمزوّد الهوية فيما يخص هذا الطرف الرئيسي. يمكن أن يجفّر معرفا الهوية الأصلي والجديد كلاهما، أو أي منهما، أو لا هذا ولا ذاك (باستخدام العنصرين <EncryptedID> و<NewEncryptedID>.

ويتعين في جميع الأحوال على المحتوى <Saml:NameID> الوارد في الطلب وعلى النعت المصاحب له SPProvidedID أن يحتويا على أحدث المعلومات الجديدة عن معرف هوية الاسم المطروح بين المزودين فيما يخص الطرف الرئيسي.

وفي حالة مزوّد له النسق من urn:oasis:names:tc:SAML:2.0:nameid-format:persistent يتعين على النعت NameQualifier أن يحتوي على معرف الهوية الوحيد لمزوّد الهوية الذي أحدث معرف الهوية. وإذا كان معرّف الهوية قد أقيم بين مزوّد الهوية وجماعة المنتسبين التي معرف الخدمة عضو فيها، يتعين على النعت SPNameQualifier أن يحتوي على معرف الهوية الوحيد لجماعة المنتسبين. وإلا فيتيعن عليه أن يحتوي على معرّف الهوية الوحيد لمزوّد الخدمة. ويمكن حذف هذه النعوت إن كانت تتواءم مع قيمة العنصر <Issuer> في رسالة البروتوكول المحتوي، ولكن لا يوصى بذلك لأنه يفسح المجال للالتباس.

وتغيير معرفي الهوية هؤلاء يحتمل أن يأخذ وقتاً طويلاً نسبياً لكي ينتشر بين الأنظمة لدى الطالب والمستجيب كليهما. وقد ترغب التطبيقات عند تنفيذها أن تسمح لكل طرف بقبول أي معرف هوية لبعض الوقت بعد الاكتمال الناجح لتغيير معرف هوية الاسم. وعدم فعل ذلك قد ينتج عنه عجز الطرف الرئيسي عن النفاذ إلى المورد.

ويجب التقيد بجميع قواعد المعالجة الأخرى المصاحبة لرسائل الطلب والاستجابة التحتية.

7.2.8 بروتوكول اختتام دورة وحيدة

يقدم بروتوكول اختتام دورة وحيدة بروتوكول تبادل رسالة، يجعل جميع الدورات التي تقدمها سلطة خاصة للدورات تختتم على التزامن تقريباً. ويستعمل بروتوكول اختتام الدورة الوحيدة إما عندما يختم طرف رئيسي الدورة لدى مشترك فيها أو

عندما يختم طرف رئيسي الدورة مباشرة لدى سلطة الدورة. ويمكن أيضاً استعمال هذا البروتوكول لاختتام الدورة لدى طرف رئيسي بسبب انقضاء الإمهال. ويمكن الإشارة إلى سبب حدث الاختتام عبر النعت Reason.

قد يكون الطرف الرئيسي أقام دورات مستيقنة مع سلطة الدورة ومع المشتركين الأفراد في الدورة، استناداً إلى تأكيدات تحتوي إعلانات استيقان تعتمدها سلطة الدورة.

عندما يثير الطرف الرئيسي عملية اختتام الدورة الوحيدة لدى مشترك في دورة، يتعين على المشترك في الدورة أن يرسل رسالة <LogoutRequest> إلى سلطة الدورة التي قدمت تأكيداً يحتوي على إعلان استيقاني متعلق بهذه الدورة لدى المشترك في الدورة.

عندما يثير طرف رئيسي عملية الاختتام لدى سلطة الدورة، أو عندما يرسل مشترك في الدورة طلب اختتام إلى سلطة الدورة محدداً هذا الطرف الرئيسي، ينبغي لسلطة الدورة أن ترسل رسالة <LogoutRequest> إلى كل مشترك في الدورة كانت قد قدمت له تأكيدات تحتوي على إعلانات استيقانية في دورته الجارية مع الطرف الرئيسي، ما عدا المشترك في الدورة الذي كان قد أرسل الرسالة <LogoutRequest> إلى سلطة الدورة. وينبغي لها أن تحاول الاتصال مع العديد من هؤلاء المشتركين، بقدر ما تستطيع، مستعملة هذا البروتوكول، وأن تنهي دورتها الخاصة مع الطرف الرئيسي، وأن ترجع أخيراً رسالة <LogoutResponse> إلى المشترك في الدورة الطالب، إن وجد.

1.7.2.8 العنصر <LogoutRequest>

يرسل المشترك في دورة أو ترسل سلطة الدورة رسالة <LogoutRequest> للدلالة على أن الدورة قد انتهت. وينبغي أن تكون الرسالة <LogoutRequest> موقّعة وإلا فمستيقنة وسلامتها محمية من قبل رابطة البروتوكول المستعملة لتسليم الرسالة.

وهذه الرسالة من النمط المعقد **LogoutRequestType** الذي يوسّع **RequestAbstractType** ويضيف العناصر والنعوت التالية:

- NotOnOrAfter [اختياري]

  الوقت الذي تنقضي عنده صلاحية الطلب، وبعده يستطيع المستلم استبعاد الرسالة. وتشفّر قيمة الوقت بالتوقيت UTC، كما هو مشروح في الفقرة 3.7.

- Reason [اختياري]

  تبيان سبب اختتام الدورة، بشكل مرجع إلى المعرف URI.

  الملاحظة 1 (للاطّلاع) – يقترح PE10 (انظر OASIS PE:2006) أن يستعاض عن النص أعلاه بالتالي:

  النعت Reason محدد بشكل سلسلة في التخطيطة. وهذه المواصفة تضع تقييدات إضافية على التخطيطة بطلبها أن يكون النعت Reason بشكل مرجع إلى المعرف URI.

- <Saml:BaseID> أو <Saml:NameID> أو <Saml:EncryptedID> [مطلوب]

  معرّف الهوية والنعوت المصاحبة (بنص واضح أو بشكل مجفّر) التي تحدد الطرف الرئيسي كما كان يعترف به مزوّد الهوية ومزوّد الخدمة قبل هذا الطلب. (انظر الفقرة الفرعية 2.1.8 لمزيد من المعلومات عن هذا العنصر).

- <SessionIndex> [اختياري]

  معرّف الهوية الذي يفهرس هذه الدورة لدى مستلم الرسالة.

الملاحظة 2 (للاطّلاع) – يوضح PE38 (انظر OASIS PE:2006) النص أعلاه:

دليل الدورة بين الطرف الرئيسي المعرفة هويته بالعنصر <Saml:BaseID> أو <Saml:NameID> أو <Saml:EncryptedID> وبين سلطة الدورة. ويتعين أن يرتبط هذا بالنعت أو SessionIndex، إن وجد، في <Saml:AuthnStatement> من التأكيد المستعمل لإقامة الدورة التي يجري اختتامها.

والقطعة التالية من التخطيطة تعرّف العنصر <LogoutRequest> ونمطه المعقد المصاحب LogoutRequestType.

```
<element name="LogoutRequest" type="samlp:LogoutRequestType"/>
    <complexType name="LogoutRequestType">
        <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <choice>
                        <element ref="saml:BaseID"/>
                        <element ref="saml:NameID"/>
                        <element ref="saml:EncryptedID"/>
                    </choice>
                    <element ref="samlp:SessionIndex" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
                <attribute name="Reason" type="string" use="optional"/>
                <attribute name="NotOnOrAfter" type="dateTime"
use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="SessionIndex" type="string"/>
```

2.7.2.8 العنصر <LogoutResponse>

يتعين على مستلم الرسالة <LogoutRequest> أن يجيب برسالة <LogoutResponse> من النمط **StatusResponseType**، من دون محتوى إضافي محدد.

وينبغي أن تكون الرسالة <LogoutResponse> موقّعة وإلا فمستيقنة وسلامتها محمية من قبل رابطة البروتوكول المستعملة لتسليم الرسالة.

والقطعة التالية من التخطيطة تعرف العنصر <LogoutResponse>:

```
<element name="LogoutResponse" type="samlp:StatusResponseType"/>
```

3.7.2.8 قواعد المعالجة

يمكن لمرسل الرسالة أن يستخدم النعت Reasaon، ليبين سبب إرسالة الطلب <LogoutRequest>. والقيم التالية تعرفها هذه التوصية لكي يستخدمها جميع مرسلي الرسائل، ويمكن أن يتم الاتفاق على قيم أخرى ما بين المشتركين:

القيمة urn:oasis:names:tc:SAML:2.0:logout:user

تحدد أن هذه الرسالة يجري إرسالها، لأن الطرف الرئيسي يرغب في إنهاء الدورة المبينة.

والقيمة urn:oasis:names:tc:SAML:2.0:logout:admin

تحدد أن هذه الرسالة يجري إرسالها، لأن مسؤولاً إدارياً يرغب في إنهاء الدورة المبينة لهذا الطرف الرئيسي.

ويجب التقيد بجميع قواعد المعالجة الأخرى المصاحبة لرسائل الطلب والاستجابة التحتية.

ويوجد في الفقرات الفرعية التالية قواعد معالجة إضافية.

1) قواعد المشترك في دورة

عندما يستلم المشترك في دورة رسالة <LogoutRequest>، يتعين على المشترك في الدورة أن يستيقن الرسالة. فإذا كانت مرسلتها هي السلطة التي تقدم تأكيداً يحتوي على إعلان استيقان مرتبط بالدورة الجارية للطرف الرئيسي، يتعين على المشترك في الدورة أن يبطل صلاحية دورة (دورات) الطرف الرئيسي المشار إليها بالعنصر <Saml:BaseID> أو <Saml:NameID> أو <Saml:EncryptedID> أو بأي واحد من العناصر <SessionIndex> المقدمة في الرسالة. وإذا لم يكن أي واحد من العناصر <SessionIndex> مقدماً، يتعين عندئذ إبطال صلاحية جميع الدورات المصاحبة للطرف الرئيسي.

يتعين على المشترك في الدورة أن يطبق رسالة طلب اختتام الدورة على أي تأكيد يستوفي الشروط التالية، حتى لو وصل التأكيد بعد طلب اختتام الدورة:

- صاحب التأكيد **يتواءم بشدة** مع العنصر <Saml:BaseID> أو <Saml:NameID> أو <Saml:EncryptedID> في الطلب <LogoutRequest>، كما هو معروف في الفقرة الفرعية 8.2.3.4.
- النعت SessionIndex لواحد من إعلانات استيقان التأكيد يتواءم مع واحد من العناصر <SessionIndex> المحددة في طلب اختتام الدورة، أو إذا كان طلب اختتام الدورة لا يحتوي على أي واحد من العناصر <SessionIndex>.
- وإلا فإن التأكيد يعتبر صالحاً، استناداً إلى شروط التوقيت المحددة في التأكيد بالذات (وخصوصاً قيمة كل النعوت NotOnOrAfter المحددة في معطيات إثبات الشروط أو الصاحب).

لم تنقض بعد صلاحية طلب اختتام الدورة (التي تتحدد بتفحص النعت NotOnOrAfter في الرسالة).

ملاحظة – تقصد هذه القاعدة إلى اتقاء حالة يستلم فيها مشترك في دورة طلب اختتام دورة مستهدفاً تأكيداً واحداً أو عدة تأكيدات (مثلما تكون هوياتها معرفة بعنصر أو بعناصر <SessionIndex>) من قبل أن يستلم التأكيد أو التأكيدات الحالية – المحتمل أن تكون بعد صالحة – التي يستهدفها طلب الاختتام. وينبغي أن يتمسك بطلب الاختتام إلى أن يتم استبعاد طلب الاختتام نفسه (جرى تجاوز قيمة النعت NotOnOrAfter الموجودة في الطلب)، أو إلى أن يكون التأكيد المستهدف بطلب الاختتام قد جرى استلامه وتمت معاملته حسب المقتضى.

2) قواعد سلطة الدورة

عندما تستلم سلطة دورة رسالة <LogoutRequest>، يتعين على سلطة الدورة أن تستيقن مرسل الرسالة. فإذا كان المرسل هو الطرف الرئيسي للدورة الذي تقدم له سلطة الدورة تأكيداً يحتوي على إعلان استيقان للدورة الجارية، ينبغي لسلطة الدورة أن تقوم بما يلي وفقاً للترتيب المحدد.

- ترسل رسالة <LogoutRequest> إلى كل سلطة دورة تفوض سلطة الدورة باسمها باستيقان الطرف الرئيسي، إلا إذا كانت السلطة الثانية هي مولدة الطلب <LogoutRequest>.
- ترسل رسالة <LogoutRequest> إلى كل مشترك في دورة تقدم سلطة الدورة له تأكيدات أثناء الدورة الجارية، وليس هو مُصْدر الطلب <LogoutRequest> الجاري.
- تنهي الدورة الحالية للطرف الرئيسي، كما هو محدد في العنصر <Saml:BaseID> أو <Saml:NameID> أو <Saml:EncryptedID>، أو أي واحد من العناصر <SessionIndex> الموجودة في رسالة طلب اختتام الدورة.

فإذا أنهت سلطة الدورة ما يخصها من دورة الطرف الرئيسي بنجاح، يتعين عليها أن تجيب على الطالب الأصلي، إن وجد، برسالة <LogoutResponse> تحتوي على شفرة حالة من المستوى الرفيع من

urn:oasis:names:tc:SAML:2.0:status:Success. وإذا كانت لا تستطيع فعل ذلك، يتعين عليها أن تجيب برسالة <LogoutResponse> تحتوي على شفرة حالة من المستوى الرفيع تدل على خطأ. وهكذا تدل الحالة من المستوى الرفيع على حالة عملية الاختتام فقط فيما يتعلق بسلطة الدورة نفسها.

ينبغي لسلطة الدورة أن تحاول الاتصال بكل مشترك في الدورةن مستخدمة أي رابطة بروتوكول قابلة للتطبيق أو للاستعمال، حتى ولو فشلت واحدة أو عدة من هذه المحاولات أو لم يمكن القيام بها (مثلاً بسبب أن الطلب الأصلي قد قام على استعمال رابطة بروتوكول لم تمكن اختتام الدورة من الانتشار على جميع المشتركين).

وفي حالة لم يجب جميع المشتركين في الدورة بنجاح على الرسائل <LogoutRequest> (أو لم يمكن الاتصال بجميع المشتركين)، يتعين على سلطة الدورة أن تورد في رسالتها <LogoutResponse> شفرة حالة من المستوى الثاني من urn:oasis:names:tc:SAML:2.0:status:PartialLogout لتبين أن المشتركين الآخرين في الدورة لم يستجب جميعهم بنجاح مع إثبات اختتام الدورة.

يمكن أن تبادل سلطة الدورة إلى اختتام دورة، لأسباب هي غير سبب استلامها طلباً <LogoutRequest> من مشترك في دورة. ومن هذه الأسباب غير الحصرية:

- إذا اتفق على فترة إمهال خارج النطاق مع مشترك فرد في دورة، يمكن لسلطة الدورة أن ترسل طلباً <LogoutRequest> إلى هذا المشترك الفرد وحده.
- إذا جرى تجاوز لفترة الإمهال الإجمالية المتفق عليها.
- إذا طلب الطرف الرئيسي، أو أي كيان آخر موثوق، اختتام دورة الطرف الرئيسي مباشرة من سلطة الدورة.
- إذا حددت سلطة الدورة أن من المحتمل أن تكون ثبوتات الطرف الرئيسي قد تعرضت للشبهات.

وعندما تركب سلطة الدورة رسالة طلب باختتام دورة، يتعين عليها أن تضع قيمة النعت <NotOnOrAfter> في الرسالة على قيمة توقيت تدل على انقضاء صلاحية الرسالة، فيستطيع المستلم بعدها استبعاد طلب اختتام الدورة. وينبغي أن توضع قيمة التوقيت هذه على قيمة تساوي أو تزيد على قيمة أي نعت NotOnOrAfter محدد في أحدث تأكيد صادر كجزء من الدورة المستهدفة (كما هو مبين بالنعت SessionIndex في طلب اختتام الدورة).

وإضافة إلى القيم المحددة في الفقرة 3.6.2.8 للنعت Reason، تكون القيم التالية متيسرة لكي تستعملها سلطة الدورة وحدها:

القيمة urn:oasis:names:tc:SAML:2.0:logout:global-timeout

تحدد أن الرسالة ترسل لأن فترة انقضاء الإمهال الإجمالية قد جرى تجاوزها.

والقيمة urn:oasis:names:tc:SAML:2.0:logout:sp-timeout

تحدد أن الرسالة ترسل لأن فترة انقضاء الأمهال المتفق عليها بين مشترك في الدورة وسلطة الدورة قد جرى تجاوزها.

8.2.8 بروتوكول وضع معرفات هوية الاسم على تقابل

عندما يرغب كيان، يتقاسم معرف الهوية لطرف رئيسي مع مزود هوية، في أن يحصل على معرف هوية اسم لنفي الطرف الرئيسي بنسق خاص أو بمكان اسم اتحادي، يستطيع إرسال طلب إلى مزود الهوية مستعملاً هذا البروتوكول.

مثال ذلك عندما يرغب مزوّد خدمة في الاتصال بمزوّد خدمة آخر، لا يتقاسم معه معرّف هوية للطرف الرئيسي، يستطيع استخدام مزوّد هوية يتقاسم معرّف هوية للطرف الرئيسي مع مزوّدي الخدمة كليهما، ليضع معرّف الهوية الخاص به على تقابل مع معرّف هوية جديد، يكون مجفراً بصورة عامة، يستطيع عن طريقه الاتصال مع مزوّد الخدمة الثاني.

وبصرف النظر عن نمط معرّف الهوية المدروس، ينبغي لمعرّف الهوية الموضوع على التقابل أن يكون مجفّراً داخل العنصر <Saml:EncryptedID>، إلا إذا كان هناك تطوير ينص على أن مثل هذه الحماية غير لازمة.

1.8.2.8 بروتوكول <NameIDMappingRequest>

عندما يريد طالب أن يطلب معرفاً بديلاً لهوية اسم طرف رئيسي، من مزوّد هوية، يرسل له رسالة <NameIDMappingRequest>. وهذه الرسالة هي من النمط المعقّد **NameIDMappingRequestType** الذي يوسّع **RequestAbstractType** ويضيف العنصرين التاليين:

- <Saml:BaseID> أو <Saml:NameID> أو <Saml:EncryptedID> [مطلوب]

  معرف الهوية ومعطيات التوصيف المصاحبة التي تحدد الطرف الرئيسي كما يعترف به حالياً الطالب والمتسجيب (انظر الفقرة الفرعية 2.1.8 لمزيد من المعلومات عن هذا العنصر).

- <NameIDPolicy> [مطلوب]

  المتطلبات الخاصة بنسق وواصف الاسم الاختياري لمعرف الهوية، المطلوب ترجيعها.

وينبغي أن تكون الرسالة موقعة وإلا فمستيقنة وسلامتها محمية من قبل رابطة البروتوكول المستعملة لتسليم الرسالة.

والقطعة التالية من التخطيطة تعرف العنصر <NameIDMappingRequest> ونمطه المعقّد **NameIDMappingRequestType**:

```
<element name="NameIDMappingRequest"
type="samlp:NameIDMappingRequestType"/>
<complexType name="NameIDMappingRequestType">
      <complexContent>
            <extension base="samlp:RequestAbstractType">
                  <sequence>
                        <choice>
                              <element ref="saml:BaseID"/>
                              <element ref="saml:NameID"/>
                              <element ref="saml:EncryptedID"/>
                        </choice>
                        <element ref="samlp:NameIDPolicy"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
```

2.8.2.8 العنصر <NameIDMappingResponse>

يتعين على مستلم الرسالة <NameIDMappingRequest> أن يجيب برسالة <NameIDMappingResponse>. وهذه الرسالة من النمط **NameMappingResponseType** الذي يوسّع **StatusResponseType** ويضيف العنصر التالي:

- <Saml:NameID> أو <Saml:EncryptedID> [مطلوب]

  معرف الهوية والنعوت المصاحبة التي تحدد الطرف الرئيسي بالكيفية المطلوبة، وتكون عادة بالشكل المجفّر (انظر الفقرة الفرعية 2.1.8 لمزيد من المعلومات عن هذا العنصر).

وينبغي أن تكون الرسالة موقعة وإلا فمستيقنة وسلامتها محمية من قبل رابطة البروتوكول المستعملة في تسليم الرسالة.

والقطعة التالية من التخطيطة تعرف العنصر <NameIDMappingResponse> ونمطه المعقد **NameMappingResponseType**:

```
<element name="NameIDMappingResponse"
type="samlp:NameIDMappingResponseType"/>
<complexType name="NameIDMappingResponseType">
      <complexContent>
            <extension base="samlp:StatusResponseType">
                  <choice>
```

```
                        <element ref="saml:NameID"/>
                        <element ref="saml:EncryptedID"/>
                    </choice>
                </extension>
            </complexContent>
</complexType>
```

3.8.2.8 قواعد المعالجة

عندما لا يتعرف المستجيب على الطرف الرئيسي المعرّفة هويته في الطلب، يمكنه أن يستجيب بحالة <Status> خطأ، تحتوي على <StatusCode> من المستوى الثاني من urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal

ويعود إلى تقدير المستجيب أن يرجع شفرة الحالة urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy لكي يبين عدم المقدرة أو عدم الرغبة في اعتماد معرّف هوية في النسق أو مكان الاسم المطلوب.

ويجب التقيد بجميع قواعد المعالجة الأخرى المصاحبة لرسائل الطلب والاستجابة التحتية.

3.8 الصيغ في اللغة SAML

تصاغ الصيغ لمجموعة التوصيات في اللغة SAML بأسلوبين مستقلين. وكل منهما معروض في الفقرات الفرعية التالية، وفيه قواعد المعالجة للكشف عن الفروق بين الصيغ والتعامل معها. كما ترد في هذه الفقرات خطوط توجيهية تبين متى ولماذا يتوقع التغيير في معلومات معينة عن الصيغة في مراجعات اللغة SAML المستقبلية.

عندما تورد المعلومات الخاصة بصيغة تعتبر بنفس الوقت صيغة أساسية وصيغة ثانوية، يعبر عن ذلك بالشكل *Major.Minor*. ويكون رقم الصيغة *Major.Minor* أكبر من رقم الصيغة $Major_B.Minor_B$ أكبر من رقم الصيغة $Major_A.Minor_A$، إذا وفقط إذا، كان:

$(Major_B > Major_A)$ OR (أو) $((Major_B = Major_A)$ AND (و) $(Minor_B > Minor_A))$

1.3.8 صيغة مجموعة من المواصفات في اللغة SAML

كل إطلاق لتوصية في اللغة SAML لابد أن يحتوي على تسمية صيغتين واحدة أساسية والأخرى ثانوية، تصفان علاقة التوصية بصيغها السابقة واللاحقة. ويعبر عن الصيغة في محتوى التوصية. وحجم التغييرات التي تطرأ على التوصية وعمق هذه التغيرات هما اللذان يفرضان بصورة غير رسمية إن كانت مجموعة هذه التغييرات تشكل مراجعة أساسية أو مراجعة ثانوية. وإذا كانت التغييرات المتراكمة تتلاءم بمفعول رجعي مع صيغة سابقةن تعتبر الصيغة الجديدة على العموم مراجعة ثانوية. والإ فإن التغييرات تشكل مراجعة أساسية.

وهذه التوصية تحددها الصيغة V2.0.

1.1.3.8 صيغة التخطيطة

من آليات التوثيق غير المعيارية، أن تحتوي كل وثيقة لتخطيطة في اللغة XML، منشورة كجزء من مجموعة مواصفات، على نعت صيغة على العنصر <xs:schema> تكون قيمته بالشكل *Major.Minor*، لتعكس صيغة مجموعة المواصفات التي تنشر فيها. وقد يستعمل تنفيذ التطبيقات الصالحة هذا النعت كوسيلة لتمييز الصيغة المستعملة من التخطيطة لإقرار صلاحية الرسائل أو لاعتماد صيغ عديدة من نفس التخطيطة المنطقية.

2.1.3.8 صيغة التأكيد في اللغة SAML

يحتوي العنصر <Assertion> في اللغة SAML على نعت للتعبير عن الصيغة الأساسية والثانوية للتأكيد في سلسلة من الشكل *Major.Minor*. وكل صيغة من مجموعة المواصفات في اللغة SAML تركب بحيث توثق قواعد التركيب (النَحْو) لتأكيدات نفس الصيغةن مع علم دلالاتها وقواعد معالجتها. وعليه فإن مجموعة المواصفات التي صيغتها 1.0، تشرح التأكيدات التي صيغتها 1.0 وهكذا.

لا توجد صراحة أي علاقة بين صيغة التأكيد ومكان الاسم المستهدف في اللغة XML المحدَّد لتعريفات التخطيطة من أجل صيغة التأكيد هذه.

وتطبق قواعد المعالجة التالية:

- يجب ألا يصدر طرف مؤكد في اللغة SML أي تأكيدن رقم صيغته *Major.Minor* لا تعتمده السلطة.
- يجب ألا يعالج طرف واثق في اللغة SAML أي تأكيد، رقم صيغته الأساسية لا يعتمده الطرف الواثق.
- يمكن لطرف واثق في اللغة SAML أن يعالج أو يرفض أي تأكيد يكون رقم صيغته الثانوية أكبر من رقم صيغة التأكيد الثانوية التي يعتمدها الطرف الواثق. ومع ذلك يتعين على جميع التأكيدات التي تتقاسم رقم صيغة التأكيد الأساسية أن تتقاسم أيضاً نفس قواعد المعالجة العامة وعلم الدلالات، ويمكن أن يعالجها تنفيذ ما بأسلوب موحّد. فإذا كان التأكيد V1.1 مثلاً يتقاسم قواعد التركيب مع التأكيد V1.0، يستطيع التنفيذ أن يعالج التأكيد وكأنه تأكيد V1.0 من دون أي آثار سلبية.

3.1.3.8 صيغة البروتوكول في اللغة SAML

تحتوي مختلف عناصر الطلب والاستجابة في بروتوكول اللغة SAML على نعت للتعبير عن الصيغتين الأساسية والثانوية لرسالة طلب أو استجابة، باستعمال سلسلة من الشكل *Major.Minor*. وكل صيغة من مجموعة المواصفات في اللغة SAML تركّب بحيث توثّق قواعد التركيب لرسائل البروتوكول في نفس الصيغة، مع علم دلالاتها وقواعد معالجتها. وعليه فإن مجموعة المواصفات التي صيغتها 1.0 تشرح الصيغة V1.0 للطلب والاستجابة وهكذا دواليك.

لا توجد صراحة أي علاقة بين صيغة البروتوكول ومكان الاسم المستهدف في اللغة XML المحدد لتعريفات التخطيطة من أجل صيغة البروتوكول هذه.

وأرقام الصيغة المستعملة في عناصر الطلب والاستجابة في بروتوكول اللغة SAML ستتواءم مع أي مراجعة خاصة لمجموعة المواصفات في اللغة SAML.

1) صيغة الطلب

تطبق قواعد المعالجة التالية على الطلبات:

- يصدر الطالب في اللغة SAML طلبات بأعلى صيغة طلب، يعتمدها كلا الطالب والمستجيب في اللغة SAML.
- إذا كان الطالب في اللغة SAML يجهل إمكانيات المستجيب في اللغة SAML، ينبغي له أن يفترض أن المتسجيب يقبل الطلبات التي يعتمدها الطالب بأعلى صيغة للطلب.
- يجب ألا يصدر طالب في اللغة SAML رسالة طلب فيها رقم صيغة الطلب *Major.Minor* يقابل رقم صيغة استجابة، لا يعتمده الطالب.
- يجب أن يرفض المستجيب في اللغة SAML أي طلب، فيه رقم صيغة الطلب الأساسية لا يعتمده المستجيب.

يمكن لمستجيب في اللغة SAML أن يعالج أو يرفض أي طلب يكون فيه رقم صيغة الطلب الثانوية أكبر من أعلى رقم صيغة طلب مقبول، يعتمده هو. ومع ذلك يتعين على جميع الطلبات التي تتقاسم رقم صيغة الطلب الأساسية أن تتقاسم أيضاً نفس قواعد المعالجة العامة وعلم الدلالات، ويمكن أن يعالجها تنفيذ ما بأسلوب موحّد. فإذا كان الطلب V1.1 مثلاً يتقاسم قواعد التركيب مع الطلب V1.0، يستطيع المستجيب أن يعالج رسالة الطلب وكأنه V1.0 من دون أي آثار سلبية.

2) صيغة الاستجابة

تطبق قواعد المعالجة التعالية على الاستجابات:

- يجب ألا يصدر المستجيب في اللغة SAML رسالة استجابة، رقم صيغة الاستجابة فيها أكبر من رقم صيغة الطلب في رسالة الطلب المقابلة.
- يجب ألا يصدر المستجيب في اللغة SAML رسالة استجابة، فيها رقم صيغة الاستجابة الأساسية أصغر من رقم صيغة الطلب الأساسية في رسالة الطلب المقابلة، إلا عند الإعلام عن خطأ: urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooHigh.
- يتعين أن ينتج عن استجابة خطأ ناجمة عن عدم تواؤم صيغ البروتوكول في اللغة SAML، إعلام عن قيمة <StatusCode> من المستوى الأعلى من: urn:oasis:names:tc:SAML:2.0:status:VersionMismatch وقد ينتج عنها إعلام عن واحدة من قيم المستوى الثاني التالية:
  - urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooHigh أو
  - urn:oasis:names:tc:SAML:2.0:status:RequestVersionTooLow أو
  - urn:oasis:names:tc:SAML:2.0:status:RequestVersionDeprecated.

3) التجميعات المسموحة في الصيغ

لا تظهر تأكيدات صيغة أساسية خاصة إلا في الاستجابة لرسائل نفس الصيغة الأساسية، كما يسمح بذلك استيراد مكان الاسم لتأكيد في اللغة SAML داخل تخطيطة البروتوكول SAML. فيمكن أن يظهر تأكيد V1.1 في رسالة استجابة V1.0 كما يمكن أن يظهر تأكيد V1.0 في رسالة استجابة V1.1، إذا كانت تخطيطة التأكيد المناسبة قد أحيل إليها أثناء استيراد مكان الاسم. لكن التأكيد V1.0 يجب ألا يظهر في رسالة استجابة V2.0 لأنهما من صيغتين أساسيتين مختلفتين.

2.3.8 صيغة مكان الاسم في اللغة SAML

تحتوي وثائق التخطيطة في اللغة XML المنشورة كجزء من مجموعة المواصفات، على مكان اسم مستهدف واحد أو على أمكنة أسماء مستهدفة، موضوعة فيها تعريفات النمط والعنصر والنعت. ويتميز كل مكان اسم عن غيره من الأمكنة، ويمثل باختصار التعريفات البنيوية والنحوية التي تشكل هذا الجزء من المواصفات.

وتحتوي المراجع إلى المعرّف URI لمكان الاسم التي تعرفها مجموعة المواصفات، على معلومات عن الصيغة بالشكل *Major.Minor* في مكان ما من المعرّف URI. ويجب أن تقابل الصيغتان الأساسية والثانوية في المعرّف URI، الصيغتين الأساسية والثانوية لمجموعة المواصفات التي يُدْخل إليها ويعرّف فيها مكان الاسم لأول مرة. وهذه المعلومات لا يستهلكها عادة معالج في اللغة XML، يعالج مكان الاسم بشكل عاتم، إلا أنها معدّة لكي تقيم العلاقة بين مجموعة المواصفات وأمكنة الأسماء التي تعرّفها. ويتبع هذه التخطيطة أيضاً معرفات هوية مبنية على معرفات URI تحددها اللغة SAML وهي واردة في قائمة في الفقرة 7.8.

ويستطيع المنفذون كقاعدة عامة أن يتوقعوا لأمكنة الأسماء وتعريفات التخطيطة المصاحبة التي تعرفها مراجعة أساسية لمجموعة المواصفات، أن تبقى صالحة ومستقرة خلال المراجعات الثانوية للمواصفات. ويمكن إدخال أمكنة أسماء جديدة، ويمكن عند اللزوم الاستعاضة عن أمكنة الأسماء القديمة، ولكن من النادر أن يحدث ذلك. وفي مثل هذه الحالات ينتظر لأمكنة الأسماء القديمة وتعريفاتها المصاحبة أن تبقى صالحة حتى المراجعة الأساسية لمجموعة المواصفات.

والحفاظ على استقرار أمكنة الأسماء مع إضافة إلى محتوى التخطيطة أو تغييره هي أهداف متناقضة. وعندما تكون بعض استراتيجيات التصميم قادرة على تسهيل مثل هذه التغييرات، يكون من المعقد جداً التنبؤ كيف سيكون رد فعل التطبيقات القديمة على أي واحد من التغييرات، مما يجعل التواؤم صعب التحقيق في المستقبل. وعلى كل حال فإن حق إجراء مثل هذه التغييرات في المراجعات الثانوية متروك معلقاً، لمصلحة استقرار مكان الاسم. ينبغي لتنفيذ التطبيقات أن يتوقع، إلا في بعض الظروف الخاصة

(مثل تصحيح نقص جسيم أو إصلاح الأخطاء)، حصول تغييرات في التخطيطة تتواءم مستقبلاً في المراجعات الثانوية، مما يتيح للرسائل الجديدة أن تصبح صالحة في التخطيطات الأكثر قدماً.

ينبغي لأعمال التنفيذ أن تتوقع وأن تستعد للتعامل مع أنماط جديدة من الرسائل والتوسّعات تكون متفقة مع قواعد المعالجة التي توضع لهذه الأنماط. وقد تدخل المراجعات الثانوية أنماطاً جديدة ترفع من عديد تسهيلات التوسّع التي تشرحها هذه التوصية. وينبغي لأعمال التنفيذ القديمة أن ترفض مثل هذه التوسّعات بلباقة عندما تصادف في سياقات تفرض دلالات إلزامية. والأمثلة تتضمن أنماطاً جديدة من الاستفهامات أو الإعلانات أو الشروط.

4.8 اللغة SAML وقواعد تركيب ومعالجة التوقيع في اللغة XML

يمكن لتأكيدات اللغة ورسائل الطلب والاستجابة في بروتوكول اللغة SAML أن تكون موقعة، مع الفوائد التالية. فالتأكيد الذي يوقعه الطرف المؤكّد يدعم سلامة التأكيد واستيقان الطرف المؤكد لطرف واثق في اللغة SAML، وإذا كان التوقيع مبنياً على زوج المفاتيح العمومي والخاص لسلطة اللغة SAML، فهو يدعم أيضاً عدم رفض الأصل. إن توقيع مولّد الرسالة على رسالة طلب أو استجابة في بروتوكول اللغة SAML يدعم سلامة الرسالة واستيقان مصدر الرسالة إلى مقصد ما، وإذا كان التوقيع مبنياً على زوج المفاتيح العمومي والخاص، فهو يدعم أيضاً عدم رفض الأصل.

وفي اللغة SAML لا يطلب دائماً التوقيع الرقمي. ففي بعض الظروف يمكن مثلاً أن تكون التوقيعات "موروثه"، كما في حالة اكتساب تأكيد غير موقع الحماية من توقيع على رسالة الاستجابة في البروتوكول الذي يحتويها. وينبغي استعمال التوقيعات "الموروثة" بكل حرص، عندما يكون الموضوع الذي تتضمنه (مثل التأكيد) معداً ليكون له عمر حياة غير عابر. والسبب في ذلك هو أن السياق بكامله يجب أن يستوقف لدراسته حتى يمنح الصلاحية، مع عرض محتوى اللغة XML وإضافة زيادة محتملة غير لازمة. وهناك مثال آخر، يمكن أن يكون الطرف الواثق أو الطالب في اللغة SAML قد حصل على تأكيد أو رسالة بروتوكول الطرف المؤكد أو المستجيب في اللغة SAML قد استيقن نفسه لدى الطرف الواثق أو المستجيب في اللغة SAML بوسائل أخرى غير التوقيع الرقمي.

وتوجد تقنيات مختلفة متيسرة للاستيقان "المباشر" وإقامة قناة مأمونة بين طرفين. وتشمل القائمة البروتوكول الأمني لطبقة النقل (TLS) وشفرة استيقان الرسالة المفرومة (HMAC) وآليات مبنية على كلمة السر وهكذا. وفوق ذلك فإن المتطلبات الأمنية تتوقف على تطبيقات الاتصال وعلى طبيعة التأكيد أو الرسالة المنقولين. ويوصى بأن تستخدم التوقيعات الرقمية في جميع السياقات الأخرى فيما يخص التأكيدات ورسائل الطلب والاستجابة. وخصوصاً:

- ينبغي لتأكيد في اللغة SAML حصل عليه طرف واثق في اللغة SAML من كيان هو غير الطرف المؤكد في اللغة SAML، أن يكون موقعاً من الطرف المؤكد في اللغة SAML.
- ينبغي لرسالة بروتوكول في اللغة SAML واصلة إلى مقصدها من كيان هو غير المرسل الأصلي، أن تكون موقعة من المرسل.
- قد تحدد الجانبيات آليات توقيع بديلة مثل التوسّعات متعددة الأغراض في بريد الإنترنت (MIME) الموقعة أو موضوعات "جافا" الموقعة التي تحتوي على وثائق اللغة SAML. وتنطبق تحذيرات استيقاف السياق والتشغيل البيني. وتوقيعات اللغة XML معدّد لتكون هي الآلية الأولى في توقيع اللغة SAML، إلا أن هذه التوصية تحاول التواؤم مع الجانبيات التي تتطلب آليات أخرى.
- ما لم تحدد إحدى الجانبيات آلية توقيع بديلة، فإن جميع التوقيعات الرقمية في اللغة XML يجب أن تكون مغلّفة.

1.4.8 توقيع التأكيدات

جميع تأكيدات اللغة SAML يمكن توقيعها باستخدام توقيع اللغة XML. ويتبين ذلك في تخطيطة التأكيدات المشروحة في البند 8.

2.4.8 توقيع الطلب/الاستجابة

جميع رسائل الطلب والاستجابة في بروتوكول اللغة SAML يمكن توقيعها باستخدام توقيع اللغة XML. ويتبين ذلك في التخطيطة المشروحة في الملحق A.

3.4.8 وراثة التوقيع

يمكن تبييت تأكيد من اللغة SAML داخل عنصر آخر من اللغة SAML، مثل تأكيد <Assertion> مغلّف أو طلب أو استجابة، يمكن توقيع أي منها. وإذا كان التأكيد في اللغة SAML لا يحتوي على العنصر <ds:Signature>، ولكنه هو محتوى في عنصر مغلّف في اللغة SAML يحتوي على العنصر <ds:Signature>، وإذا كان التوقيع ينطبق على العنصر <Assertion> وعلى جميع أطفاله، يمكن عندئذ اعتبار التأكيد وارثاً للتوقيع من العنصر المغلِّف. وينبغي أن يكون التفسير الناتج مكافئاً للحالة التي يكون فيها التأكيد نفسه قد جرى توقيعه بنفس خيارات المفتاح والتوقيع.

وكثير من حالات استعمال اللغة SAML تقتضي معطيات من اللغتين SAML وXML مغلّفة في بنى أخرى من المعطيات محميّة، مثل رسائل البروتوكول المبسط للنفاذ إلى الهدف (SOAP) الموقعة، وترزيمات التوسّعات MIME الموقعة، وتوصيلات البروتوكول الأمني لطبقة النقل (TLS) المستيقنة. ويمكن لجانبيات اللغة SAML أن تحدد قواعد إضافية لتفسير عناصر اللغة SAML كورثة للتوقيعات وغيرها من معلومات الاستيقان المأخوذة من السياق السائد المحيط، ولكن يجب ألا يفترض وجود مثل هذه الوراثة إلا إذا كانت الجانبية تحددها خصوصاً.

4.4.8 جانبية التوقيع في اللغة XML

يقدم توقيع اللغة XML:2002 التابع للتجمع W3C قواعد تركيب عامة في اللغة XML لمعطيات التوقيع مع مرونة واختيارات عديدة. وتشرح هذه الفقرة الفرعية القيود المفروضة على هذه المرافق، بحيث لا يكون على المعالجات في اللغة SAML أن تتعامل مع كامل عموميات معالجة التوقيع في اللغة XML. فهذه المعالجة تستخدم استخداماً خاصاً النعوت xs:ID-typed الموجودة على العناصر الجذرية التي تنطبق عليها التوقيعات، ولاسيما النعت ID على التأكيد <Assertion>، ومختلف عناصر الطلب والاستجابة. وجميع هذه النعوت تسمى مجتمعة في هذه الفقرة نعوت معرّف الهوية.

ولا تنطبق هذه الجانبية إلا على استخدام العناصر <ds:Signature> التي توجد مباشرة داخل التأكيدات والطلبات والاستجابات في اللغة SAML. وبقية الجانبيات التي تظهر فيها التوقيعات في مكان آخر، ولكنها تنطبق على محتوى اللغة SAML، هي حرة في تعريف مناهج أخرى.

1.4.4.8 أنساق وخوارزميات التوقيع

يستعمل التوقيع في اللغة XML ثلاث وسائل لربط التوقيع بوثيقة: أن يكون مغلِّفاً أو متغلِّفاً أو منفصلاً.

ويتعين على البروتوكولات والتأكيدات في اللغة SAML أن تستعمل التوقيعات المتغلفة، عند توقيع رسائل البروتوكول والتأكيدات. وينبغي للمعالِجَات في اللغة SAML أن تعتمد التوقيع والتحقق الواردين في الخوارزمية RSA في عمليات المفتاح العمومي طبقاً للخوارزمية المعرّفة هويتها في الفقرة 4.6 من http://www.w3.org/2000/09/xmldsig#rsa-sha1.

2.4.4.8 المراجع

يتعين على رسائل البروتوكول والتأكيدات في اللغة SAML أن تعتمد قيمة لنعت معرّف الهوية على العنصر الجذر من التأكيد أو من رسالة البروتوكول الجاري توقيعهما. والعنصر الجذر من رسالة البروتوكول أو من التأكيد، يمكن أن يكون أو لا يكون هو العنصر الجذر من الوثيقة الحقيقية في اللغة XML التي تحتوي على رسالة البروتوكول أو التأكيد الموقعين (فقد يكون مثلاً محتوى داخل غلاف البروتوكول SOAP).

ويتعين على التوقيعات أن تحتوي على <ds:Reference> وحيد يتضمن مرجع الوثيقة ذاتها إلى قيمة نعت معرف الهوية من العنصر الجذر من رسالة البروتوكول أو التأكيد الجاري توقيعهما. فإذا كانت قيمة نعت معرف الهوية تساوي "foo" مثلاً، فإن نعت المعرّف URI في العنصر <ds:Reference> يجب أن يكون "#foo".

3.4.4.8 طريقة التشريع القانوني

ينبغي لأعمال التنفيذ في اللغة SAML أن تستخدم تشريعاً قانونياً حصرياً، مع تعليقات أو بدونها، في العنصر < ds: CanonicalizationMethod > من <ds:SignedInfo>، وكخوارزمية <ds:Transform>. ويضمن التشريع القانوني الحصري أن تكون التوقيعات المحدثة على رسائل اللغة SAML المبيتة في سياق اللغة XML قابلة للتحقق منها بصورة مستقلة عن هذا السياق.

4.4.4.8 التحويلات

ينبغي ألا تحتوي الرسائل في اللغة SAML على تحويلات غير تحويل التوقيع المتغلّف (مع معرف الهوية http://www.w3.org/2000/09/xmldsig#enveloped-signature) أو غير تحويلات التشريع القانوني الحصري (مع معرف الهوية http://www.w3.org/2001/10/xml-exc-c14n# أو http://www.w3.org/2001/10/xml-exc-c14n#WithComments).

يمكن أن يرفض المتحققون من التوقيعات توقيعات تحتوي على خوارزميات تحويل أخرى باعتبارها غير صالحة. وإذا لم يفعل المتحققون ذلك، يتعين عليهم أن يتأكدوا من أنه لا يوجد أي محتوى رسالة في اللغة SAML مستبعد من التوقيع. ويمكن تحقيق ذلك عن طريق وضع اتفاق خارج النطاق يبين ما هي التحويلات المقبولة، أوعن طريق تطبيق التحويلات يدوياً على المحتوى وإعادة التحقق مما إذا كانت النتيجة تعطي نفس الرسالة في اللغة SAML.

5.4.4.8 KeyInfo (معلومات المفتاح)

يعرّف توقيع التجمع W3C استخدام العنصر <ds:KeyInfo>. إن اللغة SAML لا تتطلب استخدام <ds:KeyInfo>، ولا هي تفرض أي تقييدات على استخدامه. لذلك فإن العنصر <ds:KeyInfo> يمكن أن يكون غائباً.

6.4.4.8 مثال

إن ما يلي هو مثال على استجابة موقعة تحتوي على تأكيد موقّع. وقد أضيفت الانقطاعات في السطور لتسهيل القراءة، والتوقيعات غير صالحة ولا يمكن التحقق منها بنجاح.

```
<Response
  IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
  ID="_c7055387-af61-4fce-8b98-e2927324b306"
  xmlns="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
       <saml:Issuer>https://www.opensaml.org/IDP"</saml:Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                     <ds:CanonicalizationMethod
                            Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
                     <ds:SignatureMethod

       Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                     <ds:Reference URI="#_c7055387-af61-4fce-8b98-
e2927324b306">
                            <ds:Transforms>
                                   <ds:Transform

       Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                   <ds:Transform

       Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                          <InclusiveNamespaces
PrefixList="#default saml ds xs xsi"

       xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                   </ds:Transform>
                            </ds:Transforms>
```

```
                        <ds:DigestMethod

      Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

      <ds:DigestValue>TCDVSuG6grhyHbzhQFWFzGrxIPE=</ds:DigestValue>
                </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>

      x/GyPbzmFEe85pGD3c1aXG4Vspb9V9jGCjwcRCKrtwPS6vdVNCcY5rHaFPYWkf+5

      EIYcPzx+pX1h43SmwviCqXRjRtMANWbHLhWAptaK1ywS7gFgsD01qjyen3CP+m3D
                w6vKhaqledl0BYyrIzb4KkHO4ahNyBVXbJwqv5pUaE4=
          </ds:SignatureValue>
          <ds:KeyInfo>
                <ds:X509Data>
                        <ds:X509Certificate>

      MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVT

      MRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoT

      F1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJ

      bmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0Eg

      LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVowgYsx

      CzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNaWNoaWdhbjESMBAGA1UEBxMJQW5uIEFy

      Ym9yMQ4wDAYDVQQKEwVVQ0FJRDEcMBoGA1UEAxMTc2hpYjEuaW50ZXJuZXQyLmVk

      dTEnMCUGCSqGSIb3DQEJARYYcm9vdEBzaGliMS5pbnRlcm5ldDIuZWR1MIGfMA0G

      CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj

      IHRYQgIv6IqaGG04eTcyVMhoekE0b45QgvBIaOAPSZBl13R6+KYiE7x4XAWIrCP+

      c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE

      pmqOIfGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq

      hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n

      qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX

      8I3bsbmRAUg4UP9hH6ABVq4KQKMknxu1xQxLhpR1ylGPdiowMNTrEG8cCx3w/w==
                        </ds:X509Certificate>
                </ds:X509Data>
          </ds:KeyInfo>
      </ds:Signature>
      <Status>
          <StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </Status>
      <Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
          IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
          xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
          <Issuer>https://www.opensaml.org/IDP</Issuer>
          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                        <ds:CanonicalizationMethod

      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <ds:SignatureMethod

      Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <ds:Reference URI="#_a75adf55-01d7-40cc-929f-
dbd8372ebdfc">
                                <ds:Transforms>
                                        <ds:Transform
```

```
      Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                          <ds:Transform

      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                                <InclusiveNamespaces

      PrefixList="#default saml ds xs xsi"

      xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                          </ds:Transform>
                                    </ds:Transforms>
                                    <ds:DigestMethod

      Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

      <ds:DigestValue>Kclet6XcaOgOWXM4gty6/UNdviI=</ds:DigestValue>
                              </ds:Reference>
                        </ds:SignedInfo>
                        <ds:SignatureValue>

      hq4zk+ZknjggCQgZm7ea8fI79gJEsRy3E8LHDpYXWQIgZpkJN9CMLG8ENR4Nrw+n

      7iyzixBvKXX8P53BTCT4VghPBWhFYSt9tHWu/AtJfOTh6qaAsNdeCyG86jmtp3TD
                              MwuL/cBUj2OtBZOQMFn7jQ9YB7klIz3RqVL+wNmeWI4=
                        </ds:SignatureValue>
                        <ds:KeyInfo>
                              <ds:X509Data>
                                    <ds:X509Certificate>

      MIICyjCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakxCzAJBgNVBAYTAlVT

      MRIwEAYDVQQIEwlXaXNjb25zaW4xEDAOBgNVBAcTB01hZGlzb24xIDAeBgNVBAoT

      F1VuaXZlcnNpdHkgb2YgV2lzY29uc2luMSswKQYDVQQLEyJEaXZpc2lvbiBvZiBJ

      bmZvcm1hdGlvbiBUZWNobm9sb2d5MSUwIwYDVQQDExxIRVBLSSBTZXJ2ZXIgQ0Eg

      LS0gMjAwMjA3MDFBMB4XDTAyMDcyNjA3Mjc1MVoXDTA2MDkwNDA3Mjc1MVowgYsx

      CzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNaWNoaWdhbjESMBAGA1UEBxMJQW5uIEFy

      Ym9yMQ4wDAYDVQQKEwVVQ0FJRDEcMBoGA1UEAxMTc2hpYjEuaW50ZXJuZXQyLmVk

      dTEnMCUGCSqGSIb3DQEJARYYcm9vdEBzaGliMS5pbnRlcm5ldDIuZWR1MIGfMA0G

      CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDZSAb2sxvhAXnXVIVTx8vuRay+x50z7GJj

      IHRYQgIv6IqaGG04eTcyVMhoekE0b45QgvBIaOAPSZBl13R6+KYiE7x4XAWIrCP+

      c2MZVeXeTgV3Yz+USLg2Y1on+Jh4HxwkPFmZBctyXiUr6DxF8rvoP9W7O27rhRjE

      pmqOIfGTWQIDAQABox0wGzAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIFoDANBgkq

      hkiG9w0BAQQFAAOBgQBfDqEW+OI3jqBQHIBzhujN/PizdN7s/z4D5d3pptWDJf2n

      qgi7lFV6MDkhmTvTqBtjmNk3No7v/dnP6Hr7wHxvCCRwubnmIfZ6QZAv2FU78pLX

      8I3bsbmRAUg4UP9hH6ABVq4KQKMknxu1xQxLhpR1ylGPdiowMNTrEG8cCx3w/w==
                                    </ds:X509Certificate>
                              </ds:X509Data>
                        </ds:KeyInfo>
                  </ds:Signature>
                  <Subject>
                        <NameID
                              Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
                              scott@example.org
                        </NameID>
                        <SubjectConfirmation
```

```
      Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
            </Subject>
            <Conditions NotBefore="2003-04-17T00:46:02Z"
                        NotOnOrAfter="2003-04-17T00:51:02Z">
                  <AudienceRestriction>

      <Audience>http://www.opensaml.org/SP</Audience>
                  </AudienceRestriction>
            </Conditions>
            <AuthnStatement AuthnInstant="2003-04-17T00:46:00Z">
                  <AuthnContext>
                        <AuthnContextClassRef>

      urn:oasis:names:tc:SAML:2.0:ac:classes:Password
                        </AuthnContextClassRef>
                  </AuthnContext>
            </AuthnStatement>
      </Assertion>
</Response>
```

5.8 قواعد تركيب التجفير ومعالجته في اللغتين SAML وXML

يستخدم التجفير كوسيلة لتنفيذ السرية. وأكثر دواعي السرية شيوعاً هو حماية الحياة الخاصة الشخصية للأفراد أو حماية أسرار المنظمات للحصول على ميزة تنافسية أو على دوافع مماثلة. وقد تكون السرية مطلوبة أيضاً لتأمين فعالية بعض الآليات الأمنية الأخرى. فكلمة سرٍ أو مفتاح سريان يمكن أن يكونا مجفّرين.

وهناك وسائل عديدة لاستخدام التجفير من أجل حماية السرية لكل التأكيد أو بعضه في اللغة SAML.

- يمكن تأمين سرية الاتصالات بآليات ترافقها رابطة أو جانبية خصوصية. فرابطة البروتوكول SOAP تعتمد استخدام البروتوكول TLS (انظر طلب التعليقات RFC 2246 الصادر عن الفريق IETF) أو الآليات الأمنية لرسائل البروتوكول SOAP من أجل السرية.
- والسر <SubjectConfirmation> يمكن حمايته عن طريق استعمال العنصر <ds:KeyInfo> داخل <SubjectConfirmationData>، الذي يسمح بتجفير المفاتيح أو بأسرار أخرى.
- يمكن تجفير العنصر <Assertion> بكامله، كما هو مشروح في الفقرة الفرعية 4.3.1.8.
- يمكن تجفير العنصر <BaseID> أو العنصر <NameID>، كما هو مشروح في الفقرة الفرعية 4.2.1.8.
- يمكن تجفير العنصر <Attribute>، كما هو مشروح في الفقرة الفرعية 2.3.7.1.8.

1.5.8 اعتبارات عامة

تجفير العناصر <Assertion> و<BaseID> و<NameID> و<Attribute> متوفر باستعمال تجفير اللغة XML. فيتعين أن يستعاض بمعطيات مجفرة واختيارياً بمفتاح مجفّر أو عدة مفاتيح مجفّرة عن معلومات واضحة النص في نفس الموضع من مرحلة معينة من اللغة XML. وينبغي استعمال نعت النمط (Type) للعنصر <EncryptedData>، وعندما يكون موجوداً يتعين أن تكون له القيمة http://www.w3.org/2001/04/xmlenc#Element.

ملاحظة (للاطّلاع) – يقترح PE30 (انظر OASIS PE:2006) أن يستعاض عن مفتاح واحد أو أكثر في السطر الثاني بصفر من المفاتيح أو أكثر.

ويمكن استخدام أي واحدة من الخوارزميات المعرفة لاستخدامها في تجفير اللغة XML من أجل تحقيق التجفير. وتخطيطة اللغة SAML معرفة بحيث يؤدي إدراج معطيات مجفّرة إلى مرحلة صالحة.

2.5.8 اعتبارات عامة

يمكن الجمع بين استعمال تجفير اللغة XML واستعمال توقيعات XML. وعندما يطلب التوقيع على التأكيد وتجفيره، تطبق القواعد التالية. يتعين على طرف واثق أن يقوم بإقرار صلاحية التوقيع وبفك التجفير بالترتيب المعاكس للترتيب الذي جرى منه التوقيع والتجفير.

- عندما يجفّر العنصر <Assertion> الموقّع، يتعين أن يحسب التوقيع أولاً وأن يوضع داخل العنصر <Assetion> قبل أن يجفّر العنصر.
- عندما يجفر العنصر <Saml:BaseID> أو <Saml:NameID> أو <Attribute>، يتعين إجراء التجفير أولاً، ثم حساب التوقيع على التأكيد أو الرسالة اللذين يحتويان على العنصر المجفّر.

6.8 التوسّعية في اللغة SAML

تقبل اللغة SAML التوسّعية بأساليب متعددة، منها التوسّع في تخطيطات التأكيد والبروتوكول. انظر بند الجانبيات في اللغة SAML الوارد في هذه التوصية للاطّلاع على كيفية تعرف جانبيات جديدة، التي يمكن جمعها مع التوسّعات لكي تنشأ استخدامات جديدة في إطار عمل اللغة SAML.

1.6.8 التوسّع في التخطيطة

تجمّد العناصر في تخطيطات اللغة SAML من أن يقع لها تبديل، وهذا يعني أن أي عنصر من عناصر اللغة SAML لا يستطيع أن يعمل كعنصر رأسي في زمرة تبديل. ومع ذلك لا تُعرّف أنماط اللغة SAML على أنها نهائية، بحيث إن جميع أنماط اللغة SAML يمكن توسيعها ويمكن قَصْرها. وهذا يعني من الناحية العملية أن التوسّعات تعرّف عادة على أنها أنماط فقط بدلاً من عناصر، وتدخل في مراحل اللغة SAML عن طريق النعت xsi:type.

والفقرات الفرعية التالية تدرس فقط العناصر والأنماط التي جرى تصميمها خصيصاً لتقبّل التوسّعية.

1.1.6.8 التوسّع في تخطيطة التأكيد

إن تخطيطة التأكيد في اللغة SAML مصممة لكي تسمح بمعالجة منفصلة لترزيمة التأكيد والإعلانات التي يتضمنها، إن كانت آلية التوسّع تستعمل لكل جزء على حدة.

والعناصر التالية معدّة خصيصاً لكي تستعمل كنقاط توسّع في تخطيطة توسّع، وأنماطها موضوعة على abstract، ولذلك فهي لا تستعمل إلا كأساس لنمط مشتق:

- <BaseID> و**BaseIDAbstractType**.
- <Condition> و**ConditionAbstractType**.
- <Statement> و**StatementAbstractType**.

والتركيبات التالية التي يمكن استعمالها مباشرة كجزء من اللغة SAML، هي أهداف مهمة خصوصاً للتوسّع:

- <AuthnStatment> و**AuthnStatementType**.
- <AttributeStatement> و**AttributeStatementType**.
- <AuthzDecisionStatement> و**AuthzDecisionStatementType**.
- <AudienceRestriction> و**AudienceRestrictionType**.
- <ProxyRestriction> و**ProxyRestrictionType**.
- <OneTimeUse> و**OneTimeUseType**.

2.1.6.8 التوسّع في تخطيطة البروتوكول

عناصر البروتوكول التالية في اللغة SAML معدّة خصيصاً لكي تستعمل كنقاط توسّع في تخطيطة توسّع، وأنماطها موضوعة على abstract، ولذلك فهي لا تستعمل إلا كأساس لنمط مشتق:

- <Request> و**RequestAbstractType**.
- <SubjectQuery> و**SubjectQueryAbstractType**.

والتركيبات التالية التي يمكن استعمالها مباشرة كجزء من اللغة SAML، هي أهداف مهمة خصوصاً للتوسّع:

- <AuthnQuery> و**AuthnQueryType**.
- <AuthzDecisionQuery> و**QuthzDecisionQueryType**.
- <AttributeQuery> و**AttributeQueryType**.
- **StatusResponseType**.

2.6.8 نقاط التوسّع الاستبدالية في تخطيطة

تستخدم تخطيطات اللغة SAML تركيبات استبدالية في بعض المواقع، لكي تتيح استعمال عناصر ونعوت قادمة من أمكنة أمساء اعتباطية، لكي تستخدم كنقطة توسّع مدمجة من دون الحاجة إلى تخطيطة توسّع.

1.2.6.8 نقاط التوسّع في التأكيد

التركيبات التالية في تخطيطة التأكيد، تسمح بتركيبات داخلها قادمة من أمكنة أسماء اعتباطية:

- <SubjectConfirmationData>: تستخدم **xs:anyType** الذي يقبل أي عناصر فرعية أو نعوت.
- <AuthnContextDecl>: يستعمل **xs:anyType** الذي يقبل أي عناصر فرعية ونعوت.
- <AttributeValue>: يستعمل **xs:anyType** الذي يقبل أي عناصر فرعية ونعوت.
- <Advice> و<AdviceType>: إضافة إلى عناصر اللغة SAML المولودة فيها، يقبل هذا العنصر عناصر قادمة من أمكنة أسماء أخرىن مع عملية مرنة لإقرار صلاحية التخطيطة.

والتركيبة التالية في تخطيطة التأكيد تتيح نعوتاً عامة اعتباطية:

- <Attribute> و**AttributeType**.

2.2.6.8 نقاط التوسّع في بروتوكول

التركيبات التالية في تخطيطة البروتوكول، تسمح بتركيبات داخلها قادمة من أمكنة أسماء اعتباطية:

- <Extensions> و**ExtensionsType**: يسمح بعناصر قادمة من أمكنة أسماء أخرى، مع عملية مرنة لإقرار صلاحية التخطيطة.
- <StatusDetail> و<StatusDetailType>: يسمح بعناصر قادمة من أمكنة أسماء أخرىن مع عملية مرنة لإقرار صلاحية التخطيطة.
- <ArtifactResponse> و<ArtifactResponseType>: يسمح بعناصر قادمة من أي أمكنة أسماء، مع عملية مرنة لإقرار صلاحية التخطيطة. (وهو معدّ خصيصاً ليحمل عنصر رسالة طلب أو استجابة في اللغة SAML).

2.2.6.8 نقاط التوسّع في بروتوكول

تستخدم اللغة SAML معرفات هوية مبنية على المعرف URI من أجل عدد من الأغراض، مثل شفرات الحالة وأنساق معرف هوية الاسم، وهي تعرّف بعض معرّفات الهوية التي يمكن استخدامها لهذه الأغراض، وأغلبها معدّد في قائمة الفقرة 7.8. ومع ذلك يمكن دوماً تعريف معرفات هوية إضافية مبنية على المعرف URI من أجل هذه الأغراض. ويوصى أن يجري تعريف هذه المعرّفات الإضافية للهوية في جانبية رسمية للاستعمال. ولا يجوز بأي حال أن يتغير تغيراً محسوساً معنى معرّف URI معين مستعمل باعتباره هذا المعرّف للهوية أو أن يستعمل ليقصد شيئين مختلفين.

7.8 معرّفات هوية معرّفة في اللغة SAML

تعرّف الفقرات الفرعية التالية معرّفات هوية مبنية على المعرّف URI، لاستخدامها في أعمال النفاذ إلى موارد مشتركة وفي أنساق معرفات الهوية لأسماء الأصحاب وفي أنساق أسماء النعوت.

يستعمل اسم موحّد للموارد (URN) حيث يمكن، لتحديد بروتوكول. وفي حالة بروتوكول فريق المهام الهندسية في الإنترنت (IETF)، يستعمل الاسم URN الوارد في طلب التعليقات (RFC) الأكثر انتشاراً الذي يحدد البروتوكول. والمراجع إلى المعرّف URI المحدثة خصّيصاً للغة SAML، يكون لها واحد من الجذور التالية، حسب صيغة مجموعة المواصفات التي أدخلت فيها لأول مرة:

```
urn:oasis:names:tc:SAML:1.0:
urn:oasis:names:tc:SAML:1.1:
urn:oasis:names:tc:SAML:2.0:
```

وتستخدم هذه التوصية الجذر الأخير.

1.7.8 معرّفات هوية أمكنة أسماء الأعمال

يمكن استعمال معرفات الهوية التالية في النعت Namespace من العنصر <Action> للإحالة إلى مجموعات الأعمال المشتركة المطلوب أداؤها على الموارد.

1.1.7.8 القراءة/الكتابة/التنفيذ/الإلغاء/التحكم

URI: urn:oasis:names:tc:SAML:1.0:action:rwedc

الأعمال المعرّفة: Read Write Execute Delete Control

وتفسر هذه الأعمال كما يلي:

- Read: يتمكن الصاحب من قراءة المورد
- Write: يتمكن الصاحب من تعديل المورد
- Execute: يتمكن الصاحب من تنفيذ المورد
- Delete: يتمكن الصاحب من تنفيذ المورد
- Control: يحدد الصاحب سياسة التحكم في النفاذ إلى المورد

2.1.7.8 القراءة/الكتابة/التنفيذ/الإلغاء/التحكم مع النفي

URI: urn:oasis:names:tc:SAML:1.0:action:rwedc-negation

الأعمال المعرفة: Read Write Execute Delete Control ~Read ~Write ~Execute ~Delete ~Control

الأعمال المحددة في الفقرة الفرعية 1.1.7.8 تفسر بنفس الطريقة المشروحة هنا. أما الأعمال المسبوقة بعلامة تِلْدة (المَدَّة) فهي أذونات منفيّة، وتستخدم لتحدد بشكل أكيد أن الإذن المقرر مرفوض. وهكذا يكون الصاحب الموصوف بأنه مرخص له بأن يقوم بالعمل Read يجد نفسه مرفوضاً له إذن القراءة بالتأكيد.

ويتعين على السلطة في اللغة SAML ألا ترخّص بنفس الوقت بالعمل وبشكله المنفي.

3.1.7.8 الحصول/الترؤس/الوضع/الإرسال بالبريد

URI: `urn:oasis:names:tc:SAML:1.0:action:ghpp`

الأعمال المعروفة: `GET HEAD PUT POST`

ترتبط هذه الأعمال بالعمليات المقابلة في بروتوكول نقل النص الفائق (HTTP). فالصاحب المرخص له مثلاً بأن يقوم بالعمل GET على مورد معين، هو مرخص له أيضاً أن يحصل عليه.

والعملان GET وHEAD يقابلان بالإجمال إذن القراءة التقليدي، والعملان PUT وPOST يقابلان بالإجمال إذن الكتابة. والتقابل ليس مضبوطاً تماماً لأن العملية HTTP GET قد تتسبب في تعديل المعطيات، والعملية POST قد تتسبب في تعديلات مورد غير المورد المحدد في الطلب. لذلك يوجد مخصّص منفصل لمرجع عمل المعرف Action URI.

4.1.7.8 أذونات الملف في النظام UNIX

URI: `urn:oasis:names:tc:SAML:1.0:action:unix`

الأعمال المعرفة هي مجموعة الأذونات للنفاذ إلى ملف النظام UNIX، المعبّر عنها بالترميز الرقمي (الأثموني).

وسلسلة العمل موجودة في شفرة رقمية رباعية الأرقام:

extended user group world

حيث يكون لإذن النفاذ *extended* القيمة:

2+ إذا كان sgid هو الموضوع عليه

4+ إذا كان suid هو الموضوع عليه

ويكون لإذني النفاذ *user group* و*word* القيمة

1+ إذا كان الإذن بالتنفيذ هو المعطى

2+ إذا كان الإذن بالكتابة هو المعطى

4+ إذا كان الإذن بالقراءة هو المعطى

فمثلاً الرقم 0754 يدل على إذن النفاذ إلى ملف النظام UNIX: المستخدم يقرأ ويكتب وينفذ؛ والفريق يقرأ وينفذ؛ وبقية الناس يقرؤون.

2.7.8 معرفات الهوية لنسق اسم النعت

يمكن استعمال معرفات الهوية التالية في النعت NameFormat المعرف في النمط المعقد **AttributeType**، للإحالة إلى تصنيف أسماء النعوت لأغراض تفسير الاسم.

1.2.7.8 غير محدد (Unspecified)

URI: `urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified`

تفسير اسم النعت متروك لكل تنفيذ بمفرده.

2.2.7.8 المرجع إلى المعرّف URI

URI: urn:oasis:names:tc:SAML:2.0:attrname-format:uri

اسم النعت يلي الاصطلاح بشأن المراجع إلى المعرف URI، كما هو مستعمل مثلاً في معرفات هوية النعت في اللغة XACML (اللغة التأشيرية التوسّعية للتحكم في النفاذ). وتفسير محتوى المعرّف URI أو تخطيطة التسمية هو خاص بالتطبيق. انظر في البند 11 جانبيات النعت التي تستخدم هذا المعرّف للهوية.

3.2.7.8 أساسي (Basic)

URI: urn:oasis:names:tc:SAML:2.0:attrname-format:basic

يتعين على صنف السلاسل المقبول كاسم للنعت، أن يُسْحب من مجموعة القيم التي تنتمي إلى النمط الأصلي **xs:Name**، كما هو معرف في الفقرة الفرعية 6.3.3 من XML Datatypes الصادرة عن التجمع W3C. انظر في البند 13 جانبيات النعت التي تستخدم هذا المعرّف للهوية.

3.7.8 معرفات الهوية لنسق هوية الاسم

يمكن استعمال معرفات الهوية التالية في النعت Format من العناصر <NameID> أو <NameIDPolicy> أو <Issuer> (انظر الفقرة الفرعية 2.1.8)، من أجل الإحالة إلى الأنساق المشتركة بشأن محتوى العناصر وقواعد المعالجة التي تصحبها، إن وجدت.

ملاحظة – جرى في الصيغة SAML V2.0 سحب معرفات هوية عديدة، كانت قد اعتبرت بالية في الصيغة V1.1.

1.3.7.8 غير محدد (Unspecified)

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

تفسير محتوى العنصر متروك لكل تنفيذ بمفرده.

2.3.7.8 عنوان بريد إلكتروني (Email address)

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

يدل على أن محتوى العنصر موجود بشكل عنوان بريد إلكتروني، وخصوصاً "addr-spec" كما هو معرف في الفقرة الفرعية 1.4.3 من طلب التعليقات RFC 2822 الصادر عن فريق المهام الهندسية في الإنترنت (IETF). ويكون للعنوان addr-spec الشكل local-part@domain. ويلاحظ أن addr-spec لا تسبقه أي جمله (مثل الاسم المشترك)، ولا يليه أي تعليق عليه (مثل نص محصور بين قوسين)، وليس محصوراً بين الرمزين "<" و">".

3.3.7.8 اسم الصاحب في التوصية X.509

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

يدل على أن محتوى العنصر موجود بالشكل المحدد لمحتويات العنصر <ds:X509SubjectName> في توقيع التجمع W3C. وينبغي للمنفذين أن يلاحظوا أن توقيع اللغة XML التابع للتجع W3C يحدد قواعد التشفير لأسماء الأصحاب في التوصية X.509، وهي تختلف عن القواعد المعطاة في طلب التعليقات RFC 2253 الصادر عن الفريق IETF.

4.3.7.8 اسم موصوف للميدان Windows

URI: urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName

يدل على أن محتوى العنصر هو اسم موصوف للميدان Window. واسم المستعمل الموصوف للميدان Windows هو سلسلة من الشكل "DomainName\UserName". ويمكن حذف اسم الميدان والشرطة الفاصلة "\".

5.3.7.8 اسم طرف رئيسي في بروتوكول Kerberos

URI: urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos

يدل على أن محتوى العنصر هو بشكل اسم طرف رئيسي في بروتوكول Kerberos، يستخدم النسق name[/instance]@REALM. وقواعد التركيب والنسق والسمات الممنوحة للاسم والمرحلة وREALM مشروحة في طلب التعليقات RFC 1510 الصادر عن الفريق IETF.

6.3.7.8 معرف هوية كيان

URI: urn:oasis:names:tc:SAML:2.0:nameid-format:entity

يدل على أن محتوى العنصر هو معرف الهوية لكيان يزوّد بخدمات مبنية على اللغة SAML (مثل سلطة أو طالب او مستجيب في اللغة SAML)، أو هو مشترك في جانبيات اللغة SAML (مثل مزود الخدمة الذي يعتمد جانبية اكتتاب وحيد (SSO) لمتصفح). يمكن استعمال مثل هذا المعرف للهوية في العنصر <Issuer> لكي يعرف هوية المصدر لطلب أو استجابة أو تأكيد في اللغة SAML، أو يمكن استعماله في العنصر <NameID> لوضع تأكيدات حول كيانات في نظام تستطيع إصدار الطلبات والاستجابات والتأكيدات في اللغة SAML. ويمكن استعماله أيضاً في عناصر ونعوت أخرى ترمي إلى تعريف هوية كيان في نظام عند مختلف تبادلات البروتوكول.

وقواعد التركيب لمثل هذا المعرف هي معرف URI لا يزيد طوله على 1024 سمة. ويوصى بأن يستخدم الكيان في النظام محدد مكان URL يحتوي على اسم الميدان الخاص به لكي يعرف هويته هو بالذات.

ويتعين حذف النعوت NameQualifier وSPNameQualifier وSPProvidedID.

7.3.7.8 معرّف الهوية الدائم

URI: oasis:names:tc:SAML:2.0:nameid-format:persistent

يدل على أن محتوى هذا العنصر هو معرف هوية عاتم ودائم، لطرف رئيسي خاص بمزود هوية ومزود خدمة أو بجماعة المنتسبين من مزودي الخدمة. ويتعين على معرفات هوية الاسم الدائمة التي يولدها مزودو الهوية أن تكون مركبة باستخدام قيم شبه عشوائية، ليس لها مقابلات يمكن أن يكشفها معرف الهوية الحقيقي للصاحب (مثل اسم المستعمل). والنية متجهة إلى إحداث اسم مستعار متزاوج غير عمومي لاتقاء اكتشاف هوية الصاحب أو أنشطته. ويجب ألا يزيد طول قيم معرف هوية الاسم الدائم على 256 سمة.

وعندما يكون نعت العنصر NameQualifier موجوداً، يجب أن يحتوي على معرف هوية وحيد لمزود الهوية الذي يولد معرفات الهوية (انظر الفقرة الفرعية 6.3.7.8). ويمكن حذفه إذا كانت القيمة تشتق من سياق رسالة تحتوي على العنصر، كما في حالة مُصْدر رسالة بروتوكول أو تأكيد يحتوي على معرف الهوية داخل موضوعه. وينبغي لكيان آخر في النظام أن يصدر لاحقاً رسالة البروتوكول أو التأكيد الخاصين به ويحتويان معرف الهوية، وفي هذه الحالة لا يتغير النعت NameQualifier، ولكنه يجب أن يستمر في التعريف بهوية الكيان الذي أحدث في الأصل معرف الهوية (ويجب ألا يحذف في مثل هذه الحالة).

وعندما يكون نعت العنصر SPNameQualifier موجوداً، يجب أن يحتوي على معرف هوية وحيد لمزود الخدمة أو لجماعة المنتسبين من المزودين الذين كان قد جرى توليد معرف الهوية لهم (انظر الفقرة الفرعية 6.3.7.8). ويمكن حذفه إذا كان العنصر وارداً في رسالة معدة فقط لكي يستهلكها مباشرة مزودا الخدمة، ويمكن أ، تكون قيمته هي معرف الهوية الوحيد لمزود الخدمة هذا.

ويتعين أن يحتوي نعن العنصر SPProvidedID على معرف هوية الطرف الرئيسي البديل الذي وضعه أخيراً مزود الخدمة أو جماعة المنتسبين من المزودين، إن وجدت، (انظر الفقرة الفرعية 6.2.8). وإذا لم يكن قد وضع مثل هذا المعرف للهوية، يتعين عندئذ حذف النعت.

تعتبر معرفات الهوية الدائمة بمثابة آلية لحماية السرية، وبصفتها تلك يتعين ألا يجرى تقاسمها في نص واضح مع مزودين ليسوا هم المزودون الذين وضعوا معرف الهوية المتقاسم. وفوق ذلك يجب ألا تظهر معرفات الهوية في ملفات الدفاتر اليومية أو في مواقع مماثلة دون مراقبات وحمايات مناسبة. أما التنفيذات التي ليس لها مثل هذه المتطلبات في حرة في استخدام أنواع أخرى من معرفات الهوية في تبادلاتها في اللغة SAML، ولكن عليها ألا تحمّل هذا النسق حمولة زائدة بقيم دائمة وغير عائمة.

وبينما تستعمل معرفات الهوية الدائمة لكي تعكس بصورة عامة علاقة محاسبية بين زوج من المزودين، فإن مزود الخدمة ليس ملزماً بأن يعترف أو يستعمل معرفاً دائماً للهوية، مديد الأجل بطبيعته أو يقيم مثل هذه الوصلة. ومثل هذه العلاقة "الوحيدة الجانب" لا تختلف اختلافاً ملموساً ولا تؤثر في سلوك مزود الهوية أو في أي قواعد معالجة تخص معرفات الخدمة الدائمة في البروتوكولات المعرفة في هذه التوصية.

ويبين النعتان `NameQualifier` و`SPNameQualifier` التوجهية في عملية الإحداث، ولكنهما لا يبينان استخدامها. فإذا كان مزود هوية معين هو الذي يحدث معرفاً دائماً للهوية، تكون قيمة النعت `NameQualifier` قد وضعت في هذه اللحظة بصورة دائمة. وإذا قام مزود الخدمة الذي يستلم مثل هذا المعرف للهوية، بدور مزود الهوية وأصدر تأكيده الخاص به الذي يحتوي على معرف الهوية هذا، فإن قيمة النعت `NameQualifier` لن تتغير (وبالتأكيد لن تحذف). ويمكنه أن يختار بديلاً من ذلك فيحدث معرفاً دائماً للهوية خاصاً به ليمثل الطرف الرئيسي ويصل ما بين القيمتين. وهذا قرار يتخذه التنفيذ.

8.3.7.8 معرّف الهوية العابر

URI: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

يدل على أن محتوى العنصر هو معرف هوية بدلالة عابرة، وينبغي أن يتعامل الطرف الواثق معه على أنه قيمة مؤقتة عائمة. ويتعين توليد قيم معرف الهوية العابر طبقاً للقواعد المطبقة على معرفات الهوية في اللغة SAML (انظر الفقرة 4.7)، ويجب ألا يزيد طولها على 256 سمة.

يمكن استعمال النعتين `NameQualifier` و`SPNameQualifier` للإشارة إلى أن معرف الهوية يمثل معرف هوية متزاوجاً ومؤقتاً وعابراً. وفي مثل هذه الحالة، يمكن حذفهما طبقاً للقواعد المحددة في الفقرة الفرعية 7.3.7.8.

4.7.8 معرّف هوية الموافقة

يمكن استخدام معرفات الهوية التالية في النعت `Consent` المعرف في النعتين المعقدين **RequestAbstractType** و**StatusResponseType**، للإفادة عما إذا كان طرف رئيسي قد أعطى موافقته على الرسالة ووفق أي شروط.

Unspecified 1.4.7.8

URI: `urn:oasis:names:tc:SAML:2.0:consent:unspecified`

لم تحدث أي مطالبة تخص موافقة الطرف الرئيسي.

Obtained 2.4.7.8

URI: `urn:oasis:names:tc:SAML:2.0:consent:obtained`

يدل على أن موافقة الطرف الرئيسي قد حصل عليها مُصْدر الرسالة.

Prior 3.4.7.8

URI: `urn:oasis:names:tc:SAML:2.0:consent:prior`

يدل على أن موافقة الطرف الرئيسي كان مُصْدر الرسالة قد حصل عليها في فترة معينة تسبق العمل الذي بادرت إليه الرسالة.

Implicit 4.4.7.8

URI: `urn:oasis:names:tc:SAML:2.0:consent:current-implicit`

يدل على أن موافقة الطرف الرئيسي قد حصل عليها مُصْدر الرسالة ضمنياً أثناء العمل الذي بادرت إليه الرسالة، كجزء من دلالة أوسع على الموافقة. وتكون الموافقة الضمنية قريبة في الزمن من العمل ومن التقديم أكثر مما هي عليه الموافقة المسبقة، بصفتها جزءاً من دورة أنشطة.

Explicit 5.4.7.8

URI: urn:oasis:names:tc:SAML:2.0:consent:current-explicit

يدل على أن موافقة الطرف الرئيسي قد حصل عليها مُصدر الرسالة صراحةً أثناء العمل الذي بادرت إليه الرسالة.

Unavailable 6.4.7.8

URI: urn:oasis:names:tc:SAML:2.0:consent:unavailable

يدل على أن مُصْدر الرسالة لم يحصل على الموافقة.

Inapplicable 7.4.7.8

URI: urn:oasis:names:tc:SAML:2.0:consent:inapplicable

يدل على أن مُصْدر الرسالة لا يعتقد بأن هناك حاجة إلى الموافقة أو إلى الإبلاغ عنها.

9 المعطيات الشرحية للغة SAML

تتطلب جانبيات اللغة SAML اتفاقات بين كيانات نظام بخصوص معرفات الهوية، واعتماد الروابط والنقاط النهائية والشهادات والمفاتيح. وهكذا دواليك. ويعرف هذا البند نسقاً للمعطيات الشرحية قابلاً للتوسّع إلى كيانات نظام في اللغة SAML، فنظماً وفقاً للأدوار التي تعكسها جانبيات اللغة SAML. ومثل هذه الأدوار تشمل أدوار مزود الهوية باكتتاب التوقيع الوحيد (SSO) ومزود الخدمة باكتتاب التوقيع الوحيد (SSO)، والانتساب وسلطة النعت وطالب النعت ونقطة القرار السياسي

1.9 المعطيات الشرحية

تنظّم المعطيات الشرحية للغة SAML حول مجموعة توسّعية من الأدوار تمثل تجميعات مشتركة من بروتوكولات اللغة SAML وجانبياتها، تعتمدها كيانات النظام. ويُشْرح كل دور بعنصر مشتق من نمط أساسي توسّعي هو RoleDescriptor. ومثل هذه الواصفات تُجمَّع بدورها في العنصر الحاوي <EntityDescriptor> الذي هو الوحدة الأولى من المعطيات الشرحية للغة SAML. ويمكن أيضاً لكيان ما أن يمثل جماعة منتسبين من كيانات أخرى، مثل جماعة المنتسبين من مزودي الخدمة. والعنصر <AffiliationDescriptor> مقدّم لهذا الغرض.

ويمكن مراكمة مثل هذه المواصفات بدورها في زمر مبيّتة تستخدم العنصر <EntitiesDescriptor>.

ويمكن اعتماد آليات أمنية متنوعة لإقامة جدارة الثقة بالمعطيات الشرحية، وخصوصاً مع إمكانية التوقيع الفردي على أغلب العناصر المعرفة في هذه التوصية.

عندما تحتوي العناصر التي ترتبط بعلاقة الوالد/الولد (الأب/الابن) على نعوت مشتركة، مثل ذاكرة المخبأ أو معلومات انقضاء الصلاحية، تكون الأولوية لعنصر الوالد.

ملاحظة – يجب ألا تؤخذ المعطيات الشرحية للغة SAML بصورة عامة على أنها إعلان سلطوي على إمكانات أو خيارات كيان معين في نظام. وهذا يعني أنها بينما ينبغي لها أن تكون دقيقة، فهي لا تحتاج أن تكون حصرية. وإلغاء خيار معين لا يعني أبداً أنه معتمد أو غير معتمد، بل هو بكل بساطة غير مطلوب. وكمثال على ذلك، سلطة النعت في اللغة SAML يمكنها أن تعتمد أي عدد من النعوت غير مسماة في عنصر <AttributeAuthorityDescriptor>. وربما يعكس الإلغاء السرية أو أي عدد آخر من الاعتبارات. وعلى العكس أيضاً فإن الدلالة على اعتماد نعت معين، لا تعني أبداً أن طالباً معيناً سوف يستلمه أو يريد أن يستلمه.

1.1.9 أماكن الأسماء

تستخدم المعطيات الشرحية في اللغة SAML أماكن الأسماء التالية:

urn:oasis:names:tc:SAML:2.0:metadata

وتستخدم هذه التوصية سابقة لأماكن الأسماء :md تحيل إلى مكان الاسم العلوي.

والقطعة التالية من التخطيطة تستخدم أماكن الأسماء في وثائق المعطيات الشرحية للغة SAML:

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <import namespace="http://www.w3.org/2001/04/xmlenc#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-
20021210/xenc-schema.xsd"/>
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-metadata-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Schema for SAML metadata, first published in SAML 2.0.
        </documentation>
    </annotation>
…
</schema>
```

2.1.9 الأنماط الشائعة

تعرف هذه الفقرة الفرعية أنماطاً عديدة من المعطيات الشرحية مطلوباً استخدامها في تعريف العناصر والنعوت.

1.2.1.9 النمط البسيط

يقيّد النمط البسيط **entityIDType** النمط **anyURI** الخاص بمعطيات تخطيطة اللغة XMLن بألا يزيد طوله على 1024 سمة. ويستخدم النمط **entityIDType** كمعرّف هوية وحيد لكيانات اللغة SAML. انظر أيضاً الفقرة الفرعية 6.3.7.8. ومعرف هوية من هذا النمط يتعين أن يكون وحيداً داخل جميع الكيانات التي تتأثر (يؤثر بعضها في بعض) في تطور معين. واستخدام معرف URI مع التمسك بالقاعدة القائلة بأن معرفاً URI وحيداً يجب ألا يحيل إلى كيانات مختلفة، يلبي هذا المطلب.

والقطعة التالية من التخطيطة تعرف النمط البسيط **entityIDType**.

```
<simpleType name="entityIDType">
      <restriction base="anyURI">
            <maxLength value="1024"/>
      </restriction>
</simpleType>
```

2.2.1.9 النمط المعقّد EndpointType

يشرح النمط المعقّد **EndpoinType** نقطة نهائية لرابطة بروتوكول اللغة SAML، يستطيع كيان في اللغة SAML أن يرسل إليها رسائل بروتوكول. ويرتبط بهذا النمط العديد من عناصر البروتوكول أو من المعطيات الشرحية الخاص بالجانبيات. وهي تتكون من النعوت التالية:

- `Binding` [مطلوب]

نعت مطلوب يحدد رابطة في اللغة SAML تعتمدها نقطة نهائية. وكل رابطة مسندة إلى معرف URI لكي يعرف هويتها.

- `Location` [مطلوب]

نعت للمعرف URI مطلوب لكي يحدّد موقع النقطة النهائية. وقواعد التركيب المسموحة لهذا المعرف URI تتوقف على رابطة البروتوكول.

- `ResponseLocation` [اختياري]

يحدد اختيارياً موقعاً مختلفاً ترسل إليه رسائل الاستجابات كجزء من البروتوكول أو الجانبية. وقواعد التركيب المسموحة لهذا المعرف URI تتوقف على رابطة البروتوكول.

يستعمل النعت `ResponseLocation` لتمكين عدة نقاط نهائية من استقبال رسائل الطلب والاستجابة المرافقة لبروتوكول أو جانبية، ولكن ليس كوسائل لموازنة الحمولات أو كوسائل للإطناب (يمكن إيراد عدة عناصر من هذا النمط تحقيقاً لهذا الغرض). ولا يستعمل النعت `ResponseLocation` عندما يحتوي أحد الأدوار على عنصر من هذا النمط ينتمي إلى بروتوكول أو إلى جانبية، ينطبق عليها نوع وحيد من رسائل (طلب أو استجابة).

ملاحظة (للاطّلاع) – يوضح PE41 (انظر OASIS PE:2006) الفقرة أعلاه بإضافة الجملة التالية إلى النص:

إذا كان النعت `ResponseLocation` محذوفاً، فإن أي رسالة استجابة مرافقة لبروتوكول أو جانبية يمكن الافتراض بأنها تعامل في المعرف URI الذي يشير إليه النعت `Location`.

وتظهر عناصر هذا النمط في أغلب السياقات في تتابعات غير معينة الحدود في التخطيطة. وذلك يسمح لأحد الكيانات بتقديم بروتوكول أو جانبية في نقاط نهائية متعددة، تصحبها عادة روابط بروتوكول مختلفة لكي تتيح لمستهلك المعطيات الشرحية أن يختار النقطة النهائية حسب حاجاته. ويمكن لعدة نقاط نهائية أن تقدم توازن الحمولة أو استئناف الفشل "في جانب الزبون"، وخاصة في حالة رابطة بروتوكول متزامنة.

ويسمح هذا العنصر أيضاً باستخدام عناصر ونعوت اعتباطية معرّفة في أماكن أسماء ليست في اللغة SAML. وأي محتوى من هذا النوع يجب وصفه بكونه مكان اسم.

والقطعة التالية من التخطيطة تعرّف النمط المعقد **EndpointType**.

```
<complexType name="EndpointType">
      <sequence>
            <any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </sequence>
      <attribute name="Binding" type="anyURI" use="required"/>
      <attribute name="Location" type="anyURI" use="required"/>
      <attribute name="ResponseLocation" type="anyURI" use="optional"/>
      <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

3.2.1.9 النمط المعقّد IndexedEndpointType

النمط المعقد **IndexedEndpointType** يوسّع **EndpointType** بزوج من النعوت، لكي يتيح فهرسة النقاط النهائية المتطابقة حتى يمكن الإحالة إليها برسائل البروتوكول. ويتكون من النعتين الإضافيين التاليين:

- `Index` [مطلوب]

نعت مطلوب يسند قيمة صحيحة وحيدة إلى النقطة النهائية حتى يمكن الإحالة إليها في رسالة بروتوكول. ولا تحتاج قيمة الفهرس إلا أن تكون وحيدة ضمن مجموعة من العناصر المتماثلة المحتواة داخل العنصر الوالد نفسه (أي إنها لا تحتاج أن تكون وحيدة في كاملة المرحلة).

- `isDefault` [اختياري]

نعت بولاني اختياري يستعمل ليشير إلى نقطة نهائية بالتغيب ضمن مجموعة مفهرسة. وإذا حذف، تفترض القيمة خاطئة.

وفي أي تتابع من هذا النوع مكوّن من نقاط نهائية متماثلة مبنية على هذا النمط، تكون النقطة النهائية بالتغيب هي أول نقطة نهائية من هذا النوع، مع النعت `isDefault` موضوعاً على "صائب". وإذا كانت لا توجد مثل هذه النقاط النهائية، تكون النقطة النهائية بالتغيب هي أو نقطة نهائية من هذا النوع، بدون وضع النعت `isDefault` على "خاطئ". وإذا كانت لا توجد مثل هذه النقاط النهائية، فإن النقطة النهائية تكون هي أو عنصر في التتابع.

ملاحظة (للاطّلاع) – يقترح PE37 (انظر OASIS PE:2006) توضيح الفقرة أعلاه بما يلي:

في أي تتابع من هذا النوع مكوّن من نقاط نهائية مفهرسة تتقاسم اسم عنصر ومكان اسم مشتركين (أي جميع المراحل `<md:AssertionConsumerService>` في دور واحد)، تكون النقطة النهائية بالتغيب هي أو نقطة نهائية، مع وضع النعت `isDefault` على "صائب". وإذا كانت لا توجد مثل هذه النقاط النهائية، تكون النقطة النهائية بالتغيب هي أول نقطة نهائية، بدون وضع النعت `isDefault` على "خاطئ". وإذا كانت لا توجد مثل هذه النقاط النهائية، فإن النقطة النهائية بالتغيب تكون هي أول عنصر في التتابع.

والقطعة التالية من التخطيطة تعرّف النمط المعقّد **IndexedEndpointType**:

```
<complexType name="IndexedEndpointType">
	<complexContent>
		<extension base="md:EndpointType">
			<attribute name="index" type="unsignedShort"
use="required"/>
			<attribute name="isDefault" type="boolean"
use="optional"/>
		</extension>
	</complexContent>
</complexType>
```

4.2.1.9 النمط المعقّد localizedNameType

النمط المعقد **localizedNameType** يوسّع العنصر المقيّم بسلسلة مع نعت معياري في اللغة XML. والقطعة التالية من التخطيطة تعرف النمط المعقد **localizedNameType**:

```
<complexType name="localizedNameType">
	<simpleContent>
		<extension base="string">
			<attribute ref="xml:lang" use="required"/>
		</extension>
	</simpleContent>
</complexType>
```

5.2.1.9 النمط المعقّد localizedURIType

النمط المعقد **localizedURIType** يوسّع العنصر المقيّم بمعرّف URI مع نعت معياري في اللغة XML.

والقطعة التالية من التخطيطة تعرّف النمط المعقّد **localizedURIType**:

```
<complexType name="localizedURIType">
    <simpleContent>
              <extension base="anyURI">
                     <attribute ref="xml:lang" use="required"/>
              </extension>
       </simpleContent>
</complexType>
```

3.1.9 العناصر الجذور (الجذرية)

كل مرحلة من المعطيات الشرحية للغة SAML تشرح كياناً واحداً أوعدة كيانات. ويتعين في الحالة الأولى أن يكون العنصر الجذر هو <EntitiesDescriptor>، كما يتعين في الحالة الثانية أن يكون العنصر الجذر هو <EntitiesDescriptor>.

1.3.1.9 العنصر <EntitiesDescriptor>

يحتوي العنصر <EntityDescriptor> على المعطيات الشرحية لمجموعة من الكيانات مسماة اختيارياً من كيانات اللغة SAML. ويحتوي نمطها المعقد **EntitiesDescriptorType** على تتابع من العناصر <EntityDescriptor> أو من العناصر <EntitiesDescriptor> أو من كلا النوعين:

- **ID** [اختياري]

  معرف هوية وحيد للعنصر في كل وثيقة، يستخدم عادة كنقطة مرجعية عند التوقيع.

- **validUntil** [اختياري]

  نعت اختياري يدل على موعد انقضاء الصلاحية للمعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- **cacheDuration** [اختياري]

  نعت اختياري يدل على المهلة الزمنية العظمى التي ينبغي للمستهلك أن يضع أثناءها في ذاكرة مخبأ، المعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- **Name** [اختياري]

  اسم سلسلة يعرف هوية مجموعة من كيانات اللغة SAML في سياق أحد التطورات.

- **<ds:Signature>** [اختياري]

  توقيع في اللغة XML يستيقن العنصر الحاوي ومحتوياته، كما هو مشروح في البند 8.

- **<Extensions>** [اختياري]

  يحتوي على توسّعات اختيارية من المعطيات الشرحية، متفق عليها بين ناشر المعطيات الشرحية ومستهلكها. ويتعين على عناصر التوسّع أن تكون موصوفة بمكان اسم بواسطة مكان اسم ليس معرفاً في اللغة SAML.

- **<EntitiesDescriptor>** أو **<EntityDescriptor>** [واحد أو أكثر]

  يحتوي على المعطيات الشرحية لكيان واحد أو أكثر في اللغة SAML، أو على مجموعة مبيتة من المعطيات الشرحية الإضافية.

وعندما يكون هذا العنصر مستعملاً كعنصر جذر لمرحلة من المعطيات الشرحية، يتعين عليه أن يحتوي على أي واحد من النعتين validUntil أو cacheDuration. ويوصى بألا يحتوي على أحد النعتين إلا العنصر الجذر من مرحلة من المعطيات الشرحية.

والقطعة التالية من التخطيطة تعرف العنصر <EntityDescriptor> ونمطه المعقد **EntitiesDescriptorType**:

```
<element name="EntitiesDescriptor" type="md:EntitiesDescriptorType"/>
<complexType name="EntitiesDescriptorType">
      <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <choice minOccurs="1" maxOccurs="unbounded">
                  <element ref="md:EntityDescriptor"/>
                  <element ref="md:EntitiesDescriptor"/>
            </choice>
      </sequence>
      <attribute name="validUntil" type="dateTime" use="optional"/>
      <attribute name="cacheDuration" type="duration" use="optional"/>
      <attribute name="ID" type="ID" use="optional"/>
      <attribute name="Name" type="string" use="optional"/>
</complexType>
<element name="Extensions" type="md:ExtensionsType"/>
<complexType final="#all" name="ExtensionsType">
      <sequence>
            <any namespace="##other" processContents="lax"
maxOccurs="unbounded"/>
      </sequence>
</complexType>
```

2.3.1.9 العنصر <EntitiyDescriptor>

يحدد العنصر <EntityDescriptor> المعطيات الشرحية لكيان واحد في اللغة SAML. ويمكن للعنصر الواجد أن يلعب في عدة أدوار مختلفة معتمدة في جانبيات متعددة. وتؤيد هذه التوصية مباشرة الأدوار المحسوسة التالية وكذلك العنصر المجرد <RoleDescriptor> من أجل التوسّعية:

- مزود هوية باكتتاب التوقيع الوحيد (SSO)؛
- مزود خدمة باكتتاب التوقيع الوحيد (SSO)؛
- سلطة استيقان؛
- سلطة نعت؛
- نقطة قرار سياسي؛
- انتساب.

ويتكون نمطه المعقد **EntityDescriptorType** من العناصر والنعوت التالية:

– entityID [مطلوب]

يحدد معرف الهوية الوحيد لكيان اللغة SAML المشروحة معطياته الشرحية في محتويات العنصر.

– ID [اختياري]

معرف هوية وحيد للعنصر في كل وثيقة، يستخدم عادة كنقطة مرجعية عند التوقيع.

– validUntil [اختياري]

نعت اختياري يدل على موعد انتهاء الصلاحية للمعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- cacheDuration [اختياري]

نعت اختياري يدل على المهلة الزمنية العظمى التي ينبغي للمستهلك أن يضع أثناءها في ذاكرة مخبأ، المعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- <ds:Signature> [اختياري]

توقيع في اللغة XML يستيقن العنصر الحاوي ومحتوياته.

- <Extensions> [اختياري]

يحتوي على توسّعات اختيارية من المعطيات الشرحية، متفق عليها بين ناشر المعطيات الشرحية ومستهلكها. ويتعين على عناصر التوسّع أن تكون موصوفة بمكان اسم بواسطة مكان اسم غير معرف في اللغة SAML.

- <RoleDescriptor> أو <IDPSSODescriptor> أو <SPSSODescriptor> أو <AuthnAuthorityDescriptor> أو <AttributeAuthorityDescriptor> أو <PDPDescriptor> [واحد أو أكثر] أو

- <AffiliationDescriptor> [مطلوب]

المحتوى الأساسي للعنصر هو إما تتابع من عنصر أو أكثر من عناصر واصف الدور، وإما واصف متخصص يعرف انتساباً.

- <Organization> [اختياري]

عنصر اختياري يعرف هوية المنظمة المسؤولة عن كيان اللغة SAML الذي يصفه العنصر.

- <ContactPerson> [صفر أو أكثر]

تتابع اختياري من العناصر يعرف هوية أنواع مختلفة من الاتصالات الشخصية.

- <AdditionalMetadataLocation> [صفر أو أكثر]

تتابع اختياري من المواقع الموصوفة بأمكنة الأسماء، حيث توجد معطيات شرحية إضافية خاصة بكيان اللغة SAML. وقد يشتمل ذلك على معطيات شرحية بأنساق بديلة أو تصف الانتماء إلى توصيات أخرى ليست من اللغة SAML.

كما يمكن أن ترد أيضاً نعوت اعتباطية موصوفة بأمكان الأسماء عن طريق أماكن أسماء ليست معرفة في اللغة SAML.

وعندما يكون هذا العنصر مستعملاً كعنصر جذر لمرحلة من المعطيات الشرحية، يتعين عليه أن يحتوي على واحد من النعتين validUntil أو cacheDuration. ويوصى بألا يحتوي على أحد النعتين إلا العنصر الجذر من مرحلة المعطيات الشرحية.

ويوصى عند ظهور عناصر عديدة من واصف الدور للنمط نفسه، ألا تتقاسم قيماً متشابكة من protocolSupportEnumeration، غير أن جانبيات للمعطيات الشرحية يمكن أن تحدد الانتقاء، ربما من خلال استعمال نعوت توسّعية أخرى مميزة.

والقطعة التالية من التخطيطة تعرف العنصر <EntityDescriptor> ونمطه المعقد **EntityDescriptorType**:

```
<element name="EntityDescriptor" type="md:EntityDescriptorType"/>
<complexType name="EntityDescriptorType">
      <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <choice>
```

```
                        <choice maxOccurs="unbounded">
                                <element ref="md:RoleDescriptor"/>
                                <element ref="md:IDPSSODescriptor"/>
                                <element ref="md:SPSSODescriptor"/>
                                <element ref="md:AuthnAuthorityDescriptor"/>
                                <element
ref="md:AttributeAuthorityDescriptor"/>
                                <element ref="md:PDPDescriptor"/>
                        </choice>
                        <element ref="md:AffiliationDescriptor"/>
                </choice>
                <element ref="md:Organization" minOccurs="0"/>
                <element ref="md:ContactPerson" minOccurs="0"
maxOccurs="unbounded"/>
                <element ref="md:AdditionalMetadataLocation" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="entityID" type="md:entityIDType" use="required"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="ID" type="ID" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

1.2.3.1.9 العنصر <Organization>

يحدد العنصر <Organization> المعلومات الأساسية عن المنظمة المسؤولة عن كيان أو دور في اللغة SAML. واستعمال هذا العنصر هو اختياري دائماً. ومحتواه إعلامي بطبيعته ولا يقابل مباشرة أي عنصر أو نعت مركزي في اللغة SAML. ويتكون نمطه المعقد **OrganizationType** من العناصر التالية:

- <Extensions> [اختياري]
يحتوي على توسّعات اختيارية من المعطيات الشرحية، متفق عليها بين ناشر المعطيات الشرحية ومستهلكها. ويتعين على التوسّعات ألا تشتمل على عناصر شاملة (غير موصوفة بأمكنة الأسماء) أو على عناصر يصفها مكان اسم معرف في اللغة SAML داخل هذا العنصر.

- <OrganizationName> [واحد أو أكثر]
اسم واحد أو عدة أسماء موصوفة في لغة مقروءة أو غير مقروءة من الإنسان.

- <OrganizationDisplayName> [واحد أو أكثر]
اسم واحد أو عدة أسماء موصوفة في لغة مقروءة من الإنسان.

- <OrganizationURL> [واحد أو أكثر]
معرف هوية URI واحد أو أكثر يحدد موقعاً يوجّه إليه المستعمل لمزيد من المعلومات. ويحيل واصف اللغة إلى محتوى الماديات في الموقع المحدد.

والقطعة التالية من التخطيطة تعرف العنصر <Organization> ونمطه المعقد **OrganizationType**:

```
<element name="Organization" type="md:OrganizationType"/>
<complexType name="OrganizationType">
 <sequence>
        <element ref="md:Extensions" minOccurs="0"/>
        <element ref="md:OrganizationName" maxOccurs="unbounded"/>
        <element ref="md:OrganizationDisplayName" maxOccurs="unbounded"/>
        <element ref="md:OrganizationURL" maxOccurs="unbounded"/>
 </sequence>
 <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<element name="OrganizationName" type="md:localizedNameType"/>
<element name="OrganizationDisplayName" type="md:localizedNameType"/>
<element name="OrganizationURL" type="md:localizedURIType"/>
```

2.2.3.1.9 العنصر <ContactPerson>

يحدد العنصر <ContactPerson> المعلومات الأساسية الخاصة بالاتصال حول شخص مسؤول إلى حد ما عن كيان أو دور في اللغة SAML. واستعمال هذا العنصر هو اختياري دائماً. ومحتواه إعلامي بطبيعته، ولا يقابل مباشرة أي عنصر أو نعت مركزي في اللغة SAML. ويتكون نمطه المعقد **ContactType** من العناصر والنعوت التالية:

- contactType [مطلوب]
يحدد نمط الاتصال الذي يستخدم تعداد النمط **ContactTypeType**. والقيم المحتملة هي تقانية (technical) وداعمة (support) وإدارية (administrative) وتسميرية (billing) وغيرها.

- <Extensions> [اختياري]
يحتوي على توسّعات اختيارية من المعطيات الشرحية، متفق عليها بين ناشر المعطيات الشرحية ومستهلكها. ويتعين على عناصر التوسّع أن تكون موصوفة بمكان ا سم عن طريق مكان اسم ليس معرفاً في اللغة SAML.

- <Company> [اختياري]
عنصر اختياري من سلسلة يحدد اسم شركة الشخص المطلوب الاتصال به.

- <GivenName> [اختياري]
عنصر اختياري من سلسلة يحدد الاسم (الأول) للشخص المطلوب الاتصال به.

- <SurName> [اختياري]
عنصر اختياري من سلسلة يحدد اسم العائلة (الكُنْية) للشخص المطلوب الاتصال به.

- <EmailAddress> [صفر أو أكثر]
صفر أو أكثر من العنصر التي تحتوي على بُرُد مرسلة إلى: معرفات URI تمثل عناوين البريد الإلكتروني التي تخص الشخص المطلوب الاتصال به.

- <TelephoneNumber> [صفر أو أكثر]
صفر أو أكثر من عناصر سلسلة تحدد رقم الهاتف للشخص المطلوب الاتصال به.

كما يمكن أن ترد أيضاً نعوت اعتباطية موصوفة بأمكنة أسماء عن طريق أمكنة أسماء ليست معرف في اللغة SAML.

والقطعة التالية من التخطيطة تعرف العنصر <ContactPerson> ونمطه المعقد **ContactType**:

```
<element name="ContactPerson" type="md:ContactType"/>
<complexType name="ContactType">
       <sequence>
              <element ref="md:Extensions" minOccurs="0"/>
              <element ref="md:Company" minOccurs="0"/>
              <element ref="md:GivenName" minOccurs="0"/>
              <element ref="md:SurName" minOccurs="0"/>
              <element ref="md:EmailAddress" minOccurs="0"
maxOccurs="unbounded"/>
              <element ref="md:TelephoneNumber" minOccurs="0"
maxOccurs="unbounded"/>
       </sequence>
       <attribute name="contactType" type="md:ContactTypeType"
use="required"/>
       <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<element name="Company" type="string"/>
<element name="GivenName" type="string"/>
<element name="SurName" type="string"/>
<element name="EmailAddress" type="anyURI"/>
<element name="TelephoneNumber" type="string"/>
<simpleType name="ContactTypeType">
```

```
      <restriction base="string">
            <enumeration value="technical"/>
            <enumeration value="support"/>
            <enumeration value="administrative"/>
            <enumeration value="billing"/>
            <enumeration value="other"/>
      </restriction>
</simpleType>
```

3.2.3.1.9 العنصر <AdditionalMetadataLocation>

العنصر <AdditionalMetadataLocation> هو معرف URI لمكان اسم معرف، يحدد أين يمكن أن توجد معطيات شرحية إضافية مبنية على اللغة XML وتخص كياناً في اللغة SAML. ونمطه المعقد **AdditionalMetadataLocationType** يوسع النمط **anyURI** بنعت لمكان اسم (هو أيضاً من النمط **anyURI**). ويتعين على هذا النعت المطلوب أن يحتوي على مكان الاسم في اللغة XML الخاص بالعنصر الجذر من وثيقة المرحلة التي توجد في الموقع المحدد.

والقطعة التالية من التخطيطة تعرف العنصر <AdditionalMetadataLocation> ونمطه المعقد **AdditionalMetadataLocationType**:

```
<element name="AdditionalMetadataLocation"
type="md:AdditionalMetadataLocationType"/>
<complexType name="AdditionalMetadataLocationType">
      <simpleContent>
            <extension base="anyURI">
                  <attribute name="namespace" type="anyURI"
use="required"/>
            </extension>
      </simpleContent>
</complexType>
```

4.1.9 عناصر واصف الدور

تشكل عناصر هذه الفقرة الفرعية إجمالي المكونات التشغيلية لاعتماد المعطيات الشرحية. وكل عنصر (ما عدا العنصر المجرد) يعرف جملة محددة من أنواع السلوك التشغيلية دعماً لجانبيات اللغة SAML.

1.4.1.9 العنصر <RoleDescriptor>

العنصر <RoleDescriptor> هو نقطة توسّع مجردة، تحتوي على معلومات وصفية عامة مهيأة لتوفير معالجة موحّدة للإدوار المختلفة. ويمكن تعريف أدوار جديدة بتوسيع نمطها المعقد المجرد **RoleDescriptorType** الذي يضم العناصر والنعوت التالية:

- ID [اختياري]

  معرف هوية وحيد للعنصر في كل وثيقة، ويستخدم عادة كنقطة مرجعية عند التوقيع.

- validUntil [اختياري]

  نعت اختياري يدل على موعد انتهاء الصلاحية للمعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- cacheDuration [اختياري]

  نعت اختياري يدل على المهلة الزمنية العظمى التي ينبغي للمستهلك أن يضع أثناءها في ذاكرة مخبأ، المعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- protocolSupportEnumeration [مطلوب]

مجموعة من المعرفات URI تفصل بينها فراغات بيضاء، تعرف مجموعة مواصفات البروتوكول التي يعتمدها عنصر الدور. وفيما يخص الصيغة V2.0 من اللغة SAMLن يتعين على هذه المجموعة أن تشتمل على المعرف URI لمكان الاسم في بروتوكول اللغة SAML: urn:oasis:names:tc:SAML:2.0:protocol. والتوصيات اللاحقة في اللغة SAML تتقاسم نفس المعرف URI لمكان الاسم، ولكنها ينبغي أن توفر معرفات هوية بديلة "لاعتماد البروتوكول"، حتى يتأمن التمييز عند اللزوم.

- errorURL [اختياري]

نعت اختياري للمعرف URI يحدد موقعاً يتجه إليه من أجل حل المشاكل والدعم الإضافي المتعلقة بهذا الدور.

- <ds:Signature> [اختياري]

توقيع في اللغة XML يستيقن العنصر الحاوي ومحتوياته.

- <Extensions> [اختياري]

يحتوي على توسّعات اختيارية من المعطيات الشرحية، متفق عليها بين ناشر المعطيات الشرحية ومستهلكها. ويتعين على عناصر التوسّع أن تكون موصوفة بمكان اسم بواسطة مكان اسم ليس معرفاً في اللغة SAML.

- <KeyDescriptor> [صفر أو أكثر]

تتابع اختياري من العناصر يقدم معلومات عن مفاتيح التجفير التي يستخدمها المستعمل عندما يقوم بهذا الدور؟

- <Organization> [اختياري]

عنصر اختياري يحدد المنظمة التي تصحب هذا الدور. وهو مطابق للعنصر المستعمل داخل العنصر.

- <ContactPerson> [صفر أو أكثر]

تتابع اختياري من العنصر يحدد الاتصالات التي تصحب هذا الدور. وهو مطابق للعنصر المستعمل داخل العنصر <EntityDescriptor>.

كما يمكن أن ترد أيضاً نعوت اعتباطية موصوفة بأمكنة أسماء عن طريق أمكنة أسماء ليست معرفة في اللغة SAML.

والقطعة التالية من التخطيطة تعرّف العنصر <RoleDescriptor> ونمطه المعقد **RoleDescriptorType**:

```
<element name="RoleDescriptor" type="md:RoleDescriptorType"/>
<complexType name="RoleDescriptorType" abstract="true">
      <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:KeyDescriptor" minOccurs="0"
maxOccurs="unbounded"/>
            <element ref="md:Organization" minOccurs="0"/>
            <element ref="md:ContactPerson" minOccurs="0"
maxOccurs="unbounded"/>
      </sequence>
      <attribute name="ID" type="ID" use="optional"/>
      <attribute name="validUntil" type="dateTime" use="optional"/>
      <attribute name="cacheDuration" type="duration" use="optional"/>
      <attribute name="protocolSupportEnumeration"
type="md:anyURIListType" use="required"/>
      <attribute name="errorURL" type="anyURI" use="optional"/>
      <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<simpleType name="anyURIListType">
      <list itemType="anyURI"/>
</simpleType>
```

1.1.4.1.9 العنصر <KeyDescriptor>

يقدم العنصر <KeyDescriptor> معلومات عن مفتاح (مفاتيح) التجفير، الذي يستخدمه كيان ما للتوقيع على المعطيات أو لاستلام مفاتيح مجفرة، ومعها تفاصيل تجفيرية إضافية. ويتكون نمطه المعقد من العناصر والنعوت التالية:

- use [اختياري]
نعت إضافي يحدد الغرض من وصف المفتاح. وقيمه مأخوذة من تعداد الأنماط **KeyTypes** وهما قيمتا encryption وsigning.

- <ds:KeyInfo> [مطلوب]
عنصر اختياري يعرّف هوية مفتاح تعريفاً مباشراً وغير مباشر. انظر التوقيع في اللغة XML التابع للتجمع W3C لمزيد من التفاصيل عن استخدام هذا العنصر.

- <EncryptionMethod> [صفر أو أكثر]
عنصر اختياري يحدد خوارزمية وعمليات الضبط الخاصة بالخوارزمية التي يعتمدها كيان ما. والمحتوى المضبوط يتغير استناداً إلى الخوارزمية المعتمدة. انظر تجفير التجمع W3C من أجل تعريف النمط المعقد **xenc:EncryptionMethodType** لهذا العنصر.

والقطعة التالية من التخطيطة تعرف العنصر <KeyDescriptor> ونمطه المعقد **KeyDescriptorType**:

```
<element name="KeyDescriptor" type="md:KeyDescriptorType"/>
<complexType name="KeyDescriptorType">
    <sequence>
        <element ref="ds:KeyInfo"/>
        <element ref="md:EncryptionMethod" minOccurs="0"
maxOccurs="unbounded"/>
    </sequence>
    <attribute name="use" type="md:KeyTypes" use="optional"/>
</complexType>
<simpleType name="KeyTypes">
    <restriction base="string">
        <enumeration value="encryption"/>
        <enumeration value="signing"/>
    </restriction>
</simpleType>
<element name="EncryptionMethod" type="xenc:EncryptionMethodType"/>
```

2.4.1.9 النمط المعقد SSODescriptorType

النمط المجرد **SSODescriptorType** هو نمط أساسي مشترك للنمطين المحسوسين **SPSSODescriptorType** و**IDPSSODescriptorType** المشروحين في البنود اللاحقة. وهو يوسّع النمط **RoleDescriptorType** بالعناصر التي تعكس الجانبيات المشتركة لكلا نوعي مزودي الهوية ومزودي الخدمة الذين يعتمدون اكتتاب التوقيع (SSO)، وهو يحتوي على العناصر الإضافية التالية:

- <ArtifactResolutionService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **IndexedEndpointType** التي تصف النقاط النهائية المفهرسة التي تعتمد جانبية استبانة الشيء المصطنع المعرفة في البند 12. ويجب حذف النعت ResponseLocation.

- <SingleLogoutService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndPointType** التي تصف النقاط النهائية التي تدعم جانبيات اختتام الدورة الوحيد المعرف في البند 12.

- <ManageNameIDService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndPointType** التي تصف النقاط النهائية التي تدعم جانبيات إدارة معرف هوية الاسم المعرفة في البند 12.

- <NameIDFormat> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **anyURI** التي تعدد أنساق معرف هوية الاسم المدعومة من كيان النظام هذا الذي يؤدي هذا الدور.

والقطعة التالية من التخطيطة تعرف النمط المعقد **SSODescriptorType**:

```
<complexType name="SSODescriptorType" abstract="true">
       <complexContent>
              <extension base="md:RoleDescriptorType">
                     <sequence>
                            <element ref="md:ArtifactResolutionService"
minOccurs="0" maxOccurs="unbounded"/>
                            <element ref="md:SingleLogoutService"
minOccurs="0" maxOccurs="unbounded"/>
                            <element ref="md:ManageNameIDService"
minOccurs="0" maxOccurs="unbounded"/>
                            <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                     </sequence>
              </extension>
       </complexContent>
</complexType>
<element name="ArtifactResolutionService" type="md:IndexedEndpointType"/>
<element name="SingleLogoutService" type="md:EndpointType"/>
<element name="ManageNameIDService" type="md:EndpointType"/>
<element name="NameIDFormat" type="anyURI"/>
```

3.4.1.9 العنصر <IDPSSODescriptor>

العنصر <IDPSSODescriptor> يوسّع النمط **SSODescriptorType** بمحتوى يعكس الجانبيات الخاصة بمزودي الهوية الذين يعتمدون اكتتاب التوقيع الوحيد (SSO). ويضم نمطه المعقد **IDPSSODescriptorType** العناصر والنعوت الإضافية التالية:

- WantAuthnRequestsSigned [اختياري]
نعت اختياري يدل على المطلب الذي يقضي بالتوقيع على الرسائل <samlp:AuthnRequest> التي يستلمها هذا المزود للهوية. وإذا كان محذوفاً يفترض في القيمة أن تكون "خاطئة".

- <SingleSignOnService> [واحد أو أكثر]
عنصر واحد أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبيات بروتوكول طلب الاستيقان المعرفة في البند 12. وجميع مزودي الخدمة يدعمون بالتعريف، واحدة على الأقل في مثل هذه النقاط الانتهائية. ويتعين حذف النعت ResponseLocation.

- <NameIDMappingService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية تقابل معرفات هوية الاسم المعرفة في البند 12. ويتعين حذف النعت ResponseLocation.

- <AssertionIDRequestService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول طلب التأكيد أو رابطة المعرف URI الخاصة بطلبات التأكيد، المعرفة في البند 10.

الملاحظة 1 (للاطّلاع) – يقترح PE33 (انظر OASIS PE:2006) أن يستعاض عن بروتوكول طلب التأكيد بطلب التأكيد و/أو الاستفهام عنه.

– <AttributeProfile> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **anyURI** التي تعدد جانبيات النعت التي يدعمها هذا المزود للهوية.

– <saml:Attribute> [صفر أو أكثر]
صفر أو أكثر من العناصر التي تعرف هوية نعوت اللغة SAML التي يدعمها مزود الهوية. ويمكن اختيارياً إيراد قيمة معينة، للدلالة على أن فقط بعض القيم التي يسمح بها تعريف النعت هي مدعومة. وفي هذا السياق، فإن كلمة "يدعم" الخاصة بنتع تعني أن لمزوّد الهوية القدرة على إيرادها عند تسليم التأكيدات أثناء اكتتاب التوقيع الوحيد.

ملاحظة 2 (للاطّلاع) – يقترح PE7 (انظر OASIS PE:2006) أن يضاف النص التالي إلى نهاية الفقرة أعلاه.

إن النعت WantAuthnRequestsSigned أعدّ ليبين لمزوّدي الخدمة عما إذا كانوا يتوقعون أم لا أن يتقبل مزوّد الهوية رسالة <AuthnRequest> غير موقّعة. وليس مزود الهوية ملزماً برفض الطلبات غير الموقّعة، كما وليس مزوّد الخدمة ملزماً بالتوقيع على طلباته، وإن كان عليه أن يتوقع بكل عقلانية إمكانية رفض طلب غير موقّع. وقد لا يكون لمزود الخدمة، في بعض الحالات، حتى أن يعرف أي مزوّد هوية سيستلم في نهاية المطاف طلباته ويجيب عليها، لذلك فإن استعمال مثل هذا النعت في مثل هذه الحالة لا يمكن تحديده بالضبط. وتجدر الملاحظة فوق ذلك إلى أن الطريقة المحددة للتوقيع التي يمكن توقّعها تتوقف على الرابطة. فرابطة البروتوكول HTTP المعاد توجيهه الموجودة في الفقرة الفرعية 4.2.10 تتطلب أن يطبق التوقيع على قيمة محدد الموقع URL المشفّر، بدلاً من أن يوضع داخل رسالة في اللغة XML، بينما تسمح روابط أخرى بأن يوضع التوقيع داخل الرسالة بصورة عادية.

والقطعة التالية من التخطيطة تعرف العنصر <IDPSSODescriptor> ونمطه المعقد **IDPSSODescriptorType**.

```
<element name="IDPSSODescriptor" type="md:IDPSSODescriptorType"/>
<complexType name="IDPSSODescriptorType">
      <complexContent>
            <extension base="md:SSODescriptorType">
                  <sequence>
                        <element ref="md:SingleSignOnService"
maxOccurs="unbounded"/>
                        <element ref="md:NameIDMappingService"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="md:AssertionIDRequestService"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="md:AttributeProfile"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
                  </sequence>
                  <attribute name="WantAuthnRequestsSigned"
type="boolean" use="optional"/>
            </extension>
      </complexContent>
</complexType>
<element name="SingleSignOnService" type="md:EndpointType"/>
<element name="NameIDMappingService" type="md:EndpointType"/>
<element name="AssertionIDRequestService" type="md:EndpointType"/>
<element name="AttributeProfile" type="anyURI"/>
```

4.4.1.9 العنصر <SPSSODescriptor>

العنصر <SPSSODescriptor> يوسّع النمط **SSODescriptorType** بمحتوى يعكس الجانبيات الخاصة بمزوّدي الخدمة. ويحتوي نمطه المعقد **SPSSODescriptorType** على العناصر والنعوت التالية:

- AuthnRequestsSigned [اختياري]

نعت اختياري يبين إن كانت الرسائل <samlp:AuthnRequest> التي يرسلها هذا المزوّد للخدمة، سوف توقّع. وإذا كان محذوفاً يفترض في القيمة أن تكون "خاطئة".

ملاحظة 1 (للاطّلاع) – يقترح PE7 (انظر OASIS PE:2006) أن يضاف النص التالي إلى نهاية الفقرة أعلاه:

إن قيمة "خاطئة" (أو حذف هذا النعت) لا تنطوي على أن مزوّد الخدمة لن يوقّع أبداً على طلباته أو أن طلباً موقعاً ينبغي اعتباره خطأ. ومع ذلك يتعين على مزوّد الهوية الذي يستلم رسالة <samlp:AuthnRequest> غير موقعة، من مزوّد خدمة تحتوي معطياته الشرحية هذا النعت بقيمة "صائبة"، أن يرجع استجابة خطأ في اللغة SAML، ويتعين عليه ألا يلبي الطلب.

- WantAssertionsSigned [اختياري]

نعت اختياري يدل على المطلب الذي يقضي بالتوقيع على العناصر <saml:Assertion> التي يستلمها هذا المزوّد للخدمة، وإذا كان محذوفاً، يفترض أن تكون القيمة "خاطئة". ويضاف هذا المطلب إلى أي مطلب للتوقيع مستنتج من استعمال تجميعة خاصة من الجانبيات/الروابط.

ملاحظة 2 (للاطّلاع) – يقترح PE7 (انظر OASIS PE:2006) أن يضاف النص التالي إلى نهاية الفقرة أعلاه.

يلاحظ أن توقيعاً مغلفاً في رابطة اللغة SAML أو في طبقة البروتوكول لا يكفي لاستيفاء هذا المطلب، كأن توقّع استجابة <samlp:Response> تحتوي على تأكيد (تأكيدات) أو على توصيل بروتوكول الأمن TLS.

- <AssertionConsumerService> [واحد أو أكثر]

عنصر واحد أو أكثر من العناصر التي توصّف النقاط النهائية التي تدعم جانبيات بروتوكول طلب الاستيقان المعرّفة في هذه التوصية. وجميع مزودي الخدمة يدعمون بالتعريف نقطة نهائية واحدة من هذا النوع.

- <AttributeConsumingService> [صفر أو أكثر]

صفر أو أكثر من العناصر التي تصف تطبيقاً أو خدمة يقدمها مزوّد خدمة يتطلب أو يرغب في استعمال نعوت اللغة SAML.

ويمكن لعنصر <AttributeConsumingService> واحد على الأكثر، أن يكون له النعت isDefault موضوعاً على "صائب". وليس مسموحاً لأي واحد من العناصر الواردة أن يحتوي على النعت isDefault موضوعاً على "صائب".

والقطعة التالية من التخطيطة تعرّف العنصر <SPSSODescriptor> ونمطه المعقد **SPSSODescriptorType**:

```
<element name="SPSSODescriptor" type="md:SPSSODescriptorType"/>
<complexType name="SPSSODescriptorType">
       <complexContent>
              <extension base="md:SSODescriptorType">
                     <sequence>
                            <element ref="md:AssertionConsumerService"
maxOccurs="unbounded"/>
                            <element ref="md:AttributeConsumingService"
minOccurs="0" maxOccurs="unbounded"/>
                     </sequence>
                     <attribute name="AuthnRequestsSigned" type="boolean"
use="optional"/>
                     <attribute name="WantAssertionsSigned" type="boolean"
use="optional"/>
              </extension>
       </complexContent>
</complexType>
<element name="AssertionConsumerService" type="md:IndexedEndpointType"/>
```

1.4.4.1.9 العنصر <AttributeConsumingService>

يعرّف العنصر <AttributeConsumingService> خدمة خاصة يقدمها مزوّد الخدمة بصيغة نعوت تتطلبها الخدمة أو ترغب فيها. ويحتوي نمطها المعقد **AttributeConsumingServiceType** على العناصر والنعوت التالية:

- index [مطلوب]
نعت مطلوب لكي يسند قيمة صحيحة وحيدة للعنصر، بحيث يمكن الرجوع إليه في رسالة بروتوكول.

- isDefault [اختياري]
يعرّف بالتغيب الخدمة التي يدعمها مزوّد الخدمة. وهو مفيد إذا لم تكن الخدمة المعنية مبينة في سياق التطبيق. وإذا كان مخدوماً، يفترض في القيمة أن تكون "خاطئة".

- <ServiceName> [واحد أو أكثر]
اسم واحد أو أكثر من الأسماء الموصوفة باللغة للخدمة.

- <ServiceDescription> [صفر أو أكثر]
صفر أو أكثر من السلاسل الموصوفة باللغة لكي تصف الخدمة.

- <RequestedAttribute> [واحد أو أكثر]
عنصر واحد أو أكثر من العناصر التي تحدد النعت الذي تتطلبه الخدمة أو ترغب فيه.

والقطعة التالية من التخطيطة تعرّف العنصر <AttributeConsumingService> ونمطه المعقد **AttributeConsumingServiceType**:

```
<element name="AttributeConsumingService"
type="md:AttributeConsumingServiceType"/>
<complexType name="AttributeConsumingServiceType">
      <sequence>
            <element ref="md:ServiceName" maxOccurs="unbounded"/>
            <element ref="md:ServiceDescription" minOccurs="0"
maxOccurs="unbounded"/>
            <element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
      </sequence>
      <attribute name="index" type="unsignedShort" use="required"/>
      <attribute name="isDefault" type="boolean" use="optional"/>
</complexType>
<element name="ServiceName" type="md:localizedNameType"/>
<element name="ServiceDescription" type="md:localizedNameType"/>
```

2.4.4.1.9 العنصر <RequestedAttribute>

يحدد العنصر <RequestedAttribute> فائدة مزوّد خدمة من نعت معين في اللغة SAML، يشمل بصورة اختيارية قيماً معينة. ونمطه المعقد **RequestedAttributeType** يوسّع النمط **saml:AttributeType** بالنعت التالي:

- isRequired [اختياري]
نعت اختياري في اللغة XML يبين إن كانت الخدمة تتطلب المقابل في اللغة SAML لكي تعمل (كمقابل لإيجاد نعت بكل بساطة يكون مفيداً أو مرغوباً فيه).

وإذا كانت العناصر <saml:AttributeValue> واردة، فلا تكون إلا القيم الموائمة هي القيم ذات الصلة بالخدمة.

والقطعة التالية من التخطيطة تعرّف العنصر <RequestedAttribute> ونمطه المعقد **RequestedAttributeType**:

```
<element name="RequestedAttribute" type="md:RequestedAttributeType"/>
<complexType name="RequestedAttributeType">
      <complexContent>
            <extension base="saml:AttributeType">
                  <attribute name="isRequired" type="boolean"
use="optional"/>
            </extension>
      </complexContent>
</complexType>
```

5.4.1.9 العنصر <AuthnAuthorityDescriptor>

العنصر <AuthnAuthorityDescriptor> يوسّع النمط **RoleDescriptorType** بمحتوى يعكس الجانبيات الخاصة بسلطات الاستيقان، وهي سلطات في اللغة SAML تستجيب للرسائل <samlp:AuthnQuery>. ويحتوي نمطه المعقد **AuthnAuthorityDescriptorType** على العناصر الإضافية التالية:

- <AuthnQueryService> [واحد أو أكثر]
عنصر واحد أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول الاستفهام عن الاستيقان المعرّفة في البند 12. وجميع سلطات الاستيقان تدعم بالتعريف نقطة نهائية واحدة على الأقل من هذا النوع.

- <AssertionIDRequestService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول طلب التأكيد المعرفة في البند 12، أو رابطة المعرف URI الخاصة بطلبات التأكيد المعرفة في البند 10.

- <NameIDFormat> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **anyURI** التي تعدد أنساق معرف هوية الاسم التي تدعمها هذه السلطة (انظر الفقرة الفرعية 3.7.8 القيم المحتملة لهذا العنصر).

والقطعة التالية من التخطيطة تعرف العنصر <PDPDescriptor> ونمطه المعقد **PDPDescriptorType**:

```
<element name="PDPDescriptor" type="md:PDPDescriptorType"/>
<complexType name="PDPDescriptorType">
      <complexContent>
            <extension base="md:RoleDescriptorType">
                  <sequence>
                        <element ref="md:AuthzService"
maxOccurs="unbounded"/>
                        <element ref="md:AssertionIDRequestService"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
<element name="AuthzService" type="md:EndpointType"/>
```

6.4.1.9 العنصر <PDPDescriptor>

العنصر <PDPDescriptor> يوسّع النمط **RoleDescriptorType** بمحتوى يعكس الجانبيات الخاصة بنقاط قرار سياسي، وهي سلطات في اللغة SAML تستجيب للرسائل <samlp:AuthzDecisionQuery>. ونمطه المعقد **PDPDescriptorType** يحتوي على العناصر الإضافية التالية:

- <AuthzService> [واحد أو أكثر]
عنصر واحد أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول الاستفهام عن قرار الترخيص المعرفة في البند 12. وجميع نقاط القرار السياسي تدعم بالتعريف، واحدة على الأقل من مثل هذه النقاط النهائية.

- <AuthzService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول طلب التأكيد المعرفة في البند 12 أو رابطة المعرف URI الخاصة بطلبات التأكيد المعرفة في البند 10.

ملاحظة (للاطّلاع) – يقترح PE33 (انظر OASIS PE:2006) أن يستعاض عن بروتوكول طلب التأكيد بطلب التأكيد و/أو الاستفهام عنه.

- <NameIDFormat> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **anyURI** التي تعدد أنساق معرف هوية الاسم التي تدعمها هذه السلطة (انظر الفقرة الفرعية 3.7.8 بعض القيم المحتملة لهذا العنصر).

والقطعة التالية من التخطيطة تعرّف العنصر <PDPDescriptor> ونمطه المعقد **PDPDescriptorType**:

```
<element name="PDPDescriptor" type="md:PDPDescriptorType"/>
<complexType name="PDPDescriptorType">
      <complexContent>
            <extension base="md:RoleDescriptorType">
                  <sequence>
                        <element ref="md:AuthzService"
maxOccurs="unbounded"/>
                        <element ref="md:AssertionIDRequestService"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
<element name="AuthzService" type="md:EndpointType"/>
```

7.4.1.9 العنصر <AttributeAuthorityDescriptor>

العنصر <AttributeAuthorityDescriptor> يوسّع النمط **RoleDescriptorType** بمحتوى يعكس جانبيات خاصة بسلطات النعت، وهي سلطات في اللغة SAML تستجيب للرسائل <samlp:AttributeQuery>. ونمطه المعقد **AttributeAuthorityDescriptorType** يحتوي على العناصر الإضافية التالية:

- <AttributeService> [واحد أو أكثر]
عنصر واحد أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول الاستفهام عن نعت المعرفة في البند 12. وجميع سلطات النعت تدعم بالتعريف، واحدة على الأقل من مثل هذه النقاط النهائية.

- <AssertionIDRequestService> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **EndpointType** التي تصف النقاط النهائية التي تدعم جانبية بروتوكول طلب التأكيد المعرفة في البند 12 أو رابطة المعرّف URI الخاصة بطلبات التأكيد المعرفة في البند 10.

ملاحظة (للاطّلاع) – يقترح PE33 (انظر OASIS PE:2006) أن يستعاض عن بروتوكول طلب التأكيد بطلب التأكيد و/أو الاستفهام عنه.

- <NameIDFormat> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **anyURI** التي تعدد أنساق معرف هوية الاسم التي تدعمها هذه السلطة (انظر الفقرة الفرعية 3.7.8 بعض القيم المحتملة لهذا العنصر).

- <AttributeProfile> [صفر أو أكثر]
صفر أو أكثر من عناصر النمط **anyURI** التي تعدد جانبيات النعت التي تدعمها هذه السلطة (انظر الفقرة الفرعية 3.7.8 بعض القيم المحتملة لهذا العنصر).

- <saml:Attribute> [صفر أو أكثر]
صفر أو أكثر من العناصر التي تعرف هوية نعوت اللغة SAML التي تدعمها السلطة. ويمكن أن تدرج اختيارياً بعض القيم المعينة، لتدل على أن فقط بعض القيم التي يسمح بها تعريف النعت تكون مدعومة.

والقطعة التالية من التخطيطة تعرف العنصر <AttributeAuthorityDescriptor> ونمطه المعقد **AttributeAuthorityDescriptorType**:

```
<element name="AttributeAuthorityDescriptor"
type="md:AttributeAuthorityDescriptorType"/>
<complexType name="AttributeAuthorityDescriptorType">
      <complexContent>
            <extension base="md:RoleDescriptorType">
                  <sequence>
                        <element ref="md:AttributeService"
maxOccurs="unbounded"/>
                        <element ref="md:AssertionIDRequestService"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                        <element ref="md:AttributeProfile"
minOccurs="0" maxOccurs="unbounded"/>
                        <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
                  </sequence>
            </extension>
      </complexContent>
</complexType>
<element name="AttributeService" type="md:EndpointType"/>
```

5.1.9 العنصر <AffiliationDescriptor>

العنصر <AffiliationDescriptor> هو بديل من تتابع واصفات الدور الذي يستعمل عندما يصف العنصر <EntityDescriptor> جماعة منتسبة من كيانات اللغة SAML (عادة من مزوّدي الخدمة) بدلاً من كيان وحيد. ويقدم العنصر <AffiliationDescriptor> موجزاً عن الكيانات المنفردة التي تكوّن الجماعة المنتسبة مع معلومات عامة عن الجماعة المنتسبة نفسها. ويحتوي نمطه المعقد **AffiliationDescriptorType** على العناصر والنعوت التالية:

- affiliationOwnerID [مطلوب]
يحدد معرف الهوية الوحيد للكيان المسؤول عن الجماعة المنتسبة. ولا يفترض أن يكون المالك عضواً في الجماعة المنتسبة، فإن كان عضواً فيها يتعين أن يظهر معرف هويته في العنصر <AffiliateMember>.

- ID [اختياري]
معرف هوية وحيد للعنصر في كل وثيقة، يستعمل عادة كنقطة مرجعية عند التوقيع.

- validUntil [اختياري]
نعت اختياري يدل على موعد انقضاء الصلاحية للمعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- cacheDuration [اختياري]
نعت اختياري يدل على المهلة الزمنية العظمى التي ينبغي للمستهلك أن يضع أثناءها في ذاكرة مخبأ، المعطيات الشرحية المحتواة في العنصر وفي كل عنصر محتوى.

- <ds:Signature> [اختياري]
توقيع في اللغة XML يستيقن العنصر الحاوي ومحتوياته (انظر البند 8).

- <Extensions> [اختياري]
يحتوي على توسّعات اختيارية من المعطيات الشرحية، متفق عليها بين ناشر المعطيات الشرحية ومستهلكها. ويتعين على عناصر التوسّع أن تكون موصوفة بمكان اسم بواسطة مكان اسم ليس معرفاً في اللغة SAML.

- <AffiliateMember> [واحد أو أكثر]
عنصر واحد أو أكثر من العناصر التي تعد من أعضاء جماعة المنتسبين، بتحديد معرف الهوية الوحيد لكل عضو (انظر أيضاً الفقرة الفرعية 6.3.7.8).

- <KeyDescriptor> [صفر أو أكثر]
تتابع اختياري من العناصر، يقدم معلومات عن مفاتيح التجفير التي تستخدمها جماعة المنتسبين ككل، تمييزاً لها عن المفاتيح التي يستعملها كل عضو في الجماعة المنتسبة بمفرده، وهي منشورة في المعطيات الشرحية لهذه الكيانات.

ويمكن أيضاً إيراد نعوت اعتباطية موصوفة بمكان الاسم بواسطة أمكنة أسماء ليست معرفة في اللغة SAML.

والقطعة التالية من التخطيطة تعرف العنصر <AffiliationDescriptor> ونمطه المعقد **AffiliationDescriptorType**:

```
<element name="AffiliationDescriptor"
type="md:AffiliationDescriptorType"/>
<complexType name="AffiliationDescriptorType">
      <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:AffiliateMember" maxOccurs="unbounded"/>
            <element ref="md:KeyDescriptor" minOccurs="0"
maxOccurs="unbounded"/>
      </sequence>
      <attribute name="affiliationOwnerID" type="md:entityIDType"
use="required"/>
      <attribute name="validUntil" type="dateTime" use="optional"/>
      <attribute name="cacheDuration" type="duration" use="optional"/>
      <attribute name="ID" type="ID" use="optional"/>
      <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
<element name="AffiliateMember" type="md:entityIDType"/>
```

6.1.9 أمثلة

المثال التالي هو مثال على معطيات شرحية لكيان في نظام في اللغة SAML يقوم بدور مزوّد هوية وسلطة نعت. وهناك توقيع أدرج كممسك بالموقع، من دون أي محتوى حقيقي.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```

```
      entityID="https://IdentityProvider.com/SAML">
      <ds:Signature>...</ds:Signature>
    <IDPSSODescriptor WantAuthnRequestsSigned="true"

      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:KeyName>IdentityProvider.com SSO Key</ds:KeyName>
            </ds:KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService isDefault="true" index="0"
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

      Location="https://IdentityProvider.com/SAML/Artifact"/>
        <SingleLogoutService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

      Location="https://IdentityProvider.com/SAML/SLO/SOAP"/>
        <SingleLogoutService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect"

      Location="https://IdentityProvider.com/SAML/SLO/Browser"

      ResponseLocation="https://IdentityProvider.com/SAML/SLO/Response"/>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
        </NameIDFormat>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </NameIDFormat>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <SingleSignOnService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect"

      Location="https://IdentityProvider.com/SAML/SSO/Browser"/>
        <SingleSignOnService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST"

      Location="https://IdentityProvider.com/SAML/SSO/Browser"/>
        <saml:Attribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                    FriendlyName="eduPersonPrincipalName">
        </saml:Attribute>
        <saml:Attribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
                    FriendlyName="eduPersonAffiliation">
            <saml:AttributeValue>member</saml:AttributeValue>
            <saml:AttributeValue>student</saml:AttributeValue>
            <saml:AttributeValue>faculty</saml:AttributeValue>
            <saml:AttributeValue>employee</saml:AttributeValue>
            <saml:AttributeValue>staff</saml:AttributeValue>
        </saml:Attribute>
    </IDPSSODescriptor>
    <AttributeAuthorityDescriptor

      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:KeyName>IdentityProvider.com AA Key</ds:KeyName>
            </ds:KeyInfo>
        </KeyDescriptor>
        <AttributeService
```

```
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

      Location="https://IdentityProvider.com/SAML/AA/SOAP"/>
        <AssertionIDRequestService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
                    Location="https://IdentityProvider.com/SAML/AA/URI"/>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
        </NameIDFormat>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
        </NameIDFormat>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <saml:Attribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                    FriendlyName="eduPersonPrincipalName">
        </saml:Attribute>
        <saml:Attribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
                    FriendlyName="eduPersonAffiliation">
            <saml:AttributeValue>member</saml:AttributeValue>
            <saml:AttributeValue>student</saml:AttributeValue>
            <saml:AttributeValue>faculty</saml:AttributeValue>
            <saml:AttributeValue>employee</saml:AttributeValue>
            <saml:AttributeValue>staff</saml:AttributeValue>
        </saml:Attribute>
    </AttributeAuthorityDescriptor>
    <Organization>
        <OrganizationName xml:lang="en">Identity Providers R
US</OrganizationName>
        <OrganizationDisplayName xml:lang="en">
              Identity Providers R US, a Division of Lerxst Corp.
        </OrganizationDisplayName>
        <OrganizationURL
xml:lang="en">https://IdentityProvider.com</OrganizationURL>
    </Organization>
</EntityDescriptor>
```

والمثال التالي هو مثال على معطيات شرحية لكيان في نظام اللغة SAML يقوم بدور مزوّد خدمة. وهناك توقيع أدرج كممسك بالموقع، من دون محتوى حقيقي. ولأغراض توضيحية، اختيرت الخدمة لتكون خدمة لا تتطلب مستعملين يعرفون هوياتهم بأنفسهم بطريقة وحيدة، ولكنهم يرخصون بالنفاذ على أساس نعت الدور.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
      entityID="https://ServiceProvider.com/SAML">
      <ds:Signature>...</ds:Signature>
   <SPSSODescriptor AuthnRequestsSigned="true"

      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo>
                <ds:KeyName>ServiceProvider.com SSO Key</ds:KeyName>
            </ds:KeyInfo>
        </KeyDescriptor>
        <KeyDescriptor use="encryption">
            <ds:KeyInfo>
                <ds:KeyName>ServiceProvider.com Encrypt Key</ds:KeyName>
            </ds:KeyInfo>
            <EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        </KeyDescriptor>
```

```
        <SingleLogoutService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

      Location="https://ServiceProvider.com/SAML/SLO/SOAP"/>
        <SingleLogoutService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect"

      Location="https://ServiceProvider.com/SAML/SLO/Browser"

      ResponseLocation="https://ServiceProvider.com/SAML/SLO/Response"/>
        <NameIDFormat>
              urn:oasis:names:tc:SAML:2.0:nameid-format:transient
        </NameIDFormat>
        <AssertionConsumerService isDefault="true" index="0"
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Artifact"

      Location="https://ServiceProvider.com/SAML/SSO/Artifact"/>
        <AssertionConsumerService index="1"
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST"

      Location="https://ServiceProvider.com/SAML/SSO/POST"/>
        <AttributeConsumingService index="0">
            <ServiceName xml:lang="en">Academic Journals R
US</ServiceName>
            <RequestedAttribute

      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                          Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
                          FriendlyName="eduPersonEntitlement">
                <saml:AttributeValue>
                    https://ServiceProvider.com/entitlements/123456789
                </saml:AttributeValue>
            </RequestedAttribute>
        </AttributeConsumingService>
    </SPSSODescriptor>
    <Organization>
        <OrganizationName xml:lang="en">Academic Journals R
US</OrganizationName>
        <OrganizationDisplayName xml:lang="en">
             Academic Journals R US, a Division of Dirk Corp.
        </OrganizationDisplayName>
        <OrganizationURL
xml:lang="en">https://ServiceProvider.com</OrganizationURL>
    </Organization>
</EntityDescriptor>
```

2.9 معالجة التوقيع

يمكن لعناصر متنوعة في مرحلة من المعطيات الشرحية أن توقّع توقيعاً رقمياً (كما هو مبين في إدراج العنصر <ds:Signature>) مع الميزات التالية:

1.2.9 سلامة المعطيات الشرحية

استيقان المعطيات الشرحية بواسطة موقّع موثوق.

ولا يطلب التوقيع الرقمي دائماً، كما في حالة طرف واثق يحصل على المعلومات مباشرة من الكيان الناشر (بدون وسطاء) عبر قناة مأمونة، على أن يكون الكيان مستيقناً بالنسبة إلى الطرف الواثق ببعض الوسائل الأخرى غير التوقيع الرقمي.

وهناك عدة تقنيات مختلفة متيسرة للاستيقان "المباشر" وكذلك لإقامة قناة مأمونة بين طرفين. وتشتمل القائمة على بروتوكول أمن طبقة النقل (TLS)، وشفرة استيقان الرسالة المفرومة (HMAC)، والآليات المستندة إلى كلمة سر، إلخ. وفوق كل ذلك فإن المتطلبات الأمنية المنطبقة تتوقف على التطبيقات المتواصلة مع بعض.

وعلاوة على ذلك فإن العناصر قد ترث التوقيعات من عناصر آباء (والدين) مغلِّفة، هي ذاتها موقّع عليها.

وفي غياب مثل هذا السياق، يوصى بأن يكون العنصر الجذر من مرحلة المعطيات الشرحية موقعاً عليه على الأقل.

2.2.9 جانبية التوقيع في اللغة الإرشادية التوسّعية (XML)

مواصفة التوقيع في اللغة XML التابعة للتجمع W3C تدعو إلى سياق في اللغة XML من أجل توقيع المعطيات، يكون مرناً وفيه خيارات عديدة. وتفصّل هذه الفقرة في القيود المفروضة على هذه التسهيلات، بحيث يكون على مُعَالجات المعطات الشرحية ألا تتعامل مع كامل عموميات معالجة التوقيع في اللغة XML. ويستند هذا الاستخدام خصوصاً إلى النعوت ذات النمط **xs:ID** التي تكون موجودة على العناصر التي ينطبق عليها التوقيع. ويحال في هذه الفقرة إلى هذه النعوت بمجموعها على أنها نعوت معرف الهوية.

1) أنساق التوقيع وخوارزمياته

يستخدم التوقيع في اللغة XML ثلاث وسائل لربط توقيع بوثيقة: أن يكون مغلِّفاً أو متغلِّفاً أو منفصلاً. ويتعين على المعطيات الشرحية للغة SAML أن تستخدم توقيعات متغلِّفة عند التوقيع على عناصر معرفة في هذه التوصية. وينبغي للمُعَالِجَات في اللغة SAML أن تعتمد استعمال توقيع الخوارزمية RSA والتحقق من عمليات المفتاح العمومي طبقاً للخوارزمية المعرفة هويتها بما يلي http://www.w3.org/2000/09/xmldsig#rsa-sha1.

2) المراجـــع

يتعين على عناصر المعطيات الشرحية الموقّع عليها، أن تعتمد قيمة لنعت معرف الهوية موضوعة على العنصر الموقّع عليه. ويمكن للعنصر أن يكون أن لا يكون هو العنصر الجذري لوثيقة اللغة XML الحقيقية التي تحتوي على عنصر المعطيات الشرحية الموقّع عليها.

ويتعين أن تحتوي التوقيعات على عنصر واحد <ds:Reference> يحتوي على مرجع للمعرف URI إلى قيمة نعت معرف الهوية في عنصر المعطيات الشرحية الجاري توقيعه. فإذا كانت قيمة نعت معرف الهوية تساوي "foo" مثلاً، يتعين عندئذ على نعت المعرف URI في العنصر <ds:Reference> أن يكون "#foo".

وينتج عن ذلك أن توقيع عنصر من المعطيات الشرحية يجب أن ينطبق على محتوى العنصر الموّع عليه وعلى أي عناصر أبناء (أولاد) قد يحتوي عليها.

3) طريقة التشريع القانوني

ينبغي لأعمال التنفيذ في اللغة SAML أن تستخدم تشريعاً قانونياً حصرياً، مع تعليقات أو بدونها، في نفس الوقت في العنصر <ds:CanonicalizationMethod> من <ds:SignedInfo>، وفي خوارزمية <ds:Transform>، واستخدام تشريع قانوني حصري يضمن أن تكون التوقيعات المحدثة على معطيات شرعية مبيتة في اللغة SAML داخل سياق من اللغة XML، قابلة للتحقق منها بشكل مستقل عن السياق.

4) التحويلات

ينبغي للتوقيعات على المعطيات الشرحية في اللغة SAML ألا تحتوي على تحويلات غير ت حويل التوقيع المتغلف (مع معرف الهوية http://www.w3.org/2000/09/xmldsig#enveloped-signature) أو تحويلات التشريع القانوني الحصري (مع معرف الهوية http://www.w3.org/2001/10/xml-exc-c14n# أو http://www.w3.org/2001/10/xml-exc-c14n#WithComments).

ربما يرفض المتحققون من التوقيعات توقيعات تحتوي على خوارزميات تحويل أخرى باعتبارها غير صالحة. وإذا لم يرفض المتحققون التوقيعات، يكون عليهم أن يتأكدوا من أنه لا يوجد أي محتوى من عنصر المعطيات الشرحية الموقع عليه، وهو مستبعد من التوقيع. ويمكن تحقيق ذلك عن طريق وضع اتفاق خارج النطاق يبين ما هي التحويلات المقبولة أو عن طريق تطبيق التحويلات يدوياً على المحتوى، وإعادة التحقق من أن النتيجة متسقة تماماً مع نفس المعطيات الشرحية في اللغة SAML.

(5 KeyInfo

يعرّف توقيع اللغة XML التابع للتجمع W3C استخدام العنصر <ds:KeyInfo>. ولا تتطلب اللغة SAML استخدام العنصر <ds:KeyInfo> ولا تفرض أي تقييدات على استخدامه. لذلك فإن العنصر <ds:KeyInfo> يمكن أن يكون غائباً.

3.9 إصدار (نشر) المعطيات الشرحية واستبانتها

توجد في هذه التوصية آليتان لكي يصدر أحد الكيانات وثائق معطيات شرحية (ولكي يستبين أحد المستهلكين موقعاً لها): عبر "موقع معروف جيداً" مباشرة عن طريق التخلي عن مرجعية معرف الهوية الوحيد للكيان (المعرف URI يحال إليه بصفته *entityID* أو *providerID*)، أو بصورة غير مباشرة بنشر موقع المعطيات الشرحية في نظام أسماء الميادين (DNS). وهناك أيضاً آليات أخرى خارج النطاق مسموح بها بكل تأكيد. والمستهلك الذي يعتمد كلا النهجين، عليه أن يحاول الاستبانة عن طريق النظام DNS، قبل أن يستخدم آلية "الموقع المعرف جيداً".

وعندما يتطلب الاسترجاع نقل الوثيقة في الشبكة، ينبغي أن تتم حماية النقل بآليات توفر استيقان المخدّم وحماية السلامة. فالاستبانة المبنية على البروتوكول HTTP ينبغي حمايتها ببروتوكول أمن طبقة النقل (TLS)، كما هو معرّف في طلب التعليقات RFC 2246 المعدّل في طلب التعليقات RFC 3546 الصادرين عن فريق المهام الهندسية في الإنترنت (IETF).

وتشرح هذه الفقرة آليات متنوعة للمساعدة على وضع الثقة بدقة المعطيات الشرحية وشرعيتها، بما في ذلك استعمال توقيعات اللغة XML، واستيقان مخدّم البروتوكول TLS، وتوقيعات النظام DNS. وبصرف النظر عن الآلية أو الآليات المستعملة، ينبغي أن يكون لدى الأطراف الواثقة بعض الوسائل التي تستطيع بها وضع الثقة بمعلومات المعطيات الشرحية قبل الاعتماد عليها.

1.3.9 الإصدار والاستبانة عبر الموقع المعروف جيداً

تشرح الفقرات الفرعية التالية إصدار المعطيات الشرحية واستبانتها بواسطة الموقع المعروف جيداً.

1.1.3.9 الإصدار (النشر)

يمكن للكيانات أن تصدر (تنشر) وثائق معطياتها الشرحية في موقع معروف جيداً، بوضعها الوثيقة في الموقع الذي يحدده معرف هويته الوحيد، الذي يت عين أن يكون بشكل محدّد موقع موحد للموارد (URL) (بدلاً من اسم موحّد للموارد (URN)). ويوصى بشدة أن تستعمل لهذا الغرض المحددات URL للبروتوكولات HTTP. ويمكن استخدام آليات توجيهية تعتمدها تخطيطة المحدد URL (مثل البروتوكول HTTP 1.1 302 المعاد توجيهه). إذا لم تكن الوثيقة موضوعة مباشرة في الموقع. وإذا كان بروتوكول الإصدار يسمح بالاستيقان المبني على التوسّعات MIME في أنماط المحتوى، يجب أن يكون نمط المحتوى في مرحلة المعطيات الشرحية application/samlmetadata+xml.

ويتعين على وثيقة اللغة XML المقدمة في الموقع المعروف جيداً أن تشرح فقط المعطيات الشرحية الخاصة بالكيان الذي يمثله معرف الهوية الوحيد (وهذا يعني أن يكون العنصر الجذر هو <EntityDescriptor> مع entityID متوائم مع الموقع). وإذا احتاجت كيانات أخرى إلى الشرح، يتعين استعمال العنصر <AdditionalMetadataLocation>. وهكذا يتعين ألا يستعمل العنصر <EntitiesDescriptor> في الوثائق الصادرة باستخدام هذه الآلية، نظراً إلى أن مجموعة من الكيانات لا يعرفها مثل هذا المعرف للهوية.

2.3.9 الإصدار (النشر) والاستبانة عبر نظام أسماء الميدان (DNS)

لكي تحسّن الكيانات إمكانية النفاذ إلى وثائق المعطيات الشرحية، وتوفر تقابلات إضافية بين معرف هوية وحيد وموقع المعطيات الشرحية، يكون عليها أن تنشر مواقع وثائق المعطيات الشرحية في منطقة من نظامها DNS المقابل، كما هو معرّف في طلب التعليقات RFC 1034 الصادر عن الفريق IETF. ويستعمل معرف الهوية الوحيد للكيان (URI) كمدخل إلى العملية. ولما كانت المعرّفات URI هي معرفات هوية مرنة، فإن طرائق نشر المواقع وعملية استبانتها تحددها تخطيطة المعرفات URI والاسم الموصوف تماماً. ثم تستنتج مواقع المعرفات URI للمعطيات الشرحية لاحقاً عبر استفهامات تطرح على سجل الموارد (RR) التابع لمسدد سلطة التسمية (NAPTR)، كما هو معرف في طلبي التعليقات RFC 2914 وRFC 3403 الصادرين عن فريق المهام IETF.

وتوصى الكيانات بأن تصدر سجلات مواردها في ملفات منطقة موقّعة، مستخدمة طلب التعليقات RFC 2535 الصادر عن الفريق IETF، حتى تتمكن الأطراف الواثقة من إثبات صلاحية الموقع المنشور وسلطة المنطقة وسلامة جواب النظام DNS. وإذا كانت توقيعات النظام DNS موجودة، يتعين على الأطراف الواثقة أن تقر صلاحية التوقيع بصورة صحيحية.

1.2.3.9 الإصدار (النشر)

تستخدم هذه التوصية سجل موارد المسدّد NAPTR المشروح في طلبي التعليقات RFC 2915 وRFC 3403 الصادرين عن الفريق IETF. ويوصى بتشجيع التآلف مع هذه الوثائق.

إن النظام التحريكي (الدينامي) لاكتشاف التفويضات (DDDS) هو نظام عام الأغراض من أجل استرجاع المعلومات المبنية على سلسلة مداخل خاصة بالتطبيق وعلى تطبيق القواعد المعروفة جيداً من أجل تحويل هذه السلسلة حتى بلوغ شرط نهائي يتطلب البحث في قاعدة معطيات محددة خاصة بالتطبيق أو من أجل استبانة محدد موقع URL مبني على قواعد معرّفة من التطبيق. والنظام التحريكي DDDS يحدد نمطاً معيناً من سجل موارد النظام DNS ومن سجلات المسدّد NAPTR من أجل تخزين المعلومات في النظام DNS اللازم لتطبيق قواعد النظام التحريكي لاكتشاف التفويضات.

وقد تصدر الكيانات محددات URL منفصلة، عندما تدعو الحاجة إلى توزيع وثائق متعددة من المعطيات الشرحية، أو عندما يتطلب الأمر وثائق مختلفة من المعطيات الشرحية نظراً إلى تعدد علاقات الثقة التي تتطلب مواد تجفير منفصلة، عندما تدعو الحاجة إلى توزيع وثائق متعددة من المعطيات الشرحية، أو عندما يتطلب الأمر وثائق مختلفة من المعطيات الشرحية نظراً إلى تعدد علاقات الثقة التي تتطلب مواد تجفير منفصلة، أو عندما تتطلب السطوح البينية للخدمات إعلانات منفصلة عن المعطيات الشرحية. ويمكن تحقيق ذلك من خلال استعمال العنصر الاختياري <AdditionalMetadataLocation>، أو من خلال المرفق regexp ومجالات متعددة لتعريف الخدمات في سجل موارد المسدّد NAPTR نفسه.

وإذا كان بروتوكول الإصدار يسمح بتعريف هوية أنماط المحتوى تعريفاً مبنياً على التوسّعات المتعددة الأغراض في بريد الإنترنت (MIME)، يتعين على نمط المحتوى في مرحلة المعطيات الشرحية أن يكون application/samlmetadata+xml.

وإذا كان معرّف الهوية الوحيد للكيان هو الاسم URN، فإن نشر موقع المعطيات الشرحية المقابل يجري كما هو محدد في طلب التعليقات RFC 3404 الصادر عن الفريق IETF. وإلا فاستبانة موقع المعطيات الشرحية تجري على النحو التالي.

وما يلي هو جانبية خاصة بتطبيق النظام DDDS من أجل استبانة المعطيات الشرحية في اللغة SAML:

1) أول قاعدة معروفة جيداً

"أول قاعدة معروفة جيداً" لمعالجة استبانة المعطيات الشرحية في اللغة SAML هي القيام بتحليل معرف الهوية الوحيد للكيان واستخراج اسم الميدان الموصوف بالكامل (العبارة الفرعية 3).

2) حقل الترتيب

يبين حقل الترتيب المتّبع في معالجة كل واحد مرجّع من سجلات موارد المسدد NAPTR. وقد يتوفر للناشرين سجلات موارد عديدة للمسدد NAPTR، يتعين على التطبيق المستبين أن يعالجها بالترتيب في هذا الحقل.

3) حقل التفضيل

يعبر الناشر في سجلات الموارد الانتهائية للمسدد NATPR عن الترتيب الذي يفضل استعماله في تطبيق الاستبانة. وقد يتجاهل تطبيق الاستبانة هذا الترتيب، في الحالات التي لا تلبي فيها قيمة حقل الخدمة متطلبات التجهيز المستبين (أي سجل الموارد يرجّع بروتوكولاً لا يعتمده التطبيق).

4) حقل الراية

تستخدم استبانة المعطيات الشرحية في اللغة SAML الراية "U" مرتين، وهي مطرافية، كما إنها تستخدم قيمة الصفر (التي تقضي بمعالجة الموارد الإضافية). وتدل الراية "U" على أن نتيجة القاعدة هي معرّف URI.

5) حقل الخدمة

يعلن حقل الخدمة الخاص باللغة SAML، كما هو مشروح في شكل باكوس–ناور (BNF) التالي، عن الأساليب التي سيتيسر بها وثيقة (وثائق) المرحلة:

```
servicefield = 1("PID2U" / "NID2U") "+" proto [*(":" class) *(":"
servicetype)]
proto = 1("https" / "uddi")
class = 1[ "entity" / "entitygroup" )
servicetype = 1(si / "spsso" / "idpsso" / "authn" / "authnauth" / "pdp" /
"attrauth" / alphanum )
si = "si" [":" alphanum] [":endpoint"]
alphanum = 1*32(ALPHA / DIGIT)
```

حيث:

- `servicefield PID2U` يستبين معرف الهوية الوحيد للكيان في المحدد URL للمعطيات الشرحية.
- `servicefield NID2U` يستبين العنصر `<NameID>` لطرف رئيسي في المحدّد URL للمعطيات الشرحية.
- `proto` يشرح بروتوكول الاسترجاع (`https or uddi`). وفي حالة قاعدة الدليل UDDI، يكون المحدّد URL هو محدد URL لبروتوكول http (أو بروتوكولات)، يحيل إلى وثيقة في اللغة WSDL.
- `class` يعرّف ما إذا كانت وثيقة المعطيات الشرحية المحال إليها تشرح كياناً واحداً أو عدة كيانات. وفي الحالة الأخيرةن يتعين أن تحتوي الوثيقة المحال إليها على كيان معرّف من معرف الهوية الوحيد الأصلي، باعتباره عضواً في جماعة من الكيانات واقعة داخل الوثيقة، مثل `<EntitiesDescriptor>`.
- `servicetype` يسمح لكيان بأن ينشر معطيات شرحية لتمييز الأدوار والخدمات في وثائق منفصلة. والمستبينون الذين يصادفون إعلانات `servicetype` عديدة، يتخلون عن مرجعية المعرّف URI المناسب، حسب الخدمة المطلوبة لكل عملية (فالكيان الذي يعمل بنفس الوقت كمزوّد هوية وكمزوّد خدمة يستطيع نشر معطيات شرحية لكل دور في مواقع مختلفة). ونمط الخدمة `authn` يمثل نقطة نهائية `<SingleSignOnService>`.
- `si` (مع مركّبة نقطة نهائية اختيارية) تسمح للناشر إما أن يصدر المعطيات الشرحية مباشرة لمطابق في خدمة، وإما بمفصلة نقطة نهائية في البروتوكول SOAP (باستخدام `endpoint`) .

مثال:

- PID2U+https:entity – يمثل وثيقة المعطيات الشرحية الكاملة للكيان، المتيسرة عبر البروتوكول https.
- PID2U+uddi:entity:si:foo – يمثل موقع وثيقة اللغة WSDL التي تشرح مطابق الخدمة "foo".
- PID2U+https:entitygroup:idpsso – يمثل المعطيات الشرحية لجماعة من الكيانات تعمل كمزوّدي هوية باكتتاب التوقيع الوحيد، ويكون الكيان الأصلي عضواً فيها.
- NID2U+https:idp – يمثل المعطيات الشرحية لمزوّد هوية باكتتاب التوقيع الوحيد لطرف رئيسي.

6) حقلا regex والاستعاضة

إن النتيجة المتوقعة بعد معالجة سلسلة الدخول عبر regex يجب أن تكون محدداً صالحاً في البروتوكول https أو عنوان عقدة في قاعدة الدليل UDDI (وثيقة اللغة WDSL).

2.2.3.9 أمثلة المسدِّد NAPTR

تعطي هذه الفقرة أمثلة من المحدّد URL وعناوين البريد الإلكتروني التي يمكن أن تستخدمها كيانات تعتمد المسدّد NAPTR (انظر طلب التعليقات RFC 2915 الصادر عن الطريق IETF).

أ) أمثلة المسدّد NAPTR من المعطيات الشرحية لكيان

تنشر الكيانات المحددات URL للمعطيات الشرحية بالأسلوب التالي:

```
$ORIGIN provider.biz

;; order pref f service regexp or replacement

IN NAPTR 100 10 "U" PID2U+https:entity
      "!^.*$!https://host.provider.biz/some/directory/trust.xml!" ""
IN NAPTR 110 10 "U" PID2U+https: entity:trust
      "!^.*!https://foo.provider.biz:1443/mdtrust.xml!" ""
IN NAPTR 125 10 "U" PID2U+https:"
IN NAPTR 110 10 "U" PID2U+uddi:entity
      "!^.*$!https://this.uddi.node.provider.biz/libmd.wsdl" ""
```

ب) أمثلة من معرفات هوية الاسم

مشغل لدى طرف رئيسي هو example.int يشغّل مزوّد هوية يمكن أن تستخدمه شركة لأثاث المكاتب لكي تستيقن المشترين المرخص لهم. فتأخذ الشركة المزوّدة عناوين البريد الإلكتروني للمستعملين buyer@example.int كمدخل إلى عملية الاستبانة، وتقوم بتحليل العنوان الإلكتروني لتستخرج منه الاسم الكامل للميدان (FQDN) (example.int). فينشر المشغل سجل المسدّد NAPTR التالي في النظام DNS example.int.

```
$ORIGIN example.int

IN NAPTR 100 10 "U" NID2U+https:authn
      "!^([^@]+)@(.*)$!https://serv.example.int:8000/cgi-bin/getmd?\1!" ""
IN NAPTR 100 10 "U" NID2U+https:idp
      "!^([^@]+)@(.*)$!https://auth.example.int/app/auth?\1" ""
```

3.2.3.9 الاستبانـــة

عند استبانة معطيات شرحية من أجل كيان عبر النظام DNS، يستخدم معرف الهوية الوحيد للكيان باعتباره المدخل الأولي إلى عملية الاستبانة، بدلاً من كونه موقعاً حقيقياً. ويتّبع ما يلي:

- إذا كان معرف الهوية الوحيد هو الاسم URN، تجري خطوات الاستبانة كما هو معرف في طلب التعليقات RFC 3403 الصادر عن الفريق IETF.
- وإلا يجري تحليل معرف الهوية للحصول على الاسم الكامل للميدان (FQDN).
- يستفهم من النظام DNS عن سجلات موارد المسدّد NAPTR في الميدان، ويكرر الاستفهام إلى أن يتم ترجيع سجل الموارد المطرافي.
- يعرّف بهوية سجل الموارد الذي يستعمل استناداً إلى حقول الخدمة، ثم حقول الترتيب ثم حقول التفضيل من مجموعة النتائج.
- الحصول على الوثيقة (الوثائق) في الموقع (المواقع) المتوفر حسب تطلّب التطبيق.

وقد يلزم في بعض الحالات، عند المبادرة إلى استبانة موقع معلومات المعطيات الشرحية، أن يفكك معرف الهوية الوحيد للكيان (المعبر عنه بالمعرّف URI) إلى عنصر ذري واحد أو أكثر من عنصر.

وينبغي استعمال التعبير النظامي التالي عند المبادرة إلى عملية التفكيك:

```
^([^:/?#]+:)?/*([^:/?#]*@)?(([^/?:#]*\.)*(([^/?#:\.]+)\.([^/?#:\.]+)))(:\d+)?([^?
#]*)(\?[^#]*)?(#.*)?$
     1            2           34            56             7             8      9
10        11
```

ويتعين أن ينتج عن التعبير الفرعي 3 اسم كامل للميدان (FQDN: Fully-Qualified Domain Name) هو الذي سيكون أساس استرجاع مواقع المعطيات الشرحية انطلاقاً من هذه المنطقة.

وبعد إكمال عملية تحليل معرف الهوية، يقوم التطبيق بالاستفهام من النظام DNS بشأن المنطقة الناتجة (التعبير الفرعي 5) لسجلات موارد المسدّد NAPTR، وينبغي توقع استجابة واحدة أو أكثر. وقد تستبعد التطبيقات من مجموعة النتائج أي تعريفات للخدمة لا تتعلق بعمليات الطلب الجارية.

ويتعين على تطبيقات الاستبانة أن ترتّب بعد ذلك مجموعة النتائج وفقاً لحقل الترتيب، وقد ترتّب مجموعة النتائج استناداً إلى مجموعة التفضيلات. ولا يطلب من المستبينين أن يتّبعوا ترتيب حقل التفضيلات. وسجل أو سجلات موارد المسدّد NAPTR الناتجة تعالج معالجة تكرارية (استناداً إلى راية الترتيب) إلى أن يتم التوصل إلى سجل موارد مطرافي للمسدّد NAPTR.

وستكون النتيجة محدِّداً مطلقاً URL، مشكلاً تشكيلاً جيداً، يستعمل فيما بعد لاسترجاع وثيقة المعطيات الشرحية.

4.2.3.9 تخزين موقع المعطيات الشرحية في ذاكرة مخبأ

يتعين على تخزين الموقع في ذاكرة مخبأ ألا يتجاوز مدة الحياة (TTL) لمنطقة النظام DNS التي استنتج منها الموقع. ويتعين على أنظمة الاستبانة الحصول على نسخة جديدة من مواقع المعطيات الشرحية عندما تنقضي مدة حياة المنطقة.

وينبغي لناشري وثائق المعطيات الشرحية أن يعيروا اهتماماً كبيراً لمدة حياة المنطقة، عندما يقومون بتغييرات في مواقع وثائق المعطيات الشرحية. وإذا كان مثل هذا التغيير في الموقع سيحدث، يتعين على الناشر إما أن يحتفظ بالوثيقة في كلا الموقعين القديم والجديد إلى أن تتأكد جميع أنظمة الاستبانة من حصولها على الموقع المحيّن (أي وقت تغيير المنطقة + مدة الحياة)، وإما أن يؤمن إجابة من البروتوكول HTTP Redirect، توضع في الموقع القديم لتحدد الموقع الجديد.

3.3.9 المعالجة اللاحقة للمعطيات الشرحية

تشرح الفقرات الفرعية التالية المعالجة اللاحقة للمعطيات الشرحية.

1.3.3.9 تخزين مرحلة معطيات شرحية في ذاكرة مخبأ

يتعين على تخزين وثيقة في ذاكرة مخبأ ألا يتجاوز النعت validUntil أو النعت cacheDuration لعنصر الصاحب أو لعناصره. وإذا كان لعناصر المعطيات الشرحية عناصر آباء تحتوي على سياسات التخزين في ذاكرة مخبأ، تكون الأسبقية للعنصر الأب.

ولمعالجة النعت cacheDuration معالجة صحيحة، يجب على المستهلكين أن يحتفظوا بالتاريخ والوقت الذي جرى فيه سحب الوثيقة.

وعندما تصل وثيقة أو يصل عنصر إلى انقضاء الصلاحية، يتعين على المستهلك أن يسحب نسخة حديثة، وقد يتطلب تحديد موقع الوثيقة أو مواقعها. وينبغي للمستهلكين أن يعالجوا تخزين وثيقة في ذاكرة مخبأ معالجة مطابقة للفقرة 13 من طلب التعليقات RFC 2616 الصادر عن الفريق IETF، ويمكنهم أن يطلبوا التعديل الأخير للتاريخ والوقت من مخدّم البروتوكول HTTP. وينبغي للناشرين أن يؤمنوا معالجة مقبولة للذاكرة المخبأ، كما هو مشروح في الفقرة 5.3.10 من طلب التعليقات RFC 2616 الصادر عن فريق المهام الهندسية في الإنترنت (IETF) (304 غير معدّلة).

2.3.3.9 التعامل مع إعادات التوجيه (الإحالات) في البروتوكول HTTPS

يمكن للناشرين أن يصدروا إحالة إلى البروتوكول HTTP (301 انتقال دائم، 302 أو 307 إعادة توجيه مؤقته) كما هو معرف في طلب التعليقات RFC 2616 الصادر عن الفريق IETF، ويتعين على وكلاء المستعمل أن يتّبعوا المحدّد URL المعيّن في استجابة إعادة التوجيه. وينبغي أن تكون الإحالات من نفس بروتوكول الطلب الأولي.

3.3.3.9 معالجة التوقيعات في اللغة XML ومعالجة الثقة عامة

تقدِّم معالجة المعطيات الشرحية آليات متعددة للتفاوض بشأن الثقة، لكل من المعطيات الشرحية ذاتها وللثقة الممنوحة للكيان الذي تصفه مثل هذه المعطيات الشرحية:

- الثقة المتولدة من توقيع منطقة النظام DNS التي جرت منها استبانة المحدّد URL لموقع المعطيات الشرحية، مما يضمن صحة موقع أو مواقع وثائق المعطيات الشرحية.
- الثقة المتولدة من توقيع معالجة وثيقة المعطيات الشرحية نفسها، مما يضمن سلامة وثيقة اللغة XML.
- الثقة المتولدة من استيقان مخدّم البروتوكول TLS من المحدّد URL لموقع المعطيات الشرحية، مما يضمن هوية ناشر المعطيات الشرحية.

ويتعين على المعالجة اللاحقة لوثيقة المعطيات الشرحية أن تتضمن معالجة التوقيع على مستوى اللغة XML، ويمكن أن تتضمن أيضاً واحدة من العمليتين الأخريين. ويمكن للطرف الواثق بصورة خاصة أن يختار منح ثقته لأي سلطة مذكورة في عملية الاستبانة والتحليل. ويتعين على ناشري المعطيات الشرحية أن يستعملوا آلية لحماية سلامة الوثيقة، ويمكنهم أن يستعملوا أي واحدة من جانبيتي المعالجة الأخريين لوضع الثقة بوثيقة المعطيات الشرحية التي تحكم السياسات التنفيذية. ويجب أخذ الاعتبارات التالية بالحسبان:

1) معالجة المناطق الموقّع عليها في النظام DNS

يجب القيام بالتحقق من توقيع منطقة في النظام DNS، إن وجد، كما هو مشروح في طلب التعليقات RFC 2535 الصادر عن الفريق IEFT.

2) **معالجة المناطق الموقّع عليها أو أجزاء منها**

ينبغي لوثائق المعطيات الشرحية المنشورة أن تكون موقّعاً عليها، كما هو مشروح في هذه التوصية، سواء بشهادة صادرة إلى صاحب الوثيقة أم عن طرف موثوق آخر. ويمكن للناشرين أن يعتبروا توقيعات أطراف أخرى وسائل تبعث على الثقة.

ويتعين على مستهلكي المعطيات الشرحية أن يقروا صلاحية التوقيعات، إن وجدت، على وثيقة المعطيات الشرحية، كما هو مشروح في هذه التوصية.

3) **معالجة استيقان المخدّم أثناء استرجاع المعطيات الشرحية عبر البروتوكول TLS**

يوصى الناشرون بشدة أن ينفذوا المحدّدات URL في البروتوكول TLS، وبالتالي ينبغي للمستهلكين أن يعتبروا الثقة موروثة من مُصْدر شهادة TLS. وقد لا يقع نشر المحددات URL دائماً في ميدان صاحب وثيقة المعطيات الشرحية، وعليه ينبغي للمستهلكين ألا يفترضوا أن صاحب الشهادات هو الكيان المدروس، إذ يمكن أن يستضيفه طرف موثوق آخر.

ولما كان أساس هذه الثقة قد لا يكون متيسراً تجاه وثيقة موضوعة في ذاكرة مخبأ، ينبغي استعمال آليات أخرى في مثل هذه الظروف.

10 الروابط في اللغة SAML

يحدد هذا البند روابط البروتوكول في اللغة SAML لاستعمالها في تأكيدات اللغة SAML ورسائل الطلب والاستجابة في بروتوكولات الاتصال وأطر العمل فيها.

إن وضع تبادلات رسائل الطلب والاستجابة في اللغة SAML على تقابل مع الرسائل المعيارية أو بروتوكولات الاتصال يسمى *روابط البروتوكول* (أو *روابط* بكل بساطة) في اللغة SAML. ومرحلة من وضع تبادلات رسائل الطلب والاستجابة في اللغة SAML على تقابل مع بروتوكول الاتصال الخاص <FOO> تسمى *رابطة <FOO> في اللغة SAML* أو *رابطة <FOO> SAML*.

فمثلاً رابطة البروتوكول SOAP في اللغة SAML تشرح كيف يجري وضع تبادلات رسائل الطلب والاستجابة في اللغة SAML على تقابل مع تبادلات رسائل البروتوكول SOAP.

وترمي هذه التوصية إلى تحديد مجموعة من الروباط بتفصيلات كافية، تضمن للبرامجيات المطابقة للغة SAML والتي تعمل بصورة مستقلة أن تشتغل فيما بينها، عندما تستخدم المراسلات المعيارية أو بروتوكولات الاتصال.

وينبغي أن يفهم بالرابطة أنها حاملة إرسال كل رسالة بروتوكول في اللغة SAML مستنتجة من النمطين **samlp:RequestAbstractType** و**samlp:StatusResponseType**، ما لم يذكر غير ذلك. وفوق ذلك، عندما تحيل رابطة إلى "طلبات واستجابات في اللغة SAML"، ينبغي أن يفهم من ذلك أنها تعني أي رسائل بروتوكول مستنتجة من هذين النمطين.

وتستخدم هذه التوصية الاصطلاحات الطباعية التالية في النص: <ns:Element> وXMLAttribute و**Datatype** وOtherKeyword. وفي بعض الحالات تستخدم الحاصرات الزاوية لتدل على عناصر ليست مطرافية بدلاً من عناصر اللغة XML، ويظهر المقصود واضحاً من خلال السياق.

1.10 خطوط توجيهية لتحديد روابط بروتوكول إضافية

تعرف هذه التوصية مجموعة منتقاة من روابط البروتوكول، ولكن غيرها سوف يتم تطويره في المستقبل. وتقدم هذه الفقرة خطوطاً توجيهية لأطراف ثالثة ترغب في تحديد روابط إضافية. وفيما يلي قائمة تفقُّد القضايا التي يتعين أن تتطرق إليها كل رابطة بروتوكول:

- تحديد ثلاثة عناصر من عناصر معلومات التعريف بالهوية: المعرّف URI الذي يعرّف فقط هوية رابطة البروتوكول، ومعلومات الاتصال الإلكتروني أو البريدي حول المؤلف، ومرجع إلى روابط أو جانبيات معرّفة سابقاً، تحيّنها الرابطة الجديدة أو تجعلها بالية.
- شرح مجموعة التفاعلات القائمة بين أطراف مشتركة في الرابطة. ويجب أن تذكر صراحة كل التقييدات التي يمارسها كل طرف وكل البرتوكولات المشتركة في كل تفاعل (تآثر) على التطبيقات.
- التعريف بهوية الأطراف المشتركة في كل تفاعل، بما في ذلك عدد الأطراف المشتركة أو ما إذا كان هناك وسطاء مشتركة.
- تحديد طريقة استيقان الأطراف المشتركة في كل تفاعل، بما في ذلك كون الاستيقان مطلوباً، وما هي أنماط الاستيقان المقبولة.
- تحديد سوية الدعم لسلامة الرسالة، وهذا يشمل الآليات المستعملة لتأمين سلامة الرسالة.
- تحديد سوية دعم الائتمانية، وهذا يشمل إمكانية السماح لطرف ثالث بالاطّلاع على محتويات رسائل وتأكيدات اللغة SAML، وهل الرابطة تتطلب الائتمانية وما هي الآليات الموصى بها لتحقيق الائتمانية.
- تحديد حالات الخطأ، بما في ذلك حالات الخطأ لدى كل مشترك، وخاصة لدى المشتركين الذين يستلمون ويعالجون تأكيدات أو رسائل اللغة SAML.
- تحديد الاعتبارات الأمنية، بما في ذلك تحليل التهديدات وشرح التدابير المضادة.
- تحديد الاعتبارات الخاصة بالمعطيات الشرحية، مثل المعطيات التي تدعم رابطة مشتركة في بروتوكول اتصالات خاصة أو التي تستعمل في جانبية خاصة، والتي يجب أن تحاط علماً بطريقة فعّالة وشغّالة بينياً.

2.10 روابط البروتوكول

تعرّف الفقرات الفرعية التالية روابط البروتوكول التي تتحدد كجزء من معيار اللغة SAML.

1.2.10 اعتبارات عامة

تشرح الفقرات الفرعية التالية خصائص جميع روابط البروتوكول المعرفة للغة SAML.

1.1.2.10 استخدام "RelayState"

تعرّف بعض الروابط آلية "RelayState" للاحتفاظ بمعلومات الحالة وترحيلها. وعندما تستعمل مثل هذه الآلية في حمل رسالة طلب باعتبارها الخطوة الأولى من بروتوكول اللغة SAML، فإنها تضع متطلبات على انتقاء واستعمال الرابطة التي ستستخدم فيما بعد في حمل الاستجابة. فإذا كانت رسالة الطلب في اللغة SAML مترافقة مثلاً مع معطيات RelayState، يتعين على المستجيب في اللغة SAML أن يرجع استجابة بروتوكول SAML، مستخدماً رابطة تعتمد هي الأخرى الآلية RelayState، ويتعين عليه أيضاً أن يضع معطيات RelayState الصحيحة التي استلمها مع الطلب، داخل المعلمة المقابلة من RelayState في الاستجابة.

2.1.2.10 الأمـــن

تنطبق هذه الإعلانات الأمنية على جميع الروابط، ما لم ينص على غير ذلك. وتستطيع الروابط أن تضيف إعلانات إضافية إلى هذه الميزات الأمنية.

1) استعمال صيغة البروتوكول TLS 1.0

يتعين على المخدّمات أن تستيقن أنفسها لدى الزبائن باستعمال الشهادة الواردة في الصغية X.509 v3، في كل استخدام لرابطة SAML في صيغة البروتوكول TLS 1.0 (الطلب RFC 2246 الصادر عن الفريق

IETF)، ما لم ينص على غير ذلك. ويتعين على الزبون أن يقرر هوية المخدّم استناداً إلى محتويات الشهادة (وعادة بتفحص الحقل DN الخاص بصاحب الشهادة، من النعت `subjectAltName` إلخ).

2) استيقان مَصْدر المعطيات

إن استيقان كل من الطالب SAML والمستجيب SAML المتصاحبين في رسالة هو أمر اختياري ويتوقف على بيئة الاستعمال. ويمكن استعمال آليات الاستيقان المتيسرة في طبقة تبادل رسالة البروتوكول SOAP أو من بروتوكول الطبقة الفرعية التحتية (في روابط كثيرة مثلاً البروتوكول TLS أو HTTP) للحصول على استيقان مَصْدر المعطيات.

ولا يستوفي استيقان النقل متطلبات استيقان المَصْدر من طرف إلى طرف في الروابط التي تمر فيها رسالة بروتوكول اللغة SAML عبر وسيط – ويوصى في هذه الحالة باستيقان الرسالة.

وتقدم اللغة SAML ذاتها آليات إلى الأطراف لكي يستيقن كل منها الآخر، ولكن اللغة SAML يمكنها إضافة إلى ذلك أن تستخدم آليات استيقان أخرى لتوفير أمن اللغة SAML ذاتها.

3) سلامة الرسالة

سلامة الرسالة في طلبات اللغة SAML واسجاباتها هي أمر اختياري، وتتوقف على بيئة الاستعمال. ويمكن استعمال الطبقة الأمنية في بروتوكول الطبقة الفرعية التحتية أو استعمال آلية في طبقة تبادل رسائل البروتوكول SOAP، من أجل تأمين سلامة الرسالة. ولا تستوفي سلامة النقل متطلبات استيقان السلامة من طرف إلى طرف في الروابط التي تمر فيها رسالة بروتوكول اللغة SAML عبر وسيط – ويوصى في هذه الحالة بسلامة الرسالة.

4) ائتمانية الرسالة

ائتمانية الرسالة في طلبات اللغة SAML واستجاباتها هي أمر اختياري، وتتوقف على بيئة الاستعمال. ويمكن استعمال الطبقة الأمنية في بروتوكول الطبقة الفرعية التحتية أو استعمال آلية في طبقة تبادل رسائل البروتوكول SOAP، من أجل ضمان ائتمانية الرسالة.

ولا تستوفي ائتمانية النقل متطلبات الائتمانية من طرف إلى طرف في الروابط التي تمر فيها رسالة البروتوكول SAML عبر وسيط.

5) اعتبارات أمنية أخرى

ينبغي قبل النشر تحليل كل تجميعة من آليات الاستيقان وسلامة الرسالة وائتمانيتها، من حيث قابلية تأثرها في سياق تبادل البروتوكول وبيئة النشر (انظر التذييل I لمزيد من التفصيلات). ويشرح الطلب RFC 2617 الصادر عن الفريق IETF التهجمات المحتملة في بيئة البروتوكول HTTP، عند استعمال تخطيطات الاستيقان الأساسي أو لموجز الرسالة. وينبغي إيلاء اهتمام خاص إلى تأثير الوضع في ذاكرة مخبأ على الأمن.

2.2.10 رابطة البروتوكول SOAP في اللغة SAML

البروتوكول المبسّط للنفاذ إلى الهدف (SOAP) هو بروتوكول مخفّف أُعدّ لتبادل معلومات مُبَنْيَنَة في بيئة موزعة لا مركزية. إنه يستخدم تقانات (تكنولوجيات) اللغة الإرشادية التوسّعية (XML) لتعريف إطار عمل توسّعي للمراسلة، يشكل تركيبة رسائلية يمكن تبادلها على بروتوكولات تحتية متنوعة. وقد صمم إطار العمل ليكون مستقلاً عن أي نموذج برمجة خاص وعن أي علم دلالات خاص آخر في التنفيذ. وهناك هدفان كبيران في تصميم البروتوكول SOAP هما البساطة وقابلية التوسّع. ويسعى البروتوكول SOAP إلى استيفاء هذين الهدفين بحذفه ميزات من إطار عمل المراسلة، كانت توجد غالباً في الأنظمة الموسّعة. ومن بين ما تشتمل عليه مثل هذه

الميزات "الاعتمادية (الوثوقية)" و"الأمن" و"الترابط" و"التسيير" و"مخططات تبادل الرسائل" (MEP). دون أن تقتصر على ذلك.

ورسالة البروتوكول SOAP هي أساساً إرسال وحيد الاتجاه بين عقد البروتوكول SOAP، من مرسل في SOAP إلى مستلم في SOAP، قد يكون مسيراً عبر وسيط واحد أو وسطاء في البروتوكول SOAP. ويتوقع من رسائل البروتوكول SOAP أن تكون مدموجة في تطبيقات من أجل تنفيذ مخططات تفاعلية أكثر تعقيداً تمتد من طلب/استجابة إلى تبادلات متعددة "تحادثية" ذهاباً وإياباً.

ويعرّف البروتوكول SOAP مغلّفاً (ظرفاً) لرسالة اللغة XML يتضمن مقاطع رأسية ومَتْنيَّة، تسمح بإرسال المعطيات ومعلومات التحكم. كما يعرف البروتوكول SOAP قواعد معالجة ترافق هذا المغلّف، ومعها رابطة بروتوكول HTTP لإرسال رسالة البروتوكول SOAP.

والبروتوكول SOAP، مثل اللغة SAML، يمكن استعماله على عمليات نقل تحتية عديدة. ولهذه الرابطة جوانب استقلالية عن البروتوكول، ولكنها تدعو أيضاً إلى استخدام البروتوكول SOAP على البروتوكول HTTP حسب الطلب (تنفيذه إلزامي).

1.2.2.10 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:bindings:SOAP`

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحييبات: `urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding`

2.2.2.10 الجوانب الاستقلالية عن البروتوكول لرابطة SOAP في اللغة SAML

تحدد الفقرات التالية جوانب رابطة البروتوكول SOAP في اللغة SAML التي هي مستقلة عن البروتوكول التحتي، مثل البروتوكول HTTP، الذي تنقل عليه رسائل البروتوكول SOAP. ولا تقبل هذه الرابطة إلا استعمال الصيغة SOAP 1.1 من البروتوكول.

1.2.2.2.10 التشغيل الأساسي

تتكون رسالة البروتوكول SOAP 1.1 من ثلاثة عناصر: مغلّف (ظرف)، ومعطيات الرأسية، ومَتْن الرسالة. ويتعين أن تكون عناصر بروتوكول للطلب–الاستجابة في اللغة SAML واردة في مَتْن رسالة SOAP.

ويعرّف البروتوكول SOAP 1.1 نظاماً اختيارياً لتشفير المعطيات. ولا يستخدم هذا النظام داخل رابطة البروتوكول SOAP في اللغة SAML. وهذا يعني أن رسائل اللغة SAML يمكن نقلها باستخدام البروتوكول SOAP من دون إعادة التشفير، من تخطيطة "معيارية" في اللغة SAML إلى تخطيطة مبنية على تشفير البروتوكول SOAP.

ونموذج النظام المستعمل لمحادثات اللغة SAML على البروتوكول SOAP هو نموذج بسيط للطلب–الاستجابة.

- يقوم كيان في نظام يعمل كطالب في اللغة SAML بإرسال عنصر طلب في اللغة SAML داخل متن رسالة بروتوكول SOAP إلى كيان في نظام يعمل كمستجيب في اللغة SAML. ويتعين على الطالب SAML ألا يدرج أكثر من طلب واحد SAML في كل رسالة SOAP أو ألا يدرج أي عناصر إضافية من اللغة XML في المتن SOAP.
- يتعين على المستجيب في اللغة SAML إما أن يرجّع عنصر استجابة في اللغة SAML داخل متن رسالة أخرى SOAP وإما أن يولد خطأ بروتوكول SOAP. ويتعين على المستجيب SAML ألا يدرج أكثر من استجابة واحدة SAML في كل رسالة SOAP أو ألا يدرج أي عناصر إضافية من اللغة XML في المتن

SOAP. وإذا كان مستجيب في اللغة SAML لا يستطيع، لأي سبب كان، أن يعالج طلباً في اللغة SAML، يتعين عليه أن يولد خطأ SOAP. ويتعين ألا ترسل شفرات الخطأ SOAP للأخطاء الواقعة داخل ميدان المسألة SAML، كالعجز مثلاً عن العثور على تخطيطة توسّع أو كإشارة تدل على أن الصاحب ليس مرخصاً له بالنفاذ إلى مورد في استفهام عن ترخيص.

ملاحظة (للاطّلاع) – يقترح PE19 (انظر OASIS PE:2006) أن يستعاض عن الفقرة أعلاه بما يلي:

ينبغي للمستجيب في اللغة SAML أن يرجّع رسالة بروتوكول SOAP تحتوي إما على عنصر استجابة SAML في المتن وإما على خطأ بروتوكول SOAP. ويتعين على المستجيب SAML ألا يدرج أكثر من استجابة واحدة SAML في كل رسالة SOAP أو ألا يدرج أي عناصر إضافية من اللغة XML في المتن SOAP. وينبغي ألا ترسل شفرات الخطأ SOAP للأخطاء الواقعة داخل ميدان المسألة SAML، كالعجز مثلاً عن العثور على تخطيطة توسّع أو كإشارة تدل على أن الصاحب ليس مرخصاً له بالنفاذ إلى مورد في استفهام عن ترخيص.

عندما يستلم الطالب SAML استجابة SAML في رسالة بروتوكول SOAP، يتعين عليه ألا يرسل شفرة خطأ أو أي رسائل خطأ أخرى إلى المستجيب في اللغة SAML. ولما كان نسق مبادلة الرسائل هو مخطط بسيط للطلب–استجابة، فإن إضافة بنود إضافية مثل ظروف الخطأ ستعقّد البروتوكول بلا ضرورة.

يحيل البروتوكول SOAP في اللغة SAML إلى مشروع سابق لتوصيف تخطيطة اللغة XML يتضمن مكان اسم بالياً. فينبغي للطالبين في اللغة SAML أن يولدوا وثائق البروتوكول SOAP التي تحيل فقط إلى مكان الاسم الأخير في تخطيطة اللغة XML. ويتعين على المستجيبين في اللغة SAML أن يكونوا قادرين على معالجة مكان الاسم الوارد في تخطيطة اللغة XML المستعمل في الصيغة SOAP 1.1 (انظر البروتوكول SOAP الصادر عن التجمع W3C) وكذلك مكان الاسم الأخير في تخطيطة اللغة XML.

2.2.2.2.10 رأسيات البروتوكول SOAP

يمكن لطالب في اللغة SAML يجري محادثة في اللغة SAML على البروتوكول SOAP أن يضيف رأسيات اعتباطية إلى رسالة البروتوكول SOAP. ولا تعرّف هذه الرابطة أي رأسيات إضافية في البروتوكول SOAP.

الملاحظة 1 – إن السبب الذي يدعو إلى ضرورة السماح برأسيات أخرى هو أن بعض البرمجيات والمكتبات في البروتوكول SOAP ربما تضيف رأسيات إلى رسالة SOAP تقع خارج تحكم عملية اللغة SAML. وكذلك أيضاً فإن بعض الرأسيات ربما تحتاجها بروتوكولات تحتية تتطلب تسيير الرسائل أو تحتاجها آليات أمن الرسائل.

يتعين على المستجيب في اللغة SAML ألا يتطلب أي رأسيات في الرسالة SOAP، من أجل المعالجة الصحيحة للرسالة SAML بالذات، ولكنه يمكن أن يتطلب رأسيات إضافية تتطرق إلى التسيير التحتي أو إلى متطلبات أمن الرسائل.

الملاحظة 2 – إن من المعقول أن يتسبب تطلّب الرأسيات الإضافية، في تجزئة معيار اللغة SAMLن مما سيضر بقابلية التشغيل البيني.

3.2.2.2.10 استخدام البروتوكول SOAP فوق البروتوكول HTTP

يتعين على المعالج في اللغة الذي يطالب بالتطابق مع رابطة البروتوكول SOAP في اللغة SAML، أن ينفذ اللغة SAML على البروتوكول SOAP فوق البروتوكول HTTP. وتشرح هذه الفقرات الفرعية بعض الخصوصيات المتعلقة باستخدام البروتوكول SOAP فوق البروتوكول HTTP، بما في ذلك رأسيات البروتوكول HTTP، والوضع في ذاكرة مخبأ، والإبلاغ عن الأخطاء.

ورابطة البروتوكول HTTP للبروتوكول SOAP مشروحة في صيغة البروتوكول SOAP 6.0 الصادرة عن التجمع W3C. وهي تتطلب استعمال الرأسية `SOAPAction` كجزء من طلب البروتوكول HTTP والبروتوكول SOAP. ويتعين ألا يتوقف

مستجيب في اللغة SAML على قيمة هذه الرأسية. ويمكن لطالب في اللغة SAML أن يضع قيمة الرأسية SOAPAction كما يلي: http://www.oasis-open.org/committees/security

1.3.2.2.10 رأسيات البروتوكول HTTP

يمكن لطالب في اللغة SAML يجري محادثة SAML على البرتوكول SOAP فوق HTTP أن يضيف رأسيات اعتباطية إلى طلب البروتوكول HTTP. ولا تعرّف هذه الرابطة أي رأسيات HTTP إضافية.

الملاحظة 1 – إن السبب الذي يدعو إلى ضرورة السماح برأسيات أخرى هو أن بعض البرمجيات والمكتبات في البروتوكول HTTP ربما تضيف رأسيات إلى رسالة HTTP تقع خارج تحكم عملية اللغة SAML. وكذلك أيضاً فإن بعض الرأسيات ربما تحتاجها بروتوكولات تحتية تتطلب تسيير الرسائل أو تحتاجها آليات أمن الرسائل.

يتعين على المستجيب في اللغة SAML ألا يتطلب أي رأسيات في طلب البروتوكول HTTP، من أجل المعالجة الصحيحة للرسالة SAML بالذات، ولكنه يمكن أن يتطلب رأسيات إضافية تتطرق إلى التسيير التحتي أو إلى متطلبات أمن الرسائل.

الملاحظة 2 – إن من المعقول أن يتسبب تطلّب الرأسيات الإضافية في تجزئة معيار اللغة SAML، وهو سيضر بقابلية التشغيل البيني.

2.3.2.2.10 الوضع في ذاكرة مخبأ

ينبغي للوكلاء المفوّضين في البروتوكول HTTP ألا يضعوا رسائل بروتوكول اللغة SAML في ذاكرة مخبأ. وينبغي اتباع القواعد التالية من أجل ضمان ذلك:

ينبغي للطالبين عند استعمالهم الصيغة HTTP 1.1 أن يدرجوا:

- حقل رأسية Cache-Control موضوعاً على "no-cache, no-store" (لا ذاكرة مخبأ، ولا تخزين).
- حقل رأسية Pragma موضوعاً على "no-cache" (لا ذاكرة مخبأ)

وينبغي للمستجيبين، عند استعمالهم الصيغة HTTP 1.1:

- أن يدرجوا حقل رأسية Cache-Control موضوعاً على "no-cache, no-store, must-revalidate, private" (لا ذاكرة مخبأ، ولا تخزين، يتعين إعادة إقرار الصلاحية، خصوصي).
- أن يدرجوا حقل رأسية Pragma موضوعاً على "no-cache" (لا ذاكرة مخبأ).
- ألا يدرجوا مُقرّ صلاحية، مثل رأسية Last-Modified أو ETag.

3.3.2.2.10 الإبلاغ عن الأخطاء

المستجيب في اللغة SAML الذي يرفض القيام بتبادل رسالة مع الطالب في اللغة SAML، ينبغي له أن يرجّع الاستجابة "403 Forbidden". وفي هذه الحالة يكون محتوى متن البروتوكول HTTP غير دلالي.

وكما هو مشروح في صيغة البروتوكول SOAP 6.2 الصادرة عن التجمع W3C، عندما يحصل خطأ بروتوكول SOAP أثناء معالجة طلب بروتوكول SOAP، يتعين على مخدّم البروتوكول SOAP فوق HTTP أن يرجّع الاستجابة "500 Internal Server Error" وأن يضمّن رسالة SOAP في الاستجابة مع عنصر البروتوكول SOAP <SOAP-ENV:fault>. وينبغي ترجيع هذا النمط من الأخطاء إلى الأخطاء المتعلقة بالبروتوكول SOAP المكتشفة قبل مرور التحكم إلى المعالج في اللغة SAML، أو عندما يبلّغ المعالج في البروتوكول SOAP عن خطأ داخلي (مثل مكان الاسم باللغة XML في البروتوكول SOAP غير صحيح، ولا يمكن تحديد موقع تخطيطة اللغة SAML، والمعالج في اللغة SAML يثير استثناء، وهكذا).

ملاحظة (للاطّلاع) – يقترح PE19 (انظر [OASIS Document Errata]) أن يستعاض عن الجملة الأولى في الفقرة أعلاه بما يلي:

وكما هوي مشروح في صيغة البروتوكول SOAP 602 الصادرة عن التجمع W3C، عندما يحصل خطأ بروتوكول SOAP أثناء معالجة طلب بروتوكول SOAP، ينبغي لمخدّم البروتوكول SOAP فوق HTTP أن يرجّع الاستجابة "500 Internal Server Error" وأن يضمّن رسالة SOAP في الاستجابة مع عنصر البروتوكول SOAP <SOAP-ENV:fault>.

وفي حالة خطأ معالجة في اللغة SAML، يتعين على مخدّم البروتوكول SOAP فوق HTTP أن يستجيب بالإجابة "200 OK" وأن يدرج العنصر المعيّن باللغة SAML <samlp:Status> في استجابة اللغة SAML داخل متن البروتوكول SOAP. ولا يظهر العنصر <samlp:Status> بذاته في متن البروتوكول SOAP، ولكنه يظهر داخل استجابة في اللغة SAML من أي نوع.

ولمزيد من المعلومات حول استخدام شفرات الحالة في اللغة SAML، انظر البند المتعلق ببروتوكولات وتأكيدات اللغة SAML في هذه التوصية.

4.3.2.2.10 اعتبارات تتعلق بالمعطيات الشرحية

يجب أن ينعكس اعتماد رابطة البرتوكول SOAP بالدلالة على نقطة نهائية في محدّد URL يجب فيها إرسال الطلبات المحتواة في رسائل البروتوكول SOAP إلى بروتوكول خاص أو جانبية خاصة، أو بشكل بديل هو تعريف منفذ/نقطة نهائية في اللغة WSDL.

5.3.2.2.10 مثال على تبادل رسائل اللغة SAML باستخدام البروتوكول SOAP فوق HTTP

فيما يلي مثال على استفهام يسأل عن تأكيد يحتوي على إعلان نعت من سلطة النعت في اللغة SAML.

```
POST /SamlService HTTP/1.1
Host: www.example.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:AttributeQuery xmlns:samlp:="…"
xmlns:saml="…" xmlns:ds="…" ID="_6c3a4f8b9c2d" Version="2.0"
IssueInstant="2004-03-27T08:41:00Z"
            <ds:Signature> … </ds:Signature>
            <saml:Subject>
            …
            </saml:Subject>
        </samlp:AttributeQuery>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
Following is an example of the corresponding response, which supplies an
assertion containing the attribute statement as requested.
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:Response xmlns:samlp="…" xmlns:saml="…" xmlns:ds="…"
ID="_6c3a4f8b9c2d" Version="2.0" IssueInstant="2004-03-27T08:42:00Z">
            <saml:Issuer>https://www.example.com/SAML</saml:Issuer>
      <ds:Signature> … </ds:Signature>
            <Status>
              <StatusCode Value="…"/>
            </Status>
```

```
            <saml:Assertion>
                <saml:Subject>
                …
                </saml:Subject>
                <saml:AttributeStatement>
            …
                </saml:AttributeStatement>
             </saml:Assertion>
        </samlp:Response>
    </SOAP-Env:Body>
</SOAP-ENV:Envelope>
```

3.2.10 رابطة البروتوكول SOAP مقلوباً (PAOS)

تقوّي هذه الرابطة مواصفة رابطة البروتوكول HTTP المقلوبة للبروتوكول SOAP (انظر PAOS:2003). وعلى القائمين بالتنفيذ أن يستوفوا قواعد المعالجة العامة المحددة في PAOS، إضافة إلى القواعد المحددة في هذه التوصية. وفي حالة التنازع يكون المعيار هو Liberty Alliance POAS:2003.

1.3.2.10 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:bindings:PAOS`

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحييدات: لا يوجد.

2.3.2.10 نظرة شاملة

رابطة البروتوكول SOAP المقلوب هي آلية يستطيع بها طالب في البروتوكول HTTP أن يعلن عن قدرته على العمل كمستجيب في البروتوكول SOAP أو كوسيط في البروتوكول SOAP لطالب في اللغة SAML. والطالب في البروتوكول HTTP قادر على اعتماد مخطط يرسل فيه طلب اللغة SAML إليه في مغلّف SOAP داخل استجابة HTTP قادمة من طالب في اللغة SAML، والطالب في البروتوكول HTTP يستجيب باستجابة SAML داخل مغلّف SOAP في طلب لاحق في البروتوكول HTTP. وهذا المخطط لتبادل الرسائل يقبل الحالة المعرفة في جانبية الزبون أو الوكيل المفوض (ECP) باكتتاب التوقيع الوحيد (SSO) التي يكون فيها الطالب في البروتوكول HTTP هو وسيط في تبادل الاستيقان.

3.3.2.10 تبادل الرسائل

تشمل الرابطة PAOS مخططين لتبادل الرسائل المكوّنة:

1) يرسل الطالب في البروتوكول HTTP طلباً HTTP إلى مستجيب في اللغة SAML. فيستجيب الطالب في اللغة SAML باستجابة HTTP تحتوي على مغلّف البروتوكول SOAP يحتوي على رسالة طلب في اللغة SAML.

2) ويرسل الطلب HTTP بعد ذلك طلباً HTTP إلى الطالب SAML الأصلي، يحتوي على مغلف SOAP يضم رسالة استجابة في اللغة SAML. ويستجيب الطالب SAML باستجابة HTTP، ربما تكون استجابة لطلب الخدمة الأصلي الوارد في المرحلة 1).

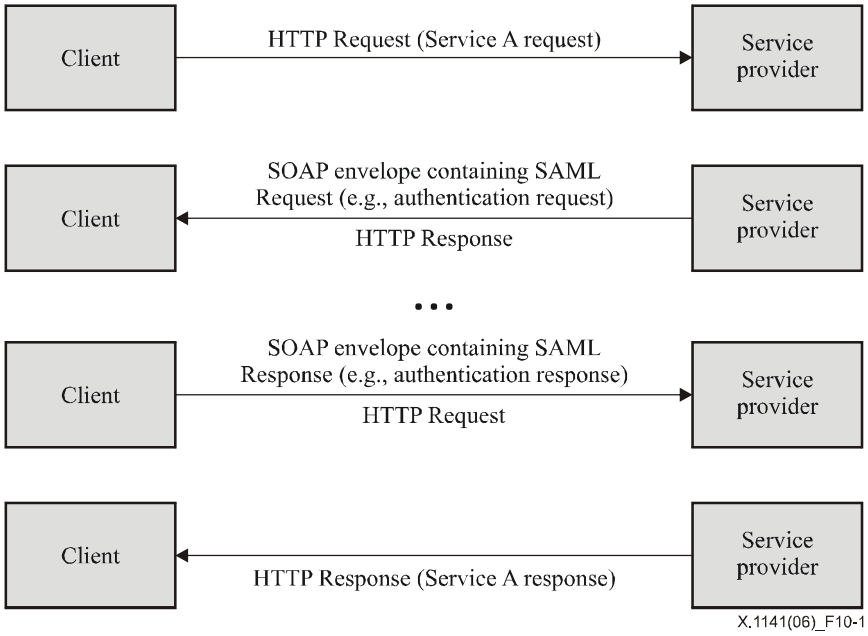
جانبية الزبون المعزز ECP تستخدم الرابطة PAOS لتوفير استيقان الزبون إلى مزوّد الخدمة قبل تقديم الخدمة. ويحدث ذلك وفق الخطوات التالية الموضحة في الشكل 10-1.

1) يطلب الزبون خدمة، مستعملاً طلب البروتوكول HTTP.

2) يستجيب مزوّد الخدمة بطلب استيقان في اللغة SAML. ويرسل هذا باستخدام طلب SOAP محمول في استجابة البروتوكول HTTP.

3) يرجّع الزبون استجابة SOAP محمولة في استجابة استيقان في اللغة SAML. وترسل هذه باستخدام طلب HTTP جديد.

4) بافتراض نجاح استيقان وترخيص مزوّد الخدمة، يمكن لمزوّد الخدمة أن يستجيب لطلب الخدمة الأصلي في الاستجابة HTTP.



الشكل X.1141/1-10 – تبادل رسائل الرابطة PAOS

يعلن الطالب في البروتوكول HTTP عن قدرته على معالجة هذه الرابطة المقلوبة في البروتوكول SAOP في طلباته HTTP التي تستعمل رأسيات البروتوكول HTTP المعرفة في المواصفة PAOS:2003. وخصوصاً:

- يتعين أن يبين حقل الرأسية `Accept` في البروتوكول HTTP القدرة على قبول نمط المحتوى `"application/vnd.paos+xml"`.
- يتعين أن يوجد حقل الرأسية PAOS في البروتوكول HTTP، وأن يحدّد صيغة PAOS مع حد أدنى `"urn:liberty:paos:2003-08"`. الملاحظة 1 (للاطّلاع) – يقترح PE21 (انظر OASIS PE:2006) إلغاء "مع حد أدنى" من النص أعلاه.

ويمكن أيضاً تحديد رأسيات إضافية PAOS مثل قيمة الخدمة، بواسطة جانبيات تستعمل الرابطة PAOS. ويستطيع الطالب في البروتوكول HTTP أن يضيف رأسيات اعتباطية إلى طلب البروتوكول HTTP. ويستطيع الطالب في البروتوكول HTTP أن يضيف رأسيات اعتباطية إلى طلب البروتوكول HTTP.

الملاحظة 2 – لا تعرّف هذه الرابطة آلية RelayStation. لذلك يترتب على الجانبيات الخاصة التي تستعمل هذه الرابطة أن تعرف مثل هذه الآلية، إن احتاج الأمر. ويقترح استعمال الرأسية SOAP لهذا الغرض.

وتقدم الفقرات الفرعية التالية مزيداً من التفصيلات عن مرحلتي تبادل الرسائل.

1.3.3.2.10 طلب HTTP مع طلب SAML في استجابة SOAP

يمكن لمستجيب HTTP في معرض استجابته لطلب HTTP اعتباطي، أن يرجّع رسالة طلب SAML باستخدام هذه الرابطة، عن طريق ترجعيه المغلف SOAP 1.1 في الاستجابة HTTP التي تحتوي على رسالة وحيدة لطلب SAML في متن البروتوكول

SOAP، من دون محتوى إضافي في المتن. ويمكن أن يحتوي المغلف SOAP على رأسيات SOAP اعتباطية، معرّفة في PAOS أو في جانبيات اللغة SAML أو في توصيات إضافية.

وعند تسليم رسالة الطلب SAML إلى الطالب HTTP، يمكن أن يكون المستلم المقصود الحقيقي هو كيان آخر في نظام، على أن يلعب الطالب في البروتوكول HTTP دور الوسيط، كما هو معرف في جانبيات معينة.

2.3.3.2.10 استجابة SAML في طلب SOAP مع استجابة HTTP

عندما يسلّم الطالب في البروتوكول HTTP رسالة استجابة في اللغة SAML إلى المستلم المقصود، مستعملاً الرابطة PAOS، يضعهان باعتبارها العنصر الوحيد من المتن SOAP، في مغلّف SOAP في طلب HTTP. ويمكن أن يكون الطالب HTTP هو مُصْدر الاستجابة SAML أو لا يكون. ويمكن أن يحتوي المغلّف SOAP على رأسيات SOAP اعتباطية، معرّفة في PAOS أو في جانبيات اللغة SAML أو في توصيات إضافية، ويعتبر التبادل SAML مكتملاً، والاستجابة HTTP لا تكون محددة بهذه الرابطة.

ويمكن أن تعرف الجانبيات قيوداً إضافية على محتوى البروتوكول HTTP غير الاستجابات SOAP، أثناء التبادلات التي تغطيها هذه الرابطة.

4.3.2.10 الوضع في ذاكرة مخبأ

ينبغي للوكلاء المفوضين في البروتوكول HTTP ألا يضعوا رسائل بروتوكول اللغة SAML في ذاكرة مخبأ. وينبغي اتباع القواعد التالية من أجل ضمان ذلك:

ينبغي للطالبين الذين يستعملون الصيغة HTTP 1.1 في إرسال رسائل بروتوكول اللغة SAML، أن يدرجوا:

- حقل رأسية `Cache-Control` موضوعاً على "`no-cache, no-store`" (لا ذاكرة مخبأ، ولا تخزين).
- حقل رأسية `Pragma` موضوعاً على "`no-cache`" (لا ذاكرة مخبأ)

وينبغي للمستجيبين، الذين يستعملوا الصيغة HTTP 1.1 في ترجيع رسائل بروتوكول اللغة SAML:

- أن يدرجوا حقل رأسية `Cache-Control` موضوعاً على "`no-cache, no-store, must-revalidate, private`" (لا ذاكرة مخبأ، ولا تخزين، يتعين إعادة إقرار الصلاحية، خصوصي).
- أن يدرجوا حقل رأسية `Pragma` موضوعاً على "`no-cache`" (لا ذاكرة مخبأ).
- ألا يدرجوا مُقرّ صلاحية، مثل رأسية `Last-Modified` أو ETag.

5.3.2.10 اعتبارات أمنية

يمكن لطالب في البروتوكول HTTP في رابطة PAOS أن يعمل كوسيط في البروتوكول SOAP، وعندما يعمل ذلك، قد لا يستوفي أمن طبقة النقل من أجل استيقان الأصل والسلامة والائتمانية، متطلبات الأمن من طرف إلى طرف. ويوصى في هذه الحالة بالأمن عند طبقة رسالة البروتوكول SOAP.

ملاحظة (للاطّلاع) – يقترح PE31 (انظر OASIS PE:2006) تغيير "ويوصى" وكتابتها بأحرف تاجية كبيرة.

1.5.3.2.10 الإبلاغ عن الأخطاء

يتعين التقيد باصطلاحات الخطأ المعياري في البروتوكولين HTTP وSOAP. ويتعين عدم الإشارة إلى الأخطاء التي تحدث أثناء معالجة اللغة SAML وإبلاغها إلى الطبقة HTTP أو SOAP، كما يتعين معالجتها باستعمال رسائل الاستجابة SAML مع عنصر الخطأ `<samlp:Status>`.

2.5.3.2.10 اعتبارات خاصة بالمعطيات الشرحية

اعتماد الرابطة PAOS ينبغي أن ينعكس بالدلالة على نقطة نهائية في المحدّد URL يجب أن ترسل فيها طلبات البروتوكول HTTP و/أو رسائل البروتوكول في اللغة SAML المحتواة في مغلّفات البروتوكول SOAP من أجل بروتوكول خاص أو جانبية خاصة. ويمكن تقديم نقطة نهائية واحدة أو نقاط نهائية متمايزة للطلب والاستجابة.

4.2.10 رابطة البروتوكول HTTP redirect (المعاد توجيهه)

تعرّف رابطة البروتوكول HTTP المعاد توجيهه آلية يمكن بواسطتها إرسال رسائل البروتوكول في اللغة SAML داخل معلمات المحدد URL. وطول المحدد URL المسموح به هو لا نهائي نظرياً، ولكنه محدود عملياً بصورة غير متوقعة. لذلك فهناك حاجة إلى تشفيرات متخصصة لحمل رسائل اللغة XML على محدد URL، فيمكن إرسال محتويات رسائل أطول أو أكثر تعقيداً باستخدام الرابطتين HTTP POST (بريد HTTP) أو HTTP Artifact.

يمكن أن تتكون هذه الرابطة من الرابطة HTTP POST (انظر الفقرة الفرعية 5.2.10) والرابطة HTTP Artifact (انظر الفقرة الفرعية 6.2.10) لكي ترسل رسائل الطلب والاستجابة في تبادل بروتوكول وحيد واستخدام رابطتين مختلفتين.

وتقتضي هذه الرابطة استعمال تشفير رسالة. وبينما يتضمن تعريف هذه الرابطة تعريف تشفير رسالة خاص، يمكن تعريف تشفيرات أخرى واستعمالها.

1.4.2.10 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد ادناه.

التحييزات: لا يوجد.

2.4.2.10 نظرة شاملة

أعدّت رابطة البروتوكول HTTP Redirect للحالات التي يحتاج فيها المرسل والمستجيب في اللغة SAML للتواصل باستخدام وكيل المستعمل في البروتوكول HTTP (كما هو معروف في الطلب RFC 2616 الصادر عن الفريق IETF) كوسيط. وهذا ضروري مثلاً إذا كان الطرفان المتواصلان لا يتقاسمان مسيراً مباشراً للتواصل. وقد يكون ذلك لازماً أيضاً إن كان المستجيب يتطلب تفاعلاً مع وكيل المستعمل من أجل تلبية الطلب، كما في الحالة التي يتعين فيها على وكيل المستعمل أن يستيقن نفسه للمستجيب.

وقد يكون لبعض وكلاء المستعملين في البروتوكول HTTP القدرة على لعب دور أكثر نشاطاً في تبادل البروتوكول، وقد يقبلون روابط أخرى تستعمل البروتوكول HTTP، مثل روابط البروتوكول SOAP والبروتوكول SOAP المقلوب. ولا تفترض هذه الرابطة شيئاً آخر، ما عدا إمكانيات متصفح شبكة الويب العادية.

3.4.2.10 RelayState

يمكن أن تكون معطيات RelayState واردة في رسالة بروتوكول اللغة SAML المرسلة مع هذه الرابطة. ويتعين ألا تزيد القيمة على 80 بايتة في الطول، وينبغي أن تكون سلامتها محمية من قبل الكيان الذي يخلق الرسالة، بصورة مستقلة عن أي حمايات أخرى قد تكون موجودة أثناء الإرسال أو لا تكون.

والتوقيع ليس واقعياً، نظراً إلى ضيق المكان، ولكن نظراً إلى أن القيمة معرضة لتلاعب طرف ثالث، ينبغي للكيان أن يتأكد من أن القيمة لم يصبها أي تلاعب، بأن يستخدم مجموعاً تدقيقياً أو قيمة شبه عشوائية أو وسائل أخرى مشابهة.

ملاحظة (للاطّلاع) – يقرر PE1 (انظر OASIS PE:2006) أن الجملة الأخيرة في الفقرة أعلاه ينبغي أن تقرأ كالتالي:

يمكن أن تكون معطيات RelayState واردة في رسالة بروتوكول اللغة SAML المرسلة مع هذه الرابطة. ويتعين ألا تزيد القيمة على 80 بايتة في الطول، وينبغي أن تكون سلامتها محمية من قبل الكيان الذي يخلق الرسالة، سواء عبر توقيع رقمي (انظر البند 10) أو بأي وسيلة مستقلة.

إذا كانت معطيات RelayState ترافق رسالة طلب في اللغة SAML، يتعين على المستجيب في اللغة SAML أن يرجّع استجابته في بروتوكول اللغة SAML باستعمال رابطة تقبل هي الأخرى آلية RelayState، ويتعين عليه أيضاً أن يضع المعطيات الصحيحة التي استلمها مع الطلب، داخل المعلمة المقابلة من RlayState في الاستجابة.

وإذا لم تكن مثل هذه القيمة واردة في رسالة طلب في اللغة SAML، أو إذا كانت رسالة الاستجابة في اللغة SAML تولدت من دون طلب يقابلها، يمكن للمستجيب في اللغة SAML إيراد معطيات RelayState لكي يفسرها المستلم استناداً إلى استعمال جانبية أو إلى اتفاق سابق بين الأطراف.

4.4.2.10 تشفير الرسالة

تشفّر الرسائل لاستعمالها مع هذه الرابطة باستخدام تقنية التشفير بالمحدد URL، وترسل باستخدام الطريقة HTTP GET. وهناك وسائل عديدة ممكنة لتشفير اللغة XML بالمحدد URL، حسب التقييدات النافذة. وتعرّف هذه التوصية واحدة من مثل هذه الطرائق، من دون أن تستبعد الطرائق الأخرى. وينبغي للنقاط النهائية في الرابطة أن تبين أي تشفيرات تقبل عند استخدام المعطيات الشرحية، حيث يلزم. ويتعين تعريف هوية التشفيرات الخاصة بطريقة وحيدة مع المعرّف URI عندما يتم تعريفه. وليس مطلوباً أن تكون جميع الرسائل الممكنة في اللغة SAML قابلة للتشفير بمجموعة خاصة من القواعد، ولكن على القواعد أن تبين بوضوح أي الرسائل أو المحتويات يمكن تشفيرها بهذه الطريقة، وأيها لا يمكن تشفيره.

ويتعين على التشفير بالمحدد URL أن يضع الرسالة بكاملها داخل سلسلة استفهام المحدد URL، ويتعين عليه أن يحتفظ ببقية المحدد URL للنقطة النهائية من مستلم الرسالة.

ويحتفظ بمعلمة سلسلة الاستفهام المسمّاة `SAMLEncoding` للتعريف بهوية آلية التشفير المستعملة. وإذا حذفت هذه المعلمة يفترض في القيمة أن تكون `urn:oasis:names:tc:SAML:2.0:bindings:URL-Encoding:DEFLATE`.

وجميع النقاط النهائية التي تعتمد هذه الرابطة يتعين عليها أن تعتمد التشفير DEFLATE المشروح فيما يلي:

1) يتعين سحب أي توقيع على رسالة بروتوكول اللغة SAML، بما في ذلك العنصر `<ds:Signature>` نفسه في اللغة XML. وإذا كان محتوى رسالة يضم توقيعاً آخر، مثل تأكيد موقّع في اللغة SAML، لا يسحب هذا التوقيع المبيّت. ومع ذلك فإن طول مثل هذه الرسالة بعد التشفير يمنع استخدام هذه الآلية. وعليه فرسائل البروتوكول SAML التي تحتوي على محتوى موقّع ينبغي ألا تشفّر باستخدام هذه الآلية.

2) وبعد ذلك تطبق آلية الانضباط DEFLATE كما هو مبين في الطلب RFC 1951 للفريق IETF، على كامل المحتوى المتبقي في اللغة XML من رسالة البروتوكول الأصلية في اللغة SAML.

3) وبعد ذلك تشفّر المعطيات المضغوطة بالأساس 64 طبقاً للقواعد المحددة في الطلب RFC 2045 للفريق IETF. ويتعين سحب تغييرات السطر وغيرها من الفراغات البيضاء من النتيجة.

4) والمعطيات المشفرة بالأساس 64 تشفّر بعدئذ بالمحدد URL، وتضاف إلى URL كمعلمة لسلسلة الاستفهام التي يجب أن تسمى `SAMLRequest` (إن كانت الرسالة طلباً في اللغة SAML) أو تسمى `SAMLResponse` (إن كانت الرسالة استجابة في اللغة SAML).

5) وإذا كانت المعطيات RelayState ترافق رسالة البروتوكول في اللغة SAML، يتعين أن تشفّر بالمحدد URL وتوضع في معلمة سلسلة استفهام إضافية تدعى `RelayState`.

6) وإذا كانت رسالة البروتوكول الأصلية في اللغة SAML موقعة باستعمال توقيع رقمي في اللغة SAML، ينبغي إضافة توقيع جديد يغطي المعطيات المشفرة بالشكل المحدد أعلاه، على أن تستخدم القواعد المذكورة أدناه.

لا تشفر التوقيعات الرقمية في اللغة XML مباشرة بالتشفير URL، وفقاً للقواعد المذكورة أعلاه بسبب إشكالات المكان. وإذا كانت رسالة البروتوكول التحتية في اللغة SAML موقعة بتوقيع في اللغة XML، يتعين أن يوقع الشكل المشفر بالمحدد URL كما يلي:

1) يتعين أن يكون معرف هوية خوارزمية التوقيع مدرجاً، باعتباره معلمة سلسلة استفهام إضافية تدعى SigAlg. وقيمة هذه المعلمة يجب أن تكون معرف هوية URI، يعرف هوية الخوارزمية المستعملة للتوقيع على رسالة البروتوكول المشفرة وفق URL في اللغة SAML، المحددة وفقاً للتوقيع في اللغة XML أو أي توصية تَحْكُم الخوارزمية.

2) ولتركيب التوقيع، تكون سلسلة من تتابع معلمات سلسلة الاستفهام التي هي RelayState (إن وجدت)، وSigAlg، وSAMLRequest (SAMLResponse) (وكل واحد منها مشفر بالمحدد URL)، ويركب كل واحد منها بواحد من السبل التالية (المرتّبة كما يلي):

أ)
```
SAMLRequest=value&RelayState=value&SigAlg=value
SAMLResponse=value&RelayState=value&SigAlg=value
```

ب) سلسلة البايتات الناتجة هي سلسلة الأثمونات التي تغذي خوارزمية التوقيع. وأي محتوى آخر موجود في سلسلة الاستفهام الأصلية لا يدرج ولا يوقّع عليه.

ج) يتعين أن تشفّر قيمة التوقيع باستخدام التشفير الذي أساسه 64 (انظر الطلب RFC 2045 للفريق IETF)، مع إزالة كل فرغ أبيض، وتدرج باعتبارها معلمة سلسلة الاستفهام المسماة Signature. وقد تحتاج بعض السمات الموجودة في قيمة التوقيع والمشفرة بالأساس 64، أن تشفر هي نفسها بالتشفير URL قبل أن تضاف.

د) خوارزميات التوقيع التالية (انظر التوقيع الصادر عن التجمع W3C) وتمثيلها بالمعرف URI يجب أن تعتمد مع آلية التشفير هذه:

- خوارزمية التوقيع الرقمي (DSA) مع خوارزمية الفرم المأمون-1 (SHA1): DSAwithSHA1 – http://www.w3.org/2000/09/xmldsig#dsa-sha1
- خوارزمية رايفست وشامير وأدلمان (RSA) مع خوارزمية الفرم المأمون-1 (SHA1): RSAwithSHA1 – http://www.w3.org/2000/09/xmldsig#rsa-sha1

ملاحظة- يشجع المعهد NIST حالياً (المعهد الوطني للمعايير والتكنولوجيا) على استعمال الخوارزمية SHA-256 (خوارزمية الفرم المأمون مع المفاتيح المشفرة بالعدد 256 من البتات) بدلاً من استعمال الخوارزمية SHA-1.

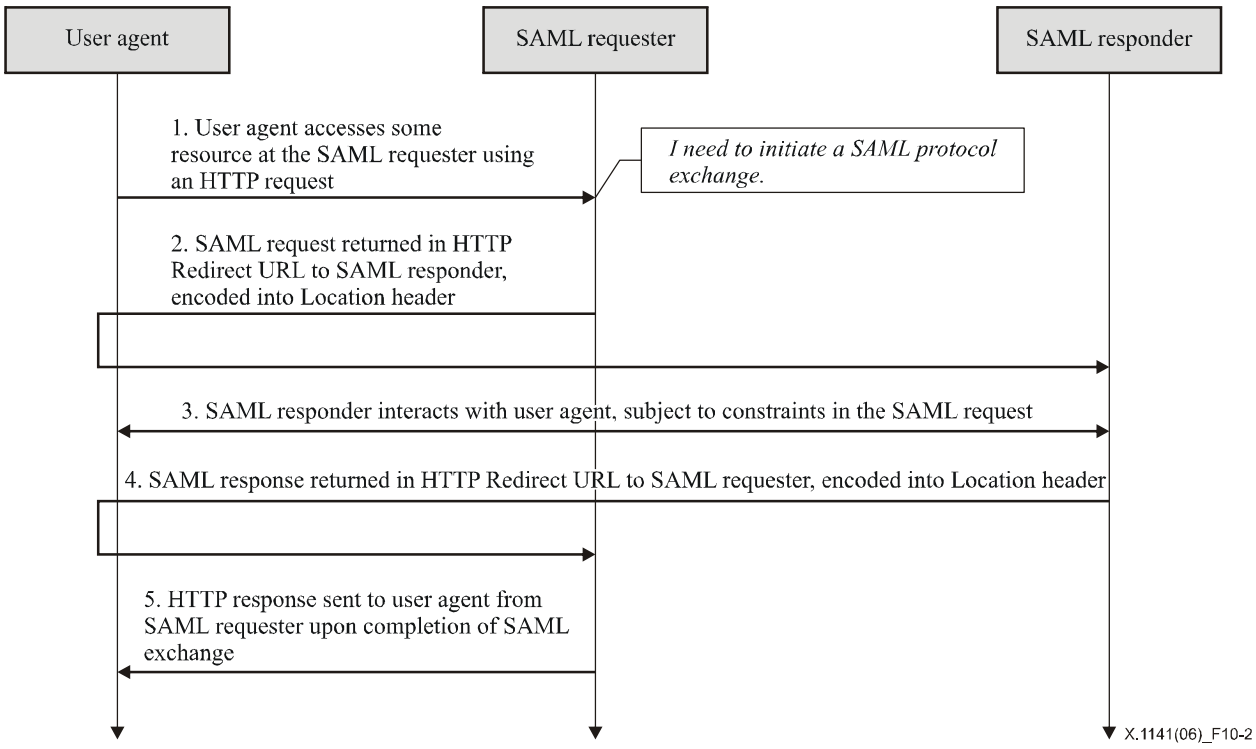
عند التحقق من التوقيعات، لا تفرض هذه الرابطة ترتيباً لمعلمات سلسلة الاستفهام على المحدد URL الناتج. ويمكن أن تظهر المعلمات بأي ترتيب كان. وقبل التحقق من توقيع ما، إن وجد، يتعين على الطرف الواثق أن يتأكد من أن قيم المعلمات المطلوب التحقق منها، مرتّبة وفق ما تتطلبه قواعد التوقيع المذكورة أعلاه.

إن التشفير بالمحدد URL ليس مشرعاً قانونياً، وهذا يعني أن هناك عدة تشفيرات شرعية لقيمة معينة، فيتعين على الطرف الواثق أن يقوم بخطوة التحقق مستعملاً القيم الأصلية المشفرة بالمحدد URL التي استلمها على سلسلة الاستفهام. ولا يكفي أن يعاد تشفير المعلمات، بعد أن كانت قد تمت معالجتها بالبرمجية، لأن التشفير الناتج قد لا يتواءم مع تشفير الموقّع.

وإذا لم تكن هناك قيمة RelayState، ينبغي حذف المعلمة بكاملها من حساب التوقيع (لا أن تدرج باعتبارها اسم معلمة خالياً).

5.4.2.10 تبادل الرسائل

إن نموذج النظام المستعمل للمحادثات في اللغة SAML عبر هذه الرابطة هو نموذج الطلب والاستجابة، ولكن هذه الرسائل ترسل إلى وكيل المستعمل داخل استجابة في البروتوكول HTTP، وتسلّم إلى مستلم الرسالة داخل طلب في البروتوكول HTTP. وتفاعلات البروتوكول HTTP قبل إجراء هذه التبادلات وأثناءها وبعدها، هي غير محددة. وكلا الطالب والمستجيب في اللغة SAML يفترض فيهما أن يكونا مستجيبين في البروتوكول HTTP. انظر المخطط التتابعي التالي (الشكل 10-2) الذي يوضح الرسائل المتبادلة.



الشكل X.1141/2-10 – تبادل رسائل HTTP redirect (المعاد توجيهه)

1) في البداية، يرسل وكيل المستعمل طلباً اعتباطياً HTTP إلى كيان في نظام. وأثناء معالجة الطلب، يقرر كيان النظام أن يبادر إلى تبادل بروتوكول في اللغة SAML.

2) يستجيب كيان النظام العامل كطالب في اللغة SAML إلى طلب البروتوكول HTTP من وكيل المستعمل في الخطوة 1 بترجيع طلب SAML. ويرجَّع الطلب SAML مشفراً في رأسية تحديد الموقع من الاستجابة HTTP، ويتعين أن تكون حالة البروتوكول HTTP هي 303 أو 302. ويمكن للطالب في اللغة SAML أن يدرج في الاستجابة HTTP تمثيلاً ومحتوى إضافيين، لكي يسهّل على وكيل المستعمل إرسال الرسالة، كما هو محدّد في الطلب RFC 2616 للفريق IETF. ويسلّم وكيل المستعمل الطلب SAML بإصداره طلباً HTTP GET إلى المستجيب SAML.

3) يمكن للمستجيب SAML عموماً أن يستجيب للطلب SAML بترجيعه فوراً استجابة SAML أو بترجيعه محتوى اعتباطياً لكي يسهّل التفاعل لاحقاً مع وكيل المستعمل، هذا التفاعل اللازم من أجل تلبية الطلب. وربما تضمنت بروتوكولات وجانبيات خاص، آليات تبين مدى استعداد الطالب للسماح بمثل هذا النوع من التفاعل (مثل النعت IsPassive في العنصر <samlp:AuthnRequest>).

4) ربما ينبغي للمستجيب أن يرجّع استجابة في اللغة SAML إلى وكيل المستعمل، لكي يتم ترجعيها إلى الطالب في SAML. وترجّع استجابة SAML بنفس الكيفية المشروحة للطلب SAML في الخطوة 2.

5) لدى استلام الطالب SAML الاستجابة SAML، يرجّع استجابة اعتباطية HTTP إلى وكيل المستعمل.

1.5.4.2.10 البروتوكول HTTP واعتبارات الوضع في ذاكرة مخبأ

ينبغي للوكلاء المفوضين في البروتوكول HTTP وللوسيط وكيل المستعمل ألا يضعوا رسائل بروتوكول اللغة SAML في ذاكرة مخبأ. ولتحقيق ذلك، ينبغي اتّباع القواعد التالية:

ينبغي للمستجيبين الذين يستعملون الصيغة HTTP 1.1، عند ترجيعهم رسائل البروتوكول في اللغة SAML، أن يدرجوا:

- حقل رأسية `Cache-Control`، موضوعاً على "`no-cache, no-store`" (لا ذاكرة مخبأ ولا تخزين).
- حقل رأسية `Pragma`، موضوعاً على "`no-cache`" (لا ذاكرة مخبأ).

2.5.4.2.10 اعتبارات أمنية

إن وجود الوسيط وكيل المستعمل يعني أن الطالب والمستجيب لا يستطيعان الاعتماد على طبقة النقل من أجل الاستيقان من طرف إلى طرف وحماية السلامة والائتمانية. ويمكن التوقيع على الرسائل المشفرة بالمحدد URL لتوفير استيقان المُصْدر والسلامة، إن كانت طريقة التشفير تحدد وسيلة للتوقيع.

إذا كانت الرسالة موقّعة، يتعين على نعت اللغة XML `Destination` في العنصر الجذر باللغة SAML من رسالة البروتوكول، أن يحتوي على محدد الموقع URL الذي كان المرسل قد أعطى تعليماته إلى وكيل المستعمل لكي يسلمه الرسالة. ويتعين على المستلم أن يتحقق من أن القيمة تتواءم مع الموقع الذي جرى فيه تسليم الرسالة.

وينبغي ألا تستعمل هذه الرابطة، إن كان محتوى الطلب أو الاستجابة ينبغي ألا يعرض على الوسيط وكيل المستعمل. وبعبارة أخرى فإن ائتمانية الطلبات والاستجابات في اللغة SAML هي اختيارية وتتوقف على بيئة الاستعمال. وبعبارة أخرى فإن ائتمانية الطلبات والاستجابات في اللغة SAML هي اختيارية وتتوقف على بيئة الاستعمال. فإذا كانت الائتمانية ضرورية، ينبغي استعمال الصيغة TLS 1.0 من البروتوكول TLS لحماية الرسالة العابرة بين وكيل المستعمل وبين الطالب والمستجيب في اللغة SAML.

ويمكن للرسائل المشفّرة بالمحدّد URL أن تعرض في العديد من سجلات البروتوكول HTTP وكذلك في الرأسية "Referrer" من البروتوكول HTTP.

ينبغي قبل النشر تحليل كل تجميعة من آليات الاستيقان وسلامة الرسالة وائتمانيتها من حيث قابلية تأثرها في سياق تبادل البروتوكول الخاص وبيئة النشر (انظر التذييل I).

وتعتمد هذه الرابطة عموماً على استيقان الرسالة وحماية سلامتها عبر التوقيع عليها، ولا تعتمد ائتمانية الرسائل القادمة من الوسيط وكيل المستعمل.

6.4.2.10 الإبلاغ عن الأخطاء

المستجيب في اللغة SAML الذي يرفض القيام بتبادل مع الطالب في اللغة SAML، ينبغي له أن يرجّع رسالة استجابة في اللغة SAML مع قيمة `<samlp:StatusCode>` من المستوى الثاني من: `urn:oasis:names:tc:SAML:2.0:status:RequestDenied`.

ويتعين على التفاعلات في البروتوكول HTTP أثناء تبادل الرسالة ألا تستعمل شفرات حالة الخطأ في البروتوكول HTTP لتدل على حالات الإخفاق في المعالجة SAML، طالما أن وكيل المستعمل ليس طرفاً كاملاً في تبادل البروتوكول SAML. انظر البند 9 أيضاً.

7.4.2.10 اعتبارات تتعلق بالمعطيات الشرحية

ينبغي أن ينعكس اعتماد رابطة البروتوكول HTTP Redirect (المعاد توجيهه) بالدلالة على نقاط نهائية للمحدّد URL، ينبغي فيها إرسال الطلبات والاستجابات إلى بروتوكول خاص أو جانبية خاصة. ويمكن تقديم نقطة نهائية واحدة أو نقاط نهائية متمايزة للطلب والاستجابة.

ملاحظة (للاطّلاع) – يقرر PE2 (انظر OASIS PE:2006) الاستعاضة عن الفقرة أعلاه بما يلي:

ينبغي أن ينعكس دعم استلام الرسائل الذي يستخدم الرابطة HTTP Artifact بالدلالة على نقاط نهائية للمحدّد URL، ينبغي فيها إرسال الطلبات والاستجابات إلى بروتوكول خاص أو جانبية خاصة. ويمكن تقديم نقطة نهائية واحدة أو نقاط نهائية متمايزة للطلب والاستجابة. أما دعم إرسال الرسائل الذي يستخدم هذه الرابطة فينبغي أن يترافق مع نقطة نهائية واحدة أو أكثر <md:ArtifactResolutionService> مفهرسة لمعالجة الرسائل <samlp:ArtifactResolve>.

8.4.2.10 مثال على تبادل الرسائل SAML الذي يستخدم الرابطة HTTP Redirect

يجري في هذا المثال تبادل زوج من الرسائل <LogoutRequest> و<LogoutResponse>، باستعمال الرابطة HTTP Redirect.

إليك في البداية الرسائل الحقيقية المتبادلة في بروتوكول اللغة SAML:

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="d2b7c388cec36fa7c39c28fd298644a8" IssueInstant="2004-01-
21T19:00:49Z" Version="2.0">
    <Issuer>https://IdentityProvider.com/SAML</Issuer>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">005a06e0-ad82-110d-a556-004005b13a2b</NameID>
    <samlp:SessionIndex>1</samlp:SessionIndex>
</samlp:LogoutRequest>

<samlp:LogoutResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="b0730d21b628110d8b7e004005b13a2b"
InResponseTo="d2b7c388cec36fa7c39c28fd298644a8"
    IssueInstant="2004-01-21T19:00:49Z" Version="2.0">
    <Issuer>https://ServiceProvider.com/SAML</Issuer>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
</samlp:LogoutResponse>
```

والطلب الأولي HTTP من وكيل المستعمل في المرحلة أعلاه لا تعرّفه هذه الرابطة. ولكي يبادر الطالب SAML إلى تبادل بروتوكول اختتام الدورة، عليه أن يرجّع الاستجابة HTTP التالية التي تحتوي على رسالة طلب موقّعة SAML. وقيمة المعلمة SAMLRequest تستنتج بالفعل من رسالة الطلب أعلاه. والجزء الخاص بالتوقيع هو توضيحي فقط، وليس نتيجة لعملية حساب فعلية. وعمليات تغيير السطر الواردة أدناه في الرأسية Location في البروتوكول HTTP هي شيء مصطنع في الوثيقةن ولا توجد عمليات تغيير السطر في قيمة الرأسية الفعلية.

```
HTTP/1.1 302 Object Moved
Date: 21 Jan 2004 07:00:49 GMT
Location:
https://ServiceProvider.com/SAML/SLO/Browser?SAMLRequest=fVFdS8MwFH0f7D%2BU
vGdNsq62oSsIQyhMESc%2B%2BJYlmRbWpObeyvz3puv2IMjyFM7HPedyK1DdsZdb%2F%2BEHfLF
fgwVMTt3RgTwzazIEJ72CFqRTnQWJWu7uH7dSLJjsg0ev%2FZFMlttiBWADtt6R%2BSyJr9msiR
H7O70sCm31Mj%2Bo%2BC%2B1KA5GlEWeZaogSQMw2MYBKodrIhjLKONU8FdeSsZkVr6T5M0GiHM
jvWCknqZXZ2OoPxF7kGnaGOuwxZ%2Fn4L9bY8NC%2By4du1XpRXnxPcXizSZ58KFTeHujEWkNPZ
ylsh9bAMYYUjO2Uiy3jCpTCMo5M1StVjmN9SO150sl9lU6RV2Dp0vsLIy7NM7YU82r9B90PrvCf
85W%2FwL8zSVQzAEAAA%3D%3D&RelayState=0043bfc1bc45110dae17004005b13a2b&SigAl
g=http%3A%2F%2Fwww.w3.org%2F200%2F09%2Fxmldsig%23rsa-
sha1&Signature=NOTAREALSIGNATUREBUTTHEREALONEWOULDGOHERE
Content-Type: text/html; charset=iso-8859-1
```

وبعد أن تحدث أي تفاعلات غير متوقعة، يرجّع المستجيب SAML الاستجابة HTTP التالية التي تحتوي على رسالة استجابة موقّعة SAML. وللمرة الثانية فإن قيمة المعلمة SAML response تستنتج بالفعل من رسالة الاستجابة أعلاه. والجزء الخاص بالتوقيع هو توضيحي فقط، وليس نتيجة لعملية حسابية فعلية.

```
HTTP/1.1 302 Object Moved
Date: 21 Jan 2004 07:00:49 GMT
Location:
https://IdentityProvider.com/SAML/SLO/Response?SAMLResponse=fVFNa4QwEL0X%2B
h8k912TaDUGFUp7EbZQ6rKH3mKcbQVNJBOX%2FvxaXQ9tYec0vHlv3nzkqIZ%2BlAf7YSf%2FBj
hagxB8Db1BuZQKMjkjrcIOpVEDoPRa1o8vB8n3VI7OeqttT1bJbbJCBOc7a8j9XTBH9VyQhqYRb
TlrEi4Yo61oUqA0pvShYZHiDQkqs411tAVpeZPqSAgNOkrOas4zzcW55ZlI4liJrTXiBJVBr4wv
CJ877ijbcXZkmaRUxtk7CU7gcB5mLu8pKVddvghd%2Ben9iDIMa3CXTsOrs5euBbfXdgh%2F9sn
DK%2FEqW69Ye%2BUnvGL%2F8CfbQnBS%2FQS3z4QLW9aT1oBIws0j%2FGOyAb9%2FV34Dw5k779
IBAAA%3D&RelayState=0043bfc1bc45110dae17004005b13a2b&SigAlg=http%3A%2F%2Fww
w.w3.org%2F200%2F09%2Fxmldsig%23rsa-
sha1&Signature=NOTAREALSIGNATUREBUTTHEREALONEWOULDGOHERE
Content-Type: text/html; charset=iso-8859-1
```

5.2.10 رابطة البروتوكول HTTP POST (إرسال بريد)

تعرّف الرابطة HTTP POST آلية ترسل بواسطتها رسائل البروتوكول SAML داخل محتوى مشفّر بالأساس 64، من تحكّم في الشكل في اللغة الإرشادية للنص الفائق (HTML).

ويمكن أن تتكون هذه الرابطة من الرابطة HTTP Redirect (انظر الفقرة 4.2.10) ومن الرابطة HTTP Redirect (انظر الفقرة 6.2.10) لكي ترسل رسائل الطلب والاستجابة في تبادل بروتوكول وحيد واستخدام رابطتين مختلفتين.

1.5.2.10 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحيينات: لا يوجد.

2.5.2.10 نظرة شاملة

أعدت رابطة البروتوكول HTTP POST (لإرسال بريد) للحالات التي يحتاج فيها المرسل والمستجيب في اللغة SAML للتواصل باستخدام وكيل مستعمل في البروتوكول HTTP (كما هو معروف في الطلب RFC 2616 للفريق IETF) كوسيط. وهذا ضروري مثلاً إذا كان الطرفان المتواصلان لا يتقاسمان مسيراً مباشراً للتواصل. وقد تدعو الحاجة إلى ذلك أيضاً إذا كان المستجيب يتطلب تفاعلاً مع وكيل المستعمل بغية تلبية الطلب، كما في الحالة التي يتعين فيها على وكيل المستعمل أن يستيقن نفسه لدى المستجيب.

وقد تكون لدى بعض وكلاء المستعمل في البروتوكول HTTP المقدرة على لعب دور أكثر نشاطاً في تبادل البروتوكول، وقد يقبلون روابط أخرى تستعمل البروتوكول HTTP، مثل روابط البروتوكول SOAP والبروتوكول SOAP المقلوب. ولا تفترض هذه الرابطة شيئاً آخر، ما عدا إمكانيات متصفح شبكة الويب العادية.

3.5.2.10 RelayState

يمكن أن تكون معطيات RelayState واردة في رسالة بروتوكول اللغة SAML المرسلة مع هذه الرابطة. ويتعين ألا تزيد القيمة على 80 بايتة في الطول، وينبغي أن تكون سلامتها محمية من قبل الكيان الذي يخلق الرسالة، بصورة مستقلة عن أي حمايات أخرى قد تكون موجودة أثناء إرسال الرسالة أو لا تكون. والتوقيع ليس واقعياً، نظراً إلى ضيق المكان، ولكن لما

كانت القيمة معرضة لتلاعب طرف ثالث، ينبغي للكيان أن يتأكد من أن القيمة لم يصبها أي تلاعب، بأن يستخدم مجموعاً تدقيقياً أو قيمة شبه عشوائية أو رسائل أخرى مشابهة.

إذا كانت معطيات RelayState ترافق رسالة طلب في اللغة SAML، يتعين على المستجيب في اللغة SAML أن يرجّع استجابته في بروتوكول اللغة SAML، باستعمال رابطة تقبل هي الأخرى آلية RelayState، ويتعين عليه أيضاً أن يضع المعطيات الصحيحة التي استلمها مع الطلب، داخل المعلمة المقابلة من RelayState في الاستجابة.

وإذا لم تكن مثل هذه القيمة واردة في رسالة طلب في اللغة SAML، أو إذا كان توليد رسالة الاستجابة في اللغة SAML قد جرى من دون طلب يقابلها، يمكن للمستجيب في اللغة SAML إيراد معطيات RelayState لكي يفسرها المستلم استناداً إلى استعمال جانبية أو إلى اتفاق سابق بين الأطراف.

ملاحظة (للاطّلاع) – يقترح PE31 (انظر OASIS PE:2006) أن يوضح الفقرة أعلاه كما يلي:

إذا كانت لا توجد معلمة RelayState واردة في رسالة طلب SAML، أو كانت رسالة الاستجابة في اللغة SAML تولدت من دون طلب يقابلها، يمكن للمستجيب في اللغة SAML إيراد معطيات RelayState لكي يفسرها المستلم استناداً إلى استعمال جانبية أو إلى اتفاق سابق بين الأطراف.

4.5.2.10 تشفير الرسائل

تشفّر الرسائل لكي تستعمل مع هذه الرابطة عن طريق تشفير اللغة XML بتحكم في الشكل في اللغة HTML، وترسل بطريقة الإرسال البريدي HTTP POST. وتشفّر رسالة البروتوكول في اللغة SAML بتشفير الشكل عن طريق تطبيق قواعد التشفير بالأساس 64، على تمثيل اللغة XML للرسالة، ثم توضع النتيجة في تحكم في الشكل مخفي داخل شكل، كما هو معرف في البند 17 من اللغة HTML الصادرة عن التجمع W3C. ويتعين أن تنتمي وثيقة اللغة HTML إلى اللغة الإرشادية التوسّعية للنص الفائق (XHTML) الصادرة عن التجمع W3C طبقاً للممارسات العامة.

إذا كانت الرسالة طلباً في اللغة SAML، يجب عندئذ تسمية التحكم في الشكل `SAMLRequest`. وإذا كانت الرسالة استجابة في اللغة SAML، يجب عندئذ تسمية التحكم في الشكل SAML response. ويمكن إدراج أي تحكم في الشكل أو تمثيل إضافيين، ولكن يجب ألا يكون ذلك مطلباً ملزماً، حتى يفسح المجال أمام المستلم لمعالجة الرسالة.

وإذا كان مطلوباً من قيمة "RelayState" أن ترافق رسالة البروتوكول SAML، يتعين وضعها في تحكم في الشكل مخفي إضافي يسمى `RelayState` داخل نفس الشكل مع الرسالة SAML.

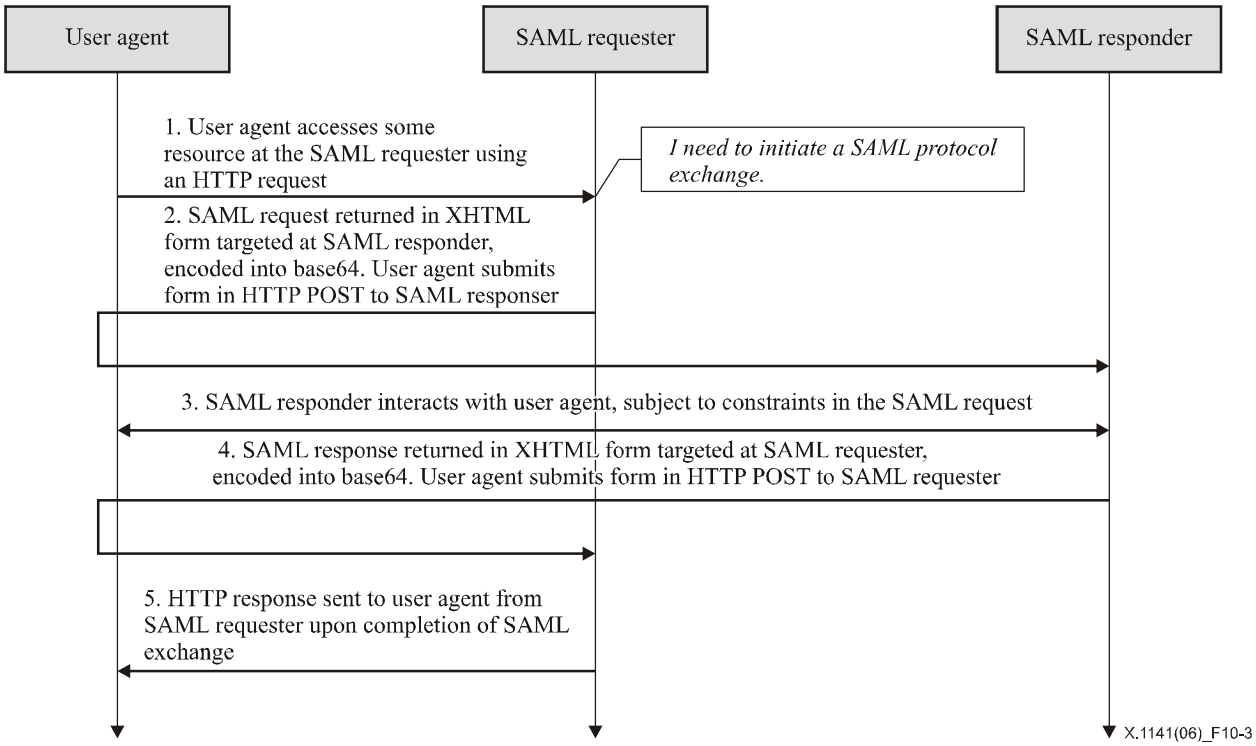
ويتعين أن يكون النعت action على الشكل هو النقطة النهائية في البروتوكول HTTP للمستلم من أجل البروتوكول أو الجانبية اللذين يستخدمان هذه الرابطة، التي يجب تسليم الرسالة لها. ويتعين أن يكون نعت الطريقة "POST".

كل تقنية يعتمدها وكيل المستعمل يمكن استعمالها لتسليم الشكل، كما يمكن إدراج أي محتوى شكل لازم لاعتماد ذلك، مثل التحكمات في التسليم وأوامر الكتابة في جانب الزبون. ومع ذلك يتعين على المستلم أن يكون قادراً على معالجة الرسالة، بصرف النظر عن الآلية التي تمت بها المبادرة إلى تسليم الشكل.

ويتعين أن يجري تحويل جميع قيم التحكم في الشكل، حتى تصبح جيدة لاحتواء وثيقة اللغة الإرشادية التوسّعية للنص الفائق (XHTML). وهذا يشمل تحويل سمات مثل القوسين المزدوجتين إلى كيانات في اللغة HTML.

5.5.2.10 تبادل الرسائل

إن نموذج النظام المستعمل للمحادثات في اللغة SAML عبر هذه الرابطة هو نموذج الطلب والاستجابة. ولكن هذه الرسائل ترسل إلى وكيل المستعمل داخل استجابة في البروتوكول HTTP، وتسلّم إلى مستلم الرسالة داخل طلب في البروتوكول HTTP. وتفاعلات البروتوكول HTTP قبل إجراء هذه التبادلات وأثناءها وبعدها، هي غير محددة. وكلا الطالب والمتسجيب في اللغة SAML يفترض فيها أن يكونا مستجيبين في البروتوكول HTTP. انظر الشكل 10-3 الذي يوضح الرسائل المتبادلة.



الشكل X.1141/3-10 – تبادل الرسائل HTTP POST

1) في البداية، يرسل وكيل المستعمل طلباً اعتباطياً HTTP إلى كيان في نظام. وأثناء معالجة الطلب، يقرر كيان النظام أن يبادر إلى تبادل بروتوكول في اللغة SAML.

2) يستجيب كيان النظام العامل كطالب في اللغة SAML إلى طلب البروتوكول HTTP من وكيل المستعمل بترجيعه طلباً SAML. ويرجّع الطلب في وثيقة باللغة XHTML تحتوي على الشكل والمحتوى المعرفين في الفقرة الفرعية 4.5.2.10. ويسلّم وكيل المستعمل الطلب SAML بإصداره طلباً HTTP POST إلى المستجيب SAML.

3) يمكن للمستجيب SAML عموماً أن يستجيب للطلب SAML بترجيعه فوراً استجابة SAML أو بترجيعه محتوى اعتباطياً لكي يسهّل التفاعل لاحقاً مع وكيل المستعمل، هذا التفاعل اللازم من أجل تلبية الطلب. وربما تضمنت بروتوكولات وجانبيات خاصة، آليات تبين مدى استعداد الطالب للسماح بمثل هذا النوع من التفاعل (مثل النعت `IsPassive` في العنصر `<samlp:AuthnRequest>`.

4) ربما ينبغي للمستجيب أن يرجّع استجابة في اللغة SAML إلى وكيل المستعمل. لكي يصار إلى ترجيعها إلى الطالب في SAML. وترجّع الاستجابة SAML بنفس الكيفية المشروحة للطلب SAML في الخطوة 2).

5) لدى استلام الطالب SAML الاستجابة SAML، يرجّع استجابة اعتباطية HTTP إلى وكيل المستعمل.

1.5.5.2.10 البروتوكول HTTP واعتبارات الوضع في ذاكرة مخبأ

ينبغي للوكلاء المفوضين في البروتوكول HTTP وللوسيط وكيل المستعمل ألا يضعوا رسائل بروتوكول اللغة SAML في ذاكرة مخبأ. ولتحقيق ذلك، ينبغي اتّباع القواعد التالية:

ينبغي للمستجيبين الذين يستعملون الصيغة HTTP 1.1، عند ترجيعهم رسائل البروتوكول في اللغة SAML، أن يدرجوا:

- حقل رأسية `Cache-Control`، موضوعاً على `"no-cache, no-store"` (لا ذاكرة مخبأ ولا تخزين).
- حقل رأسية `Pragma`، موضوعاً على `"no-cache"` (لا ذاكرة مخبأ).

ولا توجد أي تقييدات أخرى على استخدام رأسيات البروتوكول HTTP.

2.5.5.2.10 اعتبارات أمنية

إن وجود الوسيط وكيل المستعمل يعني أن الطالب والمستجيب لا يستطيعان الاعتماد على طبقة النقل من أجل الاستيقان من طرف إلى طرف وحماية السلامة والائتمانية. ويتعين عليها بدلاً من ذلك استيقان الرسائل المستلمة. وتقدم اللغة SAML التوقيع على رسائل البروتوكول من أجل الاستيقان والسلامة في مثل هذه الحالات. ويمكن التوقيع على الرسائل المشفّر شكلها، قبل تطبيق التشفير بالأساس 64.

وإذا كانت الرسالة موقّعة، يتعين على نعت اللغة XML Destination في العنصر الجذر باللغة SAML من رسالة البروتوكول، أن يحتوي على محدّد الموقع URL الذي كان المرسل قد أعطى تعليماته إلى وكيل المستعمل لكي يسلمه الرسالة. ويتعين على المستلم أن يتحقق من أن القيمة تتواءم مع الموقع الذي جرى فيه تسليم الرسالة.

وينبغي ألا تستعمل هذه الرابطة، إن كان محتوى الطلب أو الاستجابة ينبغي ألا يعرض على الوسيط وكيل المستعمل. وبعبارة أخرى فإن ائتمانية الطلبات والاستجابات في اللغة SAML هي اختيارية وتتوقف على بيئة الاستعمال. فإذا كانت الائتمانية ضرورية، ينبغي استعمال الصيغة TLS 1.0 من البروتوكول TLS لحماية الرسالة العابرة بين وكيل المستعمل وبين الطالب والمتسجيب في اللغة SAML.

وتعتمد هذه الرسالة عموماً على استيقان الرسالة وحماية سلامتها عبر التوقيع عليها، ولا تعتمد ائتمانية الرسائل القادمة من الوسيط وكيل المستعمل.

لا توجد آلية معرفة لحماية سلامة العلاقات بين رسالة البروتوكول في اللغة SAML والقيمة "RelayState" إن وجدت. وعلى ذلكن يستطيع أي متهجّم أن يعيد تركيب زوج من الاستجابات الصالحة في البروتوكول HTTP عن طريق تبديل قيم "RelayState" المصاحبة لكل رسالة بروتوكول SAML. ويمكن حماية سلامة القيم المنفردة للحالة "RelayState" وللرسالة SAML، ولكن لا يمكن حماية سلامتهما مندمجتين. وعليه يتعين على منتج معلومات "RelayState" وعلى مستهلكها أن يهتما بعدم جمع معلومات حساسة عن الحالة مع قيمة "RelayState" من دون اتخاذ احتياطات إضافية (مثل تلك التي تكون مبنية على معلومات واردة في رسالة SAML).

6.5.2.10 اعتبارات أمنية

المستجيب في اللغة SAML الذي يرفض القيام بتبادل رسالة مع الطالب في اللغة SAML، ينبغي له أن يرجّع رسالة استجابة مع قيمة <samlp:StatusCode> من المستوى الثاني من urn:oasis:names:tc:SAML:2.0:status:RequestDenied.

ويتعين على التفاعلات في البروتوكول HTTP أثناء تبادل الرسالة ألا تستعمل شفرات حالة الخطأ في البروتوكول HTTP لتدل على حالات الإخفاق في المعالجة SAML، طالما أن وكيل المستعمل ليس طرفاً كاملاً في تبادل البروتوكول SAML.

انظر الفقرة 2.8 لمزيد من المعلومات عن شفرات الحالة في اللغة SAML.

7.5.2.10 اعتبارات تتعلق بالمعطيات الشرحية

ينبغي أن ينعكس اعتماد الرابطة HTTP POST (إرسال بريد) بالدلالة على نقاط نهائية في المحدد URL، ينبغي فيها إرسال الطلبات والاستجابات إلى بروتوكول خاص أو جانبية خاصة. ويمكن تقديم نقطة نهائية واحدة أو نقاط نهائية متمايزة للطلب والاستجابة.

6.5.2.10 مثال على تبادل الرسائل SAML الذي يستخدم الرابطة HTTP POST

يتم في هذا المثال تبادل زوج من الرسائل <LogoutRequest> و<LogoutResponse>، باستعمال الرابطة HTTP POST.

إليك في البداية الرسائل الحقيقية المتبادلة في بروتوكول اللغة SAML.

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="d2b7c388cec36fa7c39c28fd298644a8" IssueInstant="2004-01-
21T19:00:49Z" Version="2.0">
    <Issuer>https://IdentityProvider.com/SAML</Issuer>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">005a06e0-ad82-110d-a556-004005b13a2b</NameID>
    <samlp:SessionIndex>1</samlp:SessionIndex>
</samlp:LogoutRequest>

<samlp:LogoutResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="b0730d21b628110d8b7e004005b13a2b"
InResponseTo="d2b7c388cec36fa7c39c28fd298644a8"
    IssueInstant="2004-01-21T19:00:49Z" Version="2.0">
    <Issuer>https://ServiceProvider.com/SAML</Issuer>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
</samlp:LogoutResponse>
```

والطلب الأولي HTTP من وكيل المستعمل في المرحلة أعلاه لا تعرّفه هذه الرابطة. ولكي يبادر الطالب SAML إلى تبادل بروتوكول اختتام الدورة، عليه أن يرجّع الاستجابة HTTP التالية التي تحتوي على رسالة طلب SAML. وقيمة المعلمة SAMLRequest تستنتج بالفعل من رسالة الطلب أعلاه.

```
HTTP/1.1 200 OK
Date: 21 Jan 2004 07:00:49 GMT
Content-Type: text/html; charset=iso-8859-1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<body onload="document.forms[0].submit()">

<noscript>
<p>
<strong>Note:</strong> Since your browser does not support JavaScript, you
must press the Continue button once to proceed.
</p>
</noscript>

<form action="https://ServiceProvider.com/SAML/SLO/Browser" method="post">
<div>
<input type="hidden" name="RelayState"
value="0043bfc1bc45110dae17004005b13a2b"/>
<input type="hidden" name="SAMLRequest"
value="PHNhbWxwOkxvZ291dFJlcXVlc3QgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1l
czp0YzpTQU1MOjIuMDpwcm90b2NvbCIgeG1sbnM9InVybjpvYXNpczpuYW1lczp0
YzpTQU1MOjIuMDphc3NlcnRpb24iDQogICAgSUQ9ImQyYjdjMzg4Y2VjMzZmYTdj
MzljMjhmZDI5ODY0NGE4IiBJc3N1ZUluc3RhbnQ9IjIwMDQtMDEtMjFUMTk6MDA6
NDlaIiBWZXJzaW9uPSIyLjAiPg0KICAgIDxJc3N1ZXI+aHR0cHM6Ly9JZGVudGl0
eVByb3ZpZGVyLmNvbS9TQU1MPC9Jc3N1ZXI+DQogICAgPE5hbWVJRCBGb3JtYXQ9
InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpuYW1laWQtZm9ybWF0OnBlcnNp
c3RlbnQiPjAwNWEwNmUwLWFkODItMTEwZC1hNTU2LTAwNDAwNWIxM2EyYjwvTmFt
ZUlEPg0KICAgIDxzYW1scDpTZXNzaW9uSW5kZXg+MTwvc2FtbHA6U2Vzc2lvbklu
ZGV4Pg0KPC9zYW1scDpMb2dvdXRSZXF1ZXN0Pg=="/>
</div>
<noscript>
<div>
<input type="submit" value="Continue"/>
</div>
</noscript>
</form>
</body>
</html>
```

وبعد أن تحدث أي تفاعلات غير متوقعة، يرجّع المستجيب SAML الاستجابة HTTP التالية التي تحتوي على رسالة استجابة SAML. وللمرة الثانية فإن قيمة المعلمة SAMLResponse تستنتج بالفعل من رسالة الاستجابة أعلاه.

```
HTTP/1.1 200 OK
Date: 21 Jan 2004 07:00:49 GMT
Content-Type: text/html; charset=iso-8859-1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<body onload="document.forms[0].submit()">

<noscript>
<p>
<strong>Note:</strong> Since your browser does not support JavaScript, you
must press the Continue button once to proceed.
</p>
</noscript>

<form action="https://IdentityProvider.com/SAML/SLO/Response"
method="post">
<div>
<input type="hidden" name="RelayState"
value="0043bfc1bc45110dae17004005b13a2b"/>
<input type="hidden" name="SAMLResponse"
value="PHNhbWxwOkxvZ291dFJlc3BvbnNlIHhtbG5zOnNhbWxwPSJ1cm46b2FzaXM6bmFt
ZXM6dGM6U0FNTDoyLjA6cHJvdG9jb2wiIHhtbG5zPSJ1cm46b2FzaXM6bmFtZXM6
dGM6U0FNTDoyLjA6YXNzZXJ0aW9uIg0KICAgIElEPSJiMDczMGQyMWI2MjgxMTBk
OGI3ZTAwNDAwNWIxM2EyYiIgSW5SZXNwb25zZVRvPSJkMmI3YzM4OGNlYzM2ZmE3
YzM5YzI4ZmQyOTg2NDRhOCINCiAgICBJc3N1ZUluc3RhbnQ9IjIwMDQtMDEtMjFU
MTk6MDA6NDlaIiBWZXJzaW9uPSIyLjAiPg0KICAgIDxJc3N1ZXI+aHR0cHM6Ly9T
ZXJ2aWNlUHJvdmlkZXIuY29tL1NBTUw8L0lzc3Vlcj4NCiAgICA8c2FtbHA6U3Rh
dHVzPg0KICAgICAgICA8c2FtbHA6U3RhdHVzQ29kZSBWYWx1ZT0idXJuOm9hc2lz
Om5hbWVzOnRjOlNBTUw6Mi4wOnN0YXR1czpTdWNjZXNzIi8+DQogICAgPC9zYW1s
cDpTdGF0dXM+DQo8L3NhbWxwOkxvZ291dFJlc3BvbnNlPg=="/>
</div>
<noscript>
<div>
<input type="submit" value="Continue"/>
</div>
</noscript>
</form>
</body>
</html>
```

6.2.10 الرابطة HTTP Artifact (الشيء المصطنع)

يرسل في الرابطة HTTP Artifact الطلب SAML أو الاستجابة SAML أو كلاهما عن طريق الإحالة باستخدام بديل صغير يدعى الشيء المصطنع. وتستخدم رابطة منفصلة متزامنة، مثل رابطة البروتوكول SOAP في اللغة SAML، لمبادلة الشيء المصطنع برسالة البروتوكول الحقيقية، عن طريق بروتوكول استبانة الشيء المصطنع المعرف في البند 8.

ويمكن أن تتألف هذه الرابطة من الرابطة HTTP Redirect (انظر الفقرة الفرعية 4.2.10) والرابطة HTTP POST (انظر الفقرة الفرعية 5.2.10) من أجل إرسال رسالتي الطلب والاستجابة في تبادل بروتوكول وحيد واستخدام رابطتين مختلفتين.

1.6.2.10 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه

التحيينات: لا يوجد

2.6.2.10 نظرة شاملة

أعدت الرابطة HTTP Artifact للحالات التي يحتاج فيها المرسل والمستجيب في اللغة SAML للتواصل باستخدام وكيل مستعمل في البروتوكول HTTP كوسيط، ولكن تحديدات الوسيط تمنع أو لا تشجع إرسال رسالة بكاملها (أو تبادل رسائل) عن طريقه. وقد يكون ذلك لأسباب تقنية أو لوجود ممانعة لغرض محتوى الرسالة على الوسيط (وإذا كان استعمال التجفير غير عملي).

ولما كانت هناك ضرورة لاستبانة الشيء المصطنع لاحقاً، باستخدام رابطة أخرى متزامنة مثل البروتوكول SOAP، لا بد من وجود مسير اتصال مباشر بين مرسل الرسالة SAML ومستلمها، في عكس اتجاه إرسال الشيء المصطنع (يتعين على مستلم الرسالة والشيء المصطنع أن يكون قادراً على إرسال طلب <samlp:ArtifactResolve> إلى الخلف إلى مُصْدر الشيء المصطنع). ويتعين على مُصْدر الشيء المصطنع أن يحتفظ بالحالة طالما الشيء المصطنع معلّق، مما يتسبب بتداعيات لبيئات موازنة الحمولات.

3.6.2.10 تشفير الرسائل

توجد طريقتان لتشفير شيء مصطنع من أجل استعماله في هذه الرابطة. ويشفّر الشيء المصطنع في إحداهما في معلمة للمحدد URL، ويوضع الشيء المصطنع في الأخرى في تحكم بالشكل في اللغة HTML. وعند استعمال التشفير بالمحدّد URL تستعمل الطريقة HTTP GET لتسليم الرسالة، بينما تستعمل طريقة POST عند التشفير بالشكل. ويتعين على جميع النقاط النهائية التي تقبل هذه الرابطة أن تعتمد التقنيتين كلتيهما.

RelayState 1.3.6.2.10

يمكن أن تكون معطيات RelayState واردة في الشيء المصطنع في اللغة SAML المرسل مع هذه الرابطة. ويتعين ألا تزيد القيمة على 80 بايتة في الطول، وينبغي أن تكون سلامتها محمية من قبل الكيان الذي يخلق الرسالة، بصورة مستقلة عن أي حمايات أخرى قد تكون موجودة أثناء إرسال الرسالة أو لا تكون. والتوقيع ليس واقعياً نظراً إلى ضيق المكان، ولكن لما كانت القيمة معرضة لتلاعب طرف ثالث، ينبغي للكيان أن يتأكد من أن القيمة لم يصبها أي تلاعب، بأن يستخدم مجموعاً تدقيقياً أو قيمة شبه عشوائية أو وسائل أخرى مشابهة.

وإذا كانت معطيات RelayState ترافق شيئاً مصطنعاً يمثل طلباً SAML، يتعين على المستجيب في اللغة SAML أن يرجّع استجابته في بروتوكول اللغة SAML، باستعمال رابطة تقبل هي الأخرى آلية RelayState، ويتعين عليه أيضاً أن يضع المعطيات الصحيحة التي استلمها مع الطلب، داخل المعلمة المقابلة من RelayState في الاستجابة.

وإذا لم تكن مثل هذه القيمة واردة في شيء مصطنع يمثل طلباً SAML، أو إذا كان توليد رسالة الاستجابة في اللغة SAML قد جرى من دون طلب يقابلها، يمكن للمستجيب في اللغة SAML إيراد معطيات RelayState لكي يفسرها المستلم استناداً إلى استعمال جانبية أو إلى اتفاق سابق بين الأطراف.

التشفير بالمحدّد URL 2.3.6.2.10

لكي يشفّر شيء مصطنع محدّد URL، تشفّر قيمة الشيء المصطنع بالمحدّد URL، وتوضع في معلمة سلسلة استفهام تسمى SAMLart.

وإذا كانت قيمة "RelayState" ترافق الشيء المصطنع في اللغة SAML، يتعين أن تكون القيمة مشفرة بالمحدد URL، وموضوعة في معلمة سلسلة استفهام إضافية تسمى RelayState.

التشفير بالشكل 3.3.6.2.10

يكون الشيء المصطنع في اللغة SAML مشفراً بالشكل، عند وضعه في تحكّم في الشكل مخفي داخل شكل، كما هو معرف في اللغة HTML التابعة للتجمع W3C. ويتعين أن تنتمي وثيقة اللغة HTML إلى اللغة الإرشادية التوسّعية للنص الفائق

(XHTML) التابعة للتجمع W3C. ويتعين تسمية التحكم في الشكل باسم SAMLart. ويمكن إدراج أي تحكم في الشكل أو تمثيل إضافيين، ولكن يجب ألا يكون ذلك مطلباً ملزماً، حتى يفسح المجال أمام المستلم لمعالجة الشيء المصطنع.

وإذا كان يطلب من قيمة "RelayState" أن ترافق شيئاً مصطنعاً في اللغة SAML، يتعين وضعها في تحكم في الشكل مخفي إضافي يسمى RelayState، داخل نفس الشكل مع رسالة اللغة SAML.

ويتعين أن يكون النعت action على الشكل هو النقطة النهائية من البروتوكول HTTP التابعة للمستلم، من أجل البروتوكول أو الجانبية اللذين يستخدمان هذه الرابطة، والتي يجب تسليم الشيء المصطنع لها. ويتعين أن يكون النعت method موضوعاً على "POST".

كل تقنية يعتمدها وكيل المستعمل يمكن استعمالها لتسليم الشكل، كما يمكن إدراج أي محتوى في الشكل لازم لاعتماد ذلك، مثل التحكمات في التسليم وأوامر الكتابة في جانب الزبون. ومع ذلك يتعين على المستلم أن يكون قادراً على معالجة الشيء المصطنع، بصرف النظر عن الآلية التي تمت بها المبادرة إلى تسليم الشكل.

ويتعين أن يجري تحويل جميع قيم التحكم في الشكل، حتى تصبح جيدة لاحتواء وثيقة اللغة الإرشادية التوسّعية للنص الفائق (XHTML). وهذا يشمل تحويل سمات مثل القوسين المزدوجتين إلى كيانات في اللغة HTML.

4.6.2.10 نسق الشيء المصطنع

الشيء المصطنع بالنسبة إلى هذه الرابطة هو سلسلة قصيرة وعاتمة. ويمكن تحديد أنماط مختلفة منه واستعمالها من دون أن يؤثر ذلك في الرابطة. وأهم خصائصه هي مقدرة مستلم الشيء المصطنع على تعرّف هوية مُصْدر الشيء المصطنع، ومقاومته للتلاعب وللتقليد، ووحدانيته، وتراصّه.

ويشمل النسق العام لأي شيء مصطنع على شفرة نمط الشيء المصطنع الإلزامية والمؤلفة من بايتين وعلى قيمة الدليل المؤلفة من بايتين والتي تعرف هوية نقطة نهائية معينة من خدمة استبانة الشيء المصطنع التابعة للمُصْدر، كما يلي:

```
SAML_artifact      := B64(TypeCode EndpointIndex RemainingArtifact)
TypeCode           := Byte1Byte2
EndpointIndex      := Byte1Byte2
```

يدل الترميز (TypeCode EndpointIndex RemainingArtifact) B64 على تطبيق التحويل بالأساس 64 (انظر طلب التعليقات RFC 2045 الصادر عن فريق المهام الهندسية في الإنترنت (IETF)) بالتعامل على TypeCode وEndpointIndex وRemainingArtifact.

ويوصى بالممارسات العملية التالية لإحداث أشياء مصطنعة في اللغة SAML:

- يسند معرف هوية URI إلى كل مُصْدر، وهو معروف أيضاً بمعرف هوية الكيان المُصْدر (أو المزوّد). انظر البند 8 لمناقشة هذا النوع من معرفات الهوية.
- يركب المُصْدر المكوّنة SourceID للشيء المصطنع، بأخذه الفَرْم SHA-1 من المحدد URL لتعريف الهوية. ولا تشفر قيمة الفرم بالنظام الستة عشري.

  الملاحظة 1 – يشجع المعهد الوطني للمعايير والتكنولوجيا (NIST) حالياً على استخدام الخوارزمية SHA-256 (خوارزمية الفرم المأمون مع مفاتيح مشفرة بالعدد 256 من البتات)،

- تركّب القيمة MessageHandle من تتابع من الأرقام شديد العشوائية أو شبه عشوائي من حيث التجفير (انظر طلب التعليقات RFC 1750 الصادر عن الفريق IETF)، يولده المُصْدر. ويتكون التتابع من قيم عددها على الأقل 16 بايتة في الطول. ويمكن تكديس هذه القيم حسب الحاجة حتى طول كلي قدره 20 بايتة.

الملاحظة 2 (للاطّلاع) – يقترح PE4 (انظر [OASIS Errata Document]) أن يضاف النص التالي إلى آخر الفقرة أعلاه.

على الرغم من أن البنية العامة للشيء المصطنع تشبه البنية المستعملة في الصيغ السابقة للغة SAML، وأن شفرة نمط النسق الوحيد المشروحة أدناه لا تتعارض مع الأنساق المعرفة سابقاً، فإنه لا يوجد صراحة أي تقابل بين الأشياء المصطنعة في الصيغة SAML 2.0 والأشياء المصطنعة التي وجدت في أي مواصفات سابقة، ويتعين ألا تستعمل مع هذه الرابطة أنساق الشيء المصطنع غير المعرفة لاستعمالها خصيصاً مع الصيغة SAML 2.0.

وفيما يلي شرح لنمط الشيء المصطنع الوحيد المعرف في الصيغة SAML 2.0.

1.4.6.2.10 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:artifact-04

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه

التحييزات: لا يوجد

2.4.6.2.10 تفاصيل النسق

تعرف الصيغة SAML V2.0 نمطاً من الشيء المصطنع شفرته 0x0004. وهذا النمط من الشيء المصطنع معرف كما يلي:

```
TypeCode          := 0x0004
RemainingArtifact := SourceID MessageHandle
SourceID          := 20-byte_sequence
MessageHandle     := 20-byte_sequence
```

وإن SourceID هو تتابع مؤلف من 20 بايتة، يستعمله مستلم الشيء المصطنع لكي يحدد هوية مُصْدر الشيء المصطنع ومجموعة محتملة من النقاط النهائية للاستبانة.

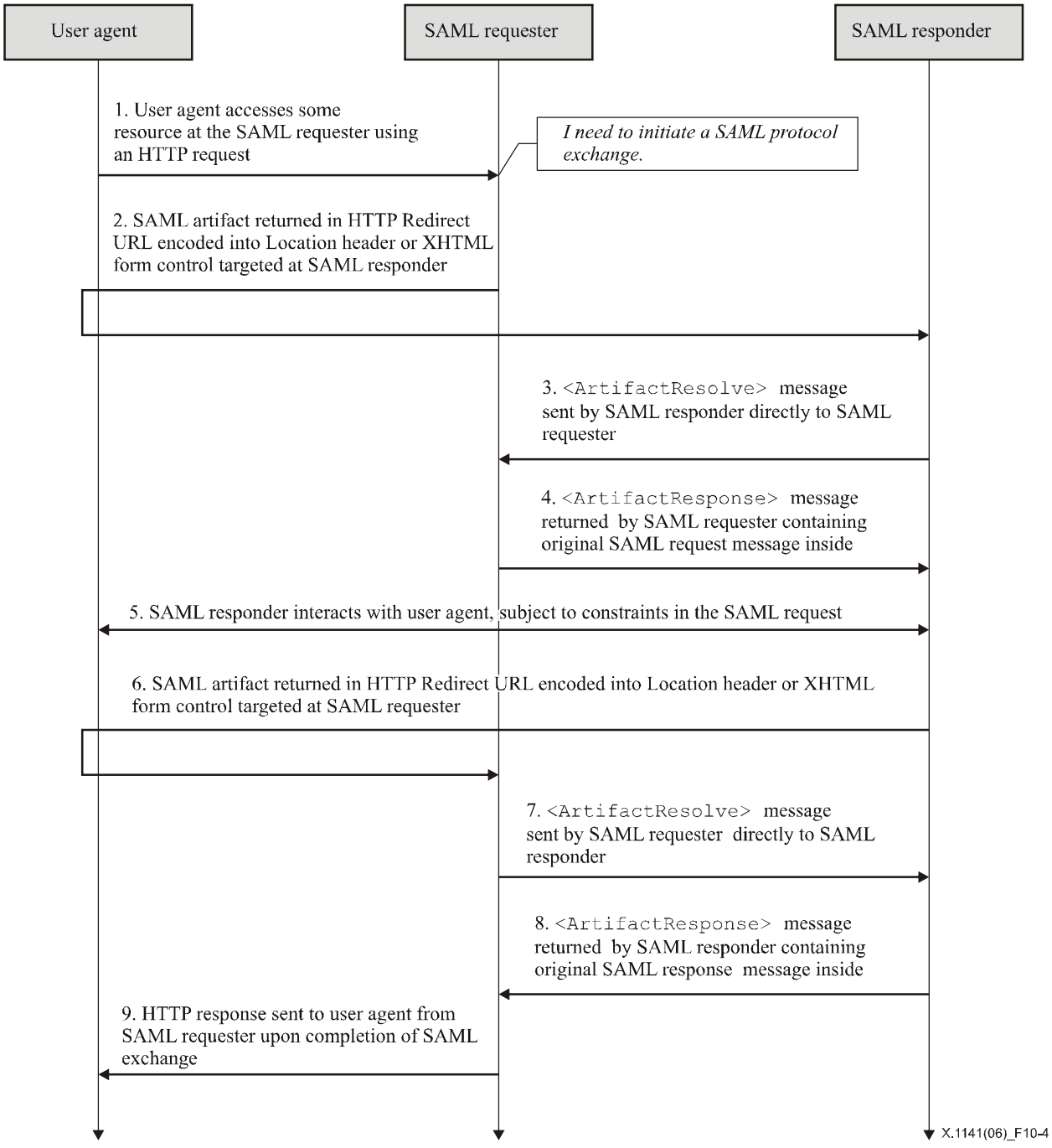
ومن المفترض أن يحتفظ موقع المقصد بجدول بقيم SourceID، وكذلك بنقطة نهائية واحدة أو أكثر للمحدد URL مفهرسة (أو بعناوين) للمستجيب المقابل في اللغة SAML. ويمكن استعمال البند 9 لهذا الغرض. وعندما يستلم مستلم الشيء المصطنع في اللغة SAML، يقوم بتحديد ما إذا كان SourceID يعود إلى مُصْدر معروف لشيء مصطنع، ويحصل على موقع المستجيب في اللغة SAML الذي يستخدم EndpointIndex، قبل أن يرسل إليه رسالة اللغة SAML <samlp:ArtifactResolve>.

5.6.2.10 تبادل الرسائل

إن نموذج النظام المستعمل للمحادثات في اللغة SAML عبر هذه الرابطة هو نموذج للطلب والاستجابة، يحل فيه المرجع إلى الشيء المصطنع محل محتوى الرسالة الفعلي، ويرسل المرجع إلى الشيء المصطنع إلى وكيل المستعمل في استجابة HTTP، ويسلم إلى مستلم الرسالة في طلب HTTP. وتفاعلات البروتوكول قبل إجراء هذه التبادلات وأثناءها وبعدها هي غير محددة. وكلا الطالب والمستجيب في اللغة SAML يفترض فيهما أن يكونا مستجيبين في البروتوكول HTTP.

وفوق ذلك، من المفترض أن يطلب المستلم، بمجرد استلامه شيئاً مصطنعاً عن طريق وكيل المستعمل، تبادلاً منفصلاً مباشراً مع مُصْدر الشيء المصطنع، مستخدماً بروتوكول استبانة الشيء المصطنع الذي تعرفه هذه التوصية. ويتعين أن يستعمل هذا التبادل رابطة لا تستعمل وكيل المستعمل HTTP كوسيط، مثل رابطة البروتوكول SOAP. وبعد أن تنجح حيازة رسالة بروتوكول SAML، يستبعد الشيء المصطنع، وتستأنف معالجة التبادل الأصلي لبروتوكول اللغة SAML (أو تنهى إن كانت الرسالة استجابة).

وإصدار واستلام شيء مصطنع، مع خطوة الاستبانة اللاحقة، تشكل نصف التبادل الكلي للبروتوكول SAML. يمكن استعمال هذه الرابطة لتسليم واحد من نصفي تبادل البروتوكول SAML أو كليهما. ويمكن استعمال رابطة قابلة للتركيب مع هذه الرابطة، مثل الرابطة HTTP Redirect (انظر الفقرة الفرعية 4.2.10) أو الرابطة POST (انظر الفقرة الفرعية 5.2.10)، لحمل النصف الآخرمن التبادل. ويفترض التتابع التالي أن رابطة الشيء المصطنع تستعمل للنصفين كليهما. انظر الشكل 10-4 الذي يوضح الرسائل المتبادلة.



الشكل X.1141/4-10 – تبادل رسائل HTTP aircraft

1) في البداية، يرسل وكيل المستعمل طلباً اعتباطياً HTTP إلى كيان في نظام. وأثناء معالجة الطلب، يقرر كيان النظام أن يبادر إلى تبادل بروتوكول في اللغة SAML.

2) يستجيب كيان النظام العامل كطالب في اللغة SAML إلى طلب البروتوكول HTTP من وكيل المستعمل، بترجيع شيء مصطنع يمثل طلباً SAML.

- إذا كان الشيء المصطنع مشفراً بالمحدد URL، يُرجَّع مشفراً في رأسية تحديد الموقع من الاستجابة HTTP، ويتعين أن تكون حالة البروتوكول HTTP هي 303 أو 302. ويمكن للطالب في اللغة SAML أن يدرج في الاستجابة HTTP تمثيلاً ومحتوى إضافيين، لكي يسهّل على وكيل المستعمل إرسال الرسالة، كما هو محدّد في الطلب RFC 2616 للفريق IETF. ويسلِّم وكيل المستعمل الشيء المصطنع مشفراً بالشكل، يُرجَّع في وثيقة اللغة XHTML التي تحتوي على الشكل والمحتوى المعرفين في الفقرة الفرعية 3.3.6.2.10. ويسلّم وكيل المستعمل الشيء المصطنع بإصداره طلباً HTTP POST إلى المستجيب SAML.
- وإذا كان الشيء المصطنع مشفراً بالشكل، يُرجَّع في وثيقة اللغة XHTML التي تحتوي على الشكل والمحتوى المعرفين في الفقرة الفرعية 3.3.6.2.10. ويسلّم وكيل المستعمل الشيء المصطنع بإصداره طلباً HTTP POST إلى المستجيب SAML.

3) يحدد المستجيب SAML من هو الطالب SAML بتفحصه الشيء المصطنع (تتوقف العملية المضبوطة على نمط الشيء المصطنع)، ويصدر طلباً <samlp:ArtifactResolve>، يحتوي على الشيء المصطنع، إلى الطالب SAML، مستخدماً رابطة SAML مباشرة، ومبادلاً الأدوار مؤقتاً.

4) بافتراض أن الشروط اللازمة مستوفاة، يرجّع الطالب SAML استجابة <samlp:ArtifactResponse> تحتوي على رسالة الطلب الأصلية SAML التي يرغب من المستجيب SAML أن يعالجها.

5) يمكن للمستجيب SAML عموماً أن يستجيب للطلب SAML بترجيعه فوراً شيئاً مصطنعاً SAML أو بترجيعه محتوى اعتباطياً لكي يسهّل التفاعل لاحقاً مع وكيل المستعمل، هذا التفاعل اللازم من أجل تلبية الطلب. وربما تضمنت بروتوكولات وجانبيات خاصة، آليات تبين مدى استعداد الطالب للسماح بمثل هذا النوع من التفاعل (مثل النعت IsPassive في العنصر <samlp:AuthnRequest>.

6) ربما ينبغي للمستجيب أن يُرجِّع شيئاً مصطنعاً في اللغة SAML إلى وكيل المستعمل، لكي يصار إلى ترجيعه إلى الطالب في SAML. ويُرجِّع الشيء المصطنع في الاستجابة SAML بنفس الكيفية المشروحة للشيء المصطنع في الطلب SAML في الخطوة 2).

7) ويحدد الطالب SAML من هوي المستجيب SAML بتفحصه الشيء المصطنع، ويُصدر طلباً <samlp:ArtifactResolve>، يحتوي على الشيء المصطنع، إلى المستجيب SAML، مستخدماً رابطة SAML مباشرة، كما في الخطوة 3).

ملاحظة (للاطّلاع) – يقترح PE31 (انظر OASIS PE:2006) أن يستعاض عن الجملة الأخيرة في الخطوة 6) بما يلي:

ويحدد الطالب SAML من هو المستجيب SAML بتفحصه الشيء المصطنع، ويُصْدر طلباً <samlp:ArtifactResolve>، يحتوي على الشيء المصطنع، إلى المستجيب SAML، مستخدماً رابطة SAML متزامنة، كما في الخطوة 3).

8) بافتراض أن الشروط اللازمة مستوفاة، يرجّع المستجيب SAML استجابة <samlp:ArtifactResponse> تحتوي على رسالة الاستجابة SAML التي يرغب من الطالب أن يعالجها، كما في الخطوة 3).

9) لدى استلام الطالب SAML الاستجابة SAML، يرجّع استجابة اعتباطية HTTP إلى وكيل المستعمل.

1.5.6.2.10 البروتوكول HTTP واعتبارات الوضع في ذاكرة مخبأ

ينبغي للوكلاء المفوضين في البروتوكول HTTP وللوسيط وكيل المستعمل ألا يضعوا أشياء مصطنعة من بروتوكول اللغة SAML في ذاكرة مخبأ. ولتحقيق ذلك، ينبغي اتّباع القواعد التالية:

- حقل رأسية Cache-Control موضوعاً على "no-cache, no-store" (لا ذاكرة مخبأ، ولا تخزين).
- حقل رأسية Pragma موضوعاً على "no-cache" (لا ذاكرة مخبأ)

ولا توجد أي تقييدات أخرى على استخدام رأسيات البروتوكول HTTP.

2.5.6.2.10 اعتبارات أمنية

تستعمل هذه الرابطة تركيبة من إرسال غير مباشر لمرجع رسالة، يتبعه تبادل مباشر لترجيع الرسالة الحقيقية. وينتج عن ذلك أن مرجع الرسالة (الشيء المصطنع) لا يحتاج أن يكون هو بالذات مستيقناً أو سلامته محمية، ولكن التبادل الراجع للطلب/الاستجابة الذي يرجّع الرسالة الحقيقية، يمكن أن يكون مستيقناً ومحمي السلامة بصورة متبادلة، حسب بيئة الاستعمال.

وإذا كانت رسالة البروتوكول SAML الحقيقية موجهة إلى مستلم معين، يتعين عندئذ على مُصْدر الشيء المصطنع أن يستيقن مرسل الرسالة اللاحقة <samlp:ArtifactResolve>، قبل أن يرجّع الرسالة الحقيقية.

وإرسال الشيء المصطنع إلى وكيل المستعمل أو منه، ينبغي أن يكون محمياً بالائتمانية، أو ينبغي استعمال الصيغة TLS 1.0. والتبادل الراجع طلب/استجابة الذي يرجّع الرسالة الحقيقية يمكن أن يكون محمياً، حسب بيئة الاستعمال.

وتعتمد هذه الرابطة عموماً على الشيء المصطنع كمرجع على المدى القصير يصعب تزويره، وتطبق تدابير أمنية أخرى على التبادل الراجع طلب/استجابة الذي يرجّع الرسالة الحقيقية. ويتعين على جميع الأشياء المصطنعة أن تكون لها دلالات وحيدة الاستعمال ينفذها مُصْدر الشيء المصطنع.

وفوق ذلك يوصى مستلمو الأشياء المصطنعة أن يطبقوا كذلك دلالات وحيدة الاستعمال على قيم الأشياء المصطنعة التي يستلمونها، لكي يمنعوا متهجماً من التداخل مع استبانة شيء مصطنع يقوم بها وكيل مستعمل، ثم يعاد تسليم الشيء المصطنع إلى مستلمه. وإذا لم تنته بنجاح محاولة استبانة شيء مصطنع، ينبغي وضع الشيء المصطنع في قائمة الأشياء المصطنعة المجمدة لفترة زمنية تتجاوز فترة القبول المعقولة التي ينبغي لمصدر الشيء المصطنع أن يستبين أثناءها الشيء المصطنع.

ولا توجد آلية محددة لحماية سلامة العلاقة بين الشيء المصطنع والقيمة "RelayState"، إن وجدت. وهذا يعني أن أي متهجم يمكنه إعادة تركيب زوج من الاستجابات الصالحة HTTP، عن طريق تبديل قيم "RelayState" التي تصاحب كل شيء مصطنع. وعليه يتعين على منتج أو مستهلك معلومات "RelayState" أن يحرص على ألا يرفق معلومات حالة حساسة، بقيمة "RelayState"، دون اتخاذ احتياطات إضافية (مثل الاعتماد على معلومات رسالة البروتوكول SAML المرجعة عبر الشيء المصطنع).

6.6.2.10 الإبلاغ عن الأخطاء

المستجيب في اللغة SAML الذي يرفض القيام بتبادل رسالة مع الطالب في اللغة SAML، ينبغي له أن يرجّع رسالة استجابة مع قيمة <samlp:StatusCode> من المستوى الثاني من: urn:oasis:names:tc:SAML:2.0:status:RequestDenied.

ويتعين على التفاعلات في البروتوكول HTTP أثناء تبادل الرسالة ألا تستعمل شفرات حالة الخطأ في البروتوكول HTTP لتدل على حالات الإخفاق في المعالجة SAML، طالما أن وكيل المستعمل ليس طرفاً كاملاً في تبادل البروتوكول SAML.

وإذا استلم مُصْدر شيء مصطنع رسالة <samlp:ArtifactResolve> يستطيع فهمها، عليه أن يرجّع <samlp:ArtifactResponse> مع قيمة <samlp:StatusCode> من

urn:oasis:names:tc:SAML:2.0:status:Success، حتى ولو لم يرجّع الرسالة المقابلة (مثلاً لأن طالب الشيء المصطنع ليس مرخصاً له أن يستقبل الرسالة أو لأن الشيء المصطنع لم يعد صالحاً).

7.6.2.10 اعتبارات تتعلق بالمعطيات الشرحية

ينبغي أن ينعكس اعتماد البروتوكول HTTP Artifact (الشيء المصطنع) بالدلالة على نقاط نهائية للمحدّد URLن ينبغي فيها إرسال الطلبات والاستجابات إلى بروتوكول خاص أو جانبية خاصة. ويمكن تقديم نقطة نهائية واحدة أو نقاط نهائية متمايزة للطلب والاستجابة. وينبغي توصيف نقطة نهائية واحدة أو أكثر لمعالجة الرسائل <samlp:ArtifactResolve>.

8.6.2.10 مثال على تبادل الرسائل SAML الذي يستخدم الرابطة HTTP Artifact

يجري في هذا المثال تبادل زوج من الرسائل <LogoutRequest> و<LogoutResponse>، باستعمال الرابطة HTTP Artifact، علماً بأن استبانة الشيء المصطنع تجري باستعمال الرابطة SOAP المربوطة بالبروتوكول HTTP.

إليك في البداية الرسائل الحقيقية المتبادلة في بروتوكول اللغة SAML:

الخطوة 1:

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="d2b7c388cec36fa7c39c28fd298644a8" IssueInstant="2004-01-
21T19:00:49Z" Version="2.0">
    <Issuer>https://IdentityProvider.com/SAML</Issuer>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">005a06e0-ad82-110d-a556-004005b13a2b</NameID>
    <samlp:SessionIndex>1</samlp:SessionIndex>
</samlp:LogoutRequest>

<samlp:LogoutResponse xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="b0730d21b628110d8b7e004005b13a2b"
InResponseTo="d2b7c388cec36fa7c39c28fd298644a8"
    IssueInstant="2004-01-21T19:00:49Z" Version="2.0">
    <Issuer>https://ServiceProvider.com/SAML</Issuer>
    <samlp:Status>
        <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    </samlp:Status>
</samlp:LogoutResponse>
```

والطلب الأولي من وكيل المستعمل في الخطوة 1 أعلاه لا تعرفه هذه الرابطة. ولكي يبادر الطالب SAML إلى تبادل بروتوكول اختتام الدورة، عليه أن يرجّع الاستجابة HTTP التالية التي تحتوي على الشيء المصطنع في اللغة SAML. وعمليات تغيير السطر في رأسية الموقع HTTP في الخطوة 2 أدناه هي نتيجة لإنساق الوثيقة، ولا توجد عمليات تغيير السطر في قيمة الرأسية الحقيقية.

الخطوة 2:

```
HTTP/1.1 302 Object Moved
Date: 21 Jan 2004 07:00:49 GMT
Location:
https://ServiceProvider.com/SAML/SLO/Browser?SAMLart=AAQAADWNEw5VT47wcO4zX
%2FiEzMmFQvGknDfws2ZtqSGdkNSbsW1cmVR0bzU%3D&RelayState=0043bfc1bc45110dae1
7004005b13a2b
Content-Type: text/html; charset=iso-8859-1
```

وبعد ذلك يستبين المستجيب SAML الشيء المصطنع الذي يستلمه في الطلب SAML الحقيقي، مستخدماً بروتوكول استبانة الشيء المصطنع ورابطة البروتوكول SOAP، كما في الخطوتين 3 و4 التاليتين:

الخطوة 3:

```
POST /SAML/Artifact/Resolve HTTP/1.1
Host: IdentityProvider.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:ArtifactResolve
              xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
              xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
              ID="_6c3a4f8b9c2d" Version="2.0"
              IssueInstant="2004-01-21T19:00:49Z">
              <Issuer>https://ServiceProvider.com/SAML</Issuer>
              <Artifact>
              AAQAADWNEw5VT47wcO4zX/iEzMmFQvGknDfws2ZtqSGdkNSbsW1cmVR0bzU=
              </Artifact>
        </samlp:ArtifactResolve>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

الخطوة 4:

```
HTTP/1.1 200 OK
Date: 21 Jan 2004 07:00:49 GMT
Content-Type: text/xml
Content-Length: nnnn

<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:ArtifactResponse
              xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
              xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
              ID="_FQvGknDfws2Z" Version="2.0"
              InResponseTo="_6c3a4f8b9c2d"
              IssueInstant="2004-01-21T19:00:49Z">
              <Issuer>https://IdentityProvider.com/SAML</Issuer>
              <samlp:Status>
                     <samlp:StatusCode
              Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
              </samlp:Status>
              <samlp:LogoutRequest ID="d2b7c388cec36fa7c39c28fd298644a8"
                     IssueInstant="2004-01-21T19:00:49Z"
                     Version="2.0">
                     <Issuer>https://IdentityProvider.com/SAML</Issuer>
                     <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">005a06e0-ad82-110d-a556-004005b13a2b</NameID>
                     <samlp:SessionIndex>1</samlp:SessionIndex>
              </samlp:LogoutRequest>
        </samlp:ArtifactResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

وبعد أن تحدث جميع التفاعلات غير المتوقعة، يرجّع المستجيب SAML شيئاً مصطنعاً ثانياً في اللغة SAML داخل استجابته في الخطوة 6:

```
HTTP/1.1 302 Object Moved
Date: 21 Jan 2004 07:05:49 GMT
Location:
https://IdentityProvider.com/SAML/SLO/Response?SAMLart=AAQAAFGIZXv5%2BQaBa
E5qYurHWJO1nAgLAsqfnyiDHIggbFU0mlSGFTyQiPc%3D&RelayState=0043bfc1bc45110da
e17004005b13a2b
Content-Type: text/html; charset=iso-8859-1
```

ثم يستبين المستجيب SAML الشيء المصطنع الذي يستلمه في الطلب SAML الحقيقي، مستخدماً بروتوكول استبانة الشيء المصطنع ورابطة البروتوكول SOAP، كما في الخطوتين 7 و8 التاليتين:

الخطوة 7:

```
POST /SAML/Artifact/Resolve HTTP/1.1
Host: ServiceProvider.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:ArtifactResolve
              xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
              xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
              ID="_ec36fa7c39" Version="2.0"
              IssueInstant="2004-01-21T19:05:49Z">
              <Issuer>https://IdentityProvider.com/SAML</Issuer>
              <Artifact>
              AAQAAFGIZXv5+QaBaE5qYurHWJO1nAgLAsqfnyiDHIggbFU0mlSGFTyQiPc=
              </Artifact>
        </samlp:ArtifactResolve>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

الخطوة 8:

```
HTTP/1.1 200 OK
Date: 21 Jan 2004 07:05:49 GMT
Content-Type: text/xml
Content-Length: nnnn

<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:ArtifactResponse
              xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
              xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
              ID="_FQvGknDfws2Z" Version="2.0"
              InResponseTo="_ec36fa7c39"
              IssueInstant="2004-01-21T19:05:49Z">
              <Issuer>https://ServiceProvider.com/SAML</Issuer>
              <samlp:Status>
                     <samlp:StatusCode
              Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
              </samlp:Status>
              <samlp:LogoutResponse ID="_b0730d21b628110d8b7e004005b13a2b"
                     InResponseTo="_d2b7c388cec36fa7c39c28fd298644a8"
                     IssueInstant="2004-01-21T19:05:49Z"
                     Version="2.0">
                     <Issuer>https://ServiceProvider.com/SAML</Issuer>
                     <samlp:Status>
                            <samlp:StatusCode
              Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
                     </samlp:Status>
              </samlp:LogoutResponse>
        </samlp:ArtifactResponse>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

7.2.10 اعتبارات تتعلق بالمعطيات الشرحية

معرفات الهوية الموحدة (URI) هي رسائل مستقلة عن البروتوكولات للإحالة إلى مورد. وهذه الرابطة ليست رابطة عامة في اللغة SAML للطب والاستجابة، بل هي داعمة لكبسلة رسالة <samlp:AssertionIDRequest> مع مرجع <saml:AssertionIDRef> واحد في استبانة معرف URI. ونتيجة طلب ناجح هي العنصر <saml:Assertion> (ولكنها ليست استجابة كاملة في اللغة SAML).

ومثل البروتوكول SOAP، فإن استبانة المعرف URI قد تحدث على العديد من عمليات النقل التحتية. ولهذه الرابطة جوانب استقلالية عن عملية النقل، ولكنها تستدعي أيضاً استخدام البروتوكول HTTP مع الصيغة TLS 1.0 حسب الطلب (التنفيذ إلزامي).

ملاحظة (للاطّلاع) – يقترح PE24 (OASIS PE:2006) أن يستعاض عن الفقرة أعلاه بما يلي:

ومثل البروتوكول SOAP، فإن استبانة المعرف URI قد تحدث على العديد من عمليات النقل التحتية. ولهذه الرابطة جوانب استقلالية عن البروتوكول، ولكنها تستدعي أيضاً التنفيذ الإلزامي للمعرفات URI في البروتوكول HTTP.

1.7.2.10 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:bindings:URI

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه

التحيينات: لا يوجد

2.7.2.10 الجوانب الاستقلالية عن البروتوكول لرابطة URI في اللغة SAML

تحدد الفقرات الفرعية التالية جوانب الرابطة URI في اللغة SAML التي هي مستقلة عن بروتوكول النقل التحتي في عملية استبانة المعرف URI.

المرجع SAML URI يعرف هوية تأكيد معين في اللغة SAML. ويتعين على نتيجة استبانة المعرف URI أن تكون رسالة تحتوي على تأكيد أو على خطأ خاص بالنقل يسمح بتوصيف المحتوى المرجَّع، مثل الصيغة HTTP 1.1، يمكن عندئذ تشفير التأكيد بأي نسق كان مسموح به. وإلا فيجب ترجيع التأكيد بشكل يمكن تفسيره بلا إبهام أو يمكن تحويله إلى تسلسل في اللغة XML للتأكيد.

إذا كان نفس مرجع المعرف URI ستتم استبانته في المستقبل، لا بد من ترجيع نفس التأكيد SAML أو ترجيع خطأ. وهذا يعني أن المرجع يمكن أن يكون دائماً، ولكنه يجب أن يميل بطريقة متماسكة إلى التأكيد نفسه، إن وجد.

3.7.2.10 اعتبارات أمنية

يمثل الاستعمال غير المباشر للتأكيد SAML أخطاراً، إذا كانت رابطة الإحالة إلى النتيجة مأمونة. وتتوقف التهديدات الخاصة وخطورتها على استعمال التأكيد. وينبغي ألا يوثق بنتيجة استبانة مرجع للمعرف URI إلى تأكيد SAML، إلا إذا كان الطالب يمكنه أن يتأكد من هوية المستجيب، وكان المحتوى لم يصبه أي تعديل أثناء العبور.

ولا يكون التوقيع على التأكيد نفسه كافياً في الغالب، لأن مراجع المعرفات URI هي بطبيعتها عائمة بالنسبة إلى الطالب. وينبغي أن يكون عند الطالب وسائل مستقلة لكي يتأكد من أن التأكيد المرجّع هو بالفعل التأكيد الذي يمثله المعرف URI، ويتحقق هذا الأمر باستيقان المستجيب وبالاعتماد على سلامة الاستجابة كليهما.

4.7.2.10 كبسلة التوسّعات MIME

فيما يخص بروتوكولات الاستبانة التي تعتمد التوسّعات المتعددة الأغراض في بريد الإنترنت (MIME) كتوصيف للمحتوى وآلية للترزيم، ينبغي ترجيع التأكيد الناتج باعتباره كياناً من التوسّعات MIME من النمط application/samlassertion+xml، كما هو محدّد في التذييل II.

5.7.2.10 استخدام المعرفات URI في البروتوكول HTTP

يتعين على السلطة SAML التي تطالب بالتطابق مع الرابطة HTTP URI أن تنفذ الاعتماد على البروتوكول HTTP. وتشرح هذه الفقرة الفرعية بعض الخصوصيات في استخدام المعرفات HTTP URI، بما في ذلك قواعد تركيب المعرف URI ورأسيات البروتوكول HTTP والإبلاغ عن الأخطاء.

1.5.7.2.10 قواعد تركيب المعرف URI

ليست هناك تقييدات عموماً على قواعد التركيب المسموح بها لمرجع المعرّف URI في اللغة SAML، طالما أن سلطة اللغة SAML المسؤولة عن المرجع هي التي تخلق الرسالة التي تحتوي على المرجع. ومع ذلك يتعين على السلطات أن تعتمد نقطة نهائية للمحدّد URL، لكي يرسل منها طلب البروتوكول HTTP مع معلمة واحدة من سلسلة الاستفهام تدعى معرف الهوية (ID). ويتعين ألا توجد أي سلسلة استفهام في المحدّد URL بالذات للنقطة النهائية بصرف النظر عن هذه المعلمة.

فعلى سبيل المثال، إذا كانت النقطة النهائية الموثقة لدى سلطة ما هي "https://saml.example.edu/assertions"، يمكن إرسال طلب تأكيد مع معرف الهوية من abcde إلى:

```
https://saml.example.edu/assertions?ID=abcde
```

ولا يسمح باستعمال السمات الاستبدالية في مثل هذه الاستفهامات عن معرفات الهوية (ID).

ملاحظة (للاطّلاع) – يقترح PE31 (انظر OASIS PE:2006) أن يستعاض عن الفقرة أعلاه بما يلي:

يلاحظ أن قواعد تركيب المعرّف URI لا تعتمد استعمال السمات الاستبدالية في مثل هذه الاستفهامات.

2.5.7.2.10 البروتوكول HTTP واعتبارات الوضع في ذاكرة مخبأ

يتعين على الوكلاء المفوضين في البروتوكول HTTP ألا يضعوا التأكيدات SAML في ذاكرة مخبأ. ولتحقيق ذلك، ينبغي اتّباع القواعد التالية:

ينبغي للمستجيبين في البرتوكول HTTP الذين يستعملون الصيغة HTTP 1.1 عند ترجيعهم تأكيدات اللغة SAML، أن يدرجوا:

- حقل رأسية Cache-Control موضوعاً على "no-cache, no-store" (لا ذاكرة مخبأ، ولا تخزين).
- حقل رأسية Pragma موضوعاً على "no-cache" (لا ذاكرة مخبأ)

3.5.7.2.10 اعتبارات أمنية

يشرح الطلب RFC 2617 للفريق IETF التهجمات المحتملة في بيئة البروتوكول HTTP، عند استعمال تخطيطات استيقان أساسي أو مختصر لرسالة.

يوصى بشدة استعمال الصيغة TLS 1.0 كوسيلة للاستيقان وحماية السلامة والائتمانية.

4.5.7.2.10 الإبلاغ عن الأخطاء

كما في حالة تبادل البروتوكول HTTP، ينبغي استعمال شفرة الحالة المناسبة في البروتوكول HTTP للدلالة على نتيجة الطلب. فالمستجيب في اللغة SAML الذي يرفض مثلاً القيام بتبادل رسالة مع الطالب SAML، ينبغي له أن يرجّع استجابة

"403 Forbidden". وإذا كان التأكيد المعين يجهله المستجيب، يتعين ترجيع استجابة "404 Not Found". وفي هذه الحالة لا يكون محتوى متن البروتوكول HTTP دلالياً.

5.5.7.2.10 اعتبارات تتعلق بالمعطيات الشرحية

اعتماد الرابطة URI فوق البروتوكول HTTP ينبغي أن ينعكس بالدلالة على النقطة النهائية في المحدّد URL التي يتم فيها إرسال الطلبات بشأن تأكيدات اعتباطية.

6.5.7.2.10 مثال على تبادل الرسائل SAML الذي يستخدم الرابطة HTTP URI

فيما يلي مثال على طلب بشأن تأكيد.

```
GET /SamlService?ID=abcde HTTP/1.1
Host: www.example.com
```

وفيما يلي مثال على الاستجابة المقابلة التي تدعم التأكيد المطلوب.

```
HTTP/1.1 200 OK
Content-Type: application/samlassertion+xml
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Length: nnnn

<saml:Assertion ID="abcde" ...>
...
</saml:Assertion>
```

11 الجانبيات في اللغة الإرشادية للتدعيم الأمني (SAML)

يحدد هذا البند الجانبيات التي تعرّف استخدام تأكيدات اللغة SAML ورسائل الطلب–الاستجابة في بروتوكولات الاتصال وأطر عمله، وكذلك الجانبيات التي تعرّف قواعد التركيب لقيمة النعت SAML واصطلاحات التسمية.

1.11 مفاهيم الجانبية

جانبية نمط في اللغة SAML تبرز معالم مجموعة من القواعد، تشرح كيف تُبيَّت تأكيدات اللغة SAML في إطار عمل أو في بروتوكول، وكيف تستخرج منها. وتشرح مثل هذه الجانبية كيف تُبيَّت تأكيدات اللغة SAML في أشياء أخرى أو تدمج معها (مثل الملفات من كل نمط، أو وحدات معطيات البروتوكول لبروتوكولات الاتصال) من قبل طرف مُصْدر لها، ومرسلة من الطرف المصدر إلى طرف مستلم، ثم تعالج لاحقاً في المقصد. وهناك مجموعة خاصة من القواعد من أجل تبييت التأكيدات SAML في صنف خاص واستخراجها منه هو صنف الأشياء <FOO>، وتسمى *الجانبية <FOO> في اللغة SAML*.

فالجانبية SOAP في اللغة SAML مثلاً تشرح كيف يمكن إضافة تأكيدات SAML إلى رسائل SOAP، وكيف تتأثر رأسيات SOAP بالتأكيدات SAML، وكيف ينبغي أن تنعكس حالات الخطأ المتعلقة باللغة SAML في رسائل البروتوكول SOAP.

وهناك نمط آخر من جانبيات اللغة SAML، يحدّد مجموعة من القيود على استعمال المقدرة العامة لبروتوكول أو تأكيد SAML في بيئة خاصة أو في سياق استعمال. والجانبيات من هذا النوع قد تقيّد الاختيار، وتتطلب استعمال وظائفية خاصة في اللغة SAML (مثل النعوت أو الشروط أو الروابط)، وهي تحدد من ناحية أخرى قواعد المعالجة التي يطلب من العناصر الفاعلة في الجانبية أن تتّبعها.

ومثال خاص من الجانبيات الأخيرة هو الجانبيات التي تتطرق إلى النعوت في اللغة SAML. إذ يقدّم العنصر <Attribute> في اللغة SAML قدراً كبيراً من المرونة في تسمية النعوت، وفي قواعد تركيب قيمتها، وفي إدراج معطيات شرحية داخل النطاق عبر استخدام نعوت اللغة XML. ويتحقق التشغيل البيني بتقييد هذه المرونة، عندما يكون مضموناً بالانتماء إلى الجانبيات التي تحدّد كيف تستعمل هذه العناصر بتخصُّصية أهم بكثير من القواعد العامة المحددة في البند 8.

توفر جانبيات النعت التعريفات الضرورية لتقييد تعبير النعت في اللغة SAML عند التعامل مع أنماط خاصة من معلومات النعت أو عند التفاعل مع أنظمة خارجية أو مع معايير مفتوحة أخرى تتطلب صرامة أكبر.

وترمي هذه التوصية إلى تحديد مجموعة من الجانبيات منتقاة من أنواع مختلفة مع تفصيلات كافية عنها تضمن التشغيل البيني لهذه المنتجات المنفذّة مستقلة عن بعضها.

2.11 مواصفة جانبيات إضافية

تحدد هذه التوصية مجموعة منتقاة من الجانبيات، ولكن غيرها يحتمل أن يتطور في المستقبل. وتقدم الفقرات الفرعية التالية مجموعة من الخطوط التوجيهية لتوصيف هذه الجانبيات.

1.2.11 الخطوط التوجيهية لتوصيف الجانبيات

تقدم هذه الفقرة الفرعية قائمة تفقّدية بالقضايا التي يتعين على كل جانبية أن تتطرق إليها.

1) أن تحدد معرف هوية URI، يعرّف الهوية تعريفاً وحيد التقابل للجانبية، ولمعلومات الاتصال الإلكتروني أو البريدي الخاصة بالمؤلف، ويوفر مرجعاً إلى الجانبيات المعرّفة سابقاً والتي تحيّنها الجانبية الجديدة أو تجعلها قديمة بالية.

2) أن تصف مجموعة من التفاعلات ما بين الأطراف المشتركة في الجانبية. ويتعين عليها أن تذكر صراحة كل التقييدات على التطبيقات التي يستعملها كل طرف، والبروتوكولات المشتركة في كل تفاعل (تآثر).

3) أن تعرّف هوية الأطراف المشتركة في كل تفاعل، بما في ذلك عدد الأطراف المشتركة، وما إذا كان هناك وسطاء مشتركون.

4) أن تحدّد طريقة استيقان الأطراف المشتركة في كل تفاعل، بما في ذلك إن كان الاستيقان مطلوباً، وما هي أنماط الاستيقان المقبولة.

5) أن تعرّف مستوى الدعم المطلوب لسلامة الرسالة، بما في ذلك الآليات المستعملة لتأمين سلامة الرسالة.

6) أن تعرّف مستوى الدعم المطلوب للائتمانية بما في ذلك إن كان يمكن لطرف ثالث أن يطلع على محتويات الرسائل والتأكيدات في اللغة SAML، وما إذا كانت الجانبية تتطلب الائتمانية، وما هي الآليات الموصى بها لتحقيق الائتمانية.

7) أن تعرّف حالات الخطأ، بما في ذلك حالات الخطأ لكل مشترك، وخاصة المشتركون الذين يستلمون ويعالجون تأكيدات ورسائل اللغة SAML.

8) أن تعرّف الاعتبارات الأمنية، بما في ذلك تحليل التهديدات ووصف التدابير المضادة.

9) أن تعرّف معرفات هوية طريقة التثبيت في اللغة SAML، والتي تحددها و/أو تستخدمها الجانبية.

10) أن تعرّف المعطيات الشرحية ذات الصلة في اللغة SAML، والتي تحددها و/أو تستخدمها الجانبية.

2.2.11 الخطوط التوجيهية لتوصيف جانبيات النعت

تقدم هذه الفقرة الفرعية قائمة تفقّدية بالبنود التي يتعين على جانبيات النعت أن تتطرق إليها.

1) أن تحدد معرّف هوية URI، يعرّف الهوية تعريفاً وحيد التقابل للجانبية، ولمعلومات الاتصال الإلكتروني أو البريدي الخاصة بالمؤلف، ويوفر مرجعاً إلى الجانبيات المعرّفة سابقاً والتي تحيّنها الجانبية الجديدة أو تجعلها قديمة بالية.

2) أن تضع قواعد التركيب والتقييدات بشأن القيم المقبولة للنعتين NameFormat وName بخصوص العناصر <Attribute> في اللغة SAML.

3) أن تحدد جميع النعوت الإضافية في اللغة XML لمكان الاسم الموصوف، والتي يمكن أن تستعمل للعناصر <Attribute> في اللغة SAML.

4) أن تعين القواعد التي تحدد تساوي العناصر <Attribute> في اللغة SAML، كما هي معرفة في الجانبية، من أجل استعمالها عند معالجة النعوت والاستفهامات وغيرها.

5) أن تضع قواعد التركيب والتقييدات بشأن القيم المقبولة في العنصر <AttributeValue> في اللغة SAML، بما في ذلك إن كان النعت xsi:type في اللغة XML يمكن أو ينبغي استعماله.

3.11 معرفات الهوية بطريقة التثبيت

يعرّف البند 8 العنصر <SubjectConfirmation> باعتباره Method ومعه <SubjectConfirmationData> بصورة اختيارية. وينبغي للطرف الواثق أن يستعمل العنصر <SubjectConfirmation> لكي يثبت أن الطلب أو الرسالة قادمان من كيان نظام مترافق مع صاحب التأكيد، داخل سياق جانبية خاصة.

يدل النعت Method على الطريقة الخاصة التي ينبغي للطرف الواثق أن يستعملها ليقوم بهذا التحديد. وقد يكون لذلك أو لا يكون علاقة مع استيقان كان قد أجري سابقاً. وبصرف النظر عن سياق الاستيقان، فإن طريقة تثبيت الصاحب تكون مصحوبة غالباً بمعلومات إضافية، مثل شهادة أو مفتاح، في العنصر <SubjectConfirmationData>، مما يسمح للطرف الواثق بأن يقوم بالتحقق اللازم. وتوجد مجموعة عامة معرّفة من النعوت يمكن استعمالها للحدّ من الشروط التي يمكن ضمنها القيام بالتحقق.

ومن المتوقع أن تعرّف الجانبيات قيماً مختلفة للعنصر <ConfirmationMethod> وأن تستعملها، وتكون كل منها تقابل سيناريو استعمال مختلف في اللغة SAML. والطرائق التالية محددة لكي تستعملها جانبيات معرّفة داخل هذه التوصية، وغيرها من الجانبيات التي تراها مفيدة.

1.3.11 حامل المفتاح

URI: urn:oasis:names:tc:SAML:2.0:cm:holder-of-key

ويتعين وجود عنصر واحد أو أكثر من العناصر <ds:KeyInfo> داخل العنصر <SubjectConfirmationData>. ويمكن أن يوجد نعت xsi:type في العنصر <SubjectConfirmationData>، وإذا كان موجوداً يتعين وضعه على **saml:KeyInfoConfirmationDataType** (وسابقة مكان الاسم اختيارية، ولكنها يجب أن تحيل إلى مكان اسم التأكيد SAML).

وكما هو مشروح في توقيع التجمع W3C، فإن كل عنصر <ds:KeyInfo> يحمل مفتاحاً أو معلومات تسمح لتطبيق بالحصول على مفتاح. وحامل مفتاح معيّن يعتبره الطرف المؤكِّد صاحب التأكيد.

وطبقاً لتوقيع التجمع W3C، يتعين على كل عنصر <ds:KeyInfo> أن يعرّف هوية مفتاح تجفيري واحد. ويمكن تعريف هوية عدة مفاتيح، بواسطة عناصر <ds:KeyInfo> منفصلة، كما هي الحال عندما تحتاج أطراف واثقة مختلفة إلى مفاتيح تثبيت عديدة.

مثال: يمكن لحامل مفتاح مسمّى "By-Tor" أو لحامل مفتاح مسمّى "Snow Dog"، أن يثبت نفسه كصاحب.

```
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-
key">
      <SubjectConfirmationData
xsi:type="saml:KeyInfoConfirmationDataType">
            <ds:KeyInfo>
```

```
                        <ds:KeyName>By-Tor</ds:KeyName>
                </ds:KeyInfo>
                <ds:KeyInfo>
                        <ds:KeyName>Snow Dog</ds:KeyName>
                </ds:KeyInfo>
        </SubjectConfirmationData>
</SubjectConfirmation>
```

2.3.11 كفالة المرسل

URI: urn:oasis:names:tc:SAML:2.0:cm:sender-vouches

تدل على أنه لا توجد معلومات أخرى متيسرة بشأن استخدام التأكيد. وينبغي للطرف الواثق أن يستخدم وسائل أخرى ليحدّد إن كان سيعالج التأكيد لاحقاً، مع مراعاة القيود الاختيارية على التثبيت التي تستعمل نعوتاً قد تكون موجودة في العنصر <SubjectConfirmationData>.

3.3.11 الحامل

URI: urn:oasis:names:tc:SAML:2.0:cm:bearer

صاحب التأكيد هو حامل التأكيد، مع مراعاة القيود الاختيارية على التثبيت التي تستعمل نعوتاً قد تكون موجودة في العنصر <SubjectConfirmationData>، كما هو معرف في البند 8.

مثال: يستطيع حامل التأكيد أن يثبت أنه هو نفسه الصاحب، شريطة أن يكون التأكيد مسلَّماً في رسالة مرسلة إلى "https://www.serviceprovider.com/saml/consumer" قبل الساعة 1:37 بعد الظهر بتوقيت غرينتش من يوم التاسع عشر من مارس 2004، استجابةً لطلب معرف هويته (ID) "1234567890_".

```
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <SubjectConfirmationData InResponseTo="_1234567890"
                Recipient="https://www.serviceprovider.com/saml/consumer"
                NotOnOrAfter="2004-03-19T13:27:00Z"
        </SubjectConfirmationData>
</SubjectConfirmation>
```

4.11 جانبيات التوقيع الوحيد (SSO) في اللغة SAML

هناك مجموعة من الجانبيات معرّفة لاعتماد التوقيع الوحيد (SSO) للمتصفحين ولأجهزة زبائن أخرى.

- تعرف جانبية مبنية على متصفح شبكة الويب، لبروتوكول طلب الاستيقان الوارد في البند 8، من أجل اعتماد الاكتتاب بالتوقيع الوحيد على شبكة الويب.
- تعرف جانبية إضافية للاكتتاب بالتوقيع الوحيد على شبكة الويب، من أجل دعم الزبائن المعززين.
- تعرف جانبية خاصة ببروتوكولي اختتام الدورة الوحيد وإدارة معرف هوية الاسم واردة في البند 8، وهي معرفة على كلتا رابطتي القناة الجبهية (متصفح) والقناة الخلفية.
- وتعرف جانبية إضافية لاكتشاف مزود الهوية باستخدام الكعكات.

1.4.11 جانبيات الاكتتاب بالتوقيع الوحيد لمتصفح على شبكة الويب

في السيناريو الذي تعتمده جانبية الاكتتاب بالتوقيع الوحيد (SSO) لمتصفح على شبكة الويب، يمكن لمستعمل الويب أن ينفذ إلى مورد لدى مزود الخدمة أو أن ينفذ إلى مزود هوية بحيث يكون مزود الخدمة والمورد المرغوب مفهومين أو ضمنيين. فيستيقن مستعمل الويب نفسه (أو قد يكون استيقن نفسه بالفعل) لدى مزود الهوية، الذي يصدر بعدئذ تأكيد استيقان (ربما

بإسهام من مزود الخدمة)، فيستهلك مزود الخدمة التأكيد حتى ينشئ سياقاً أمنياً لمستعمل الويب. وأثناء هذه العملية ينبغي أيضاً إقامة معرف هوية اسم بين المزودين من أجل الطرف الرئيسي، بمراعاة معلمات التفاعل والحصول على موافقة الأطراف.

ولتنفيذ هذا السيناريو، تستعمل جانبية لبروتوكول طلب الاستيقان في اللغة SAML، بالاشتراك مع الروابط HTTP Redirect وHTTP POST وHTTP Artifact.

ومن المفترض أن المستعمل يستخدم متصفحاً تجارياً عادياً، ويمكنه أن يستيقن نفسه لدى مزود الهوية ببعض الوسائل الواقعة خارج نطاق اللغة SAML.

1.1.4.11 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:profiles:SSO:browser`

معلومات الاتصال: security-services-comment@lists.oasis-open.org

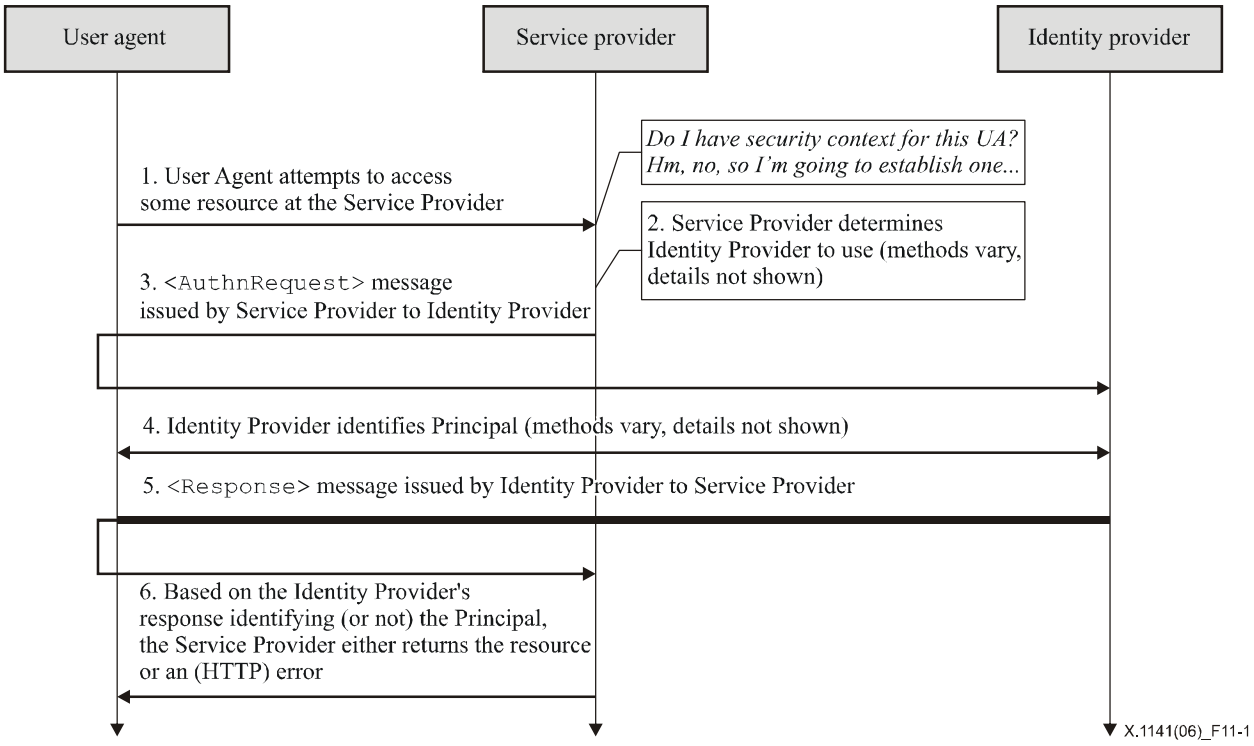
معرفات الهوية لطريقة التثبيت في اللغة SAML: تستخدم هذه الجانبية معرف الهوية لطريقة تثبيت "الحامل" في الصيغة SAML V2.0، `urn:oasis:names:tc:SAML:2.0:cm:bearer`.

الوصف: وارد أدناه.

التحيينات: لا يوجد.

2.1.4.11 نظرة شاملة إلى الجانبيات

يوضح الشكل 11-1 التخطيطة الأساسية لإنجاز الاكتتاب بالتوقيع الوحيد (SSO). والجانبية تشرح الخطوات التالية. وقد يقع في إحدى الخطوات لوحدها، تبادل واحد أو عدة تبادلات لرسائل حقيقية، حسب الرابطة المستعملة لهذه الخطوة، وغيرها من أوجه السلوك المتوقفة على التنفيذ.



الشكل X.1141/1-11 – التخطيطة الأساسية لإنجاز الاكتتاب SSO

1) طلب البروتوكول HTTP إلى مزود الخدمة

يقوم الطرف الرئيسي في الخطوة 1، عبر وكيل المستعمل في HTTP، بتقديم طلب HTTP وإلى مورد مأمون لدى مزود الخدمة، من دون سياق أمني.

2) مزود الخدمة يحدد مزود الهوية

يحصل مزود الخدمة في الخطوة 2 على موقع نقطة نهائية لدى مزود الهوية من أجل بروتوكول طلب الاستيقان الذي يعتمد رابطته المفضلة. والوسائل التي يتحقق بها ذلك تتوقف على التنفيذ. وقد يستعمل مزود الخدمة جانبية اكتشاف مزود الهوية في اللغة SAML، كما هو مشروح في الفقرة الفرعية 4.7.8.

3) إصدار مزود الخدمة رسالة <AuthnRequest> إلى مزود الهوية

يصدر مزود الخدمة في الخطوة 3 رسالة <AuthnRequest>، لكي يسلمها وكيل المستعمل إلى مزود الهوية. ويمكن استعمال أي واحدة من الروابط HTTP Redirect أو HTTP POST أو HTTP Artifact من أجل نقل الرسالة إلى مزوّد الهوية عبر وكيل المستعمل.

4) مزود الهوية يعرف هوية الطرف الرئيسي

يقوم مزوّد الهوية في الخطوة 4 بتعريف هوية الطرف الرئيسي بواسطة وسائل لا تقع في نطاق هذه الجانبية. وقد يتطلب ذلك عمل استيقان جديداً أو قد يعاد استعمال دورة مستيقنة موجودة.

5) إصدار مزوّد الهوية رسالة <Response> إلى مزود الخدمة

يصدر مزوّد الهوية في الخطوة 5 رسالة <Response>، لكي يسلمها وكيل المستعمل إلى مزوّد الخدمة. ويمكن استعمال أي واحدة من الرابطتين HTTP POST أو HTTP Artifact لنقل الرسالة إلى مزوّد الخدمة عبر وكيل المستعمل. وقد تشير الرسالة إلى خطأ أو قد تحتوي على تأكيد استيقان (على الأقل). ويتعين ألا تستعمل الرابطة HTTP Redirect، طالما أن الاستجابة ستتجاوز عموماً طول المحدِّد URL الذي يسمح به معظم وكلاء المستعمل.

6) مزوّد الخدمة يمنح النفاذ للطرف الرئيسي أو يرفضه له

بعد أن يستلم مزوّد الخدمة الاستجابة من مزوّد الهوية، يمكنه في الخطوة 6 أن يستجيب لوكيل المستعمل للطرف الرئيسي مع خطأه الخاص، أو يمكنه أن ينشئ سياقه الأمني الخاص بالطرف الرئيسي، ويرجّع المورد المطلوب.

يستطيع مزوّد الخدمة المبادرة إلى هذه الجانبية من الخطوة 5، ويصدر رسالة <Response> إلى مزود الخدمة، من دون الخطوات التي قبلها.

3.1.4.11 وصف الجانبية

إذا كان مزوّد الخدمة هو الذي يبتدر الجانبية، يبدأ بالفقرة الفرعية 1.3.1.4.11. وإذا كان مزوّد الهوية هو الذي يبتدر الجانبية، يبدأ بالفقرة الفرعية 5.3.1.4.11. وفي الوصف التالي، يعود ما يلي إلى:

خدمة التوقيع الوحيد

هذه هي النقطة النهائية لبروتوكول طلب الاستيقان لدى مزوّد الهوية، التي فيها يسلّم وكيل المستعمل الرسالة <AuthnRequest> (أو الشيء المصطنع الذي يمثلها).

خدمة مستهلك التأكيد

هذه هي النقطة النهائية لبروتوكول طلب الاستيقان لدى مزوّد الخدمة، التي فيها يسلّم وكيل المستعمل الرسالة <Response> (أو الشيء المصطنع الذي يمثلها).

1.3.1.4.11 طلب البروتوكول HTTP إلى مزود الخدمة

إذا كان النفاذ الأول هو إلى مزوّد الخدمة، يمكن أن يبتدر الجانبية طلب اعتباطي إلى مورد. ولا يوجد أي قيود على شكل الطلب. ومزوّد الخدمة حُرّ في أن يستخدم أي وسائل تناسبه لكي يرفق التفاعلات اللاحقة مع الطلب الأصلي. فتقدم كل واحدة من الروابط آلية RelayState، يستطيع مزوّد الخدمة أن يستعملها، لكي يرفق تبادل الجانبيات مع الطلب الأصلي. وينبغي لمزوّد الخدمة أن يكشف أقل ما يمكن من الطلب في القيمة RelayState، إلا إذا كان استعمال الجانبية لا يتطلب مثل هذه التدابير للسرية.

2.3.1.4.11 مزوّد الخدمة يحدّد مزوّد الهوية

تتوقف هذه الخطوة على التنفيذ. يمكن لمزوّد الخدمة أن يستخدم جانبية اكتشاف مزوّد الهوية في اللغة SAMLن المشروحة في الفقرة الفرعية 3.4.11. ويمكنه أيضاً أن يختار إعادة توجيه وكيل المستعمل إلى خدمة أخرى قادرة على تحديد مزوّد هوية مناس. وفي هذه الحالة، يمكن أن يصدر مزوّد الخدمة رسالة <AuthnRequest> (كما في الخطوة التالية) إلى هذه الخدمة لكي يجري ترحليها إلى مزوّد الهوية، أو يمكنه الاعتماد على الخدمة المتوسطة لكي تصدر رسالة <AuthnRequest> باسمه.

3.3.1.4.11 مزوّد الخدمة يصدر رسالة <AuthnRequest> إلى مزوّد الهوية

بمجرد أن يتم انتقاء مزوّد الهوية، يتحدد موقع خدمته للتوقيع الوحيد، استناداً إلى رابطة اللغة SAML التي يختارها مزوّد الخدمة لإرسال الرسالة <AuthnRequest>. ويمكن استخدام المعطيات الشرحية لهذا الغرض. وفي استجابة وكيل المستعمل إلى طلب البروتوكول HTTP، يتم ترجيع استجابة HTTP تحتوي على رسالة <AuthnRequest> أو على شيء مصطنع، حسب رابطة اللغة SAML المستعملة، مطلوب تسليمها إلى خدمة التوقيع الوحيد لدى مزوّد الهوية.

وتحدد رابطة اللغة SAML المستعملة، النسق المضبوط لهذه الاستجابة HTTP وللطلب HTTP اللاحق إلى خدمة التوقيع الوحيد. وتتضمن الفقرة الفرعية 1.4.1.4.11 القواعد الخاصة بالجانبية بشأن محتوى الرسالة <AuthnRequest>. فإذا كانت الرابطة المستعملة هي HTTP Redirect، فإن مزوّد الهوية يستخدم جانبية استبانة الشيء المصطنع المحددة في الفقرة الفرعية 6.4.11، ويقوم مزوّد الهوية باستدعاء مزوّد الخدمة لكي يسترجع الرسالة <AuthnRequest> مستخدماً رابطة البروتوكول SOAP مثلاً.

ويوصى بأن تجري تبادلات البروتوكول HTTP في هذه الخطوة على الصيغة TLS 1.0 للحفاظ على الائتمانية وسلامة الرسالة. ويمكن التوقيع على الرسالة <AuthnRequest>، إذا كان استيقان مُصْدر الطلب مطلوباً. وإذا كانت الرابطة HTTP Artifact مستعملة، فهي توفر وسيلة أيضاً يستعاض بها عن استيقان مُصْدر الرسالة عند التخلي عن مرجعية الشيء المصطنع.

ويتعين على مزوّد الهوية أن يعالج الرسالة <AuthnRequest> كما هو مشروح في هذه التوصية. وهذا ربما يقيّد التفاعلات اللاحقة مع وكيل المستعمل، كما يحدث عندما يكون النعت IsPassive مدرجاً.

4.3.1.4.11 معرّف الهوية يعرّف هوية الطرف الرئيسي

في أي وقت كان، أثناء الخطوة السابقة أو بعد انتهائها، يتعين على مزوّد الهوية أن يقرر هوية الطرف الرئيسي (إلا إذا كان يرجّع خطأ إلى مزوّد الخدمة). والنعت ForceAuthn <AuthnRequest>، إن كان موجوداً بقيمة "صائب"، يلزم مزوّد الهوية بأن يقرر هذه الهوية من جديد، بدلاً من أن يعتمد على دورة موجودة، يمكن أن تعقد له مع الطرف الرئيسي. وإلا فمن جميع وجهات النظر الأخرى، يستطيع مزود الهوية استعمال أي وسيلة لكي يستيقن وكيل المستعمل، مع مراعاة جميع المتطلبات المدرجة في الرسالة <AuthnRequest> بشكل العنصر <RequestedAuthnContext>.

5.3.1.4.11 مزوّد الهوية يصدر رسالة <Response> إلى مزوّد الخدمة

بصرف النظر عن نجاح أو فشل الرسالة <AuthnRequest>، ينبغي لمزوّد الهوية أن يُصْدر استجابة HTTP إلى وكيل المستعمل تحتوي على رسالة <Response> أو على شيء مصطنع، حسب رابطة اللغة SAML المستعملة، مطلوب تسليمها إلى خدمة مستهلك التأكيد لدى مزوّد الخدمة.

وتحدد رابطة اللغة SAML المستعملة، النسق المضبوط لهذه الاستجابة HTTP وللطلب HTTP اللاحق إلى خدمة مستهلك التأكيد. وتتضمن الفقرة الفرعية 2.4.1.4.11 القواعد الخاصة بالجانبية بشأن محتوى الرسالة <Response>. فإذا كانت الرابطة المستعملة هي HTTP POST، تسلّم الرسالة <Response> مباشرة إلى مزوّد الخدمة في هذه الخطوة. أما إذا كانت الرابطة المستعملة هي HTTP Artifact، فإن مزود الخدمة يستخدم جانبية استبانة الشيء المصطنع المحددة في الفقرة الفرعية 6.4.11، ويقوم مزوّد الخدمة باستدعاء مزوّد الهوية لكي يسترجع الرسالة <Response>، مستخدماً رابطة البروتوكول SOAP مثلاً.

ويمكن تحديد موقع خدمة مستهلك التأكيد باستعمال المعطيات الشرحية. ويتعين على مزوّد الهوية أن تكون لديه الوسائل ليقرر أن هذا الموقع خاضع بالفعل لمزوّد الخدمة. ويمكن لمزوّد الخدمة أن يبين الرابطة SAML وخدمة مستهلك التأكيد الخاصة، المطلوب استعمالها في رسالته <AuthnRequest>، وعلى مزوّد الخدمة أن يكرم ذلك، إن استطاع.

ويوصى بأن تجري الطلبات HTTP في هذه الخطوة على الصيغة TLS 1.0 للحفاظ على الائتمانية وسلامة الرسالة. ويتعين التوقيع على العنصر أو العناصر <Assertion> في <Response>، إن كانت الرابطة HTTP POST هي المستعملة، ويمكن أن تكون موقعة إن كانت الرابطة HTTP-Artifact هي المستعملة.

ويتعين على مزوّد الخدمة أن يعالج الرسالة <Response> وأي عناصر <Assertion> محتواة فيها، كما هو مشروح في هذه التوصية.

6.3.1.4.11 مزوّد الخدمة يمنح النفاذ لوكيل المستعمل أو يرفضه له

لكي يكمل مزوّد الخدمة الجانبية، فإنه يعالج واحداً أو عديداً من Response> و<Assertion>، ويمنح أو يرفض النفاذ إلى المورد. يمكن لمزوّد الخدمة أن ينشئ سياقاً أمنياً مع وكيل المستعمل مستخدماً أي آلية دورة يختارها هو. وكل استعمال لاحق لواحد أو لعديد من <Assertion> متروك لتقدير مزوّد الخدمة وغيره من الأطراف الواثقة الأخرى، مع مراعاة جميع تقييدات الاستعمال التي تتضمنها.

4.1.4.11 استعمال بروتوكول طلب الاستيقان

تستند هذه الجانبية إلى بروتوكول طلب الاستيقان المعرف في هذه التوصية. ومزوّد الخدمة هنا هو مُصْدر الطلب وهو الطرف الواثق، والطرف الرئيسي هو المقدم والصاحب المطلوب وكيان التثبيت. ويمكن أن يوجد كذلك أطراف واثقة وكيانات تثبت إضافية حسب تقدير مزوّد الهوية.

1.4.1.4.11 استعمال <AuthnRequest>

يمكن لمزوّد الخدمة أن يدرج محتوى أي رسالة، كما هو مشروح في هذه التوصية. وجميع قواعد المعالجة مشروحة كما هو وارد في هذه التوصية. ويتعين أن يكون العنصر <Issuer> موجوداً، وأن يحتوي على معرف الهوية الوحيد لمزوّد الخدمة الطالب. كما يتعين أن يكون النعت Format محذوفاً، أو له قيمة من: urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

وإذا كان مزوّد الخدمة لا يقدر على تلبية الطالب أو لا يرغب في ذلك، يتعين عليه أن يستجيب بالرسالة <Response> التي تحتوي على الشفرة أو الشفرات المناسبة لحالة الخطأ.

وإذا كان مزوّد الخدمة يرغب في السماح لموّد الهوية أن يقرر معرف هوية جديداً للطرف الرئيسي، إن كان لا يوجد له واحد، يتعين عليه أن يدرج العنصر <NameIDPolicy> مع النعت AllowCreate، موضوعاً على القيمة "صائب". وإلا فلا يمكن أن يستيقن بنجاح إلا الطرف الرئيسي الذي كان مزوّد الهوية قد قرر له معرف هوية يستعمله مزوّد الخدمة.

يمكن لمزوّد الخدمة أن يدرج العنصر <Subject> في الطلب الذي يسمي الهوية الحقيقة التي يرغب في استلام تأكيد بموجبها. ويتعين على هذا العنصر ألا يحتوي على العنصر <SubjectConfirmation>. وإذا كان مزوّد هوية لا يتعرف إلى الطرف الرئيسي بموجب هذه الهوية، يتعين عليه أن يجيب برسالة <Response> تحتوي على حالة خطأ، ومن دون تأكيدات.

ويمكن أن تكون الرسالة <AuthnRequest> موقّعة (كما تشير إلى ذلك الرابطة SAML المستعملة). وإذا كانت الرابطة HTTP Artifact هي المستعملة، يكون استيقان الأطراف اختيارياً، ويمكن استعمال كل آلية تسمح بها الرابطة.

وإذا كانت الرسالة <AuthnRequest> غير مستيقنة و/أو سلامتها محمية، يتعين ألا يوثق بالمعلومات الواردة فيها، إلا على سبيل الاستشارة. سواء كان الطلب موقعاً أو غير موقّع، يتعين على مزوّد الهوية أن يتأكد من أن كل عنصر <AssertionConsumerServiceURL> أو <AssertionConsumerServiceIndex> موجود في الطلب، قد جرى التحقق من كونه ينتمي إلى مزوّد الخدمة الذي سترسل الاستجابة إليه. وقد ينتج عن عدم القيام بذلك تهجم اقتحامي.

2.4.1.4.11 استعمال <Response>

ملاحظة 1 (للاطّلاع) – يقترح PE26 (انظر OASIS PE:2006) إيضاحات للمراد من هذه الفقرة الفرعية، انظر التفصيلات التوضيحية في التذييل VIII.

إذا كان مزوّد الهوية يرغب في ترجيع خطأ، يتعين عليه ألا يدرج أي تأكيدات في الرسالة <Response>. وإلا فإذا كان الطلب ناجحاً (أو إذا كانت الاستجابة غير مترافقة مع طلب)، يتعين على العنصر <Response> أن يتطابق مع ما يلي:

- يمكن أن يكون العنصر <Issuer> محذوفاً، ولكنه إذا كان موجوداً يتعين عليه أن يحتوي على معرف الهوية الوحيد لمزوّد الهوية المُصْدر، كما يتعين أن يكون النعت Format محذوفاً، أو له قيمة من: urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

  ملاحظة 2 (للاطّلاع) – يقترح PE17 (انظر OASIS PE:2006) أن يستعاض عن الفقرة أعلاه بما يلي:

  إذا كانت الرسالة <Response> موقّعة، أو كان تأكيد مدرج مجفّراً، يتعين أن يكون العنصر <Issuer> موجوداً. وإلا فيمكن أن يكون محذوفاً. وإذا كان تأكيد مدرج مجفراً يتعين عليه أن يحتوي على معرف الهوية الوحيد لمزوّد الهوية المُصْدر. والنعت Format يتعين أن يكون محذوفاً، أو له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

- يتعين أن يحتوي على الأقل <Assertion> واحداً. ويتعين على كل عنصر <Issuer> من تأكيد أن يحتوي على معرف الهوية الوحيد لمزوّد الهوية المُصْدر. ويتعين أن يكون النعت Format محذوفاً، أو له قيمة من: urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

- يتعين على مجموعة من تأكيد واحد أو من تأكيدات أن تحتوي على الأقل عنصراً واحداً <AuthnStatement> يعكس استيقان الطرف الرئيسي لدى مزوّد الخدمة.

- يتعين على تأكيد واحد على الأقل يحتوي عنصراً <AuthnStatement>، أن يحتوي على عنصر <Subject> مع عنصر واحد على الأقل هو <SubjectConfirmation> أن يحتوي على Method من: urn:oasis:names:tc:SAML:2.0:cm:bearer. وإذا كان مزود الهوية يقبل الجانبية Single Logout المعرفة في الفقرة 4.4.11، يتعين على مثل هذه الإعلانات الاستيقانية أن تحتوي على النعت SessionIndex لكي تنشط طلبات اختتام الدورة لكل دورة، الصادرة عن مزوّد الخدمة.

- يتعين على العنصر الحامل <SubjectConfirmation> المشروح أعلاه، أن يحتوي على العنصر المحدّد URL لخدمة مستهلك التأكيد التابعة لمزوّد الخدمة، كما يتعين عليه أن يحتوي على النعت NotOnOrAfter الذي يحدّ النافذة التي يمكن أثناءها تسليم التأكيد. ويمكنه أن يحتوي على النعت Address الذي يحدّ عنوان الزبون الذي يمكن تسليم التأكيد اعتباراً منه. ويجب ألا يحتوي النعت

NotBefore. وإذا كانت الرسالة الحاوية هي استجابة للعنصر <AuthnRequest>، يتعين عندئذ أن يتواءم النعت InResponseTo مع معرف هوية الطلب.

- يمكن إدراج إعلانات وطرائق تثبيت أخرى في تأكيد أو تأكيدات، حسب تقدير مزوّد الهوية. ويمكن بصورة خاصة إدراج العناصر <AttributeStatement>. ويمكن أن يحتوي الطلب <AuthnRequest> على نعت في اللغة XML هو AttributeConsumingServiceIndex محيلاً المعلومات عن النعوت المرغوبة أو المطلوبة كما في البند 9. ويمكن أن يتجاهل ذلك مزوّد الهوية، كما يمكنه إرسال نعوت أخرى، حسب تقديره.
- والتأكيد أو التأكيدات التي تتضمن تثبيت الصاحب الحامل، يتعين عليها أن تحتوي على <AudienceRestriction>، بما في ذلك معرف الهوية الوحيد لمزوّد الخدمة، وكأنه عنصر <Audience>.
- ويمكن إدراج شروط أخرى (وعناصر <Audience> أخرى) حسب طلب مزوّد الخدمة أو حسب تقدير مزوّد الهوية. (لا شك أن مثل هذه الشروط يجب أن تكون مفهومة ومقبولة من قبل مزوّد الخدمة، بغية اعتبار التأكيد صالحاً). وليس مزوّد الهوية ملزماً بتكريم المجموعة المطلوبة من <Conditions> في الرسالة <AuthnRequest>، إن وجدت.

3.4.1.4.11 قواعد معالجة الرسالة <Response>

ملاحظة (للاطّلاع) – يقدم PE26 (انظر OASIS PE:2006) توضيحاً للمراد من هذه الفقرة الفرعية، انظر التذييل VIII لمزيد من التفاصيل.

بصرف النظر عن رابطة اللغة SAML المستعملة، يتعين على مزوّد الخدمة أن يفعل التالي:

- التحقق من أي توقيعات موجودة على التأكيد (التأكيدات) أو على الاستجابة.
- التحقق من أن النعت Recipient في أي <SubjectConfirmationData> للحامل يتواءم مع المحدّد URL لخدمة مستهلك التأكيدات التي سلّمت لها الاستجابة <Response> أو الشيء المصطنع.
- التحقق من أن النعت NotOnOrAfter في أي <SubjectConfirmationData> للحامل لم يمر، مع مراعاة انحراف الميقاتيات المسموح بين المزوّدين.
- التحقق من أن النعت InResponseTo في <SubjectConfirmationData> للحامل يساوي معرف الهوية لرسالته الأصلية <AuthnRequest>، ما لم تكن الاستجابة غير مطلوبة، وهي الحالة التي يتعين ألا يكون النعت موجوداً فيها.
- التحقق من أن أي تأكيد يعتمد عليه هو صالح بالنسبة إلى الجوانب الأخرى.
- إذا كانت أي معطيات <SubjectConfirmationData> للحامل، تشتمل على النعت Address، يمكن أن يتحقق مزوّد الخدمة من عنوان زبون وكيل المستعمل بمقابلته بهذا النعت.
- كل تأكيد ليس صالحاً أو لا يمكن تلبية متطلباته الخاصة بتثبيت الصاحب، ينبغي استبعاده وعدم استعماله لإنشاء السياق الأمني للطرف الرئيسي.
- إذا كان العنصر <AuthnStatement> المستعمل لإنشاء سياق أمني للطرف الرئيسي، يحتوي على النعت SessionNotOnOrAfter، ينبغي استبعاد السياق الأمني، بمجرد بلوغ هذا الوقت، إلا إذا كان مزوّد الخدمة يعيد تكوين هوية الطرف الرئيسي بتكراره استعمال هذه الجانبية.

4.4.1.4.11 قواعد معالجة الرسالة <Response> الخاصة بالشيء المصطنع

إذا كانت الرابطة HTTP Artifact هي المستعملة لتسليم الرسالة <Response>، يتعين أن يكون التخلي عن مرجعية الشيء المصطنع باستعمال جانبية استبانة الشيء المصطنع، مستيقناً ومحمي السلامة ومؤتمناً بشكل متبادل.

يتعين أن يتأكد مزوّد الهوية من أن مزوّد الخدمة الذي أُصْدرت له الرسالة <Response> هو وحده الذي يستلم الرسالة كنتيجة للطلب <ArtifactResolve>.

وإن كانت رابطة اللغة SAML مستعملة للتخلي عن مرجعية الشيء المصطنع أو توقيعات الرسائل، إلا أنها يمكن استعمالها لاستيقان الأطراف وحماية الرسائل.

5.4.1.4.11 قواعد المعالجة الخاصة بالرابطة POST

ملاحظة (للاطّلاع) – يقدم PE26 (انظر OASIS PE:2006) توضيحاً للمراد من هذه الفقرة الفرعيةن انظر التذييل VIII لمزيد من التفاصيل.

إذا كانت الرابطة HTTP POST هي المستعملة لتسليم الرسالة <Response>، يتعين أن يكون التأكيد أو التأكيدات الواردة منها موقّعة.

ويتعين على مزوّد الخدمة أن يتأكد من أن تأكيدات الحامل ليست مكررة، باحتفاظه بمجموعة قيم معرفات الهوية المستعملة طوال الوقت الذي يمكن اعتبار التأكيد فيه صالحاً، استناداً إلى النعت NotOnOrAfter في <SubjectConfirmationData>.

5.1.4.11 الاستجابات غير المطلوبة (غير الملتمسة)

يمكن أن يبتدر مزوّد هوية هذه الجانبية، بتسليمه رسالة <Response> غير مطلوبة إلى مزوّد خدمة.

ويتعين ألا تحتوي الاستجابة <Response> غير المطلوبة نعتاً هو InResponseTo، وألا يحتويه كذلك أي عنصر من عناصر الحامل <SubjectConfirmationData>. وإذا كانت المعطيات الشرحية مستعملة، ينبغي تسليم <Response> أو الشيء المصطنع إلى النقطة النهائية <md:AssertionConsumerService> لمزوّد الخدمة المسمى بالتغيب.

وينبغي التنويه خصوصاً بأن مزوّد الهوية قد يشتمل على المعلمة "RelayState" الخاصة بالرابطة، والتي تبيّن، استناداً إلى اتفاق متبادل مع مزوّد الخدمة، كيف تجري معاملة التفاعلات اللاحقة مع وكيل المستعمل. وقد يكون ذلك هو المحدّد URL لمورد لدى مزوّد الخدمة. وينبغي لمزوّد الخدمة أن يكون مستعداً لمعاملة الاستجابات غير المطلوبة، بتسميته موقعاً بالتغيب يرسل إليه وكيل المستعمل إثر معالجة استجابة معالجة ناجحة.

6.1.4.11 استخدام المعطيات الشرحية

تحدّد الفقرة الفرعية 5.2.4.11 عنصر نقطة نهائية <md:SingleSignOnService>، من أجل وصف الروابط والمواقع المقبولة التي يمكن لمزوّد خدمة أن يرسل إليها الطلبات إلى مزوّد هوية يستخدم هذه الجانبية.

ويمكن استعمال النعت WantAuthnRequestsSigned الخاص بالعنصر <md:IDPSSODescriptor> من قبل مزوّد هوية من أجل الإعلام عن مطلب يتطلب التوقيع على الطلبات. ويمكن أن يستعمل مزوّد الخدمة النعت AuthnRequestsSigned الخاص بالعنصر <md:SPSSODescriptor> لتوثيق نية التوقيع على جميع طلباته.

يستطيع المزوّدان أن يوثقا المفتاح أو المفاتيح المستعملة للتوقيع على الطلبات والاستجابات والتأكيدات بواسطة العناصر <md:KeyDescriptor> مع نعت استعمال التوقيع. عند تجفير عناصر في اللغة SAML، يمكن استعمال العناصر <md:KeyDescriptor> مع نعت استعمال التجفير للإعلام عن خوارزميات التجفير وعمليات الضبط المقبولة، والمفاتيح العمومية المستعملة لاستلام مفاتيح التجفير المجملة.

ويستعمل عنصر النقطة النهائية المفهرس <md:AssertionConsumerService> من أجل وصف الروابط والمواقع المقبولة التي يمكن لمزوّد هوية أن يرسل إليها الاستجابات إلى مزوّد خدمة يستخدم هذه الجانبية. ويستخدم النعت index لتمييز النقاط النهائية المحتملة التي يمكن تعيينها بالإحالة في الرسالة <AuthnRequest>. ويستخدم النعت isDefault لتعيين النقطة النهائية الواجب استعمالها، إن لم تكن معينة في طلب.

ويمكن استعمال النعت WantAssertionsSigned الخاص بالعنصر <md:SPSSODescriptor> من قبل مزوّد خدمة من أجل الإعلام عن مطلب يتطلب التوقيع على التأكيدات المسلّمة مع هذه الجانبية. هذا بالإضافة إلى أن أي متطلبات توقيع يفرضها استعمال رابطة معينة. وليس مزوّد الهوية ملزماً بذلك، ولكنه ينبّه إلى أن هناك احتمالاً قوياً في أن يكون التأكيد غير الموقّع غير كافٍ.

وإذا كان الطلب أو رسالة الاستجابة يسلّمان باستخدام الرابطة HTTP Artifact، يتعين على مُصْدر الشيء المصطنع أن يوفر عنصراً واحداً على الأقل من النقطة النهائية <md:ArtifactResolutionService> في معطياته الشرحية.

ويمكن أن يحتوي العنصر <md:IDPSSODescriptor> على العناصر <md:NameIDFormat> و<md:AttributeProfile> و<saml:Attribute> لكي يبين الإمكانية العامة لدعم أنساق معرف هوية الاسم، أو جانبيات نعت، أو نعوت وقيم خاصة. وتتوقف إمكانية دعم مثل هذه الميزات أثناء تبادل استيقان معيّن، على السياسة وعلى تقدير مزوّد الهوية.

ويمكن أيضاً استخدام العنصر <md:SPSSODescriptor> للإعلام عن حاجة مزوّد الخدمة أو عن رغبته في تسليم النعوت SAML مع معلومات عن الاستيقان. ويبقى دوماً إدراج النعوت الحقيقي وقفاً على تقدير مزوّد الهوية. ويمكن أن يدرج عنصر واحد أو أكثر من العناصر <md:AttributeConsumingService> في معطياته الشرحية، على أن يكون لكل منها فهرس نعت يميز الخدمات المختلفة التي يمكن أن تكون محددة بالإحالة في الرسالة <AuthnRequest>. ويستخدم النعت isDefault لتحديد مجموعة من متطلبات النعت بالتغيب.

2.4.11 جانبية الربون أو الوكيل المفوّض المعزّز (ECP)

إن *الزبون أو الوكيل المفوّض المعزّز* (ECP) هو كيان نظام يعرف كيف يتصل بمزوّد هوية مناسب، وربما بأسلوب يتوقف على السياق، ويعتمد على الرابطة Reverse SOAP (PAOS) (انظر البند 10).

ومثال على سيناريو تنشطه هذه الجانبية هو كما يأتي: الطرف الرئيسي الذي يسيطر على زبون ECP يستخدمه إما للنفاذ إلى مورد لدى مزوّد الخدمة وإما للنفاذ إلى مزوّد هوية يكون فيه مزوّد الخدمة والمورد المرغوب مفهومين أو متضمنين. فيستيقن الطرف الرئيسي نفسه (أو يكون قد استيقن نفسه بالفعل) لدى مزوّد الهوية الذي يصدر عندئذ تأكيداً بالاستيقان (وقد يكون ذلك بإسهام من مزوّد الخدمة). وعندئذ يستهلك مزوّد الخدمة التأكيد، وينشئ بالتالي سياقاً أمنياً للطرف الرئيسي. وقد يكون أثناء هذه العملية قد أحدث معرف هوية اسم للطرف الرئيسي ما بين المزوّدين، مع مراعاة معلمات التفاعل وحصول الموافقة من جانب الطرف الرئيسي.

وهذه الجانبية مبنية على بروتوكول طلب الاستيقان في اللغة SAML بالاشتراك مع الرابطة PAOS.

ملاحظة – إن الوسائل المستعملة لكي يستيقن طرف رئيسي نفسه لدى معرف هوية تقع خارج نطاق اللغة SAML.

1.2.4.11 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp (وهذا هو أيضاً مكان الاسم المستهدف المسند في تخطيطة الجانبية ECP في الملحق A).

معلومات الاتصال: security-services-comment@lists.oasis-open.org

معرفات الهوية لطريقة التثبيت في اللغة SAML: تستخدم هذه الجانبية معرف الهوية لطريقة تثبيت الحامل "bearer" في الصيغة SAML V2.0: urn:oasis:names:tc:SAML:2.0:cm:bearer.

الوصف: وارد أدناه.

التحييزات: لا يوجد.

2.2.4.11 نظرة شاملة إلى الجانبية

كما هو مبين أعلاه، فإن الجانبية ECP تحدّد التفاعلات (التآثرات) بين الزبائن أو الوكلاء المفوّضين المعزّزين وبين مزوّدي الخدمة ومزوّدي الهوية. إنها تطبيق خاص من جانبية التوقيع الوحيد (SSO) المشروحة في الفقرة الفرعية 1.4.11. وإذا لم تشر هذه الجانبية إلى قواعد أخرى، وإذا لم تكون القواعد مخصوصة لاستعمال روابط مبنية عل المتصفح، يتعين التقيد بالقواعد الواردة في الفقرة الفرعية 1.4.11.

إن الزبون ECP هو زبون أو وكيل مفوض يستوفي الشرطين التاليين:

- يمتلك معلومات عن مزوّد الهوية، أو يعرف كيف يحصل عليها، والطرف الرئيسي المتصاحب مع الزبون ECP يرغب في استعمالها، في سياق تفاعل (تآثر) مع مزوّد خدمة.

وهذا يتيح لمزوّد خدمة أن يقدم طلب استيقان إلى الزبون ECP، من دون أن يحتاج إلى معرفة أو اكتشاف مزوّد الهوية المناسب (بالقفز فوق الخطوة 2 من الجانبية SSO في الفقرة الفرعية 1.4.11).

- قادر على استخدام رابطة SOAP مقلوب (PAOS) كما هي مبينة جانبيتها هنا من أجل طلب استيقان والاستجابة له.

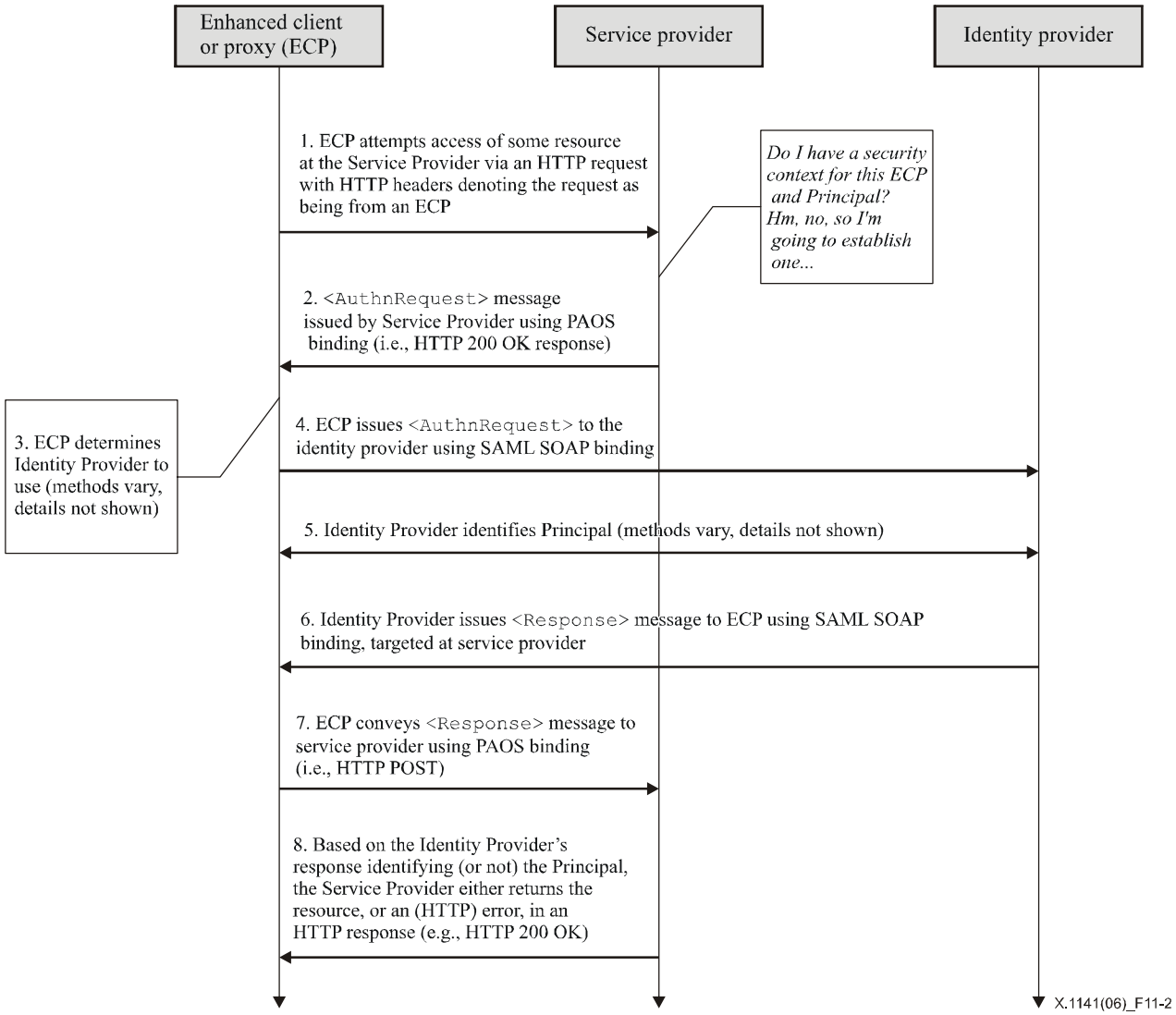
وهذا يمكّن مزوّد خدمة من الحصول على تأكيد استيقان عبر زبون ECP، ليس هو في غير ذلك (أي خارج سياق التفاعل الفوري) بالضرورة قابلاً للتوجيه إليه مباشرة ولا هو متيسر باستمرار. وهذا يرفع أيضاً من فوائد البروتوكول SOAP، بينما يثابر على استخدام تخطيطة وجانبية لتبادل محدّد تحديداً جيداً من أجل تحسين التشغي البيني. ويمكن النظر إلى الزبون أو الوكيل المفوّض المعزّز (ECP) على أنه وسيط SOAP بين مزوّد الخدمة ومزوّد الهوية.

يمكن أن يكون الزبون المعزّز متصفحاً أو أي وكيل مستعمل آخر يعتمد الوظائفية المشروحة في هذه الجانبية. بينما يكون الوكيل المفوّض المعزّز وكيلاً مفوّضاً HTTP ينافس زبوناً معزّزاً. وإذا لم يشر إلى غير ذلك، فإن الإعلانات التي تحيل إلى زبائن معزّزين، يجب أن تفهم على أنها إعلانات بنفس الوقت عن الزبائن المعزّزين وعن الوكلاء المفوّضين عن زبائن معزّزين.

وكما يستطيع الزبون المعزّز أن يرسل ويستلم الرسائل داخل متن الطلبات والاستجابات في البروتوكول HTTPن كذلك لا يوجد له قيود اعتباطية على قدوم رسائل البروتوكول.

وتعزز هذه الجانبية من الرابطة SOAP المقلوب (PAOS) (انظر البند 10). ويتعين أن يتّبع منفذو هذه الجانبية قواعد الدلالات HTTP لاعتماد PAOS المحددة في هذه الرابطة، إضافة إلى القواعد المحددة في هذه الجانبية، تستخدم هذه الجانبية فِدرة رأسية SOAP PAOS محمولة بين المستجيب HTTP والزبون ECP، ولكنها لا تعرّف البروتوكول PAOS بالذات. إن هذه الجانبية تعرّف فِدر الرأسية SOAP التي ترافق الطلبات والاستجابات في اللغة SAML. ويمكن أن تكون فِدر الرأسية هذه مركّبة مع فِدر رأسيات SOAP وغيرها بالقدر اللازم، مثلاً مع فِدرة رأسية أمن الرسالة SOAP لإضافة خصائص أمنية عند اللزوم، مثل توقيع رقمي يضاف إلى طلب الاستيقان.

وتستخدم مجموعتان من فِدر رأسية الطلب أو الاستجابة في البروتوكول SOAP: أولاهما فِدر الرأسية PAOS لمعلومات PAOS العامة، والثانية فِدر الرأسية الخاصة بالجانبية ECP من أجل حمل المعلومات الخاصة بوظائفية الجانبية ECP.



الشكل X.1141/2-11 – انسياب المعالجة في جانبية الزبون ECP

يوضّح الشكل 11-2 التخطيطة الأساسية لإنجاز الاكتتاب بالتوقيع الوحيد (SSO) باستخدام زبون ECP. والجانبية تشرح الخطوات التالية. وقد يقع في إحدى الخطوات لوحدها، تبادل واحد أو عدة تبادلات لرسائل حقيقية، حسب الرابطة المستعملة لهذه الخطوة، وغيرها من أوجه السلوك المتوقفة على التنفيذ.

1) يُصْدر الزبون ECP طلب البروتوكول HTTP إلى مزوّد الخدمة

يقوم الطرف الرئيسي في الخطوة 1، عبر الزبون ECP، بتقديم طلب HTTP إلى مورد مأمون لدى مزوّد الخدمة، حيث لا يكون لدى مزوّد الخدمة سياق أمني منشأ للزبون ECP وللطرف الرئيسي.

2) يُصْدر مزوّد الخدمة رسالة <AuthnRequest> إلى الزبون ECP

يُصدر مزوّد الخدمة في الخطة 2، رسالة <AuthnRequest> إلى الزبون ECP، المطلوب منه أن يسلمها إلى مزوّد الهوية المناسب. وتستعمل هنا الرابطة Reverse SOAP (PAOS) (انظر البند 10).

3) الزبون ECP يحدد مزوّد الهوية

يحصل الزبون ECP في الخطوة 3 على موقع نقطة نهائية لدى مزوّد الهوية من أجل بروتوكول طلب الاستيقان الذي يعتمد رابطته المفضّلة. والوسائل التي يتحقق بها ذلك تتوقف على التنفيذ. وقد يستعمل الزبون ECP جانبية اكتشاف مزوّد الهوية في اللغة SAML، كما هو مشروح في الفقرة الفرعية 3.4.11.

ملاحظة (للاطّلاع) – يقترح PE18 (انظر OASIS PE:2006) إلغاء السطر الأخير من الفقرة أعلاه.

4) يحمل الزبون ECP رسالة <AuthnRequest> إلى مزوّد الهوية

يحمل الزبون ECP في الخطوة 4 رسالة <AuthnRequest> إلى مزوّد الهوية المعرّفة هويته في الخطوة 3، مستخدماً شكلاً معدّلاً من الرابطة SAML SOAP (انظر البند 10)، مع السماح الإضافي لمزوّد الهوية بأن يتبادل رسائل اعتباطية HTTP مع الزبون ECP قبل الاستجابة للطلب SAML.

5) مزوّد الهوية يعرّف هوية الطرف الرئيسي

يقوم مزوّد الهوية في الخطوة 5 بتعريف هوية الطرف الرئيسي بواسطة وسائل لا تقع في نطاق هذه الجانبية. وقد يتطلب ذلك عمل استيقان جديداً أو قد يعاد استعمال دورة مستيقنة موجودة.

6) يُصدر مزوّد الهوية رسالة <Response> إلى الزبون ECP، مستهدفة مزوّد الخدمة

يُصدر مزوّد الهوية في الخطوة 6 رسالة <Response>، مستخدماً الرابطة SAML SOAP، لكي يسلمها الزبون ECP إلى مزوّد الخدمة. وقد تشير الرسالة إلى خطأ، أو قد تحتوي على تأكيد استيقان (على الأقل).

7) يحمل الزبون ECP الرسالة <Response> إلى مزوّد الخدمة

يحمل الزبون ECP في الخطوة 7 الرسالة <Response> إلى مزوّد الخدمة، مستخدماً الرابطة PAOS.

8) مزوّد الخدمة يمنح النفاذ للطرف الرئيسي أو يرفضه له

بعد أن يستلم مزوّد الخدمة الرسالة <Response> من مزوّد الهوية، يمكنه في الخطوة 8 أن ينشئ سياقه الأمني الخاص بالطرف الرئيسي ويرجّع المورد المطلوب، أو يمكنه أن يستجيب للزبون ECP لدى الطرف الرئيسي مع خطأ.

3.2.4.11 وصف الجانبية

تقدم الفقرات الفرعية التالية تعريفات مفصّلة عن الخطوات الإفرادية.

1.3.2.4.11 يُصدر الزبون ECP طلب البروتوكول HTTP إلى مزوّد الخدمة

يرسل الزبون ECP طلباً HTTP إلى مزوّد الخدمة، محدداً مورداً معيناً. ويتعين أن يتطابق هذا الطلب HTTP مع الرابطة PAOS، مما يعني أن الطلب يجب أن يحتوي على حقول الرأسية التالية في البروتوكول HTTP:

1) حقل الرأسية Accept في البروتوكول HTTP الذي يدل على إمكانية قبول النمط MIME "application/vnd.paos+xml".

2) حقل الرأسية PAOS في البروتوكول HTTP الذي يحدد صيغة PAOS بالتالي urn:liberty:paos:2003-08 على الأقل.

3) وفوق ذلك، يتعين أن يتحدد اعتماد هذه الجانبية في حقل الرأسية PAOS في البروتوكول HTTP باعتباره قيمة خدمة مع القيمة urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp. وينبغي لهذه القيمة أن تقابل نعت الخدمة في قدرة الرأسية في البروتوكول SOAP في الطلب PAOS. ويمكن لوكيل مستعمل مثلاً أن يطلب من مزوّد الخدمة صفحة كالتالية:

```
GET /index HTTP/1.1
Host: identity-service.example.com
Accept: text/html; application/vnd.paos+xml
PAOS: ver='urn:liberty:paos:2003-08' ;
'urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp'
```

2.3.2.4.11 مزوّد الخدمة يُصدر رسالة <AuthnRequest> إلى الزبون ECP

عندما يتطلب مزوّد الخدمة سياقاً أمنياً للطرف الرئيسي قبل منح النفاذ إلى المورد المعين، أي قبل أن يقدم خمة أو معطيات، يمكنه الاستجابة إلى طلب البروتوكول HTTP، مستخدماً الرابطة PAOS مع رسالة <AuthnRequest> داخل الاستجابة HTTP. ويصدر مزوّد الخدمة استجابة HTTP 200 OK إلى الزبون ECP تحتوي على مغلّف واحد SOAP.

ويتعين أن يحتوي المغلّف SOAP على:

1) عنصر <AuthnRequest> في متن البروتوكول SOAP، مهيأ للمستلم الأخير في SOAP الذي هو مزوّد الهوية.

2) فِدرة رأسية PAOS SOAP تستهدف الزبون ECP باستخدام قيمة العنصر الفاعل SOAP من: http://schemas.xmlsoap.org/soap/actor/next. وتقدم هذه الفِدرة الرأسية معلومات تحكّم، مثل محدّد الموقع URL الذي يجب أن ترسل إليه الاستجابة في هذه التخطيطة لتبادل الرسائل ذات الاستجابة المطلوبة.

3) فِدرة رأسية SOAP لطلب معين بجانبية الزبون ECP، تستهدف الزبون ECP مستخدمة العنصر الفاعل SOAP: http://schemas.xmlsoap.org/soap/actor/next. وتعرف الفِدرة الرأسية في طلب الزبون ECP معالجته، مثل قائمة بمزوّدي الهوية يقبلها مزوّد الخدمة، إن كان الزبون ECP يستطيع التفاعل (التآثر) مع الطرف الرئيسي عبر الزبون، كما تعرّف اسم مزوّد الخدمة المقروء من الإنسان ويمكن عرضه على الشاشة أمام الطرف الرئيسي.

ويمكن أن يحتوي المغلّف SOAP على فِدرة رأسية SOAP RelayState للزبون ECP، تستهدف الزبون ECP مستخدمة قيمة العنصر الفاعل في SOAP من: http://schemas.xmlsoap.org/soap/actor/next. وتحتوي الرأسية على معلومات الحالة المطلوب ترجعيها إلى الزبون ECP مع الاستجابة SAML.

3.3.2.4.11 الزبون ECP يحدّد مزوّد الهوية

الزبون ECP هو الذي يقرر أي مزوّد هوية هو المناسب، ويسير الرسالة SOAP وفقاً لذلك.

4.3.2.4.11 الزبون ECP يُصدر رسالة <AuthnRequest> إلى مزود الهوية

يتعين على الزبون ECP أن يزيل فِدر الرأسية PAOS وECP RelayState وECP Request قبل أن يمرر الرسالة <AuthnRequest> إلى مزوّد الهوية، مستخدماً شكلاً معدلاً من الرابطة SAML SOAP. ويُسلَّم الطلب SAML عن طريق SOAP بالأسلوب العادي، غير أن مزوّد الهوية يمكنه أن يستجيب لطلب الزبون ECP في البروتوكول HTTP، باستجابة HTTP تحتوي مثلاً على شكل اكتتاب HTML أو على استجابة أخرى موجهة نحو التمثيل. ويمكن أن يحدث تتابع من التبادلات، ولكن يتعين في نهاية المطاف على مزوّد الهوية أن يكمل التبادل SAML SOAP، وأن يرجّع استجابة SAML عبر الرابطة SOAP.

ويستطيع مزوّد الخدمة أن يوقّع على العنصر <AuthnRequest> بالذات. وفي هذا الصدد، يتعين اتّباع قواعد الرسالة المحددة في جانبية المتصفح SSO الواردة في الفقرة الفرعية 1.4.1.4.11.

وقبل هذه الخطوة أو بعدها، يتعين على مزود الهوية أن يقرر هوية الطرف الرئيسي ببعض الوسائل، أو يتعين عليه أن يرجع خطأ <Response>، كما هو مشروح أدناه في الفقرة الفرعية 6.3.2.4.11.

5.3.2.4.11 مزوّد الهوية يعرف هوية الطرف الرئيسي

في أي وقت كان، أثناء الخطوة السابقة أو بعد انتهائها، يتعين على مزوّد الهوية أن يقرر هوية الطرف الرئيسي (إلا إذا كان يرجّع خطأ إلى مزوّد الخدمة). والنعت <AuthnRequest> ForceAuthn، إن كان موجوداً بقيمة "صائب"، يلزم مزوّد

الهوية بأن يقرر هذه الهوية من جديد، بدلاً من أن يعتمد على دورة موجودة، يمكن أن تعقد له مع الطرف الرئيسي. وإلا فمن جميع وجهات النظر الأخرى، ويستطيع مزوّد الهوية استعمال أي وسيلة لكي يستيقن وكيل المستعمل، مع مراعاة جميع المتطلبات المدرجة في الرسالة <AuthnRequest> بشكل العنصر <RequestedAuthnContext>.

6.3.2.4.11 مزوّد الهوية يصدر رسالة <Response> إلى الزبون ECP، وتستهدف مزوّد الخدمة

يرجّع مزوّد الهوية رسالة <Response> في اللغة SAML (أو خطأ SOAP)، عندما تقدم مع طلب استيقان، بعد أن يكون قد قرر هوية الطرف الرئيسي. وتُحمَل الاستجابة SAML باستخدام الرابطة SAML SOAP في رسالة SOAP مع العنصر <Response> في متن البروتوكول SOAP، مهيأة لإرسالها إلى مزوّد الخدمة باعتباره المستلم الأخير في البروتوكول SOAP. ويتعين اتّباع قواعد الاستجابة المحددة في جانبية المتصفح SSO الواردة في الفقرة الفرعية 2.4.1.4.11.

ويتعين أن تحتوي رسالة الاستجابة الصادرة عن مزوّد الهوية على فِدرة الهوية على فِدرة رأسية SOAP لاستجابة الزبون ECP الخاصة بالجانبية، ويمكن أن تحتوي على فِدرة رأسية ECP RelayState؛ وكلتاهما تستهدفان الزبون ECP.

7.3.2.4.11 يحمل الزبون ECP الرسالة <Response> إلى مزوّد الخدمة

يزيل الزبون ECP الفِدرة (الفِدر) الرأسية، ويمكنه أن يضيف فِدرة رأسية SOAP لاستجابة PAOS، وفِدرة رأسية ECP RelayState قبل تمرير الاستجابة SOAP إلى مزوّد الخدمة باستعمال الرابطة PAOS.

وتستعمل عادة الفِدرة الرأسية SOAP <paos:Response> في الاستجابة الممررة إلى مزوّد الخدمة، من أجل ربط هذه الاستجابة بطلب سابق من مزوّد الخدمة. وفي هذه الجانبية، لا يكون نعت الارتباط refToMessageID مطلوباً، طالما أن النعت InResponseTo الخاص بالعنصر <Response> في اللغة SAML، يمكن استعماله لهذا الغرض، ولكن إذا كان لفِدرة الرأسية SOAP <paos:Response> رسالة messageID، يجب عندئذ استعمال فِدرة الرأسية SOAP <paos:Response>.

ومزوّد الخدمة هو الذي يقدم قيمة فِدرة الرأسية <ecp:RelayState> عادة إلى الزبون ECP مع طلبه، ولكن إذا كان مزوّد الهوية يقوم بإنتاج استجابة غير ملتمسة (غير مطلوبة) (من دون أن يستلم طلباً مقابلها)، يمكنه أن يدرج فِدرة رأسية RelayState تبين، استناداً إلى اتفاق متبادل مع مزوّد الخدمة، كيفية معاملة التفاعلات (التآثرات) اللاحقة مع الزبون ECP. وقد يكون ذلك هو محدّد الموقع URL لمورد لدى مزوّد الخدمة.

وإذا ضمّن مزوّد الخدمة في طلبه إلى الزبون ECP، فِدرة رأسية SOAP <ecp:RelayState>، أو إذا ضمّن مزوّد الخدمة في استجابته فِدرة رأسية مطابقة مع الاستجابة SAML المرسلة إلى مزوّد الخدمة. وتكون الأولوية لقيمة مزوّد الخدمة لهذه الفِدرة الرأسية (إن وجدت).

4.2.4.11 استعمال تخطيطة جانبية الزبون ECP

تعرّف تخطيطة اللغة XML لجانبية الزبون ECP، فِدر الرأسية للطلب أو الاستجابة SOAP التي تستعملها هذه الجانبية. وفيما يلي قائمة كاملة بوثيقة هذه التخطيطة.

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
        schemaLocation="saml-schema-protocol-2.0.xsd"/>
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
```

```
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://schemas.xmlsoap.org/soap/envelope/"
        schemaLocation="http://schemas.xmlsoap.org/soap/envelope/"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-ecp-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Custom schema for ECP profile, first published in SAML 2.0.
        </documentation>
    </annotation>

    <element name="Request" type="ecp:RequestType"/>
    <complexType name="RequestType">
        <sequence>
            <element ref="saml:Issuer"/>
            <element ref="samlp:IDPList" minOccurs="0"/>
        </sequence>
        <attribute ref="S:mustUnderstand" use="required"/>
        <attribute ref="S:actor" use="required"/>
        <attribute name="ProviderName" type="string" use="optional"/>
        <attribute name="IsPassive" type="boolean" use="optional"/>
    </complexType>

    <element name="Response" type="ecp:ResponseType"/>
    <complexType name="ResponseType">
        <attribute ref="S:mustUnderstand" use="required"/>
        <attribute ref="S:actor" use="required"/>
        <attribute name="AssertionConsumerServiceURL" type="anyURI"
use="required"/>
    </complexType>

    <element name="RelayState" type="ecp:RelayStateType"/>
    <complexType name="RelayStateType">
        <simpleContent>
            <extension base="string">
                <attribute ref="S:mustUnderstand" use="required"/>
                <attribute ref="S:actor" use="required"/>
            </extension>
        </simpleContent>
    </complexType>
</schema>
```

والفقرات الفرعية التالية تشرح كيف يجب أن تستعمل هذه التركيبات من اللغة XML.

1.4.2.4.11 فِدرة رأسية الطلب PAOS: من مزوّد الخدمة (SP) إلى الزبون أو الوكيل المفوّض المعزّز (ECP)

تشير فِدرة رأسية الطلب PAOS إلى استعمال المعالجة PAOS وتحتوي على النعوت التالية:

- `responseConsumerURL` [مطلوب]

يحدّد إلى أين يجب على الزبون ECP أن يرسل استجابة خطأ. ويستخدم أيضاً للتحقق من صحة استجابة مزوّد الهوية، بالتحقق المتقاطع بين هذا الموقع والمحدّد `AssertionServiceConsumerURL`، في فِدرة رأسية استجابة الزبون ECP. ويتعين أن تكون هذه القيمة هي نفس القيمة `AssertionServiceConsumerURL` (أو المحدّد URL المحال إليه في المعطيات الشرحية) المحمولة في `<AuthnRequest>`.

ملاحظة (للاطّلاع) – يقترح PE22 (انظر OASIS PE:2006) أن يستعاض عن `AssertionServiceConsumerURL` في الجملة الأخيرة بالتالي `AssertionConsumerServiceURL`.

- `service` [مطلوب]

يبين أن الخدمة PAOS المستعملة حالياً هي هذه الجانبية SAML للاستيقان. ويجب أن تكون القيمة هي: `urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp`.

- SOAP-ENV:mustUnderstand [مطلوب]

يتعين على القيمة أن تكون 1 (صائبة). ويتعين توليد الخطأ في SOAP، إذا كانت فِدرة الرأسية PAOS ليست مفهومة.

- SOAP-ENV:actor [مطلوب]

يجب أن تكون القيمة هي: http://schemas.xmlsoap.org/soap/actor/next.

- messageID [اختياري]

يسمح بترابط استجابة اختياري. يمكن أن يستعمل في هذه الجانبية، ولكنه ليس مطلوباً، طالما أن هذه الوظائفية توفرها طبقة البروتوكول SAML، عبر نعت معرّف الهوية في <AuthnRequest> والنعت InResponseTo في <Response>.

ولا يوجد عنصر محتوى في فِدرة الرأسية SOAP من الطلب PAOS.

2.4.2.4.11 فِدرة رأسية طلب الزبون ECP: من المزوّد SP إلى الزبون ECP

تستعمل فِدرة الرأسية SOAP في طلب الزبون ECP، لكي تحمل المعلومات التي يحتاجها الزبون ECP لمعالجة طلب الاستيقان. وهي إلزامية ووجودها يشير إلى استعمال هذه الجانبية. وهي تحتوي على العناصر والنعوت التالية:

- SOAP-ENV:mustUnderstand [مطلوب]

يتعين على القيمة أن تكون 1. ويتعين توليد الخطأ SOAP، إذا كانت فِدرة رأسية الزبون ECP غير مفهومة.

- SOAP-ENV:actor [مطلوب]

يتعين أن تكون القيمة هي: http://schemas.xmlsoap.org/soap/actor/next.

- ProviderName [اختياري]

اسم مقروء من الإنسان لمزوّد الخدمة الطالب.

- IsPassive [اختياري]

قيمة بولانية. فإذا كانت "صائبة"، يتعين على مزوّد الخدة وعلى الزبون نفسه ألا يستلما التحكم في السطح البيني للمستعمل من مُصْدر الطلب، وأن يتفاعلا مع الطرف الرئيسي بأسلوب محسوس. وإذا لم تكن القيمة مقدّمة، فالقيمة بالتغيب هي "صائبة".

- <saml:Issuer> [مطلوب]

يتعين أن يحتوي هذا العنصر على معرف الهوية الوحيد لمزوّد الخدمة الطالب. ويتعين حذف النعت Format أو تكون له القيمة: urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

- <samlp:IDPList> [اختياري]

قائمة اختيارية بمزودي هوية، يعترف بهم مزوّد الخدمة، ومنهم يمكن أن يختار الزبون ECP ليخدم الطلب.

3.4.2.4.11 فِدرة رأسية حالة الترحيل (RelayState) للزبون ECP: من المزوّد SP إلى الزبون ECP

تستعمل فِدرة الرأسية SOAP لحالة ترحيل الزبون ECP، لكي تحمل معلومات الحالة الواردة من مزوّد الخدمة والتي سيحتاجها لاحقاً عند معالجة الاستجابة القادمة من الزبون ECP. إنها اختيارية ولكنها عندما تستعمل، يتعين على الزبون ECP أن يدرج فِدرة رأسية مطابقة في الاستجابة الواردة في الخطوة 5 من الشكل 11-2. وهي تشتمل على النعتين التاليين:

ملاحظة (للاطّلاع) – يقترح PE27 (انظر OASIS PE:2006) أن يستعاض عن الخطوة 5 بالخطوة 7 في النص أعلاه.

– SOAP-ENV:mustUnderstand [مطلوب]

يتعين على القيمة أن تكون 1 (صائبة). ويتعين توليد خطأ SOAP إذا كانت فِدرة الرأسية غير مفهومة.

– SOAP-ENV:actor [مطلوب]

يتعين أن تكون القيمة هي: http://schemas.xmlsoap.org/soap/actor/next.

إن محتوى عنصر فِدرة الرأسية هو سلسلة تحتوي على معلومات الحالة التي خلقها الطالب. وإذا كان متوفراً، يتعين على الزبون ECP أن يدرج نفس القيمة في فِدرة الرأسية RelayState عندما يستجيب لمزوّد الخدمة في الخطوة 5. ويتعين ألا تزيد قيمة السلسلة على 80 بايتة في الطول وأن تكون سلامتها محمية من قبل الطالب، بصرف النظر عن الحمايات الأخرى التي قد تكون أو لا تكون موجودة أثناء إرسال الرسالة.

وفيما يلي مثال على طلب الاستيقان SOAP الذاهب من مزوّد الخدمة إلى الزبون ECP:

```
<SOAP-ENV:Envelope
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <paos:Request xmlns:paos="urn:liberty:paos:2003-08"
       responseConsumerURL="http://identity-service.example.com/abc"
       messageID="6c3a4f8b9c2d" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next" SOAP-
ENV:mustUnderstand="1"
      service="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp">
    </paos:Request>
    <ecp:Request xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
      SOAP-ENV:mustUnderstand="1" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next"
       ProviderName="Service Provider X" IsPassive="0">
      <saml:Issuer>https://ServiceProvider.example.com</saml:Issuer>
      <samlp:IDPList>
        <samlp:IDPEntry ProviderID="https://IdentityProvider.example.com"
            Name="Identity Provider X"
            Loc="https://IdentityProvider.example.com/saml2/sso"
        </samlp:IDPEntry>
        <samlp:GetComplete>
        https://ServiceProvider.example.com/idplist?id=604be136-fe91-441e-
afb8
        </samlp:GetComplete>
      </samlp:IDPList>
    </ecp:Request>
    <ecp:RelayState
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
      SOAP-ENV:mustUnderstand="1" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next">
      ...
    </ecp:RelayState>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <samlp:AuthnRequest> ... </samlp:AuthnRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

وكما ذُكر أعلاه يقوم الزبون ECP بإزالة الفِدرتين الرأسيتين PAOS وECP من الرسالة SOAP قبل إرسال طلب الاستيقان إلى الأمام إلى مزوّد الهوية. وفيما يلي مثال على طلب استيقان مرسل من الزبون ECP إلى مزوّد الهوية.

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
```

```
  <SOAP-ENV:Body>
    <samlp:AuthnRequest> ... </samlp:AuthnRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

4.4.2.4.11 فِدرة الرأسية في استجابة الزبون ECP: من مزوّد الهوية (IdP) إلى الزبون ECP

يتعين استعمال فِدرة الرأسية SOAP في استجابة الزبون ECP على الاستجابة القادمة من مزوّد الهوية إلى الزبون ECP. وهي تحتوي على النعوت التالية:

- `SOAP-ENV:mustUnderstand` [مطلوب]

  يتعين على القيمة أن تكون 1 (صائبة). ويتعين توليد خطأ SOAP إذا كانت فِدرة رأسية الزبون ECP غير مفهومة.

- `SOAP-ENV:actor` [مطلوب]

  يتعين أن تكون القيمة هي: `http://schemas.xmlsoap.org/soap/actor/next`.

- `AssertionConsumerServiceURL` [مطلوب]

  مضبوط من مزوّد الهوية، استناداً إلى الرسالة `<AuthnRequest>` أو إلى المعطيات الشرحية لمزوّد الخدمة الحاصل عليها مزوّد الهوية.

يتعين على الزبون ECP أن يؤكد أن هذه القيمة تقابل القيمة التي حصل عليها الزبون ECP في المحدّد `responseConsumerURL` في فِدرة الرأسية SOAP في الطلب PAOS الذي استلمه من مزوّد الخدمة. ولما كان `AssertionConsumerServiceURL` هو مطلق، فالأمر يتطلب بعض المعالجة أو التقييس.

وتستخدم هذه الآلية لأغراض أمنية من أجل تأكيد مقصد الاستجابة الصحيح. وإذا كانت القيم لا تتواءم، يتعين على الزبون ECP أن يولّد استجابة خطأ SOAP إلى مزوّد الخدمة، ويتعين ألا يرجّع الاستجابة SAML.

ولا يوجد عنصر محتوى في الرأسية SOAP من استجابة الزبون ECP.

وفيما يلي مثال على استجابة من مزوّد IdP إلى زبون ECP.

```
<SOAP-ENV:Envelope
       xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
     <ecp:Response SOAP-ENV:mustUnderstand="1" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next"
AssertionConsumerServiceURL="https://ServiceProvider.example.com/ecp_asser
tion_consumer"/>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <samlp:Response> ... </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

5.4.2.4.11 فِدرة الرأسية في الاستجابة PAOS: من الزبون ECP إلى المزوّد SP

تحتوي فِدرة الرأسية في الاستجابة PAOS على النعوت التالية:

- `SOAP-ENV:mustUnderstand` [مطلوب]

  يتعين على القيمة أن تكون 1 (صائبة). ويتعين توليد خطأ SOAP إذا كانت فِدرة الرأسية PAOS غير مفهومة.

- `SOAP-ENV:actor` [مطلوب]

يتعين أن تكون القيمة هي: http://schemas.xmlsoap.org/soap/actor/next.

– refToMessageID [اختياري]

يسمح بالارتباط مع الطلب PAOS. وتتعين إضافة هذا النعت الاختياري (والفِدرة الرأسية ككل) من قبل الزبون ECP، إذا كان الطلب PAOS قد حدّد النعت messageID. وتقدّم الوظائفية المكافئة في اللغة SAML باستخدام الترابط <AuthnRequest> و<Response>.

وفيما يلي مثال على استجابة من زبون ECP إلى مزوّد SP.

```
<SOAP-ENV:Envelope
       xmlns:paos="urn:liberty:paos:2003-08"
       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
    <paos:Response refToMessageID="6c3a4f8b9c2d" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next/" SOAP-
ENV:mustUnderstand="1"/>
    <ecp:RelayState
xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
       SOAP-ENV:mustUnderstand="1" SOAP-
ENV:actor="http://schemas.xmlsoap.org/soap/actor/next">
      ...
    </ecp:RelayState>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <samlp:Response> ... </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

5.2.4.11 اعتبارات أمنية

ينبغي أن توقّع الرسالة <AuthnRequest>. ووفقاً للقواعد التي تحددها جانبية المتصفح SSO، يتعين أن توقّع التأكيدات المدرجة في <Response>. وتسليم الاستجابة في المغلَّف SOAP عبر PAOS هو مماثل بشكل أساسي لاستعمال الرابطة HTTP POST، وتستعمل التدابير الأمنية المضادة والمناسبة لهذه الرابطة.

وينبغي أن تكون رأسيات البروتوكول SOAP محمية السلامة، كما في سلامة الرسالة SOAP أو عبر استعمال بروتوكول أمن طبقة النقل (TLS) على كل تبادل HTTP مع الزبون.

وينبغي استيقان مزوّد الخدمة لدى الزبون ECP، مثلاً مع الاستيقان TLS في جانب المخدّم.

وينبغي استيقان الزبون ECP لدى مزوّد الهوية، كما في حالة الاحتفاظ بدورة مستيقنة. وأي تبادلات HTTP لاحقة لتسليم الرسالة <AuthnRequest>، وقبل ترجيع مزوّد الهوية للاستجابة <Response>، يتعين إرفقاها أمنياً مع الطلب الأصلي.

ملاحظة (للاطّلاع) – يقترح PE20 (انظر OASIS PE:2006) إضافة فقرة فرعية تناقش اعتبارات المعطيات الشرحية للزبون ECP على النحو الآتي:

القواعد المحدّدة في جانبية المتصفح SSO في البند 11، تنطبق هنا كذلك. ويمكن خصوصاً استعمال عنصر النقطة النهائية المفهرس <md:AssertionConsumerService> مع الرابطة: urn:oasis:names:tc:SAML:2.0:bindings:PAOS، لشرح الرابطة المدعومة والموقع أو المواقع التي مكن لمزوّد الهوية أن يرسل الاستجابات منها إلى مزوّد الخدمة مستخدماً هذه الجانبية. وفوق ذلك يمكن استعمال النقطة النهائية <md:SingleSignOnService> مع الرابطة: urn:oasis:names:tc:SAML:2.0:bindings:SOAP، لشرح الرابطة المدعومة والموقع أو المواقع التي يمكن لمزوّد الخدمة أن يرسل الطلبات منها إلى مزوّد الهوية مستخدماً هذه الجانبية.

3.4.11 جانبية اكتشاف مزوّد الهوية

تحدّد هذه الفقرة الجانبية التي يستطيع مزوّد الخدمة أن يكتشف بها، أي مزوّدي هوية يستخدم الطرف الرئيسي مع جانبية متصفح شبكة الويب بتوقيع وحيد. وفي التطويرات التي يكون فيها أكثر من مزوّد هوية واحد، يحتاج مزوّدو الخدمة إلى وسيلة يكتشفون بها، أي مزوّد أو مزوّدي هوية يستعمل الطرف الرئيسي. وتعتمد جانبية الاكتشاف على كعكة مكتوبة في ميدان، هو مشترك بين مزوّدي الهوية. ومزوّدي الخدمة في تطوير ما. ويعرف الميدان الذي يحدده التطوير مسبقاً بالميدان المشترك في هذه الجانبية، والكعكة التي تحتوي على قائمة مزوّدي الهوية تعرف بكعكة الميدان المشترك.

وتحديد الكيانات التي تستضيف مخدّمات شبكة الويب في الميدان المشترك هو مسألة تخص التطوير، وهو يقع خارج نطاق هذه الجانبية.

ملاحظة (للاطّلاع) – يقترح PE32 (انظر OASIS PE:2006) أن يضاف الآتي لوصف المعلومات المطلوبة:

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:profiles:SSO:idp-discovery`

معلومات الاتصال: security-services-comment@lists.oasis-open.org

1.3.4.11 كعكة الميدان المشترك

يتعين أن يكون اسم الكعكة "`_saml_idp`". ويتعين أن يكون نسق قيمة الكعكة مجموعة مؤلفة من قيمة واحدة أو أكثر من قيم المعرف URI المشفر بالأساس 64، تفصل بينها سمة فرغ واحدة. وكل معرف هوية URI هو معرف الهوية الوحيد لمزوّد هوية، كما هو محدّد في البند 7. وتكون المجموعة النهائية من القيم هي عندئذ المحدّد URL المشفّر.

ينبغي لخدمة كتابة كعكة الميدان المشترك أن تضيف في ذيل القائمة معرف الهوية الوحيد لمزوّد الهوية. فإذا كان معرف الهوية موجوداً بالفعل في القائمة، يمكنه أن يسحبه منها ثم يضيفه إلى الذيل. والغاية من ذلك هي أن أحدث دورة مقررة لمزوّد الهوية هي الأخيرة في القائمة.

ويتعين أن تكون الكعكة مضبوطة بسابقة المسير Path التي هي الشرطة المائلة "/". ويتعين أن يكون الميدان مضبوطاً على "[common-domain]." حيث "[common-domain]." هو الميدان المشترك المقام داخل التطوير الذي سيستعمل مع هذه الجانبية. ويتعين أن تكون هناك فترة تعلّم. ويتعين أن تكون الكعكة موسومة بأنها مأمونة.

وينبغي أن تكون قواعد تركيب الكعكة متوافقة مع طلب التعليقات RFC 2965 الصادر عن الفريق IETF. ويمكن أن تكون الكعكة صالحة لدورة فقط أو دائمة. ويتم هذا الاختيار داخل التطوير، ولكنه ينبغي أن يطبق تطبيقاً منتظماً على جميع مزوّدي الهوية في التطوير.

2.3.4.11 ضبط كعكة الميدان المشترك

بعد أن يستيقن مزوّد الهوية طرفاً رئيسياً، يمكنه ضبط كعكة الميدان المشترك. والوسيلة التي يضبط بها مزوّد الهوية الكعكة هي خاصة بالتنفيذ، طالما أن الكعكة موضوعة بنجاح مع المعلمات المعطاة أعلاه. وفيما يلي استراتيجية تنفيذ محتملة، ولكن ينبغي ألا تعتبر معيارية. ويمكن لمزوّد الهوية:

- أن ينشئ لنفسه مسبقاً اسماً مستعاراً في النظام DNS وفي بروتوكول الإنترنت في الميدان المشترك.
- أن يعيد توجيه وكيل المستعمل إلى نفسه باستخدام الاسم المستعار في النظام DNS مستخدماً محدداً للموقع URL ليحدّد "https" كتخطيطة للمحدّد URL. وبنية المحدد URL هي خاصة بالتنفيذ، ويمكن أن تحتوي على معلومات دورة يحتاجها تعريف هوية وكيل المستعمل.
- أن يضبط الكعكة على وكيل المستعمل المعاد توجيهه، مستخدماً المعلمات المحدّدة أعلاه.
- أن يعيد توجيه وكيل المستخدم ثانية إلى نفسه، أو إلى مزوّد الخدمة، إن كان ذلك مناسباً.

3.3.4.11 الحصول على كعكة الميدان المشترك

عندما يحتاج مزوّد خدمة أن يكتشف أي مزوّدي الهوية يستعملهم الطرف الرئيسي، ينفذ تبادلاً مصمماً لتقديم كعكة الميدان المشترك إلى مزوّد الخدمة، بعد أن يكون قد قرأها مخدّم البروتوكول HTTP في الميدان المشترك.

وإذا كان مخدّم البروتوكول في الميدان المشترك يشغّله مزوّد الخدمة، أو إذا كانت هناك ترتيبات أخرى، يمكن لمزوّد الخدمة أن يستخدم مخدّم البروتوكول HTTP في الميدان المشترك، لترحيل طلبه <AuthnRequest> إلى مزوّد الهوية من أجل عملية توقيع وحيد مستمثلة.

والوسائل الخاصة التي يقرأ بها مزوّد الخدمة الكعكة هي خاصة بالتنفيذ، طالما هي قادرة على جعل وكيل المستعمل يقدم الكعكات التي وضعت مع المعلمات المعطاة في الفقرة الفرعية 1.3.4.11. وفيما يلي شرح لاستراتيجية تنفيذ محتملة، ولكن ينبغي ألا تعتبر معيارية. وفوق ذلك يمكن أن تكون تحت المثلى بالنسبة إلى بعض التطبيقات.

- أن ينشئ لنفسه مسبقاً اسماً مستعاراً في النظام DNS وفي بروتوكول الإنترنت في الميدان المشترك.
- أن يعيد توجيه وكيل المستعمل إلى نفسه باستخدام الاسم المستعار في النظام DNS مستخدماً محدداً للموقع URL ليحدد "https" كتخطيطة للمحدّد URL. وبنية المحدّد URL هي خاصة بالتنفيذ، ويمكن أن تحتوي على معلومات دورة يحتاجها تعريف هوية وكيل المستعمل.
- أن يعيد توجيه وكيل المستعمل ثانية إلى نفسه، أو إلى مزوّد الهوية، إن كان ذلك مناسباً.

4.4.11 جانبية اختتام دورة وحيد

بمجرد أن يستيقن طرف رئيسي لدى معرف هوية، يستطيع الكيان المستيقن إقامة دورة مع الطرف الرئيسي (عادة عن طريق كعكة، أو إعادة كتابة محدّد URL، أو بوسائل أخرى خاصة بالتنفيذ). ويمكن لمزوّد الهوية أن يصدر لاحقاً تأكيدات إلى مزوّدي الخدمة أو إلى أطراف واثقة أخرى، استناداً إلى حدث الاستيقان هذا. ويمكن لطرف واثق ما أن يستخدم هذا الحدث ويقيم مع الطرف الرئيسي دورته *الخاصة به*.

وفي مثل هذه الحالة يستطيع مزوّد الهوية أن يعمل كسلطة دورة، وأن تعمل الأطراف الواثقة كمشتركين في الدورة. وقد يرغب الطرف الرئيسي، بعد بعض الوقت، في أن ينهي دورته (أو دورتها) إما مع مشترك فردي في الدورة أو مع جميع المشتركين في الدورة، وذلك في دورة تديرها سلطة الدورة. وتعتبر الحالة الأولى واقعة خارج نطاق هذه التوصية، بينما يمكن أن تكون الحالة الأخيرة مستوفاة باستخدام هذه الجانبية الخاصة ببروتوكول اختتام الدورة الوحيد في اللغة SAML (انظر الفقرة 4.11).

ويمكن أن يختار طرف رئيسي (أو مسؤول إداري ينهي دورة طرف رئيسي) إنهاء هذه الدورة "الكلية" إما بالاتصال بسلطة الدورة وإما بالاتصال بفرد مشترك في الدورة. وكذلك يمكن لمزوّد هوية عامل كسلطة دورة أن يعمل *بنفسه* كمشترك في دورة في حالات يكون هو فيها طرفاً واثقاً بمزوّد هوية آخر بشأن تأكيدات تخص هذا الطرف الرئيسي.

تتيح الجانبية بأن يندمج البروتوكول مع رابطة متزامنة، مثل الرابطة SOAP، أو مع روابط "قناة جبهية" غير متزامنة، مثل الروابط HTTP Redirect أو POST أو Artifact. ويمكن أن تكون رابطة قناة جبهية مطلوبة مثلاً في حالات لا تكون فيها دورة طرف رئيسي موجودة إلا لدى وكيل مستعمل وبشكل كعكة، ويكون مطلوباً فيها تفاعل مباشر بين وكيل المستعمل ومشترك في الدورة أو سلطة الدورة. وكما هو مبين أدناه، ينبغي للمشتركين في الدورة، إذا أمكنهم، أن يستعملوا رابطة "قناة جبهية" عند المبادرة إلى هذه الجانبية، من أجل زيادة إمكانية سلطة الدورة إلى أقصى حد، لكي تستطيع نشر اختتام الدورة بنجاح على جميع المشتركين.

1.4.4.11 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:profiles:SSO:logout`

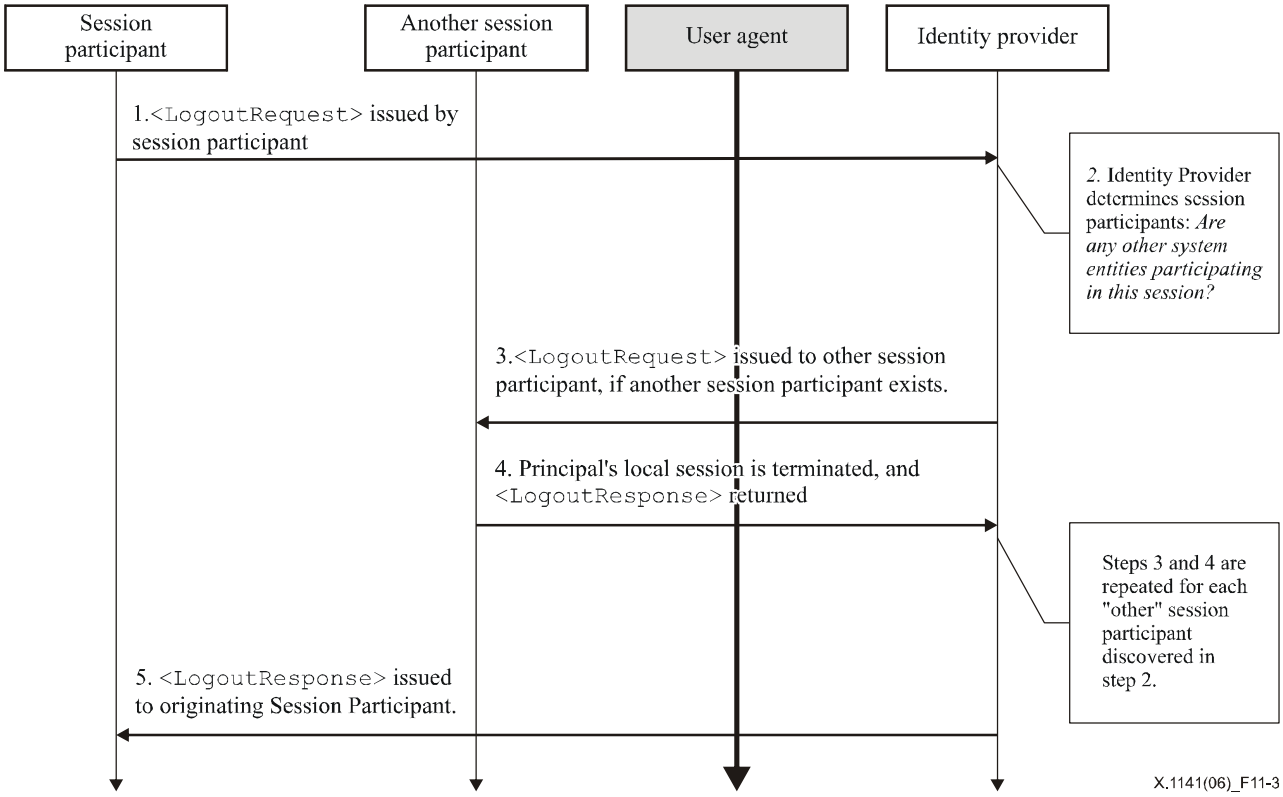
معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحييزات: لا يوجد

2.4.4.11 نظرة شاملة إلى الجانبية

يوضح الشكل 11-3 التخطيطة الأساسية لإنجاز اختتام الدورة الوحيد:



الشكل X.1141/3-11 – تخطيطة لإنجاز اختتام دورة وحيد

يوضح تظليل وكيل المستعمل بالرمادي أن تبادل الرسالة يمكن أن يحدث عبر وكيل المستعمل أو بدونه فيكون تبادلاً مباشراً ما بين كيانات النظام، وهذا يتوقف على رابطة اللغة SAML المستعملة لتنفيذ الجانبية.

والجانبية تشرح الخطوات التالية. قد يوجد داخل خطوة واحدة فردية تبادل واحد أو أكثر لرسائل حقيقية، حسب الرابطة المستعملة لهذه الخطوة وغيرها من أنماط السلوك المتوقفة على التنفيذ.

1) <LogoutRequest> صادر عن مشترك في الدورة إلى مزوّد الهوية

يبادر المشترك في الدورة في الخطوة 1 إلى اختتام دورة وحيد، وينهي دورة أو دورات طرف رئيسي بإرساله رسالة <LogoutRequest> إلى مزوّد الهوية الذي كان قد استلم منه تأكيد الاستيقان المقابل. ويمكن إرسال الطلب مباشرة إلى مزوّد الهوية أو إرساله بطريقة غير مباشرة عبر وكيل المستعمل.

2) مزوّد الهوية يحّد المشتركين في الدورة

يستخدم مزوّد الهوية في الخطوة 2 محتويات الرسالة <LogoutRequest> (أو يستخدم آلية أخرى إن كان هو المبادر إلى الاختتام الوحيد) ليحدّد الدورة أو الدورات التي يجري اختتامها. فإذا لم يكن هناك أي مشترك آخر في الدورة، تنتقل الجانبية إلى الخطوة 5. وإلا فتكرر الخطوتان 3 و4 لكل مشترك في الدورة تم التعريف بهويته.

3) <LogoutRequest> صادر عن مزوّد الهوية غلى مشترك الدورة أو إلى سلطة الدورة

يصدر مزوّد الهوية في الخطوة 3 رسالة <LogoutRequest> إلى مشترك في الدورة أو إلى سلطة الدورة ذات الصلة بالدورة الواحدة أو بالدورات التي يجري اختتامها. ويمكن إرسال الطلب مباشرة إلى الكيان أو بصورة غير مباشرة عبر وكيل المستعمل (إن كان متّسقاً مع شكل الطلب في الخطوة 1).

4) يصدر المشترك في الدورة أو سلطة الدورة <LogoutResponse> إلى مزود الهوية

ينهي المشترك في الدورة أو سلطة الدورة في الخطوة 4 دورة أو دورات الطرف الرئيسي كما جاء في الطلب (إن أمكن)، ويرجّع <LogoutResponse> إلى مزوّد الهوية. ويمكن ترجيع الاستجابة مباشرة إلى مزوّد الهوية أو بصورة غير مباشرة عبر وكيل المستعمل (إن كان متّسقاً مع شكل الطلب في الخطوة 3).

5) يصدر مزوّد الهوية <LogoutResponse> إلى المشترك في الدورة

يصدر مزوّد الهوية في الخطوة 5 رسالة <LogoutResponse> إلى المشترك في الدورة الطالب الأصلي. ويمكن ترجيع الاستجابة مباشرة إلى المشترك في الدورة أو بصورة غير مباشرة عبر وكيل المستعمل (إن كان متّسقاً مع شكل الطلب في الخطوة 1).

يستطيع مزوّد الهوية (العامل كسلطة دورة) المبادرة إلى هذه الجانبية من الخطوة 2، وإصدار <LogoutRequest> إلى جميع المشتركين في الدورة، والقفز من فوق الخطوة 5.

3.4.4.11 وصف الجانبية

إذا بادر مشترك في الدورة إلى الجانبية، فليبدأ بالفقرة الفرعية 1.3.4.4.11. أما إذا بادر إليها مزوّد الهوية فليبدأ بالفقرة الفرعية 2.3.4.4.11. وفي الوصف التالي يتم الرجوع إلى ما يلي:

- **خدمة اختتام الدورة الوحيد**

هذه هي النقطة النهائية الوحيدة من بروتوكول اختتام الدورة، لدى مزوّد هوية أو مشترك في دورة، تسلم إليها الرسالتان <LogoutRequest> أو <LogoutResponse> (أو شيء مصطنع يمثلها). وقد تستخدم نفس النقاط النهائية أو نقاط نهائية مختلفة من أجل الطلبات والاستجابات.

1.3.4.4.11 يُصدر المشترك في الدورة <LogoutRequest> إلى مزوّد الهوية

إذا كان مشترك في الدورة هو الذي يبادر إلى جانبية اختتام الدورة، فإنه يتفحص تأكيد أو تأكيدات الاستيقان التي استلمها، وهي تخص الدورة أو الدورات الجاري اختتامها، ويجمّع القيمة أو القيم SessionIndex التي استلمها من مزوّد الهوية. وإذا كان يشترك العديد من مزوّدي الهوية، يتعين تكرار الجانبية لكل واحد منهم على حدة.

ولكي يبادر المشترك في الدورة إلى الجانبية، يصدر رسالة <LogoutRequest> إلى النقطة النهائية لطلب خدمة اختتام الدورة الوحيد الخاصة بمزوّد الهوية، التي تحتوي على عنصر واحد أو أكثر من العناصر <SessionIndex> المنطبقة. ويتعين احتواء عنصر واحد على الأقل. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية، والروابط التي يعتمدها مزوّد الهوية.

الروابط غير المتزامنة (القناة الجبهية)

ينبغي للمشترك في الدورة (إن كان وكيل مستعمل الطرف الرئيسي موجوداً) أن يستخدم رابطة غير متزامنة، مثل الروابط HTTP Redirect أو POST أو Artifact (انظر البند 10)، لإرسال الطلب إلى مزوّد الخدمة عبر وكيل المستعمل. وبعد ذلك ينبغي لمزوّد الهوية أن ينشر أي رسائل مطلوبة لاختتام الدورة على المشتركين الإضافيين في الدورة، كما هو مطلوب

باستعمال رابطة متزامنة أو غير متزامنة. ويفضل استعمال رابطة غير متزامنة للطلب الأصلي، لأنها تعطي مزوّد الهوية أفضل فرصة لنجاح نشر اختتام الدورة على المشتركين الآخرين في الدورة أثناء الخطوة 3 من الفقرة الفرعية 2.4.4.11.

وإذا كانت الرابطة HTTP Redirect أو POST هي المستعملة، تسلّم الرسالة <LogoutRequest> إلى مزوّد الهوية في هذه الخطوة. وأما إذا كانت الرابطة HTTP Artifact هي المستعملة، يستخدم معرف الهوية جانبية استبانة الشيء المصطنع المعرفة في الفقرة الفرعية 6.4.11، وهو يقوم باستدعاء خلفي إلى المشترك في الدورة لكي يستعيد الرسالة <LogoutRequest> باستخدام الرابطة SOAP مثلاً.

ويوصى بأن تجري التبادلات HTTP في هذه الخطوة على الصيغة TLS 1.0 للاحتفاظ بائتمانية الرسالة وسلامتها. ويجب أن تكون الرسالة <LogoutRequest> موقّعة، إذا كانت الرابطة HTTP POST أو Redirect هي المستعملة. وعند استعمال الرابطة HTTP Artifact، فإنها تقدم وسيلة بديلة لاستيقان مُصْدر الطلب، عند التخلي عن مرجعية الشيء المصطنع.

وتقدم كل واحدة من هذه الروابط آلية للحالة RelayState، يستطيع المشترك في الدورة استعمالها لإرفاق تبادل الجانبية مع الطلب الأصلي. وينبغي للمشترك في الدورة أن يكشف عن أقل ما يمكن من المعلومات في القيمة RelayState، إلا إذا كانت الجانبية لا تتطلب مثل هذه التدابير اللازمة للسرية.

الروابط المتزامنة (القناة الخلفية)

وبطريقة أخرى، يستطيع المشترك في الدورة استخدام رابطة متزامنة، مثل الرابطة SOAP (انظر البند 10)، لإرسال الطلب مباشرة إلى مزوّد الهوية. وعندئذ ينبغي لمزوّد الهوية أن ينشر أي رسائل مطلوبة لاختتام دورة على مشتركين آخرين في الدورة، كما هو مطلوب عند استخدام رابطة متزامنة. ويتعين على الطالب أن يستيقن نفسه لدى مزوّد الهوية، سواء بالتوقيع على <LogoutRequest> أم باستعمال أي آلية أخرى تعتمدها الرابطة.

وتتضمن الفقرة الفرعية 1.4.4.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <LogoutRequest>.

2.3.4.4.11 مزوّد الهوية يُحدّد المشتركين في الدورة

إذا كان مزوّد الهوية هو الذي يبادر إلى جانبية اختتام الدورة، أو كان مزوّد الهوية يقوم بمعالجة الطلب لدى استلامه رسالة <LogoutRequest> صالحه، يتعين عليه أن يتفّحص معرف الهوية والعناصر <SessionIndex>، ويحدّد الدورات المطلوب اختتامها.

عندئذ يتبع مزوّد الهوية الخطوتين 3 و4 الواردتين في الشكل 11-3، فيما يخص كل كيان مشترك في الدورة أو الدورات الجاري اختتامها، هو غير المشترك في الدورة الطالب الأصلي (إن وجد) كما هو مشروح في الفقرة الفرعية 7.2.8.

3.3.4.4.11 يصدر مزوّد الهوية <LogoutRequest> إلى المشترك في الدورة أو إلى سلطة الدورة

لكي ينشر مزوّد الهوية اختتام الدورة، يصدر الطلب <LogoutRequest> الخاص به إلى سلطة الدورة أو إلى المشترك في دورة يجري اختتامها. ويرسل الطلب باستخدام رابطة SAML متّسقة مع إمكانية المستجيب ومع تيسر وكيل المستعمل لدى مزوّد الهوية.

والرابطة التي جرى بها استلام الطلب الأصلي في الخطوة 1 في الشكل 11-3، لا تفرض عادة الرابطة التي يمكن استعمالها في هذه الخطوة، ما عدا ما هو مذكور في الخطوة 1. واستعمال رابطة متزامنة تلتف حول وكيل المستعمل، يضطر مزوّد الهوية إلى استعمال رابطة مماثلة لكي ينشر طلبات إضافية.

وتتضمن الفقرة الفرعية 1.4.4.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <LogoutRequest>.

4.3.4.4.11 يُصدر المشترك في دورة أو سلطة الدورة <LogoutRequest> إلى مزوّد الهوية

يتعين على المشترك في الدورة أو سلطة الدورة معالجة الرسالة <LogoutRequest> كما هو محدّد في الفقرة الفرعية 7.2.8. وبعد معالجة الرسالة أو عند مصادفة خطأ، يتعين على الكيان أن يصدر رسالة <LogoutResponse> تحتوي على شفرة الحالة المناسبة، يرسلها إلى مزوّد الخدمة الطالب لإكمال تبادل البروتوكول SAML.

الروابط المتزامنة (القناة الخلفية)

إذا كان مزوّد الهوية يستعمل رابطة متزامنة، مثل الرابطة SOAP (انظر البند 10)، يتم ترجيع الاستجابة مباشرة لإكمال الاتصال المتزامن. ويتعين على المستجيب أن يستيقن نفسه لدى مزوّد الهوية الطالب، سواء بالتوقيع على الاستجابة <LogoutResponse> أم باستعمال أي آلية تدعمها الرابطة.

الروابط غير المتزامنة (القناة الجبهية)

إذا كان مزوّد الهوية يستعمل رابطة غير متزامنة، مثل الروابط HTTP Redirect أو POST أو Artifact (انظر البند 10)، يتم ترجيع <LogoutResponse> (أو الشيء المصطنع) عبر وكيل المستعمل إلى النقطة النهائية في استجابة خدمة اختتام الدورة الوحيد الخاصة بمزوّد الهوية. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية، والروابط التي يعتمدها مزوّد الهوية. كما يمكن استعمال أي رابطة غير متزامنة يعتمدها كلا الكيانين.

وإذا كانت الرابطة HTTP Redirect أو POST هي المستعملة، تسلّم الرسالة <LogoutResponse> عندئذ إلى مزوّد الهوية في هذه الخطوة. وإذا كانت الرابطة HTTP Artifact هي المستعملة، يستعمل مزوّد الهوية جانبية استبانة الشيء المصطنع المعرفة في الفقرة الفرعية 6.4.11، وهو يقوم باستدعاء خلفي إلى الكيان المستجيب، لكي يستعيد الرسالة <LogoutResponse> باستخدام الرابطة SOAP.

ويوصى بأن تجري التبادلات HTTP في هذه الخطوة على الصيغة TLS 1.0 للاحتفاظ بائتمانية الرسالة وسلامتها. ويجب أن تكون الرسالة <LogoutResponse> موقّعة، إذا كانت الرابطة HTTP POST أو Redirect هي المستعملة. وعند استعمال الرابطة HTTP Artifact، فإنها تقدّم وسيلة بديلة لاستيقان مُصدر الاستجابة عند التخلي عن مرجعية الشيء المصطنع.

وتتضمن الفقرة الفرعية 2.4.4.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <LogoutResponse>.

5.3.4.4.11 يُصدر مزوّد الهوية <LogoutResponse> إلى المشترك في الدورة

بعد معالجة الرسالة <LogoutRequest> الواردة من المشترك الأصلي في الدورة، كما هو مشروح في الخطوات السابقة، يتعين على مزوّد الهوية أن يستجيب للطلب الأصلي باستجابة <LogoutResponse>، تحتوي على شفرة حالة مناسبة لإكمال تبادل البروتوكول SAML.

وترسل الاستجابة إلى المشترك الأصلي في الدورة، باستخدام الرابطة SAML المتّسقة مع الرابطة المستعملة في الطلب الأصلي ومع إمكانية المستجيب وتيسر وكيل المستعمل لدى مزوّد الهوية. وبافتراض أن رابطة غير متزامنة كانت قد استعملت في الخطوة 1 في الشكل 11-3 يمكن عندئذ استعمال أي رابطة يعتمدها كلا الكيانين.

وتتضمن الفقرة الفرعية 2.4.4.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <LogoutResponse>.

4.4.4.11 استعمال بروتوكول اختتام الدورة الوحيد

تشرح هذه الفقرة الفرعية استعمال الرسالتين <LogoutRequest> و<LogoutResponse>.

1.4.4.4.11 استعمال <LogoutRequest>

يتعين أن يكون العنصر <Issuer> موجوداً، ويتعين عليه أن يحتوي على معرف الهوية الوحيد للكيان الطالب. ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

ويتعين على الطالب أن يستيقن نفسه لدى المستجيب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية خاصة بالرابطة.

ويتعين التعريف بهوية الطرف الرئيسي في الطلب باستعمال معرف هوية **يتواءم تواؤماً شديداً** مع معرف الهوية في تأكيد الاستيقان الذي يصدره أو يستلمه الطالب، بشأن الدورة الجاري اختتامها، وفقاً لقواعد المواءمة المحددة في الفقرة 7.2.8.

وإذا كان الطالب هو مشترك في دورة، يتعين عليه أن يدرج في الطلب على الأقل عنصراً واحداً من العناصر <SessionIndex>. وإذا كان الطالب هو سلطة الدورة (أو يعمل باسمها)، يمكنه عندئذ حذف أي عنصر من مثل هذه العناصر، لكي يبين انتهاء جميع الدورات المنطبقة الخاصة بالطرف الرئيسي.

ملاحظة (للاطّلاع) – يوضّح PE38 (انظر OASIS PE:2006) الفقرة أعلاه كما يلي:

إذا كان الطالب هو مشترك في دورة، يتعين عليه أن يدرج في الطلب على الأقل عنصراً واحداً من العناصر <SessionIndex>. (منذ الفقرة 4.11 والمشترك في الدورة يستلم دائماً نعتاً SessionIndex بين العناصر <saml:AuthnStatement> التي يستلمها لكي يتدر الدورة). وإذا كان الطالب هو سلطة الدورة (أو يعمل باسمها)، يمكنه عندئذ حذف أي عنصر من مثل هذه العناصر، لكي يبين انتهاء جميع الدورات المنطبقة الخاصة بالطرف الرئيسي.

2.4.4.4.11 استعمال <LogoutResponse>

يتعين أن يكون العنصر <Issuer> موجوداً، ويتعين عليه أن يحتوي على معرف الهوية الوحيد للكيان المستجيب. ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

ويتعين على المستجيب أن يستيقن نفسه لدى الطالبن وأن يضمن سلامة الرسالة سواء بالتوقيع على الرسالة أم باستعمال آلية خاصة بالرابطة.

5.4.4.11 استخدام المعطيات الشرحية

عنصر النقطة النهائية <md:SingleLogoutService> يشرح الروابط والموقع أو المواقع المعتمدة التي يستطيع أحد الكيانات إرسال الطلبات والاستجابات منها. مستخدماً هذه الجانبية. فالطالب يستطيع، عندما يجفّر معرف هوية الطرف الرئيسي، استعمال عنصر المستجيب <md:KeyDescriptor> مع نعت use of encryption، لكي يحدد خوارزمية تجفير مناسبة مع عمليات ضبط استعمالها، ومعها المفتاح العمومي الواجب استعماله له عند تسليم مفتاح تجفير مجمل.

5.4.11 جانبية إدارة معرف هوية الاسم

في السيناريو الذي تعتمده جانبية إدارة معرف هوية الاسم، يكون مزوّد هوية قد تبادل شكلاً من معرف الهوية الدائم لطرف رئيسي مع مزوّد الخدمة، الأمر الذي يسمح لهما بتقاسم معرف هوية مشترك لفترة زمنية معينة. وبعد ذلك يمكن لمزوّد الهوية أن يرغب في تبليغ مزوّد الخدمة بتغيير حصل في النسق (و/أو القيمة) الذي سوف يستعمله للتعريف بهوية نفس الطرف الرئيسي في المستقبل. كما يمكن حدوث العكس أيضاً، فقد يرغب مزوّد الخدمة في أن يرفق بالطرف الرئيسي "اسماً مستعاراً" خاصاً به، لكي يتأكد من أن مزوّد الهوية سوف يدرجه، عندما يتصل به في المستقبل بشأن الطرف الرئيسي. وأخيراً قد يرغب أحد المزوّدين الاثنين في إعلام الآخر بأنه لن يصدر أو يقبل بعد الآن رسائل تستعمل معرف هوية خاصاً. ويستعمل بروتوكول إدارة معرف هوية الاسم في اللغة SAML، لتنفيذ هذه السيناريوهات.

ملاحظة (للاطّلاع) – يقترح PE12 (انظر OASIS PE:2006) أن تعاد كتابة الجملة الثانية في الفقرة أعلاه على النحو التالي:

وبعد ذلك يمكن لمزوّد الهوية أن يرغب في تبليغ مزوّد الخدمة بتغيير في القيمة التي سوف يستعملها للتعريف بهوية نفس الطرف الرئيسي في المستقبل.

وتتيح الجانبية للبروتوكول بأن يندمج مع رابطة متزامنة، مثل الرابطة SOAP، أو مع روابط غير متزامنة في القناة الجبهية، مثل الروابط HTTP Redirect أو POST أو Artifact. وقد تُطلب رابطة من القناة الجبهية مثلاً في حالات يكون فيها التفاعل المباشر بين وكيل المستعمل والمزوّد المستجيب مطلوباً من أجل إجراء التغيير.

1.5.4.11 المعلومات المطلوبة

تعريف الهوية: `urn:oasis:names:tc:SAML:2.0:profiles:SSO:nameid-mgmt`

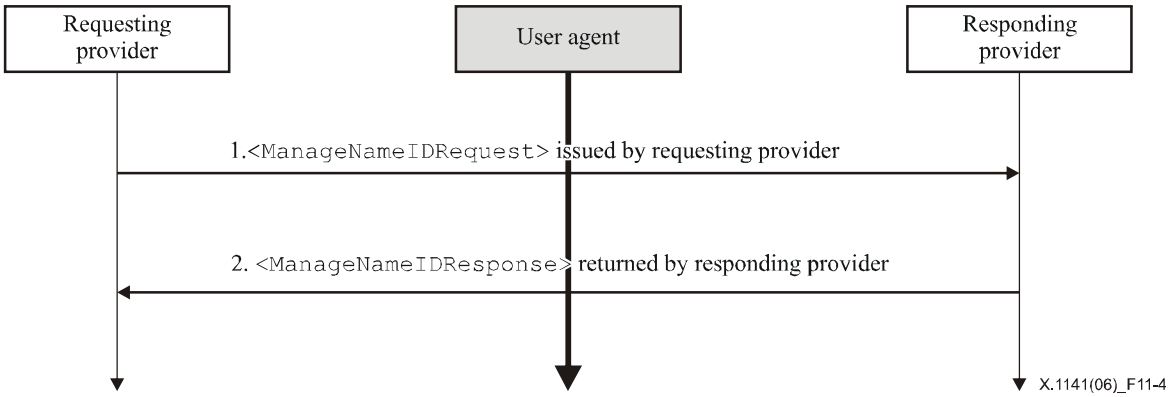
معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحييزات: لا يوجد

2.5.4.11 نظرة شاملة إلى الجانبية

يوضّح الشكل 11-4 التخطيطة الأساسية لجانبية إدارة معرف هوية الاسم.



الشكل X.1141/4-11 – جانبية إدارة معرف هوية الاسم

يوضّح تظليل وكيل المستعمل بالرمادي تبادل الرسالة يمكن أن يحدث عبر وكيل المستعمل أو بدونه فيكون تبادلاً مباشراً ما بين كيانات النظام، وهذا يتوقف على رابطة اللغة SAML المستعملة لتنفيذ الجانبية.

والجانبية تشرح الخطوتين التاليتين. قد يوجد داخل واحدة من الخطوتين منفردة تبادل واحد أو أكثر لرسائل حقيقية، حسب الرابطة المستعملة لهذه الخطوة وغيرها من أنماط السلوك المتوقفة على التنفيذ.

1) **مزوّد الخدمة (أو الهوية) الطالب يصدر <ManageNameIDRequest>**

يبادر مزوّد الخدمة أو الهوية في الخطوة 1 إلى الجانبية، بإرساله رسالة `<ManageNameIDRequest>` إلى المزوّد الآخر الذي يرغب في إبلاغه بالتغيير. ويمكن إرسال الطلب مباشرة إلى المزوّد المستجيب أو يمكن إرساله عبر وكيل المستعمل.

2) **مزوّد الخدمة (أو الهوية) المستجيب يصدر <ManageNameIDResponse>**

يصدر المزوّد المستجيب في الخطوة 2 (بعد معالجته الطلب)، رسالة `<ManageNameIDResponse>` إلى المزوّد الأصلي الطالب. ويمكن ترجيع الاستجابة مباشرة إلى المزوّد الطالب أو بصورة غير مباشرة عبر وكيل المستعمل (إن كان متسقاً مع شكل الطلب في الخطوة 1).

3.5.4.11 وصف الجانبية

في الوصف التالي، يتم الرجوع إلى ما يلي:

خدمة إدارة معرف هوية الاسم

هذا هو اسم النقطة النهائية في بروتوكول إدارة معرف الهوية لدى مزوّد خدمة أو هوية يمكن أن تسلّم إليهما الرسالتان <ManageNameIDRequest> و<ManageNameIDResponse> (أو الشيء المصطنع الذي يمثلها). ويمكن استعمال نفس النقاط النهائية أو استعمال نقاط نهائية مختلفة للطلبات وللاستجابات.

1.3.5.4.11 مزوّد الخدمة (أو الهوية) الطالب يصدر <ManageNameIDRequest>

لكي يبادر المزوّد الطالب إلى الجانبية، يصدر رسالة <ManageNameIDRequest> إلى النقطة النهائية لطلب خدمة إدارة معرف هوية الاسم التابعة لمزوّد آخر. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية، والروابط التي يدعمها المزوّد المستجيب.

- **الروابط المتزامنة (القناة الخلفية)**

  يمكن أن يستعمل المزوّد الطالب رابطة متزامنة، مثل رابطة البروتوكول SOAP (انظر البند 10)، لإرسال طلب مباشرة إلى المزوّد الآخر. ويتعين على الطالب أن يستيقن نفسه لدى المزوّد الآخر، سواء بالتوقيع على الرسالة <ManageNameIDRequest> أم باستعمال أي آلية أخرى تدعمها الرابطة.

- **الروابط غير المتزامنة (القناة الجبهية)**

  وفي حالة مقابلة، يمكن للمزوّد الطالب (إذا كان وكيل المستعمل للطرف الرئيسي موجوداً) أن يستعمل رابطة غير متزامنة، مثل الروابط HTTP Redirect أو POST أو Artifact (انظر البند 10)، لإرسال طلب إلى المزوّد الآخر عبر وكيل المستعمل.

إذا كانت الرابطة HTTP Redirect أو POST هي المستعملة، تسلّم عندئذ الرسالة <ManageNameIDRequest> إلى المزوّد الآخر في هذه الخطوة. وإذا كانت الرابطة HTTP Artifact هي المستعملة، يستخدم المزوّد الآخر جانبية استبانة الشيء المصطنع المحددة في الفقرة الفرعية 6.4.11، ويقوم المزوّد الآخر باستدعاء خلفي إلى المزوّد الطالب من أجل استرجاع الرسالة <ManageNameIDRequest>، باستخدام الرابطة SOAP مثلاً.

ويوصى بأن تجري التبادلات HTTP في هذه الخطوة على الصيغة TLS 1.0 للاحتفاظ بائتمانية الرسالة وسلامتها. ويتعين أن تكون الرسالة <ManageNameIDRequest> موقّعة، إن كانت الرابطة HTTP POST أو Redirect هي المستعملة. وتوفر الرابطة HTTP Artifact، عندما تستعمل، وسيلة بديلة لاستيقان مُصدر الطلب عند التخلي عن مرجعية الشيء المصطنع.

وتوفر كل واحدة من هذه الروابط آلية RelayState، يستطيع المزوّد الطالب استعمالها للجمع بين تبادل الجانبية والطلب الأصلي. وينبغي للمزوّد الطالب أن يكشف عن أقل ما يمكن من المعلومات في قيمة RelayState، ما لم يكن استعمال الجانبية لا يتطلب مثل هذه التدابير عن السرية.

تتضمن الفقرة الفرعية 1.4.5.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <ManageNameIDRequest>.

2.3.5.4.11 مزوّد الخدمة (أو الهوية) المستجيب يصدر <ManageNameIDResponse>

يتعين على المستلم أن يعالج الرسالة <ManageNameIDRequest>. وبعد معالجة الرسالة أو مصادفة خطأ، يتعين على المستلم أن يصدر رسالة <ManageNameIDResponse> تحتوي على شفرة حالة مناسبة، إلى المزوّد الطالب لإكمال تبادل البروتوكول SAML.

- **الروابط المتزامنة (القناة الخلفية)**

إذا كان المزوّد الطالب قد استعمل رابطة متزامنة، مثل الرابطة SOAP (انظر البند 10)، يتم ترجيع الاستجابة مباشرة لإكمال الاتصال المتزامن. ويتعين على المستجيب أن يستيقن نفسه لدى المزوّد الطالب، سواء بالتوقيع على الرسالة <ManageNameIDResponse> أم بأي آلية أخرى تعتمدها الرابطة.

- **الروابط غير المتزامنة (القناة الجبهية)**

إذا كان المزوّد الطالب قد استعمل رابطة غير متزامنة، مثل الروابط HTTP Redirect أو POST أو Artifact (انظر البند 10)، يتم ترجيع الاستجابة <ManageNameIDResponse> (أو Artifact) عبر وكيل المستعمل إلى النقطة النهائية للاستجابة في خدمة إدارة معرف هوية الاسم التابعة للمزوّد الطالب. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية والروابط التي يعتمدها المزوّد الطالب. ويمكن استعمال أي رابطة يعتمدها كلا الكيانين.

وإذا كانت الرابطة HTTP Redirect أو POST هي المستعملة، تسلّم عندئذ الرسالة <ManageNameIDResponse> إلى المزوّد الطالب في هذه الخطوة. وإذا كانت الرابطة HTTP Artifact هي المستعملة، يستعمل المزوّد الطالب جانبية استبانة الشيء المصطنع المحددة في الفقرة الفرعية 6.4.11، وهو يقوم باستدعاء خلفي إلى المزوّد المستجيب لكي يسترجع الرسالة <ManageNameIDResponse>، مستعملاً الرابطة SOAP مثلاً.

ويوصى بأن تجري التبادلات HTTP في هذه الخطوة على الصيغة TLS 1.0 للاحتفاظ بائتمانية الرسالة وسلامتها. ويتعين أن تكون الرسالة <ManageNameIDResponse> موقعة، إن كانت الرابطة HTTP POST أو Redirect هي المستعملة. وتوفر الرابطة HTTP Artifact، عندما تستعمل، وسيلة بديلة لاستيقان مُصْدر الاستجابة، عند التخلي عن مرجعية الشيء المصطنع.

تتضمن الفقرة الفرعية 2.4.5.4.11 القواعد الخاصة بالجانبية المتعلقة بالرسالة <ManageNameIDResponse>.

4.5.4.11 استعمال بروتوكول إدارة معرف هوية الاسم

تشرح هذه الفقرة الفرعية استعمال الرسالتين ManageNameIDRequest وManageNameIDResponse.

1.4.5.4.11 استعمال <ManageNameIDRequest>

يتعين أن يكون العنصر <Issuer> موجوداً، ويتعين عليه أن يحتوي على معرف الهوية الوحيد للكيان الطالب. ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

ويتعين على المستجيب أن يستيقن نفسه لدى الطالب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية خاصة بالرابطة.

5.5.4.11 استعمال المعطيات الشرحية

عنصر النقطة النهائية <md:ManageNameIDService> يشرح الروابط والموقع أو المواقع المعتمدة التي يستطيع أحد الكيانات إرسال الطلبات والاستجابات منها، مستخدماً هذه الجانبية. فالطالب يستطيع، عندما مجفّر معرف هوية الطرف الرئيسي، استعمال عنصر المستجيب <md:KeyDescriptor> مع نعت تجفير لكي يحدد خوارزمية تجفير مناسبة مع عمليات ضبط استعمالها، ومعها المفتاح العمومي الواجب استعماله عند تسليم مفتاح تجفير مجمل.

6.4.11 جانبية استبانة الشيء المصطنع

يحدّد البند 10 بروتوكول استبانة الشيء المصطنع للتخلي عن مرجعية شيء مصطنع في اللغة SAML إلى رسالة بروتوكول مقابل. والرابطة HTTP Artifact (انظر البند 10) تزيد من هذه الآلية لكي تمرر بالإحالة رسائل البروتوكول SAML. وتشرح هذه الجانبية استعمال هذا البروتوكول مع رابطة متزامنة، مثل الرابطة SOAP المحددة في البند 10.

1.6.4.11 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:artifact

معلومات الاتصال: security-services-comment@lists.oasis-open.org

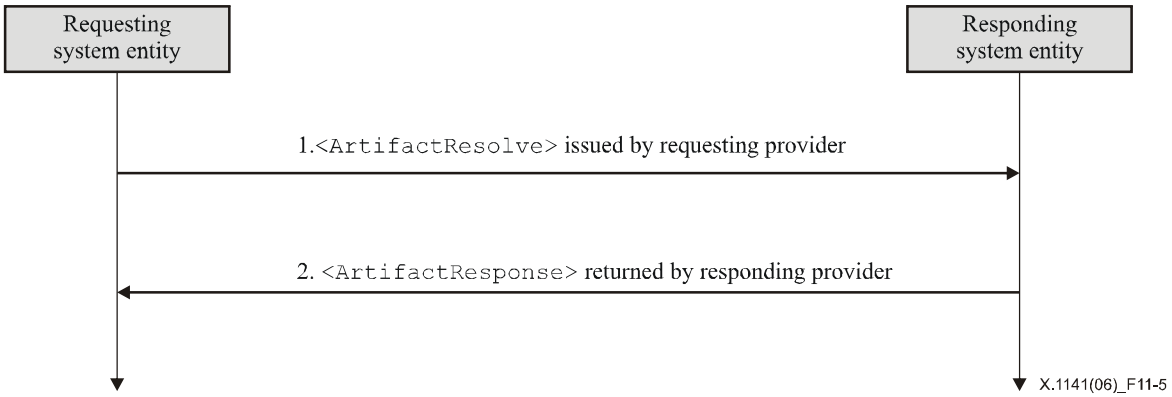
الوصف: وارد أدناه.

التحييدات: لا يوجد.

2.6.4.11 نظرة شاملة إلى الجانبية

يحدّد البند 8 بالتفصيل اللازم تبادل الرسائل وقواعد المعالجة الأساسية التي تحكم هذه الجانبية. وهو يحدّد الرسائل المطلوب تبادلها، مجتمعة مع الرابطة المستعملة لتبادل الرسائل. ويحدد البند 10 ربط تبادل الرسائل مع الصيغة SOAP V1.1. وتطبق جميع المتطلبات المحددة في هذه المواصفات، إلا إذا ورد تنويه خاص في هذه التوصية.

ويوضح الشكل 11-5 التخطيطة الأساسية لجانبية استبانة الشيء المصطنع.



الشكل X.1141/5-11 – التخطيطة الأساسية لجانبية استبانة الشيء المصطنع

وتشرح الجانبية الخطوتين التاليتين:

1) الكيان الطالب يُصدر <ArtifactResolve>

يبادر الطالب في الخطوة 1 إلى الجانبية بإرساله رسالة <ArtifactResolve> إلى مُصدر الشيء المصطنع.

2) الكيان المستجيب يصدر <ArtifactResponse>

يصدر المستجيب في الخطوة 2 (بعد معالجته الطلب) رسالة <ArtifactResponse> إلى الطالب.

3.6.4.11 وصف الجانبية

في الوصف التالي، يتم الرجوع إلى التالي:

- **خدمة استبانة الشيء المصطنع**

هذه هي النقطة النهائية في بروتوكول استبانة الشيء المصطنع لدى مُصدر الشيء المصطنع، وإليها تسلَّم الرسائل <ArtifactResolve>.

1.3.6.4.11 الكيان الطالب يصدر <ArtifactResolve>

لكي يبادر الطالب إلى الجانبية، بعد أن استلم الشيء المصطنع، وحدّد مُصدره مستخدما SourceID، يرسل رسالة <ArtifactResolve> تحتوي على الشيء المصطنع، إلى النقطة النهائية في خدمة استبانة الشيء المصطنع التابعة لمُصدر الشيء المصطنع. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية، والروابط التي يعتمدها مُصدر الشيء المصطنع.

ويتعين على الطالب أن يستعمل رابطة متزامنة، مثل الرابطة SOAP (انظر البند 10)، لإرسال الطلب مباشرة إلى مصدر الشيء المصطنع. وينبغي للطالب أن يستيقن نفسه لدى المستجيب، سواء بالتوقيع على الرسالة <ArtifactResolve> أم باستخدام آلية أخرى تعتمدها الرابطة. وقد تفرض بعض الجانبيات الخاصة التي تستخدم الرابطة HTTP Artifact متطلبات إضافية، كأن يكون الاستيقان إلزامياً.

وتتضمن الفقرة الفرعية 1.4.6.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <ArtifactResolve>.

2.3.6.4.11 الكيان المستجيب يصدر <ArtifactResponse>

يتعين على مُصدر الشيء المصطنع أن يعالج الرسالة <ArtifactResolve> كما هو محدد في البند 8. ويتعين على مُصدر الشيء المصطنع، بعد معالجته الرسالة أو بعد مصادفته خطأ، أن يرجّع رسالة <ArtifactResponse> تحتوي على شفرة حالة مناسبة، إلى الطالب لإكمال تبادل بروتوكولات اللغة SAML. ويجب أيضاً إدراج رسالة البروتوكول SAML بالتخلي عن المرجعية المتعلقة بالشيء المصطنع، إن كان ذلك ناجحاً.

ويتعين على المستجيب أن يستيقن نفسه لدى الطالب، سواء بالتوقيع على الرسالة <ArtifactResponse> أو باستخدام آلية أخرى تعتمدها الرابطة.

وتتضمن الفقرة الفرعية 2.4.6.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <ArtifactResponse>.

4.6.4.11 استعمال بروتوكول استبانة الشيء المصطنع

تشرح هذه الفقرة الفرعية استعمال الرسالتين ArtifactResolve وArtifactResponse.

1.4.6.4.11 استعمال <ArtifactResolve>

يتعين أن يكون العنصر <Issuer> موجوداً، ويتعين عليه أن يحتوي على معرف الهوية الوحيد للكيان الطالب، ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

وينبغي للطالب أن يستيقن نفسه لدى المستجيب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية خاصة بالرابطة. وقد تفرض بعض الجانبيات الخاصة التي تستعمل الرابطة HTTP Artifact متطلبات إضافية، كأن يكون الاستيقان إلزامياً.

2.4.6.4.11 استعمال <ArtifactResponse>

يتعين أن يكون العنصر <Issuer> موجوداً، ويتعين عليه أن يحتوي على معرف الهوية الوحيد لمُصدر الشيء المصطنع. ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

ويتعين على المستجيب أن يستيقن نفسه لدى الطالب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية خاصة بالرابطة.

5.6.4.11 استخدام المعطيات الشرحية

يحدّد البند 9 عنصر النقطة النهائية مفهرساً هو <md:ArtifactResolutionService>، لوصف الروابط والموقع أو المواقع المعتمدة، التي يمكن لطالب أن يرسل الطلبات إليها مستخدماً هذه الجانبية. ويستعمل النعت index لتمييز النقاط النهائية المحتملة التي يمكن تحديدها بالإحالة في الحقل EndpointIndex التابع للشيء المصطنع.

7.4.11 جانبية طلب التأكيد أو الاستفهام عنه

يحدد البند 10 بروتوكولاً لطلب تأكيدات موجودة بالإحالة أو بالاستفهام على أساس الصاحب ومعايير إضافية خاصة بتصريح. وتصف هذه الجانبية استخدام هذا البروتوكول مع رابطة متزامنة، مثل الرابطة SOAP المحددة في البند 10.

1.7.4.11 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:query

معلومات الاتصال: security-services-comment@lists.oasis-open.org

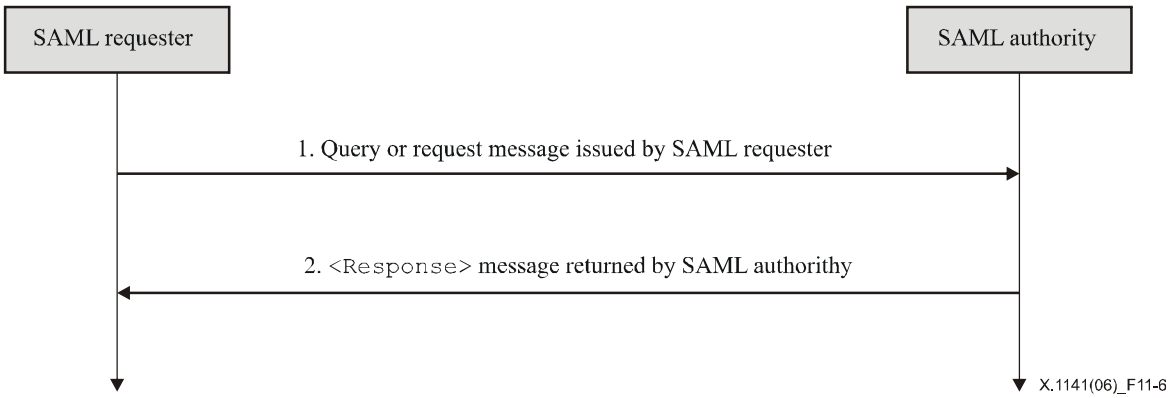
الوصف: وارد أدناه.

التحييزات: لا يوجد.

2.7.4.11 نظرة شاملة إلى الجانبية

يحدد البند 8 بالتفصيل اللازم تبادل الرسائل وقواعد المعالجة الأساسية التي تحكم هذه الجانبية، وهو يحدد الرسائل المطلوب تبادلها، مجتمعة مع الرابطة المستعملة لتبادل الرسائل. ويحدد البند 10 ربط تبادل الرسائل مع الصيغة SOAP V1.1. وتطبق جميع المتطلبات المحددة في هذه المواصفات، إلا إذا ورد تنويه خاص في هذه التوصية.

ويوضح الشكل 11-6 التخطيطة الأساسية لجانبية الطلب أو الاستفهام.



الشكل X.1141/6-11 – التخطيطة الأساسية لجانبية الطلب أو الاستفهام

تشرح الجانبية الخطوتين التاليتين:

1) **الطالب SAML** يصدر طلباً أو استفهاماً

يبادر الطالب SAML في الخطوة 1 إلى الجانبية بإرساله رسالة <AssertionIDRequest> أو <SubjectQuery> أو <AuthnQuery> أو <AttributeQuery> أو <AuthzDecisionQuery> إلى السلطة SAML.

2) **السلطة SAML تصدر <Response>**

تصدر السلطة المستجيبة SAML في الخطوة 2 (بعد معالجة الاستفهام أو الطلب) رسالة <Response> إلى الطالب SAML.

3.7.4.11 وصف الجانبية

في الأوصاف التالية، يتم الرجوع إلى التالي:

- **خدمة الطلب أو الاستفهام**

هذه هي النقطة النهائية في بروتوكول الطلب أو الاستفهام لدى السلطة SAML، وإليها تسلّم رسائل الاستفهام أو <AssertionIDRequest>.

1.3.7.4.11 الطالب SAML يصدر الطلب أو الاستفهام

لكي يبادر الطالب SAML إلى الجانبية، فإنه يصدر رسالة <AssertionIDRequest> أو <SubjectQuery> أو <AuthnQuery> أو <AttributeQuery> أو <AuthzDecisionQuery>، إلى النقطة النهائية من خدمة الطلب أو الاستفهام التابعة لسلطة SAML. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية، والروابط التي تعتمدها السلطة SAML.

ويتعين على الطالب SAML أن يستعمل رابطة متزامنة، مثل الرابطة SOAP (انظر البند 10)، لإرسال الطلب مباشرة إلى مزوّد الهوية. وينبغي للطالب أن يستيقن نفسه لدى السلطة SAML، سواء بالتوقيع على الرسالة أم باستعمال أي آلية أخرى تعتمدها الرابطة.

وتتضمن الفقرة الفرعية 1.4.7.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات مختلف الرسائل.

2.3.7.4.11 السلطة SAML تصدر <Response>

يتعين على السلطة SAML أن تعالج رسالة الطلب أو الاستفهام، كما هو محدّد في البند 8. وبعد أن تعالج السلطة SAML الرسالة أو بعد أن تصادف خطأ، يتعين عليها ترجيع رسالة <Response> تحتوي على شفرة حالة مناسبة، إلى الطالب SAML لإكمال تبادل البروتوكول SAML. وإذا نجح الطلب في تحديد موقع تأكيد واحد أو أكثر من التأكيدات المتوائمة، تدرج أيضاً في الاستجابة.

وينبغي للمستجيب أن يستيقن نفسه لدى الطالب، سواء بالتوقيع على <Response> أو باستعمال أي آلية أخرى تعتمدها الرابطة.

وتتضمن الفقرة الفرعية 2.4.7.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <Response>.

4.7.4.11 استعمال بروتوكول الطلب أو الاستفهام

تحدد هذه الفقرة الفرعية النقطة النهائية في بروتوكول الطلب أو الاستفهام التابعة لسلطة SAML، والتي إليها تسلّم رسائل الاستفهام.

1.4.7.4.11 استعمال الطلب أو الاستفهام

يتعين أن يكون العنصر <Issuer> موجوداً.

وينبغي للطالب أن يستيقن نفسه لدى المستجيب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية تعتمدها الرابطة.

2.4.7.4.11 استعمال <Response>

يتعين أن يكون العنصر <Issuer> موجوداً، وأن يحتوي على معرف الهوية الوحيد للسلطة SAML المستجيبة. ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity. ولا تتواءم هذه الحاجة بالضرورة مع العنصر <Issuer> في التأكيد أو التأكيدات الراجعة.

وينبغي للمستجيب أن يستيقن نفسه لدى الطالب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية تعتمدها الرابطة.

5.7.4.11 استخدام المعطيات الشرحية

يحدّد البند 9 عدة عناصر من نقطة نهائية <md:AssertionIDRequestService> و<md:AuthnQueryService> و<md:AttributeService> و<md:AuthzService> لكي يشرح الروابط والموقع أو المواقع المعتمدة التي يستطيع طالب أن يرسل منها الطلبات والاستفهامات مستخدماً هذه الجانبية.

والسلطة SAML يمكنها، عندما تجفّر التأكيدات الناتجة أو محتويات التأكيدات من أجل كيان خاص، أن تستعمل العنصر <md:KeyDescriptor> من هذا الكيان مع نعت استعمال التجفير "encryption"، لكي يحدّد خوارزمية تجفير مناسبة مع عمليات ضبط استعمالها، ومعها المفتاح العمومي الواجب استعماله عند تسليم مفتاح تجفير مجمل.

يمكن أن تحتوي الواصفات المختلفة للدور على العناصر <md:NameIDFormat> و<md:AttributeProfile> و<saml:Attribute> (حسبما ينطبق) لتبين المقدرة العامة التي تدعم أنساق معرفات هوية الاسم الخاصة، أو جانبيات النعت، أو نعوتاً وقيماً خاصة. ومقدرة دعم مثل هذه الميزات أثناء طلب معين تتوقف على السياسة وتعود إلى تقدير السلطة.

8.4.11 جانبية وضع معرف هوية الاسم على تقابل

تحدّد الفقرة الفرعية 6.2.8 بروتوكول وضع معرف هوية الاسم على تقابل، من أجل وضع معرف هوية الاسم لطرف رئيسي على تقابل مع معرف هوية اسم مختلف لنفس الطرف الرئيسي. وتشرح هذه الفقرة استعمال هذا البروتوكول مع رابطة متزامنة، مثل الرابطة SOAP المحددة في البند 10، مع خطوط توجيهية إضافية لحماية سرية الطرف الرئيسي مع تجفير وحدّ من استعمال معرف الهوية الموضوع على تقابل.

1.8.4.11 المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:nameidmapping

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحيينات: لا يوجد.

2.8.4.11 نظرة شاملة إلى الجانبية

يحدّد البند 8 بالتفصيل اللازم تبادل الرسائل وقواعد المعالجة الأساسية التي تحكم هذه الجانبية، وهو يحدّد الرسائل المطلوب تبادلها، مجتمعة مع الرابطة المستعملة لتبادل الرسائل. ويحدّد البند 10 ربط تبادل الرسائل بالصيغة SOAP V1.1. وتطبق جميع المتطلبات المحددة في هذه المواصفات، إلا إذا ورد تنويه خاص في هذه التوصية.

ويوضّح الشكل 11-7 التخطيطة الأساسية لجانبية وضع معرف هوية الاسم على تقابل.

الشكل X.1141/7-11 – التخطيطة الأساسية لجانبية معرف هوية الاسم

تشرح الجانبية الخطوتين التاليتين:

1) الكيان الطالب يصدر <NameIDMappingRequest>

يبتدر الطالب في الخطوة 1 الجانبية بإرساله رسالة <NameIDMappingRequest> إلى مزوّد الهوية.

2) مزوّد الهوية يصدر <NameIDMappingResponse>

يصدر مزوّد الهوية المستجيب في الخطوة 2 (بعد معالجة الطلب) رسالة <NameIDMappingResponse> إلى الطالب.

3.8.4.11 وصف الجانبية

تستعمل هذه الفقرة الفرعية خدمة وضع معرف هوية الاسم على تقابل، وهي النقطة النهائية في بروتوكول وضع معرف هوية الاسم على تقابل التابعة لمزوّد هوية، تسلّم إليها الرسائل <NameIDMappingRequest>.

1.3.8.4.11 الكيان الطالب يصدر <NameIDMappingRequest>

يبتدر الطالب الجانبية بإصداره رسالة <NameIDMappingRequest> إلى النقطة النهائية في خدمة وضع معرف هوية الاسم على تقابل والتابعة لمزوّد الهوية. ويمكن استعمال المعطيات الشرحية لتحديد موقع هذه النقطة النهائية والروابط التي يعتمدها مزوّد الهوية.

ويتعين على الطالب أن يستخدم رابطة متزامنة، مثل الرابطة SOAP (انظر البند 10)، لكي يرسل الطلب مباشرة إلى مزوّد الهوية. ويتعين على الطالب أن يستيقن نفسه لدى مزوّد الهوية، سواء بالتوقيع على <NameIDMappingRequest> أم باستخدام أي آلية أخرى تعتمدها الرابطة.

وتتضمن الفقرة الفرعية 1.4.8.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <NameIDMappingRequest>.

2.3.8.4.11 مزوّد الهوية يصدر <NameIDMappingResponse>

يتعين على مزوّد الهوية أن يعالج الرسالة <ManageNameIDRequest> كما هو محدد في البند 8. ويتعين على مزوّد الهوية، بعد معالجته الرسالة أو بعد مصادفته خطأ، أن يرجّع رسالة <NameIDMappingResponse> تحتوي على شفرة حالة مناسبة إلى الطالب لإكمال تبادل البروتوكول SAML.

ويتعين على المستجيب أن يستيقن نفسه لدى الطالب، سواء بالتوقيع على الرسالة <NameIDMappingResponse> أم باستعمال أي آلية أخرى تعتمدها الرابطة.

وتتضمن الفقرة الفرعية 2.4.8.4.11 القواعد الخاصة بالجانبية المتعلقة بمحتويات الرسالة <NameIDMappingResponse>.

4.8.4.11 استعمال بروتوكول وضع معرف هوية الاسم على تقابل

يحدد البند 8 بروتوكول وضع معرف هوية الاسم على تقابل، من أجل وضع معرف هوية الاسم لطرف رئيسي على تقابل مع معرف هوية اسم مختلف لنفس الطرف الرئيسي. ويشرح هذا البند استعمال هذا البروتوكول مع خطوط توجيهية إضافية لحماية سرية الطرف الرئيسي، كالحدّ من استعمال معرف الهوية الموضوع على تقابل.

1.4.8.4.11 استعمال <NameIDMappingRequest>

يتعين أن يكون العنصر <Issuer> موجوداً.

ويتعين أن يستيقن الطالب نفسه لدى المستجيب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية تعتمدها الرابطة.

2.4.8.4.11 استعمال <NameIDMappingResponse>

يتعين أن يكون العنصر <Issuer> موجوداً، ويتعين أن يحتوي على معرف الهوية الوحيد لمزوّد الهوية المستجيب. ويتعين حذف النعت Format أو أن تكون له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.

ويتعين أن يستيقن المستجيب نفسه لدى الطالب، وأن يضمن سلامة الرسالة، سواء بالتوقيع على الرسالة أم باستعمال آلية تعتمدها الرابطة.

وتحدد الفقرة الفرعية 3.2.2 من التجفير الصادر عن التجمع W3C، استعمال التجفير لتطبيق السرية على معرف هوية الاسم. وفي أغلب الأحيان، يترتب على مزوّد الهوية أن يشفّر معرف هوية الاسم الموضوع على تقابل الذي يرجّعه إلى الطالب، لكي يحمي سرية الطرف الرئيسي. ويستطيع الطالب استخراج العنصر <EncryptedID> ووضعه في رسائل البروتوكول أو التأكيدات اللاحقة.

الحدّ من استعمال معرف الهوية الموضوع على تقابل

يمكن أن يطبّق مزوّد الهوية قيوداً إضافية على استعمال معرف الهوية الناتج، وذلك بترجيعه معرف هوية الاسم المقابل في شكل <Assertion> يحتوي على معرف الهوية في الحقل <Subject> منه، ولكن من دون أي إعلانات. وبعد ذلك يجفّر التأكيد، وتستخدم النتيجة كعنصر <EncryptedData> في المعرف <EncryptedID> المرجّع إلى الطالب. وقد يتضمن التأكيد العنصر <Conditions> لكي يحدّ من الاستعمال، كما هو محدّد في البند 8، كالقيود المحدودة بزمن أو المقصورة في الاستعمال على أطراف واثقة محددة، ويتعين أن يكون التأكيد موقّعاً لحماية السلامة.

5.8.4.11 استعمال المعطيات الشرحية

تحدّد هذه الفقرة الفرعية عنصر النقطة النهائية <md:NameIDMappingService> لشرح الروابط والموقع أو المواقع المعتمدة التي يستطيع الطالب إرسال الطلبات إليها مستخدماً هذه الجانبية.

يمكن لمزوّد الهوية الذي يجفّر معرف الهوية الناتج لكيان خاص، أن يستعمل العنصر <md:KeyDescriptor> لهذا الكيان مع النعت use للتجفير "encryption" من أجل تحديد خوارزمية تجفير مناسبة مع عمليات ضبط استعمالها، مع مفتاح عمومي يستعمل لتسليم مفتاح تجفير مجمل.

9.4.11 جانبيات النعت SAML

تقدم جانبيات النعت التعريفات اللازمة للحدّ من تعبير النعوت SAML، عندما تعالج أنماط خاصة من معلومات النعت أو عند التفاعل مع أنظمة خارجية تتطلب صرامة أكبر. وتحدد هذه الفقرة الفرعية جانبية النعت الأساسي في اللغة SAML، وجانبية البروتوكول المخفّف للنفاذ إلى الدليل (LDAP) الوارد في التوصيات X.500، وجانبيات معرف الهوية الوحيد العالمي (UUID)، وجانبية اللغة التأشيرية التوسّعية للتحكم في النفاذ (XACML).

1.9.4.11 جانبية النعت الأساسي

تحدّد جانبية النعت الأساسي "Basic" تسمية مبسّطة، ولكنها ليست وحيدة، لنعوت اللغة SAML، وكذلك قيم النعوت المبنية على أنماط المعطيات المدمجة في Datatypes الصاردة عن التجمع W3C، مزيلة الحاجة إلى تخطيطات توسّعية لإقرار صلاحية النحو (قواعد التركيب).

المعلومات المطلوبة: urn:oasis:names:tc:SAML:2.0:profiles:attribute:basic

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحيينات: لا يوجد.

تسمية نعوت اللغة SAML

يتعين أن يكون النعت NameFormat من اللغة XML في العناصر <Attribute> هو urn:oasis:names:tc:SAML:2.0:attrname-format:basic.

والنعت Name من اللغة XML يتعين أن يلتزم بالقواعد المحددة لهذا النسق، كما هو محدّد في البند 8.

– **مقارنة اسم النعت**

يعود عنصران <Attribute> إلى نفس النعت في اللغة SAML إذا، وفقط إذا، كانت قيمتا نعتيهما Name XML متساويتين (بالمعنى المشروح في البند 8).

نعوت اللغة XML الخاصة بالجانبية

لا يوجد أي نعت XML إضافي معرفاً لاستعماله مع العنصر <Attribute>.

قيم النعت في اللغة SAML

إن نمط تخطيطة المحتوى للعنصر <AttributeValue> يتعين أن يسحب من واحد من الأنماط المعرفة في الملحق A. وعلى النعت xsi:type أن يكون موجوداً وأن تكون له القيمة المناسبة.

مثال

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"
        Name="FirstName">
 <saml:AttributeValue xsi:type="xs:string">By-Tor</saml:AttributeValue>
</saml:Attribute>
```

2.9.4.11 جانبية نعت البروتوكول المخفّف للنفاذ إلى الدليل X.500/(LDAP)

إن الأدلّة المبنية على مجموعة سلسلة التوصيات X.500 الصادرة عن قطاع تقييس الاتصالات (ITU-T) وعلى طلب التعليقات RFC 3377 الصادر عن فريق المهام الهندسية في الإنترنت (IETF)، منتشرة على نطاق واسع. وتستخدم تخطيطة الدليل لنمذجة المعلومات المطلوب تخزينها في هذه الأدلّة. فتعريفات نمط النعت في التوصيات X.500 تُستخدم خصوصاً لتحديد قواعد التركيب وغيرها من ميزات النعوت، وهي وحدة التخزين الأساسية في الدليل (ويحال إلى هذه النعوت في هذه التوصية باسم "نعوت الدليل"). وأنماط نعوت الدليل معرفة بشكل تخطيطات في التوصيات X.500 ومواصفات البروتوكول LDAP بالذات، وتخطيطات في وثائق عامة أخرى (مثل التخطيطة inetOrgperson (انظر الطلب RFC 2798 للفريق IETF))، وتخطيطات معرفة لأغراض خاصة. وفي أي واحدة من هذه الحالات، يكون من المفيد لمسؤولي الانتشار أن يستفيدوا من هذه الأنماط لنعوت الدليل في سياق الإعلانات عن النعوت SAML، من دون الاضطرار إلى إحداث تعريفات نعت خاصة بهذه الأنماط في اللغة SAML إحداثاً يدوياً، والاضطرار إلى القيام بذلك بأسلوب تشغيل بيني.

وتعرف جانبية النعت للبروتوكول LDAP في التوصيات X.500 اصطلاحاً عاماً لتسمية وتمثيل هذه النعوت حين يعبر عنها كنعوت في اللغة SAML.

المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500 (وهذا هو أيضاً مكان الاسم المستهدف المخصص في تخطيطة الجانبية للبروتوكول X.500/LDAP في الملحق A).

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحيينات: لا يوجد.

تسمية النعوت في اللغة SAML

يجب أن يكون النعت XML NameFormat في العناصر <Attribute> هو urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

ويستخدم مكان الاسم oid (معرف هوية الشيء) في URN (الاسم الموحّد للموارد) المشروح في الطلب RFC 3061 للفريق IETF، في سبيل تركيب أسماء النعوت. ويبنى النعت XML على معرف هوية الشيء المسند إلى نمط نعت الدليل.

مثال:

urn:oid:2.5.4.3

ومنذ أن تطلبت إجراءات التوصيات X.500 أن يجري تعريف كل نمط نعت بواسطة معرف وحيد لهوية الشيء، ضمنت هذه التخطيطة للتسمية أن تكون الأسماء المشتقة للنعوت في اللغة SAML لا يعتريها أي غموض أو لبس.

ولتمكين الإنسان من قراءة الأسماء، ربما تحتاج بعض التطبيقات إلى مطلب أيضاً هو حمل سلسلة النعت XML الاختياري OID URN (كما هي معرفة في الطلب RFC 3061 للفريق IETF). ويمكن استعمال النعت XML الاختياري FriendlyName (المعرف في البند 8) لهذا الغرض. وإذا كان تعريف نمط نعت الدليل يشتمل على واصف (الاسم المختصر) واحد أو أكثر لنمط النعت، ينبغي لقيمة FriendlyName، إن وجدت، أن تكون هي واحدة من الواصفات المعرفة.

ويعود عنصران اثنان <Attribute> إلى نفس النعت SAML، إذا، وفقط إذا، كانت قيمتا النعت XML Name متساويتين فيهما، بالمعنى الوارد في الطلب RFC 3061 للفريق IETF. ولا يلعب النعت FriendlyName أي دور في هذه المقارنة.

النعوت XML الخاصة بالجانبية

لا توجد نعوت XML إضافية معرفة لاستعمالها مع العنصر <Attribute>.

قيم النعوت SAML

تحدد تعريفات أنماط نعوت الدليل التي تستعمل في أدلة التوصيات X.500 الأصلية، قواعد تركيب النعت مستخدمة ترميز قواعد التركيب المجرد.1 (ASN.1). ولكي تستعمل تعريفات نعوت الدليل في البروتوكول LDAP فإنها تضمن إضافة إلى ذلك قواعد تركيب خاصة بالبروتوكول LDAP، تحدد كيفية تمثيل قيم نعت أو تأكيد مطابقين لقواعد التركيب، عندما تنقل إلى البروتوكول LDAP (وتسمى التشفير الخاص بالبروتوكول LDAP). وينتج هذا التشفير LDAP عادة سمات الشفرة الموحدة (Unicode) بالشكل UTF-8. تحدد هذه الجانبية الخاصة بالنعوت SAML شكل قيم النعت SAML فقط لنعوت الدليل التي لها قواعد تركيب خاصة بالبروتوكول LDAP. وقد تعرف التوسّعات المستقبلية لهذه الجانبية أنساق قيم نعت لنعوت الدليل التي تحدد قواعد تركيبها تشفيرات أخرى.

وعند تمثيل قواعد التشفير المستعملة لقيمة نعت معينة، يتعين أن يحتوي العنصر <AttributeValue> على نعت XML يسمى التشفير "Encoding"، وهو معرف في مكان الاسم XML urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500.

وفيما يخص كل نعت دليل، يكون التشفير الخاص بالبروتوكول LDAP الموجود في قواعد تركيبه لا ينتج إلا سلاسل السمات بالشكل UTF-8 باعتبارها القيم، تشفّر قيمة النعت SAML بكل بساطة مثل السلسلة UTF-8 نفسها، وكأنها محتوى النعت <AttributeValue>، من دون أي فراغات بيضاء إضافية. وفي مثل هذه الحالات، يتعين على النعت XML xsi:type أن يوضع على **xs:string**. ويقدم النعت XML للتشفير الخاص بالجانبية، مع قيمة من البروتوكول LDAP.

وفيما يلي قائمة ببعض قواعد التركيب لنعوت البروتوكول LDAP (ومعها المعرفات OID المصاحبة) التي ينطبق عليها هذا الأمر.

وصف نمط الدليل	1.3.6.1.4.1.1466.115.121.1.3	Attribute Type Description
سلسلة بتات	1.3.6.1.4.1.1466.115.121.1.6	Bit String
بولاني	1.3.6.1.4.1.1466.115.121.1.7	Boolean
سلسلة البلد	1.3.6.1.4.1.1466.115.121.1.11	Country String
DN	1.3.6.1.4.1.1466.115.121.1.12	DN
سلسلة الدليل	1.3.6.1.4.1.1466.115.121.1.15	Directory String
رقم هاتف الفاكس	1.3.6.1.4.1.1466.115.121.1.22	Facsimile Telephone Number
التوقيت المعمّم	1.3.6.1.4.1.1466.115.121.1.24	Generalized Time
السلسلة IA5	1.3.6.1.4.1.1466.115.121.1.26	IA5 String
عدد صحيح	1.3.6.1.4.1.1466.115.121.1.27	INTEGER
وصف قواعد التركيب للبروتوكول LDAP	1.3.6.1.4.1.1466.115.121.1.54	LDAP Syntax Description
وصف قاعدة التواؤم	1.3.6.1.4.1.1466.115.121.1.30	Matching Rule Description
وصف استعمال قاعدة التواؤم	1.3.6.1.4.1.1466.115.121.1.31	Matching Rule Use Description
الاسم ومعرف الهوية الوحيد (UID) الاختياري	1.3.6.1.4.1.1466.115.121.1.34	Name And Optional UID
وصف شكل الاسم	1.3.6.1.4.1.1466.115.121.1.35	Name Form Description
سلسلة رقمية	1.3.6.1.4.1.1466.115.121.1.36	Numeric String
وصف صنف الشيء	1.3.6.1.4.1.1466.115.121.1.37	Object Class Description
سلسلة أثمونات	1.3.6.1.4.1.1466.115.121.1.40	Octet String
OID (معرف هوية الشيء)	1.3.6.1.4.1.1466.115.121.1.38	OID
صندوق بريد آخر	1.3.6.1.4.1.1466.115.121.1.39	Other Mailbox
عنوان بريدي	1.3.6.1.4.1.1466.115.121.1.41	Postal Address
عنوان تقديم	1.3.6.1.4.1.1466.115.121.1.43	Presentation Address
سلسلة تُطْبَع	1.3.6.1.4.1.1466.115.121.1.44	Printable String
سلسلة فرعية للتأكيد	1.3.6.1.4.1.1466.115.121.1.58	Substring Assertion
رقم هاتف	1.3.6.1.4.1.1466.115.121.1.50	Telephone Number
UTC (التوقيت العالمي المنسّق)	1.3.6.1.4.1.1466.115.121.1.53	UTC Time

وتكون قيمة النعت مشفّرة في جميع قواعد التركيب الأخرى الخاصة بالبروتوكول المخفف للنفاذ إلى الدليل (LDAP)، باعتبارها محتوى العنصر <AttributeValue>، على أن تشفّر بالأساس 64 قيمة نعت البروتوكول LDAP المشفرة بسلسلة الأثمونات في الترميز ASN.1 السائدة. ويتعين وضع النعت XML xsi:type بالشكل **xs:base64Binary**. ويقدم النعت XML للتشفير الخاص بالجانبية، مع قيمة من "LDAP".

وعند مقارنة تساوي قيم النعت SAML، يتم التقيد بقواعد التواؤم الخاصة بأنماط نعوت الدليل المقابلة (مثل التحسس بصندوق حروف الطباعة).

التخطيطة الخاصة بالجانبية

قائمة التخطيطات التالية تبين تعريف النعت XML الخاص بالجانبية Encoding (انظر الملحق A).

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <annotation>
        <documentation>
            Document identifier: saml-schema-x500-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Custom schema for X.500 attribute profile, first published
in SAML 2.0.
        </documentation>
    </annotation>
    <attribute name="Encoding" type="string"/>
</schema>
```

مثال

فيما يلي مثال على تقابل نعت الدليل "givenName" الذي يمثل الاسم الأول (الشخصي) لصاحب التأكيد في اللغة SAML. ومعرف هوية شيئه هو {joint-iso-itu-t(2) ds(5) attributeType(4) givenName(42)} وقواعد تركيبه في البروتوكول LDAP هي Directory String (سلسلة الدليل):

```
<saml:Attribute
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
              Name="urn:oid:2.5.4.42" FriendlyName="givenName">
      <saml:AttributeValue xsi:type="xs:string"
              x500:Encoding="LDAP">Steven</saml:AttributeValue>
</saml:Attribute>
```

3.9.4.11 جانبية النعت معرف الهوية الوحيد العالمي (UUID)

تقيس جانبية النعت UUID التعبير عن قيم المعرفات UUID بأسماء وقيم نعوت في اللغة SAML. وتنطبق حيث يكون النظام المصدر للنعت هو نظام يعرف نعت أو قيمة بمعرف الهوية الوحيد العالمي (UUID).

المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:attribute:UUID

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحيينات: لا يوجد.

تسمية النعوت في اللغة SAML

يجب أن يكون النعت XML NameFormat في العناصر <Attribute> هو urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

إذا كان التمثيل التحتي لاسم النعت هو معرف UUID، يستعمل عندئذ اسم المكان UUID من URN الموصوف في التوصية ITU-T X.667. وفي هذا النهج يكون النعت XML Name مبنياً على شكل الاسم URN للمعرف UUID التحتي الذي يعرف هوية النعت.

مثال:

```
urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
```

وإذا لم يكن التمثيل التحتي لاسم النعت هو معرف UUID، يستعمل عندئذ أي شكل للمعرف URI في النعت XML Name.

ولتمكين الأنسان من قراءة الأسماء، ربما تحتاج بعض التطبيقات إلى مطلب أيضاً هو حمل سلسلة أسماء اختيارية إلى جانب المعرف URI. ويمكن استعمال النعت XML الاختياري FriendlyName لهذا الغرض.

يعود عنصران اثنان <Attribute> إلى نفس النعت SAML، إذا، وفقط إذا، كانت قيمتا النعت XML Name متساويتين فيهما، بالمعنى الوارد في التوصية ITU-T X.667. ولا يلعب النعت FriendlyName أي دور في هذه المقارنة.

النعوت XML الخاصة بالجانبية

لا توجد نعوت XML إضافية معرفة لاستعمالها مع العنصر <Attribute>.

قيم النعوت SAML

في الحالات التي تكون فيها قيمة النعت هي أيضاً معرف UUID، يتعين استعمال نفس قواعد التركيب الخاصة بالاسم URN المشروح أعلاه، للتعبير عن القيمة داخل العنصر <AttributeValue>. والنعت XML xsi:type يتعين وضعه على **xs:anyURI**.

وإذا لم تكن قيمة النعت هي معرف UUID، لا تعود توجد عندئذ قيود على استعمال العنصر <AttributeValue>.

مثال

فيما يلي مثال على نعت سجل موسع في بيئة حساب موزع (DCE)، مضبوط وضعه على "pre_auth_req"، له معرف هوية UUID معروف جيداً هو 6c9d0ec8-dd2d-11cc-abdd-080009353559 وقيمة أعداد صحيحية.

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
              Name="urn:uuid:6c9d0ec8-dd2d-11cc-abdd-080009353559"
              FriendlyName="pre_auth_req">
      <saml:AttributeValue xsi:type="xs:integer">1</saml:AttributeValue>
</saml:Attribute>
```

4.9.4.11 جانبية نعت اللغة التأشيرية التوسّعية للتحكم في النفاذ (XACML)

يمكن استعمال تأكيدات النعت في اللغة SAML كمداخل إلى قرارات الترخيص المتخذة وفقاً للتوصية ITU-T X.1142. وطالما أن نسق النعت SAML يختلف عن نسق النعت XACML، لا بد من إجراء عملية وضع على تقابل. وجانبية نعت اللغة XACML تسهل هذا التقابل، عن طريق تقييس التسمية، وقواعد تركيب القيم، والمعطيات الشرحية للنعت الإضافية. والنعوت SAML المولدة طبقاً لهذه الجانبية، يمكن أن توضع على التقابل أوتوماتياً مع النعوت XACML، وتستخدم مدخلاً إلى قرارات الترخيص في اللغة XACML.

المعلومات المطلوبة

تعريف الهوية: urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML (وهذا هو أيضاً مكان الاسم المستهدف المخصص في تخطيطة الجانبية XACML المقابلة في الملحق A).

معلومات الاتصال: security-services-comment@lists.oasis-open.org

الوصف: وارد أدناه.

التحييزات: لا يوجد.

تسمية نعوت اللغة SAML

يجب أن يكون النعت XML NameFormat في العناصر <Attribute> هو urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

ويتعين على النعت XM Name أن يلتزم بالقواعد المحددة لهذا النسق، كما هو معرف في البند 8.

ولتمكين الإنسان من قراءة الأسماء، ربما تحتاج بعض التطبيقات إلى مطلب أيضاً هو حمل سلسلة أسماء احتيارية إلى جانب OID URN. ويمكن استعمال النعت XML الاختياري FriendlyName (المعرف في البند 8) لهذا الغرض، ولكنه غير قابل لترجمته إلى نعت XACML مكافئ.

ويعود عنصران اثنان <Attribute> إلى نفس النعت SAML، إذا، وإذا فقط، كانت قيمتا النعت XML Name متساويتين فيهما عند المقارنة الاثنينية. ولا يلعب النعت FriendlyName أي دور في هذه المقارنة.

النعوت XML الخاصة بالجانبية

تتطلب اللغة XACML أن يحمل كل نعت نمط معطيات صريحاً. ولكي تقدم قيمة هذا النمط من المعطيات، يعرف نعت XML جديد مقيم في المعرف URI، يحمل الاسم DataType ويقع في مكان الاسم XML: urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML.

ويتعين على العناصر <Attribute> في اللغة SAML المطابقة لهذه الجانبية أن تشتمل على النعت DataType الموصوف بمكان الاسم، أو يفترض في قيمته أن تكون http://www.w3.org/2001/XMLSchema#string.

وإذا استخدمت قيم غير مقيسة، فإن كل نقطة قرار سياسي (PDP) في اللغة XACML تستهلك نعوتاً SAML متقابلة مع قيم غير مقيسة من DataType، يتعين توسيعها لتتقبل الأنماط الجديدة من المعطيات.

قيم النعت في اللغة SAML

يتعين أن تتقابل قواعد تركيب محتوى العنصر <AttributeValue> مع نمط المعطيات المعبّر عنه في النعت DataType XML الخاص بالجانبية والذي يظهر في العنصر <Attribute> الوالد. وفيما يخص أنماط المعطيات التي تقابل الأنماط المعرفة في البند 8، ينبغي أيضاً استعمال النعت XML xsi:type على العنصر أو العناصر <AttributeValue>.

التخطيطة الخاصة بالجانبية

تبين قائمة التخطيطات التالية كيف يعرف النعت XML الخاص بالجانبية DataType (الملحق A).

```
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
```

```
    <annotation>
        <documentation>
            Document identifier: saml-schema-xacml-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V2.0 (March, 2005):
              Custom schema for XACML attribute profile, first published in
SAML 2.0.
        </documentation>
    </annotation>
    <attribute name="DataType" type="anyURI"/>
</schema>
```

مثال

فيما يلي مثال على مقابلة النعت "givenName" في البروتوكول LDAP الوارد في التوصيات X.500، الذي يمثل الاسم الأول (الشخصي) لصاحب التأكيد في اللغة SAML. وهو يوضح كذلك أن نعتاً واحداً SAML يمكن أن يتطابق مع جانبيات نعت عديدة، عندما تكون متوائمة بعضها مع بعضها الآخر.

```
<saml:Attribute
xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
       xmlns:ldapprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:LDAP
"
              xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#string"
              ldapprof:Encoding="LDAP"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
              Name="urn:oid:2.5.4.42" FriendlyName="givenName">
       <saml:AttributeValue xsi:type="xs:string">By-
Tor</saml:AttributeValue>
</saml:Attribute>
```

ملاحظة (للاطّلاع) – يوضح PE39 (انظر OASIS PE:2006) المثال أعلاه بما يلي:

```
<saml:Attribute
  xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
      xmlns:ldapprof="urn:oasis:names:tc:SAML:2.0:profiles:AttributeValue:LDAP"
           xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#string"
           ldapprof:Encoding="LDAP"
           NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
           Name="urn:oid:2.5.4.42" FriendlyName="givenName">
      <saml:AttributeValue xsi:type="xs:string">By-Tor</saml:AttributeValue>
</saml:Attribute>
```

12 سياق الاستيقان في اللغة SAML

تعرف هذه التوصية قواعد التركيب اللازمة لتعريف إعلانات سياق الاستيقان، وقائمة أولية بأصناف سياق الاستيقان.

1.12 مفاهيم سياق الاستيقان

إذا كان لطرف واثق أن يعتمد على استيقان طرف رئيسي من قبل سلطة استيقان، فقد يحتاج هذا الطرف الوايق إلى معلومات تضاف إلى التأكيد نفسه، حتى يستطيع تقدير سوية الثقة التي يمكنه أن يضعها في هذا التأكيد. وتعرف هذه التوصية تخطيطة في اللغة XML لإحداث إعلانات سياق الاستيقان – وهي وثائق في اللغة XML تتيح لسلطة الاستيقان أن تقدم هذه المعلومات الإضافية إلى الطرف الواثق. وتعرف هذه التوصية فوق ذلك عدداً من أصناف الاستيقان، وهي فئات تقع ضمنها إعلانات سياق الاستيقان، مما يسهل تفسيرها.

ولا تفرض اللغة SAML تقانة (تكنولوجيا) واحدة ولا بروتوكولاً واحداً ولا سياسة واحدة على الإجرائيات التي تصدر بها سلطات الاستيقان هويات الأطراف الرئيسية التي يستيقن بها هؤلاء الأطراف الرئيسيون أنفسهم فيما بعد لدى سلطة الاستيقان. وتختار سلطات الاستيقان المختلفة تقانات مختلفة، وتتبع إجرائيات مختلفة، وترتبط بالتزامات قانونية مختلفة حول أسلوبها في التيقن من الأطراف الرئيسية.

والاختيارات التي تقوم بها سلطة الاستيقان هنا، ستكون منساقة إلى حد كبير مع متطلبات الأطراف الواثقة التي تتفاعل معها سلطة الاستيقان. هذه المتطلبات بالذات ستحددها طبيعة الخدمة (أي حساسية المعلومة المتبادلة، أو القيمة المالية المصاحبة، أو تسامح الأطراف الواثقة تجاه المخاطر وغير ذلك) التي يقوم الطرف الواثق بتقديمها إلى الطرف الرئيسي.

وعليه إذا كان على الطرف الواثق أن يضع ثقته، فيما يخص أي شيء آخر غير الخدمات التافهة، في تأكيدات الاستيقان التي يستلمها من سلطة الاستيقان، سيضطر إلى أن يعرف أي تقانات (تكنولوجيات) وبروتوكولات وإجرائيات كانت مستعملة أو متبعة في آلية الاستيقان الأصلية التي استند إليها تأكيد الاستيقان. وبعد أن يتسلح الطرف الواثق بهذه المعلومات، ويثق بصل التأكيد الحقيقي يصبح أفضل قدرة على اتخاذ قرار مُحِق بشأن الخدمات التي ينبغي السماح لصاحب تأكيد الاستيقان بالنفاذ إليها.

ويعرف سياق الاستيقان بأنه المعلومات التي تضاف إلى تأكيد الاستيقان بالذات والتي ربما يتطلبها الطرف الواثق قبل اتخاذه قراراً مُحِقاً بشأن تأكيد استيقان. وقد يحتوي مثل هذا السياق على طريقة الاستيقان الحقيقية المستعملة، ولكنه لا يقتصر عليها.

2.12 إعلان سياق الاستيقان

إذا كان لطرف واثق أن يعتمد على استيقان كيان آخر من قبل سلطة استيقان، فقد يحتاج الطرف الواثق إلى معلومت تضاف إلى الاستيقان بالذات، لكي يتمكن من وضع الاستيقان في سياق إدارة المخاطرة. ويمكن أن تتضمن هذه المعلومات:

- آليات استيقان المستعمل الأصلية (مثل وجهاً لوجه أو مباشرة على الخط أو سرية متقاسمة).
- آليات التخفيض إلى أقصى حد من تشويه الثبوتيات (مثل تواتر تجديد الثبوتيات، أو توليد المفاتيح في جانب الزبون).
- آليات تخزين الثبوتيات وحمايتها (مثل البطاقات الذكية وقواعد كلمة السر).
- آلية الاستيقان أو طريقته (مثل كلمة السر).

إن التغيرات في الخصائص المعددة أعلاه وتبديلاتها، تضمن ألا تكون لجميع تأكيدات الاستيقان نفس الدرجة من الثقة التي يمكن للطرف الواثق أن يصفهاه فيها. ويتميز تأكيد استيقان معين بقيم كل واحد من هذه المتغيرات ومن غيرها.

ويمكن لسلطة استيقان في اللغة SAML أن تمنح طرفاً واثقاً المعلومات الإضافية اللازمة لسياق الاستيقان في شكل إعلان عن سياق الاستيقان، وهي وثيقة في اللغة XML تدرج مباشرة أو يحال إليها في تأكيد استيقان تقدمه سلطة الاستيقان إلى الطرف الواثق.

يستطيع الطالبون في اللغة SAML أن يطلبوا تطابق الاستيقان مع سياق استيقان محدد، عن طريق تعريف هوية هذا السياق في طلب استيقان. ويمكن للطالب أيضاً أن يحدد أن يجري الاستيقان مع سياق استيقان *يتجاوز* بعض القيم المقررة (مع تعريف متفق عليه "للتجاوز").

1.2.12 نموذج المعطيات

إن الإعلان عن سياق الاستيقان الخاص المعرف في هذه التوصية سيضم خصائص العمليات الإجرائية والإجراءات والآليات التي تحققت بها سلطة الاستيقان من الصاحب، قبل إصدار هوية، وحَمَتْ الأسرار التي تبنى عليها الاستيقانات اللاحقة والآليات التي استعملت لهذا الاستيقان. وهذه الخصائص موضوعة في فئات في تخطيطة سياق الاستيقان كما يلي:

- تعريف الهوية – الخصائص التي تشرح الإجرائيات والآليات التي تستخدمها سلطة الاستيقان، لكي تخلق في البداية تصاحباً بين الصاحبة والهوية (أو الاسم) التي سيعرف بها الصاحب.
- الحماية التقنية – الخصائص التي تشرح كيف يحتفظ "بالسر" مأموناً (الذي يسمح للصاحب، بسبب معرفته به أو امتلاكه له، بأن يستيقن نفسه لدى سلطة الاستيقان).
- الحماية التشغيلية – الخصائص التي تشرح المراقبات الأمنية الإجرائية التي تقوم بها سلطة الاستيقان (مثل التدقيقات الأمنية وتسجيلات المحفوظات (الأرشيف)).
- طريقة الاستيقان – الخصائص التي تحدد الآليات التي يستيقن بها صاحب التأكيد الصادر نفسه، لدى سلطة الاستيقان (مثل كلمة السر مقابل البطاقة الذكية).
- الاتفاقات الحاكمة – الخصائص التي تشرح إطار العمل القانوني (مثل المسؤولية والالتزامات التعاقدية) الذي يختفي وراء حدث الاستيقان و/أو البنية التحتية للاستيقان التقني المصاحب.

2.2.12 التوسّعية (قابلية التوسّع)

لقد عرّفت تخطيطة إعلان سياق الاستيقان نقاط التوسّعية تعريفاً جيداً عبر العنصر <Extension>. وتستطيع سلطات الاستيقان استخدام هذا العنصر لإدراج التفاصيل الإضافية لسياق الاستيقان من أجل التأكيدات SAML التي تصدرها (بافتراض أن الطرف الواثق المستهلك سيكون قادراً على فهم هذه التوسّعات). ويتعين أن تقع هذه العناصر الإضافية في مكان اسم XML منفصل عن مكان الاسم لقاعدة إعلان سياق الاستيقان أو لتخطيطة الصنف التي تنطبق على الإعلان بالذات.

3.2.12 قواعد المعالجة

قواعد المعالجة الإضافية لإعلانات سياق الاستيقان محددة في البند 8. وقواعد المعالجة هذه تصل بالتطويرات إلى حد تقاسم التفسيرات المشتركة للشدة النسبية لإعلانات سياق الاستيقان الخاصة أو لنوعيتها، ولا يمكن التعبير عنها بمصطلحات مطلقة أو تقديمها على أنها قواعد يتعين على عمليات التنفيذ اتباعها.

4.2.12 التخطيطة

هذه الفقرة الفرعية ليست معيارية.

ويقدم التذييل VI قائمة كاملة بتخطيطة XML لأنماط سياق الاستيقان، وبتخطيطة XML لسياق الاستيقان نفسه، المستعملة في إقرار صلاحية الإعلانات المعممة الفردية.

3.12 أصناف سياق الاستيقان

إن عدد التبديلات في الخصائص المختلفة يؤكد نظرياً وجود عدد لا نهائي من سياقات الاستيقان الوحيدة. وهذا يقتضي نظرياً أن أي طرف خاص يعتبر قادراً على تحليل أي إعلان اعتباطي لسياق استيقان، والمهم أ:ثر أنه يعتبر قادراً على تحليل الإعلان بقصد تقدير "نوعية" تأكيد الاستيقان المصاحب. والقيام بمثل هذا التقدير ليس أمراً تافهماً.

ولحسن الحظ أن هناك مجالاً للاستمثال. في الواقع العملي ستقع سياقات استيقان عديدة ضمن فئات تحددها الممارسات والتقانة الصناعية. فمثلاً سيُعرَّف العديد من سياقات استيقان متصفحي شبكة الويب، من مجال الأعمال إلى المستهلك، تعريفاً (جزئياً) عند استيقان طرف رئيسي لدى سلطة استيقان، عبر تقديم كلمة سر إلى دورة يحميها البروتوكول TLS. وفي عالم الشركات، فإن الاستيقان المبني على الشهادة شائع. لا شك في أن سياق الاستيقان بكامله ليس مقصوراً على خصوصيات كيفية استيقان طرف رئيسي. ومع ذلك فإن طريقة الاستيقان هي غالباً الخاصية *المرئية* أكثر من غيرها، وهي بذلك يمكن أن تخدم كمصنِّف مفيد لصنف من سياقات الاستيقان ذات الصلة.

ويعبّر عن هذا المفهوم في هذه التوصية باعتباره تعريفاً لسلسلة من *أصناف سياقات الاستيقان*. وكل صنف يعرّف مجموعة فرعية خاصة من المجموعة الكاملة من سياقات الاستيقان. وكانت الأصناف قد اختيرت باعتبارها تمثل الممارسات والتقانات الحالية لتقنيات الاستيقان، وتقدم إلى الأطراف المؤكدة والأطراف الواثقة مختصراً مناسباً للرجوع إلى مسائل السياق الاستيقاني.

فيمكن لسلطة استيقان مثلاً أن تورد مع إعلان سياق الاستيقان الكامل الذي تقدمه إلى الطرف الواثق، تأكيداً على أن سياق الاستيقان ينتمي أيضاً إلى صنف سياق استيقاني. ويكون هذا التأكيد، بالنسبة إلى بعض الأطراف الواثقة، تفصيلاً كافياً يجعل منه قادراً على إعطاء سوية مناسبة من الثقة إلى تأكيد الاستيقان المصاحب. بينما قد تفضل أطراف واثقة أخرى أن تتفحص إعلان سياق الاستيقان نفسه بالكامل. ويبدو من المعقول أن تكون القدرة على الرجوع إلى صنف سياق استيقان بدلاً من الاضطرار إلى وضع قائمة بكامل التفاصيل لإعلان سياق استيقاني خاص، عملية تسهل على الطرف الواثق التعبير عن رغباته و/أو تطلباته من سلطة استيقان.

1.3.12 مزايا أصناف سياق الاستيقان

يرمي إدخال طبقات إضافية من الأصناف وتعريف قائمة أولية من الأصناف التمثيلية والمرنة إلى ما يلي:

- تسهيل التوصل إلى اتفاق على سلطة الاستيقان والأطراف الواثقة، بخصوص تحديد سياقات الاستيقان المقبولة، عن طريق تقديم إطار عمل لهم في المناقشة.
- التسهيل على الأطراف الواثقة لكي تبين أفضلياتها، حين تطلب من سلطة الاستيقان الارتقاء بتأكيد الاستيقان.
- تخفيف العبء عن الأطراف الواثقة بخصوص معالجة إعلانات سياق الاستيقان، بإعطائهم الخيار بأن يرتضوا بالصنف المصاحب.
- عزل الأطراف الواثقة عن التأثر بتقانات الاستيقان الجديدة.
- التسهيل على سلطات الاستيقان نشر قدراتها الاستيقانية، عبر لغة وصف خدمات الويب (WSDL) مثلاً.

2.3.12 قواعد المعالجة

توجد قواعد معالجة أخرى في البند 8 بشأن أصناف سياق الاستيقان. وفي أغلب الجوانب، تصل قواعد المعالجة هذه بالتطويرات إلى حد تقاسم التفسيرات المشتركة للشدة النسبية لأصناف سياق الاستيقان الخاصة ولنوعيتها، ولا يمكن التعبير عنها بمصطلحات مطلقة أو تقديمها على أنها قواعد يتعين على عمليات التنفيذ اتباعها.

3.3.12 التوسّعية (قابلية التوسّع)

كما تفعل التخطيطة المركزية لإعلان سياق الاستيقان، كذلك تسمح التخطيطات المنفصلة لأصناف سياق الاستيقان بوجود العنصر <Extension> في بعض مواقع البنية الشجرية. وحيثما يظهر العنصر <Extension> باعتباره ابناً لعنصر <xs:choice>، أزيل هذا الخيار، بخلق تعريف لتخطيطة صنف خاصة باعتبارها تقييداً للنمط الأساسي. وعندما يظهر العنصر <Extension> بصفته ابناً اختيارياً لعنصر <xs:sequence>، يسمح للعنصر <Extension> بالبقاء إضافة إلى أي عناصر مطلوبة.

وعليه يمكن لإعلانات سياق الاستيقان أن تتضمن العنصر <Extension> (مع عناصر إضافية في أمكنة أسماء مختلفة) وأن تبقى مطابقة لتخطيطات أصناف سياق الاستيقان (بالطبع، إن كانت تستوفي المتطلبات الأخرى للتخطيطة).

إن تخطيطات أصناف سياق الاستيقان تقيّد تعريفات النمط في التخطيطة الأساسية لسياق الاستيقان. وباعتبار تخطيطات أصناف سياق الاستيقان نقطة توسّع، يمكن تقييدها فيما بعد – تعريفاتها للنمط الذي سيستخدم كأنماط أساسية في بعض التخطيطات الأخرى (التي ربما تكون بعض الجماعات قد عرفتها، رغبة منها في تعريف أشد صرامة لصنف سياق الاستيقان).

ولاجتناب حدوث عدم اتساق منطقي، لا يمكن لمثل هذه التوسّعات في التخطيطة أن تقيّد في المستقبل إلا تعريفات النمط في تخطيطة الصنف. ويوضع هذا التقييد موضع التنفيذ، تعرّف تخطيطات أصناف سياق الاستيقان مع النعت finalDefault="extension" فوق العنصر <schema> لاتقاء هذا النمط من الانعطاف.

4.3.12 التخطيطات

تحتوي الفقرات الفرعية التالية على قائمة بأصناف سياق الاستيقان. والأصناف معدّدة وفق الترتيب الهجائي (بالإنكليزي)، ولا تنطوي القائمة على ترتيب آخر للأصناف. ويستطيع القائمون بالتنفيذ اختيار الأصناف التي يدعمونها، وفقاً للخطوط التوجيهية الواردة في هذه التوصية بشأن المطابقة (انظر البند 13). وتعرف هوية الأصناف فقط بالمعرفات URI مع:

```
urn:oasis:names:tc:SAML:2.0:ac:classes
```

وتعرف تخطيطات الأصناف على أنها تقييدات من أجزاء التخطيطة الأساسية لسياق الاستيقان "types". ومطابقات اللغة XML التي تستيقن نفسها بالنسبة إلى تخطيطة صنف من سياق الاستيقان يقال عنها إنها *مطابقة* لهذا الصنف من سياق الاستيقان.

ولما كانت تخطيطة الأصناف تستورد العناصر والأنماط وتعيد تعريفها في مكان الاسم من تخطيطة الأصناف، فإن إعلاناً من سياق الاستيقان مطابقاً لأحد الأصناف، لا يمكنه أن يستيقن نفسه بنفس الوقت بالنسبة إلى التخطيطة الأساسية لسياق الاستيقان.

1.4.3.12 بروتوكول الإنترنت (IP)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol

ويستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ينطبق صنف بروتوكول الإنترنت، عندما يستيقن طرف رئيسي نفسه باستخدام عنوان IP مقدّم.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
```

```
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="IPAddress"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

2.4.3.12 InternetProtocolPassword (كلمة السر في بروتوكول الإنترنت)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword

يلاحظ أن هذا المعرّف يستخدم أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ينطبق صنف كلمة السر في بروتوكول الإنترنت، عندما يستيقن طرف رئيسي نفسه باستخدام عنوان IP مقدّم، إضافة إلى اسم مستعمل/كلمة سر.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
        Document identifier: saml-schema-authn-context-ippword-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>
```

```
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="Password"/>
            <xs:element ref="IPAddress"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

3.4.3.12 Kerberos

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

يستخدم هذا المعرّف أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

وينطبق هذا الصنف عندما يستيقن طرف رئيسي نفسه باستخدام كلمة سر لدى سلطة الاستيقان المحلية، بغية الحصول على بطاقة "كيربروس". ثم تستخدم بطاقة كيربروس هذه لاستيقان الشبكة فيما بعد.

ملاحظة 1 – يمكن لسلطة الاستيقان أن تبين (عبر صنف السياق هذا) نمط معطيات يسبق الاستيقان، كان يستعمله مركز كيربروس لتوزيع المفاتيح (الطلب RFC 1510 للفريق IETF) عند استيقان الطرف الرئيسي. والطريقة التي تستعملها سلطة الاستيقان للحصول على هذه المعلومة تقع خارج نطاق هذه التوصية، ولكنه يشدد على التوصية بوضع طريقة موثوقة لتمرير نمط المعطيات الذي يسبق الاستيقان، وكل تفاصيل سياق ذي صلة بكيربروس (مثل مدة حياة البطاقة)، إلى سلطة الاستيقان.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
        Document identifier: saml-schema-authn-context-kerberos-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
              <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SharedSecretChallengeResponse"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
        <xs:restriction base="SharedSecretChallengeResponseType">
          <xs:attribute name="method" type="xs:anyURI"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

وأحد الأمثلة على مطابق في اللغة XML يطابق هذه التخطيطة للسياق هو كالتالي:

```
<AuthenticationContextDeclaration
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos">

  <AuthnMethod>

    <PrincipalAuthenticationMechanism preauth="0">
      <RestrictedPassword>
        <Length min="4"/>
      </RestrictedPassword>
    </PrincipalAuthenticationMechanism>

    <Authenticator>
      <AuthenticatorSequence>
        <SharedSecretChallengeResponse
method="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
      </AuthenticatorSequence>
    </Authenticator>

  </AuthnMethod>

</AuthenticationContextDeclaration>
```

ملاحظة 2 – استعمال SSL معروض في التذييل IV.

4.4.3.12 MobileOneFactorUnregistered

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered

يستخدم هذا المعرف أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ولا يبين أي إجراءات لتسجيل مشترك متنقل واستيقان جهاز متنقل، من دون أن يتطلب ذلك تفاعلاً صريحاً مع المستعمل النهائي. وصنف السياق هذا يستيقن الجهاز فقط ولا يستيقن المستعمل قط، وهو مفيد عندما ترغب خدمات أخرى غير المشغّل المتنقل، في إضافة استيقان جهاز مأمون إلى إجرائية استيقانها.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema

targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnre
gistered"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
```

```
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
        Document identifier: saml-schema-authn-context-mobileonefactor-
unreg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="ZeroKnowledge"/>
              <xs:element ref="SharedSecretChallengeResponse"/>
              <xs:element ref="SharedSecretDynamicPlaintext"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="MobileNetworkNoEncryption"/>
              <xs:element ref="MobileNetworkRadioEncryption"/>
```

```
              <xs:element ref="MobileNetworkEndToEndEncryption"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="OperationalProtectionType">
      <xs:complexContent>
        <xs:restriction base="OperationalProtectionType">
          <xs:sequence>
            <xs:element ref="SecurityAudit"/>
            <xs:element ref="DeactivationCallCenter"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
        <xs:restriction base="TechnicalProtectionBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PrivateKeyProtection"/>
              <xs:element ref="SecretKeyProtection"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecretKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="SecretKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
                <xs:enumeration value="smartcard"/>
```

```
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

ملاحظة – استعمال SSL معروض في التذييل IV.

5.4.3.12 MobileTwoFactorUnregistered

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ولا يبين أي إجراءات لتسجيل مشترك متنقل واستيقان قائم على عاملين، مثل جهاز مأمون ورقم تعريف الهوية الشخصي PIN للمستعمل. وصنف السياق هذا مفيد عندما ترغب خدمة أخرى غير المشغّل المتنقل في وصل معرف هوية المشترك لديها بخدمة استيقان ثنائي العوامل يقدمها متنقل، بالتقاطها معطيات الهاتف المتنقل لدى التسجيل.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnre
gistered"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
```

```
  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
        Document identifier: saml-schema-authn-context-mobiletwofactor-
unreg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="ZeroKnowledge"/>
              <xs:element ref="SharedSecretChallengeResponse"/>
              <xs:element ref="SharedSecretDynamicPlaintext"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
              <xs:element ref="ComplexAuthenticator"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="ComplexAuthenticatorType">
      <xs:complexContent>
        <xs:restriction base="ComplexAuthenticatorType">
```

```
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SharedSecretChallengeResponse"/>
              <xs:element ref="SharedSecretDynamicPlaintext"/>
            </xs:choice>
            <xs:element ref="Password"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="MobileNetworkNoEncryption"/>
              <xs:element ref="MobileNetworkRadioEncryption"/>
              <xs:element ref="MobileNetworkEndToEndEncryption"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="OperationalProtectionType">
      <xs:complexContent>
        <xs:restriction base="OperationalProtectionType">
          <xs:sequence>
            <xs:element ref="SecurityAudit"/>
            <xs:element ref="DeactivationCallCenter"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
        <xs:restriction base="TechnicalProtectionBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PrivateKeyProtection"/>
              <xs:element ref="SecretKeyProtection"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyActivation"/>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecretKeyProtectionType">
```

```
      <xs:complexContent>
        <xs:restriction base="SecretKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyActivation"/>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

ملاحظة – استعمال SSL معروض في التذييل IV.

6.4.3.12 MobileOneFactorContract

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ويبين إجراءات تسجيل مشترك في عقد متنقل مع استيقان قائم على عامل واحد. مثل جهاز توقيع رقمي مع ذاكرة عصيّة على التلاعب لتخزين المفاتيح، مثل رقم الشبكة ISDN الدولي لمشترك متنقل (MSISDN)، ولكن لا يطلب رقم تعريف الهوية الشخصي (PIN) أو عناصر قياس الحياة لاستيقان مستعمل في الوقت الفعلي.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema

targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
        Document identifier: saml-schema-authn-context-mobileonefactor-reg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
```

```
            <xs:element ref="ZeroKnowledge"/>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkNoEncryption"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
            <xs:element ref="WTLS"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
    <xs:complexType name="SecretKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="SecretKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="smartcard"/>
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="PhysicalVerification"/>
            <xs:element ref="WrittenConsent"/>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="verinymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

ملاحظة – استعمال SSL معروض في التذييل IV.

8.4.3.12 Password (كلمة السر)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Password

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ينطبق صنف كلمة السر عندما يستيقن طرف رئيسي نفسه لدى سلطة استيقان عبر تقديمه كلمة سر فوق دورة HTTP غير محمية.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        Document identifier: saml-schema-authn-context-pword-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
```

```
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

وفيما يلي مثال على تطابق في اللغة XML يطابق تخطيطة صنف السياق.

```
<AuthenticationContextDeclaration
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password">

  <AuthnMethod>
    <Authenticator>
      <AuthenticatorSequence>
        <RestrictedPassword>
          <Length min="4"/>
        </RestrictedPassword>
      </AuthenticatorSequence>
    </Authenticator>
  </AuthnMethod>

</AuthenticationContextDeclaration>
```

9.4.3.12 PasswordProtectedTransport

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ينطبق الصنف PasswordProtectedTransport عندما يستيقن طرف رئيسي نفسه لدى سلطة استيقان عبر تقديمه كلمة سر فوق دورة محمية.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTr
ansport"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        Document identifier: saml-schema-authn-context-ppt-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
```

```
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="MobileNetworkRadioEncryption"/>
              <xs:element ref="MobileNetworkEndToEndEncryption"/>
              <xs:element ref="WTLS"/>
              <xs:element ref="IPSec"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

ملاحظة – استعمال SSL معروض في التذييل IV.

10.4.3.12 PreviousSession

URI: `urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession`

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ينطبق الصنف PreviousSession عندما يكون طرف رئيسي قد استيقن نفسه لدى سلطة استيقان في نقطة ما في الماضي، مستخدماً أي سياق استيقان تعتمده سلطة الاستيقان هذه. وعليه فإن حدث الاستيقان اللاحق الذي ستؤكده سلطة الاستيقان إلى الطرف الواثق، قد يكون منفصلاً في الزمن بشكل محسوس عن الطلب الحالي للنفاذ إلى المورد من الطرف الرئيسي.

وسياق الدورة المستيقنة سابقاً هو ليس وارداً صراحة في صنف السياق هذا، لأن المستعمل لم يستيقن ذاته أثناء هذه الدورة، وهكذا فالآلية التي استخدمها المستعمل لاستيقان ذاته في دورة سابقة ينبغي ألا تستعمل كجزء من القرار الخاص بالسماح بالنفاذ إلى مورد.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
        Document identifier: saml-schema-authn-context-session-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="PreviousSession"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

11.4.3.12 Public key – X.509 (المفتاح العمومي)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:X509

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

يدل صنف السياق X.509 على أن الطرف الرئيسي يستيقن نفسه بواسطة التوقيع الرقمي، حيث تم إقرار صلاحية المفتاح، كجزء من البنية التحتية للمفتاح العمومي في التوصية X.509.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
        Document identifier: saml-schema-authn-context-x509-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
```

```
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

12.4.3.12 Public key – X.509 (المفتاح العمومي)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

يدل صنف السياق PGP (سرية جيدة نوعاً ما) على أن الطرف الرئيسي يستيقن ذاته بواسطة توقيع رقمي حيث أقرت صلاحية المفتاح كجزء من بنية تحتية PGP لمفتاح عمومي.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
        Document identifier: saml-schema-authn-context-pgp-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
```

```
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

13.4.3.12 Public key – SPKI (المفتاح العمومي–البنية التحتية البسيطة للمفتاح العمومي)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

يدل صنف السياق SPKI على أن الطرف الرئيسي قد استيقن نفسه بواسطة توقيع رقمي حيث كان المفتاح قد أقرت صلاحيته عبر بنية تحتية بسيطة للمفتاح العمومي (SPKI).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
        Document identifier: saml-schema-authn-context-spki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
```

```
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

Public key – XML digital signature 14.4.3.12

URI: `urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig`

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة للملحق A.

يدل صنف السياق هذا على أن الطرف الرئيسي قد استيقن نفسه بواسطة توقيع رقمي وفقاً لقواعد المعالجة المحددة في توقيع اللغة XML التابع للتجمع W3C.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
        Document identifier: saml-schema-authn-context-xmldsig-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
```

```
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
fixed="urn:ietf:rfc:3075"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

15.4.3.12 Smartcard (البطاقة الذكية)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

تعرف هوية البطاقة الذكية عندما يستيقن طرف رئيسي ذاته إلى سلطة الاستيقان باستخدام بطاقة ذكية.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
        Document identifier: saml-schema-authn-context-smartcard-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="Smartcard"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

SmartcardPKI 16.4.3.12

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

وينطبق الصنف SmartcardPKI عندما يستيقن طرف رئيسي نفسه إلى سلطة الاستيقان عبر آلية استيقان قائم على عاملين باستخدام بطاقة ذكية مع مفتاح خاص ورقم شخصي PIN موضوعين ضمنها.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
        Document identifier: saml-schema-authn-context-smartcardpki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
        <xs:restriction base="TechnicalProtectionBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PrivateKeyProtection"/>
            </xs:choice>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="Smartcard"/>
            <xs:element ref="ActivationPin"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyActivation"/>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyActivationType">
      <xs:complexContent>
        <xs:restriction base="KeyActivationType">
          <xs:sequence>
            <xs:element ref="ActivationPin"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

SoftwarePKI 17.4.3.12

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

وينطبق الصنف SoftwarePKI عندما يستخدم طرف رئيسي شهادة X.509 مخزونة في برمجية، لكي يستيقن نفسه لدى سلطة استيقان.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
        Document identifier: saml-schema-authn-context-softwarepki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
        <xs:restriction base="TechnicalProtectionBaseType">
          <xs:sequence>
            <xs:choice>
```

```
              <xs:element ref="PrivateKeyProtection"/>
            </xs:choice>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="ActivationPin"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyActivation"/>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyActivationType">
      <xs:complexContent>
        <xs:restriction base="KeyActivationType">
          <xs:sequence>
            <xs:element ref="ActivationPin"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="memory"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
```

```
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>
</xs:schema>
```

18.4.3.12 Telephony (مهاتفة)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony

يستخدم هذا المعرف URI كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ويستعمل هذا الصنف ليدل على أن الطرف الرئيسي قد استيقن ذاته بتقديمه رقم هاتف ثابت، منقول عبر بروتوكول المهاتفة مثل خط مشترك رقمي لا تناظري (ADSL).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
        Document identifier: saml-schema-authn-context-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SubscriberLineNumber"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

19.4.3.12 Telephony (nomadic) (مهاتفة ترحّلية)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ويدل على أن الطرف الرئيسي جوّال "roaming" (وربما يستخدم بطاقة هاتفية) ويستيقن نفسه عن طريق رقم خط هاتفي، ولاحقة مستعمل، وعنصر كلمة السر.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
        Document identifier: saml-schema-authn-context-nomad-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
```

```
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="Password"/>
            <xs:element ref="SubscriberLineNumber"/>
            <xs:element ref="UserSuffix"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

20.4.3.12 Telephony (personalized) (مهاتفة شخصانية)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTele

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ويستعمل هذا الصنف ليدل على أن الطرف الرئيسي قد استيقن ذاته بتقديمه رقم هاتف ثابت، ولاحقة مستعمل منقولين عبر بروتوكول هاتف مثل الخط ADSL.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
        Document identifier: saml-schema-authn-context-personal-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SubscriberLineNumber"/>
            <xs:element ref="UserSuffix"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
```

```
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

21.4.3.12 Telephony (authenticated) (مهاتفة مستيقنة)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ويدل على أن الطرف الرئيسي قد استيقن نفسه بواسطة رقم خط هاتفي، ولاحقة المستعمل، وعنصر كلمة السر.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTeleph
ony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
        Document identifier: saml-schema-authn-context-auth-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
```

```
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="Password"/>
            <xs:element ref="SubscriberLineNumber"/>
            <xs:element ref="UserSuffix"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>

</xs:schema>
```

22.4.3.12 Secure remote password (كلمة سر بعيدة مأمونة)

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ينطبق الصنف SecureRemotePassword عندما يؤدي الاستيقان بواسطة كلمة سر بعيدة مأمونة كما هو محدد في طلب التعليقات RFC 2945 الصادر عن فريق المهام الهندسية في الإنترنت (IETF).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
        Document identifier: saml-schema-authn-context-srp-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
```

```
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SharedSecretChallengeResponse"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
        <xs:restriction base="SharedSecretChallengeResponseType">
          <xs:attribute name="method" type="xs:anyURI" fixed="urn:ietf:rfc:2945"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

23.4.3.12 استيقان زبون مبني على شهادة TLS

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient

يستخدم المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

ويدل هذا الصنف على أن الطرف الرئيسي استيقن ذاته عن طريق شهادة الزبون المأمونة بالنقل TLS.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
        Document identifier: saml-schema-authn-context-sslcert-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
```

```
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

ملاحظة – استخدام SSL معروض في التذييل IV.

24.4.3.12 TimeSyncToken

URI: `urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken`

يستخدم هذا المعرف URI أيضاً كمكان اسم هدف في تخطيطة أصناف سياق الاستيقان المقابلة في الملحق A.

وينطبق الصنف TimeSyncToken عندما يستيقن طرف رئيسي نفسه من خلال إذنه مزامنة زمنياً.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
        Document identifier: saml-schema-authn-context-timesync-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
```

```
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="Token"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TokenType">
      <xs:complexContent>
        <xs:restriction base="TokenType">
          <xs:sequence>
            <xs:element ref="TimeSyncToken"/>
            <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="TimeSyncTokenType">
      <xs:complexContent>
        <xs:restriction base="TimeSyncTokenType">
          <xs:attribute name="DeviceType" use="required">
            <xs:simpleType>
              <xs:restriction base="DeviceTypeType">
                <xs:enumeration value="hardware"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>

          <xs:attribute name="SeedLength" use="required">
            <xs:simpleType>
              <xs:restriction base="xs:integer">
                <xs:minInclusive value="64"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
```

```
          <xs:attribute name="DeviceInHand" use="required">
            <xs:simpleType>
              <xs:restriction base="booleanType">
                <xs:enumeration value="true"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

25.4.3.12 Unspecified

URI: urn:oasis:names:tc:SAML:2.0:ac:classes:Unspecified

يدل الصنف Unspecified على أن الاستيقان قد جرى بوسائل غير محدّدة.

13 متطلبات التطابق مع اللغة SAML

يشرح هذا البند الميزات الإلزامية والميزات الاختيارية لعمليات التنفيذ التي تطالب بالتوافق مع SAML.

وهذه التوصية تعرف عدداً من الجانبيات المسماة. وكل جانبية (غير جانبيات النعت) تشرح تفاصيل تدفقات منتقاة من رسائل اللغة SAML، ويمكن النظر إليها على أنها وظائفية غير قابلة للانقسام، يمكن أن تنفذها مكونة برمجية. وتنفيذ جانبية ما يقتضي استخدام رابطة لكل واحد من تبادلات الرسائل الواردة في الجانبية. ويمكن النظر إلى الرابطة على أنها تقنية تنفيذ خاصة لإنجاز عملية تبادل رسائل.

ويعدّد هذا البند جميع الجانبيات المختلفة المعرفة في هذه التوصية. ويعدّد في القائمة، لكل جانبية، تدفقات رسائل الصيغة SAML V2.0 ذات الصلة، كما أن مجموعة الروابط المحتملة لكل تدفق رسائل مشروحة أيضاً. وتدعى التجميعة المكونة من الجانبية وتبادل الرسائل والروابط المنتقاة *ميزة الصيغة* SAML V2.0.

ويشرح البند أيضاً مصفوفة التطابق مع الصيغة SAML V2.0. وتُعرَّف هوية عدد من *الأساليب التشغيلية* المختلفة أو الأدوار. وتشرح مصفوفة التطابق مجموعة الميزات التي يتعين على كل واحد من أساليب التشغيل أن ينفذها.

1.13 جانبيات اللغة SAML وعمليات التنفيذ الممكنة

يعدّد الجدول 1 جميع الجانبيات التي تعرف بأنها جانبيات اللغة SAML. ومع كل جانبية تشرح تدفقات رسائل البروتوكول التي توجد داخل الجانبية. وترد في العمود الأخير اليميني قائمة بالروابط ذات الصلة بكل تدفق من الرسائل.

الجدول X.1141/1 – عمليات التنفيذ الممكنة

الجانبية	تدفق الرسائل	الرابطة
التوقيع الوحيد في شبكة الويب.	<AuthnRequest> من SP إلى IdP	HTTP Redirect
		HTTP POST
		HTTP Artifact
	<Response> من IdP إلى SP	HTTP POST
		HTTP Artifact
التوقيع الوحيد للزبون/الوكيل المفوض المعزّز SSO.	من ECP إلى SP، من SP إلى ECP إلى IdP	PAOS
	من IdP إلى ECP إلى SP، من SP إلى ECP	PAOS
اكتشاف مزوّد الهوية	واضع الكعكة	HTTP
	نائل الكعكة	HTTP
اختتام الدورة الوحيد	<LogoutRequest>	HTTP Redirect
		HTTP POST
		HTTP Artifact
		SOAP
	<LogoutResponse>	HTTP Redirect
		HTTP POST
		HTTP Artifact
		SOAP
إدارة معرف هوية الاسم	<ManageNameIDRequest>	HTTP Redirect
		HTTP POST
		HTTP Artifact
		SOAP
	<ManageNameIDResponse>	HTTP Redirect
		SOAP
استبانة الشيء المصطنع	<ArtifactResolve>, <ArtifactResponse>	SOAP
استفهام عن استيقان	<AuthnQuery>, <Response>	SOAP
استفهام عن نعت	<AttributeQuery>, <Response>	SOAP
استفهام عن قرار ترخيص	<AuthzDecisionQuery>, <Response>	SOAP
طلب تأكيد بمعرف هوية	<AssertionIDRequest>, <Response>	SOAP
تقابل معرفات هوية الأسماء	<NameIDMappingRequest>, <NameIDMappingResponse>	SOAP
الرابطة SAMLURI	GET, HTTP Response	HTTP
جانبية النعت UUID		
جانبية نعت الشهادات PAC في البيئة DCE		
جانبية النعت X.500		
جانبية النعت XACML		
معطيات شرحية	تبادل	

2.13 التطابق

تشرح هذه الفقرة متطلبات التطابق التقني مع الصيغة SAML V2.0.

1.2.13 الأساليب التشغلية

تستخدم هذه التوصية جملة "الأسلوب التشغيلي"، لكي تشرح دوراً يمكن أن تقوم به مكوّنة برمجية في التطابق مع اللغة SAML. والأساليب التشغيلية هي كالتالي:

- IdP – مزود هوية
- IdP lite – مزود هوية خفيف
- SP – مزوّد خدمة
- SP lite – مزوّد خدمة خفيف
- ECP – زبون/وكيل مفوض معزّز
- سلطة نعت SAML
- سلطة قرار ترخيص SAML
- سلطة نعت SAML
- سلطة قرار ترخيص SAML
- سلطة استيقان SAML
- طالب SAML

2.2.13 مصفوفة الميزات

تعرف المصفوفات التالية (انظر الجدول 2) هويات مجموعات وحيدة من متطلبات التطابق بواسطة ثلاثية مأخوذة من الجدول 1 من الشكل: جانبية، ورسالة (رسائل)، ورابطة. ولا ترد دوماً مكوّنة الرسالة، عندما تكون واضحة من السياق.

الجدول X.1141/2 – مصفوفة الميزات

الميزة	IdP	IdP lite	SP	SP lite	ECP
SSO في الويب، <AuthnRequest>، HTTP redirect	يجب	يجب	يجب	يجب	لا ينطبق
SSO في الويب، <Response>، HTTP POST	يجب	يجب	يجب	يجب	لا ينطبق
SSO في الويب، <Response>، HTTP aircraft	يجب	يجب	يجب	يجب	لا ينطبق
استبانة الشيء المصطنع، SOAP	يجب	يجب	يجب	يجب	لا ينطبق
SSO لزبون/وكيل مفوض معزز، PAOS	يجب	يجب	يجب	يجب	لا ينطبق
إدارة معرف هوية الاسم، HTTP redirect (بمبادرة من IdP)	يجب	يجب ألا	يجب	يجب ألا	لا ينطبق
إدارة معرف هوية الاسم، SOAP، (بمبادرة من IdP)	يجب	يجب ألا	اختياري	يجب ألا	لا ينطبق
إدارة معرف هوية الاسم، HTTP redirect ملاحظة (للاطّلاع) – يقترح PE11 (انظر OASIS PE:2006) إضافة (بمبادرة من SP)	يجب	يجب ألا	يجب	يجب ألا	لا ينطبق
إدارة معرف هوية الاسم، SOAP، (بمبادرة من SP)	يجب	يجب ألا	اختياري	يجب ألا	لا ينطبق
إدارة معرف هوية الاسم، SOAP (بمبادرة من SP)	يجب	يجب	يجب	يجب	لا ينطبق
اختتام دورة وحيد (بمبادرة من IdP) – SOAP	يجب	اختياري	يجب	اختياري	لا ينطبق
اختتام دورة وحيد (بمبادرة من SP) – HTTP redirect	يجب	يجب	يجب	يجب	لا ينطبق
اختتام دورة وحيد (بمبادرة من SP) – SOAP	يجب	اختياري	يجب	اختياري	لا ينطبق
اكتشاف مزوّد هوية (كعكة)	يجب	يجب	اختياري	اختياري	لا ينطبق

الملاحظة 1 (للاطّلاع) – يقترح PE16 (انظر OASIS PE:2006) أن يستعاض عن "لا ينطبق" بكلمة "اختياري" في السطر الأخير من العمود الأخير في الجدول 2.

الملاحظة 2 (للاطّلاع) – يقترح PE25 (انظر OASIS PE:2006) أن يضاف التالي إلى آخر الجدول 2.

الميزة	IdP	IdP Lite	SP	SP Lite	ECP
بنى المعطيات الشرحية	اختياري	اختياري	اختياري	اختياري	لا ينطبق
التشغيل البيني للمعطيات الشرحية	اختياري	اختياري	اختياري	اختياري	لا ينطبق

الملاحظة 3 (للاطّلاع) – يقترح PE29 (انظر OASIS PE:2006) أن يضاف التالي إلى آخر الجدول 2.

الميزة	IdP	IdP Lite	SP	SP Lite	ECP
بنى المعطيات الشرحية	اختياري	لا ينطبق	لا ينطبق	لا ينطبق	لا ينطبق
التشغيل البيني للمعطيات الشرحية	اختياري	لا ينطبق	لا ينطبق	لا ينطبق	لا ينطبق

ويلخص الجدول 3 الأساليب التشغيلية التي توسّع الأساليب IdP أو SP المعرفة أعلاه. ويجب أن تفهم على أنها تجميعة من الأسلوب IdP أو SP من الجدول أعلاه مع مجموعة الميزات الموسّعة المقابلة أدناه.

الجدول X.1141/3 – IdP وSP الموسّعان

الميزة	IdP الموسع	SP الموسع
وكيل مفوّض مزوّد الهوية	يجب	يجب
تقابل معرف هوية الاسم، SOAP	يجب	يجب

ويلخص الجدول 4 متطلبات التطابق للسلطات والطالبين في اللغة SAML.

الجدول X.1141/4 – مصفوفة السلطات والطالبين في اللغة SAML

الميزة	سلطة الاستيقان في SAML	سلطة النعت في SAML	سلطة قرار الترخيص في SAML	طالب في SAML
استفهام عن استيقان، SOAP	يجب	اختياري	اختياري	اختياري
استفهام عن نعت، SOAP	اختياري	يجب	اختياري	اختياري
استفهام عن قرار ترخيص، SOAP	اختياري	اختياري	يجب	اختياري
طلب تأكيد بمعرف هوية، SOAP	يجب	يجب	يجب	اختياري
الرابطة SAML URI	يجب	يجب	يجب	اختياري

ملاحظة 4 (للاطّلاع) – يقترح PE25 (انظر OASIS PE:2006) تعديل الجدول 4 إلى التالي.

الميزة	سلطة الاستيقان في SAML	سلطة النعت في SAML	سلطة قرار الترخيص في SAML	طالب في SAML
استفهام عن استيقان، SOAP	يجب	لا ينطبق	لا ينطبق	اختياري
استفهام عن نعت، SOAP	N/A	يجب	لا ينطبق	اختياري
استفهام عن قرار ترخيص، SOAP	N/A	لا ينطبق	يجب	اختياري
طلب تأكيد بمعرف هوية، SOAP	يجب	يجب	يجب	اختياري
الرابطة SAML URI	يجب	يجب	يجب	اختياري
بنى المعطيات الشرحية	اختياري	اختياري	اختياري	اختياري
التشغيل البيني للمعطيات الشرحية	اختياري	اختياري	اختياري	اختياري

3.2.13 تنفيذ معرفات هوية معرفة في اللغة SAML

يتعين على جميع الأساليب التشغيلية ذات العلاقة أن تنفذ معرفات الهوية التالية المعرفة في اللغة SAML:

- جميع معرفات الهوية لنسق اسم النعت المعرفة في البند 8.
- جميع معرفات الهوية لنسق معرف هوية الاسم المعرفة في البند 8.

يتعين على عمليات التنفيذ المطابقة للغة SAML أن تتيح استعمال جميع ثوابت معرف الهوية (انظر الفقرتين 1.8 و2.8) عند إنتاج واستهلاك الرسائل SAML. ويتعين أن يكون منتجو الرسائل SAML قادرين على خلق رسائل، وأن يكون مستهلكو الرسائل SAML قادرين على معالجة الرسائل من جميع الثوابت المعرفة في هاتين الفقرتين.

وتعرف فقرات معرفات هوية الاسم الدائمة ومعرفات هوية الاسم العابرة قواعد معالجة معيارية من أجل منتج مثل هذه المعرفات. ويتعين على جميع قواعد المعالجة المعيارية أن تكون معتمدة من عمليات التنفيذ المطابقة. ومعرفات الهوية المتبقية لا تحدد قواعد معالجة معيارية. ولذلك لا يكون لتوليد واستهلاك هذه المعرفات للهوية أي مغزى، إلا عندما يكون بين الأطراف المولدة والمستهلكة اتفاق محدد خارجياً بشأن تفسير علم الدلالات لمعرفات الهوية هذه.

ملاحظة – في هذا السياق، تعني كلمة "عملية" أن التنفيذ يجب أن يحلل ويعالج بنجاح تام معرف الهوية من دون إخفاق أو ترجيع خطأ. والطريقة التي يتعامل التنفيذ بها مع معرف الهوية بعد معالجته على هذا الصعيد، تقع خارج نطاق هذه التوصية.

ربما يقدم تنفيذ في اللغة SAML المرافق المشروحة أعلاه، عبر اعتماد التنفيذ مباشرة معرفات الهوية أو عبر استعمال سطوح بينية معتمدة في البرمجة. ويتعين على السطوح البينية المقدمة لهذا الغرض أن تسمح للتنفيذ في SAML أن يجري توسيعه برمجياً لمعالجة جميع معرفات الهوية التي لم يعالجها التنفيذ في الأصل.

4.2.13 تنفيذ العناصر المجفّرة

يتعين على جميع الأساليب التشغيلية ذات العلاقة أن تكون قادرة على معالجة أو توليد العناصر المجفّرة التالية في أي سياق تكون مطلوبة فيه لمعالجة أو توليد العناصر المجفّرة المقابلة، وهي <saml:NameID> أو <saml:Assertion> أو <saml:Attribute>.

- <saml:EncryptedID>
- <saml:EncryptedAssertion>
- <saml:EncryptedAttribute>

5.2.13 النموذجات الأمنية للرابطتين SOAP وURI

إن تنفيذ النموذجات الأمنية التالية إلزامي لجميع الجانبيات المنفذة باستعمال الرابطة SOAP وكذلك الرابطة SAML URI. ويتعين على السلطات والطالبين في اللغة SAML تنفيذ طرائق الاستيقان التالية:

- لا يوجد استيقان زبون أو مخدّم.
- استيقان أساس HTTP مع الصيغة TLS 1.0 أو من دونها، ويتعين على الطالب في اللغة SAML أن يرسل مسبقاً رأسية الترخيص مع الطلب الأولي.
- استيقان مخدّم HTTP فوق الصيغة TLS 1.0 مع شهادة في جانب المخدّم.
- استيقان متبادل HTTP فوق الصيغة TLS 1.0 مع شهادة في كلا جانبي المخدّم والزبون.

وإذا كانت السلطة SAML تستخدم الصيغة TLS 1.0، يتعين عليها أن تستخدم شهادة في جانب المخدّم.

ملاحظة 1 (للاطّلاع) – يقترح PE25 (انظر OASIS PE:2006) أن تضاتف فقرة فرعية إلى بنى المعطيات الشرحية كما يلي:

يمكن لعمليات التنفيذ التي تطالب بالتطابق مع اللغة SAML أن تعلن عن مطابقة كل أسلوب تشغيلي للمعطيات الشرحية في SAML باختيارها خيار بنى المعطيات الشرحية. وفيما يخص كل أسلوب تشغيلي فإن مثل هذا التطابق يسترعي الآتي:

تنفيذ المعطيات الشرحية SAML وفقاً للنسق الموسّع للمعطيات الشرحية SAML في جميع الحالات التي يكون فيها لندّ في التشغيل البيني الخيار، في أن يكون متعلقاً بوجود المتعلقات الشرحية SAML، كما تنص على ذلك مواصفات اللغة SAML. وينتج عن خيار انتقاء بنى المعطيات الشرحية أن يُطْلب تيسر مثل هذه المعطيات الشرحية للندّ المشتغل بينياً. وميزة الاشتغال البيني، المشروح أدناه، توفر وسيلة لاستيفاء هذا المطلب.

إن إرجاع ندّ مشتغل بينياً إلى المعطيات الشرحية SAML، واستهلاكها والانتماء إليها، وفقاً لهذه التوصية، عندما تكون للمعطيات الشرحية المعروفة الخاصة بهذا الندّ، والتشغيل المدروس، والتبادل الجاري قد انقضت صلاحيتها أو لم تعد صالحة بعد الآن في ذاكرة مخبأ، شريطة أن تكون المعطيات الشرحية متيسرة وليست محظورة بسياسة أو بالتشغيل المدروس وهذا التبادل الخاص.

ملاحظة 2 (للاطّلاع) – يقترح PE25 (انظر OASIS PE:2006) أن تضاف فقرة فرعية جديدة عن التشغيل البيني للمعطيات كما يلي:

إن انتقاء خيار التشغيل البني للمعطيات الشرحية يتطلب أن يقدّم التنفيذ، إضافة إلى أي آليات أخرى، آلية معروفة جيداً لتحديد الموقع والإصدار والاستبانة التي يشرحها البند 9 في المعطيات الشرحية.

3.13 التوقيع الرقمي XML والتجفير XML

تستخدم الصيغة SAML V2.0 التوقيع في اللغة XML لتنفيذ وظيفية التوقيع والتجفير في اللغة XML من أجل حماية السلامة واستيقان المصدر. وتستخدم الصيغة SAML V2.0 التجفير في اللغة XML لتنفيذ الائتمانية بما في ذلك معرّفات الهوية المجفّرة والتأكيدات المجفّرة والنعوت المجفّرة.

1.3.13 خوارزمية التوقيع XML

إن الفقرة 1.6 في توقيع اللغة XML التابع للتجمع W3C تُلْزم باستخدام التالي:

- Digest: SHA-1؛
- MAC: HMAC-SHA1؛

- التشريع القانوني XML: CanonicalXML (دون تعليقات)؛
- Transform (تحويل): توقيع متغلِّف.

وعليه يتعين تطبيقها بعمليات تنفيذ مطابقة للصيغة SAML V2.0.

وفوق ذلك ومن أجل تمكين التشغيل البيني، يتعين تطبيق التالي بعمليات تنفيذ مطابقة للصيغة SAML V2.0:

- التوقيع: RSA مع SHA-1 (موصى بهما في التوقيع W3C، ولازمتان للتشغيل البيني).

وعلى الرغم من أن التوقيع XML يلزم بخوارزمية التوقيع DSAwithSHA1، فإن الصيغة SAML V2.0 لا تتطلبها، ولكنها توصي بها.

ملاحظة – يشجع المعهد الوطني للمعايير والتكنولوجيا (NIST) في الوقت الحاضر استعمال SHA-256 (خوارزمية الفرم المأمون مع مفاتيح مشفرة بعدد من البتات قدره 256 بتة) بدلاً من SHA-1.

2.3.13 خوارزمية التجفير XML

- تلزم الفقرتان 1.2.5 و2.2.5 من التجفير XML التابع للتجمع W3C باستخدام الخوارزميات التالية: تجفير الفِدرة: الثلاثي DES وAES-128 وAES-256.
- نقل المفاتيح: RSA-v1.5 وRSA-OAEP.

وعليه يتعين تطبيق الخوارزميات أعلاه بعمليات تنفيذ مطابقة للصيغة SAML V2.0.

4.13 استعمال صيغة البروتوكول TLS 1.0

في أي استخدام من الصيغة SAML V2.0 لصيغة البروتوكول TLS 1.0، يتعين على المخدّمات أن تستيقن ذاتها لدى الزبائن باستعمال الشهادة X.509 v3. ويتعين على الزبون أن ينشئ هوية المخدّم استناداً إلى محتويات الشهادة (وعادة بتفحص الحقل DN من صاحب الشهادة).

1.4.13 الرابطتان SOAP وURI في اللغة SAML

يتعين على عمليات التنفيذ بقدرة TLS أن تطبق متتابعة التجفير TLS_RSA_WITH_3DES_EDE_CBC_SHA ويمكنها أن تطبق متتابعة التجفير TLS_RSA_AES_128_CBC_SHA.

ويتعين على عمليات التنفيذ بقدرة TLS FIPS أن تطبق متتابعة التجفير المقابلة TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA ويمكنها أن تطبق متتابعة التجفير المقابلة TLS_RSA_FIPS_AES_128_CBC_SHA.

2.4.13 جانبيات التوقيع الوحيد (SSO) لشبكة الويب من اللغة SAML

يتعين على عمليات التنفيذ بقدرة TLS أن تطبق متتابعة التجفير TLS_RSA_WITH_3DES_EDE_CBC_SHA (انظر طلب التعليقات RFC 2246 الصادر عن فريق المهام الهندسية في الإنترنت (IETF).

الملحق A

تخطيطات اللغة SAML

يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية. وهو يقدم قائمة بتخطيط اللغة SAML المطلوبة.

1.A تخطيطة SAML للتأكيد

هذه قائمة بتخطيطة SAML للتأكيد.

```
<?xml version="1.0" encoding="US-ASCII"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <import namespace="http://www.w3.org/2001/04/xmlenc#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-
schema.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-assertion-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V1.0 (November, 2002):
              Initial Standard Schema.
            V1.1 (September, 2003):
              Updates within the same V1.0 namespace.
            V2.0 (March, 2005):
              New assertion schema for SAML V2.0 namespace.
        </documentation>
    </annotation>
    <attributeGroup name="IDNameQualifiers">
        <attribute name="NameQualifier" type="string" use="optional"/>
        <attribute name="SPNameQualifier" type="string" use="optional"/>
    </attributeGroup>
    <element name="BaseID" type="saml:BaseIDAbstractType"/>
    <complexType name="BaseIDAbstractType" abstract="true">
        <attributeGroup ref="saml:IDNameQualifiers"/>
    </complexType>
    <element name="NameID" type="saml:NameIDType"/>
    <complexType name="NameIDType">
        <simpleContent>
            <extension base="string">
                <attributeGroup ref="saml:IDNameQualifiers"/>
                <attribute name="Format" type="anyURI" use="optional"/>
                <attribute name="SPProvidedID" type="string" use="optional"/>
            </extension>
        </simpleContent>
    </complexType>
    <complexType name="EncryptedElementType">
        <sequence>
            <element ref="xenc:EncryptedData"/>
            <element ref="xenc:EncryptedKey" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
    </complexType>
    <element name="EncryptedID" type="saml:EncryptedElementType"/>
    <element name="Issuer" type="saml:NameIDType"/>
```

```
    <element name="AssertionIDRef" type="NCName"/>
    <element name="AssertionURIRef" type="anyURI"/>
    <element name="Assertion" type="saml:AssertionType"/>
    <complexType name="AssertionType">
        <sequence>
            <element ref="saml:Issuer"/>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="saml:Subject" minOccurs="0"/>
            <element ref="saml:Conditions" minOccurs="0"/>
            <element ref="saml:Advice" minOccurs="0"/>
            <choice minOccurs="0" maxOccurs="unbounded">
                <element ref="saml:Statement"/>
                <element ref="saml:AuthnStatement"/>
                <element ref="saml:AuthzDecisionStatement"/>
                <element ref="saml:AttributeStatement"/>
            </choice>
        </sequence>
        <attribute name="Version" type="string" use="required"/>
        <attribute name="ID" type="ID" use="required"/>
        <attribute name="IssueInstant" type="dateTime" use="required"/>
    </complexType>
    <element name="Subject" type="saml:SubjectType"/>
    <complexType name="SubjectType">
        <choice>
            <sequence>
                <choice>
                    <element ref="saml:BaseID"/>
                    <element ref="saml:NameID"/>
                    <element ref="saml:EncryptedID"/>
                </choice>
                <element ref="saml:SubjectConfirmation" minOccurs="0"
maxOccurs="unbounded"/>
            </sequence>
            <element ref="saml:SubjectConfirmation" maxOccurs="unbounded"/>
        </choice>
    </complexType>
    <element name="SubjectConfirmation" type="saml:SubjectConfirmationType"/>
    <complexType name="SubjectConfirmationType">
        <sequence>
            <choice minOccurs="0">
                <element ref="saml:BaseID"/>
                <element ref="saml:NameID"/>
                <element ref="saml:EncryptedID"/>
            </choice>
            <element ref="saml:SubjectConfirmationData" minOccurs="0"/>
        </sequence>
        <attribute name="Method" type="anyURI" use="required"/>
    </complexType>
    <element name="SubjectConfirmationData"
type="saml:SubjectConfirmationDataType"/>
    <complexType name="SubjectConfirmationDataType" mixed="true">
        <complexContent>
            <restriction base="anyType">
                <sequence>
                    <any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
                <attribute name="NotBefore" type="dateTime" use="optional"/>
                <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
                <attribute name="Recipient" type="anyURI" use="optional"/>
                <attribute name="InResponseTo" type="NCName" use="optional"/>
                <attribute name="Address" type="string" use="optional"/>
                <anyAttribute namespace="##other" processContents="lax"/>
            </restriction>
        </complexContent>
    </complexType>
    <complexType name="KeyInfoConfirmationDataType" mixed="false">
        <complexContent>
            <restriction base="saml:SubjectConfirmationDataType">
                <sequence>
                    <element ref="ds:KeyInfo" maxOccurs="unbounded"/>
```

```
                </sequence>
            </restriction>
        </complexContent>
    </complexType>
    <element name="Conditions" type="saml:ConditionsType"/>
    <complexType name="ConditionsType">
        <choice minOccurs="0" maxOccurs="unbounded">
            <element ref="saml:Condition"/>
            <element ref="saml:AudienceRestriction"/>
            <element ref="saml:OneTimeUse"/>
            <element ref="saml:ProxyRestriction"/>
        </choice>
        <attribute name="NotBefore" type="dateTime" use="optional"/>
        <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
    </complexType>
    <element name="Condition" type="saml:ConditionAbstractType"/>
    <complexType name="ConditionAbstractType" abstract="true"/>
    <element name="AudienceRestriction" type="saml:AudienceRestrictionType"/>
    <complexType name="AudienceRestrictionType">
        <complexContent>
            <extension base="saml:ConditionAbstractType">
                <sequence>
                    <element ref="saml:Audience" maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="Audience" type="anyURI"/>
    <element name="OneTimeUse" type="saml:OneTimeUseType" />
    <complexType name="OneTimeUseType">
        <complexContent>
            <extension base="saml:ConditionAbstractType"/>
        </complexContent>
    </complexType>
    <element name="ProxyRestriction" type="saml:ProxyRestrictionType"/>
    <complexType name="ProxyRestrictionType">
    <complexContent>
        <extension base="saml:ConditionAbstractType">
            <sequence>
                <element ref="saml:Audience" minOccurs="0"
maxOccurs="unbounded"/>
            </sequence>
            <attribute name="Count" type="nonNegativeInteger" use="optional"/>
        </extension>
   </complexContent>
    </complexType>
    <element name="Advice" type="saml:AdviceType"/>
    <complexType name="AdviceType">
        <choice minOccurs="0" maxOccurs="unbounded">
            <element ref="saml:AssertionIDRef"/>
            <element ref="saml:AssertionURIRef"/>
            <element ref="saml:Assertion"/>
            <element ref="saml:EncryptedAssertion"/>
            <any namespace="##other" processContents="lax"/>
        </choice>
    </complexType>
    <element name="EncryptedAssertion" type="saml:EncryptedElementType"/>
    <element name="Statement" type="saml:StatementAbstractType"/>
    <complexType name="StatementAbstractType" abstract="true"/>
    <element name="AuthnStatement" type="saml:AuthnStatementType"/>
    <complexType name="AuthnStatementType">
        <complexContent>
            <extension base="saml:StatementAbstractType">
                <sequence>
                    <element ref="saml:SubjectLocality" minOccurs="0"/>
                    <element ref="saml:AuthnContext"/>
                </sequence>
                <attribute name="AuthnInstant" type="dateTime" use="required"/>
                <attribute name="SessionIndex" type="string" use="optional"/>
                <attribute name="SessionNotOnOrAfter" type="dateTime"
use="optional"/>
```

```
            </extension>
        </complexContent>
    </complexType>
    <element name="SubjectLocality" type="saml:SubjectLocalityType"/>
    <complexType name="SubjectLocalityType">
        <attribute name="Address" type="string" use="optional"/>
        <attribute name="DNSName" type="string" use="optional"/>
    </complexType>
    <element name="AuthnContext" type="saml:AuthnContextType"/>
    <complexType name="AuthnContextType">
        <sequence>
            <choice>
                <sequence>
                    <element ref="saml:AuthnContextClassRef"/>
                    <choice minOccurs="0">
                        <element ref="saml:AuthnContextDecl"/>
                        <element ref="saml:AuthnContextDeclRef"/>
                    </choice>
                </sequence>
                <choice>
                    <element ref="saml:AuthnContextDecl"/>
                    <element ref="saml:AuthnContextDeclRef"/>
                </choice>
            </choice>
            <element ref="saml:AuthenticatingAuthority" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
    </complexType>
    <element name="AuthnContextClassRef" type="anyURI"/>
    <element name="AuthnContextDeclRef" type="anyURI"/>
    <element name="AuthnContextDecl" type="anyType"/>
    <element name="AuthenticatingAuthority" type="anyURI"/>
    <element name="AuthzDecisionStatement"
type="saml:AuthzDecisionStatementType"/>
    <complexType name="AuthzDecisionStatementType">
        <complexContent>
            <extension base="saml:StatementAbstractType">
                <sequence>
                    <element ref="saml:Action" maxOccurs="unbounded"/>
                    <element ref="saml:Evidence" minOccurs="0"/>
                </sequence>
                <attribute name="Resource" type="anyURI" use="required"/>
                <attribute name="Decision" type="saml:DecisionType"
use="required"/>
            </extension>
        </complexContent>
    </complexType>
    <simpleType name="DecisionType">
        <restriction base="string">
            <enumeration value="Permit"/>
            <enumeration value="Deny"/>
            <enumeration value="Indeterminate"/>
        </restriction>
    </simpleType>
    <element name="Action" type="saml:ActionType"/>
    <complexType name="ActionType">
        <simpleContent>
            <extension base="string">
                <attribute name="Namespace" type="anyURI" use="required"/>
            </extension>
        </simpleContent>
    </complexType>
    <element name="Evidence" type="saml:EvidenceType"/>
    <complexType name="EvidenceType">
        <choice maxOccurs="unbounded">
            <element ref="saml:AssertionIDRef"/>
            <element ref="saml:AssertionURIRef"/>
            <element ref="saml:Assertion"/>
            <element ref="saml:EncryptedAssertion"/>
        </choice>
    </complexType>
```

```
    <element name="AttributeStatement" type="saml:AttributeStatementType"/>
    <complexType name="AttributeStatementType">
        <complexContent>
            <extension base="saml:StatementAbstractType">
                <choice maxOccurs="unbounded">
                    <element ref="saml:Attribute"/>
                    <element ref="saml:EncryptedAttribute"/>
                </choice>
            </extension>
        </complexContent>
    </complexType>
    <element name="Attribute" type="saml:AttributeType"/>
    <complexType name="AttributeType">
        <sequence>
            <element ref="saml:AttributeValue" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="Name" type="string" use="required"/>
        <attribute name="NameFormat" type="anyURI" use="optional"/>
        <attribute name="FriendlyName" type="string" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="AttributeValue" type="anyType" nillable="true"/>
    <element name="EncryptedAttribute" type="saml:EncryptedElementType"/>
</schema>
```

2.A تخطيطة SAML لسياق الاستيقان

هذه تخطيطة SAML لسياق الاستيقان.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac"
  blockDefault="substitution"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
      Document identifier: saml-schema-authn-context-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New core authentication context schema for SAML V2.0.
          This is just an include of all types from the Shema
          referred to in the include statement below.
    </xs:documentation>
  </xs:annotation>

  <xs:include schemaLocation="saml-schema-authn-context-types-2.0.xsd"/>

</xs:schema>
```

3.A تخطيطة SAML للمهاتفة المستيقنة في سياق الاستيقان

تخطيطة SAML لسياق الاستيقان المتعلق بالمهاتفة.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
```

```
    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony
        Document identifier: saml-schema-authn-context-auth-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="Password"/>
            <xs:element ref="SubscriberLineNumber"/>
            <xs:element ref="UserSuffix"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>
```

```
</xs:schema>
```

4.A تخطيطة SAML لسياق الاستيقان المتعلق ببروتوكول الإنترنت (IP)

تخطيطة SAML لسياق الاستيقان المتعلق ببروتوكول الإنترنت.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="IPAddress"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>
```

```
</xs:schema>
```

5.A تخطيطة SAML لسياق الاستيقان IPPWord

تخطيطة SAML لسياق الاستيقان المتعلق ببروتوكول الإنترنت مع كلمة سر (IPPWord).

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
  xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
        Document identifier: saml-schema-authn-context-ippword-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="Password"/>
            <xs:element ref="IPAddress"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
```

```
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

6.A تخطيطة SAML لسياق الاستيقان Kerberos

تقدم هذه القائمة تخطيطة SAML لسياق الاستيقان المتعلق بكيربروس.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
        Document identifier: saml-schema-authn-context-kerberos-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
```

```
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SharedSecretChallengeResponse"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
        <xs:restriction base="SharedSecretChallengeResponseType">
          <xs:attribute name="method" type="xs:anyURI"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>
</xs:schema>
```

7.A تخطيطة SAML لسياق الاستيقان MobileOneFactor-reg

تحتوي هذه القائمة على تخطيطة صنف السياق SAML من أجل MobileOneFactorContract المسجل.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
        Document identifier: saml-schema-authn-context-mobileonefactor-reg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
<xs:complexType name="AuthnMethodBaseType">
  <xs:complexContent>
    <xs:restriction base="AuthnMethodBaseType">
      <xs:sequence>
        <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
        <xs:element ref="Authenticator"/>
        <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorBaseType">
  <xs:complexContent>
    <xs:restriction base="AuthenticatorBaseType">
      <xs:sequence>
        <xs:choice>
          <xs:element ref="DigSig"/>
          <xs:element ref="ZeroKnowledge"/>
          <xs:element ref="SharedSecretChallengeResponse"/>
          <xs:element ref="SharedSecretDynamicPlaintext"/>
          <xs:element ref="AsymmetricDecryption"/>
          <xs:element ref="AsymmetricKeyAgreement"/>
        </xs:choice>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorTransportProtocolType">
  <xs:complexContent>
    <xs:restriction base="AuthenticatorTransportProtocolType">
      <xs:sequence>
        <xs:choice>
          <xs:element ref="SSL"/>
          <xs:element ref="MobileNetworkNoEncryption"/>
          <xs:element ref="MobileNetworkRadioEncryption"/>
          <xs:element ref="MobileNetworkEndToEndEncryption"/>
          <xs:element ref="WTLS"/>
        </xs:choice>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="OperationalProtectionType">
  <xs:complexContent>
    <xs:restriction base="OperationalProtectionType">
      <xs:sequence>
        <xs:element ref="SecurityAudit"/>
        <xs:element ref="DeactivationCallCenter"/>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="TechnicalProtectionBaseType">
  <xs:complexContent>
    <xs:restriction base="TechnicalProtectionBaseType">
      <xs:sequence>
        <xs:choice>
          <xs:element ref="PrivateKeyProtection"/>
          <xs:element ref="SecretKeyProtection"/>
        </xs:choice>
        <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
```

```
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="SecretKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyStorageType">
    <xs:complexContent>
      <xs:restriction base="KeyStorageType">
        <xs:attribute name="medium" use="required">
          <xs:simpleType>
            <xs:restriction base="mediumType">
              <xs:enumeration value="smartcard"/>
              <xs:enumeration value="MobileDevice"/>
              <xs:enumeration value="MobileAuthCard"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecurityAuditType">
    <xs:complexContent>
      <xs:restriction base="SecurityAuditType">
        <xs:sequence>
          <xs:element ref="SwitchAudit"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="IdentificationType">
    <xs:complexContent>
      <xs:restriction base="IdentificationType">
        <xs:sequence>
          <xs:element ref="PhysicalVerification"/>
          <xs:element ref="WrittenConsent"/>
          <xs:element ref="GoverningAgreements"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="nym">
          <xs:simpleType>
            <xs:restriction base="nymType">
              <xs:enumeration value="anonymity"/>
              <xs:enumeration value="verinymity"/>
              <xs:enumeration value="pseudonymity"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
```

```
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

8.A تخطيطة SAML لسياق الاستيقان MobileOneFactor-unreg

تحتوي هذه القائمة على تخطيطة صنف السياق SAML من أجل MobileOneFactorContract غير المسجل.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregister
ed"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
        Document identifier: saml-schema-authn-context-mobileonefactor-unreg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
```

```
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="ZeroKnowledge"/>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkNoEncryption"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
            <xs:element ref="WTLS"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
```

```
        <xs:restriction base="SecretKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

9.A تخطيطة SAML لسياق الاستيقان MobileTwoFactor-reg

تحتوي هذه القائمة على تخطيطة صنف السياق SAML من أجل MobileTwoFactorContract المسجل.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract
        Document identifier: saml-schema-authn-context-mobiletwofactor-reg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="ZeroKnowledge"/>
              <xs:element ref="SharedSecretChallengeResponse"/>
              <xs:element ref="SharedSecretDynamicPlaintext"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
              <xs:element ref="ComplexAuthenticator"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="ComplexAuthenticatorType">
      <xs:complexContent>
        <xs:restriction base="ComplexAuthenticatorType">
          <xs:sequence>
```

```
          <xs:choice>
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
          </xs:choice>
          <xs:element ref="Password"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkNoEncryption"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
            <xs:element ref="WTLS"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="SecretKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
```

```
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="PhysicalVerification"/>
            <xs:element ref="WrittenConsent"/>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="verinymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>

</xs:schema>
```

10.A تخطيطة SAML لسياق الاستيقان MobileTwoFactor-unreg

تحتوي هذه القائمة على تخطيطة صنف السياق SAML من أجل MobileTwoFactorUnregistered غير المسجل.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregister
ed"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered"
```

```
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
        Document identifier: saml-schema-authn-context-mobiletwofactor-unreg-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="DigSig"/>
              <xs:element ref="ZeroKnowledge"/>
              <xs:element ref="SharedSecretChallengeResponse"/>
              <xs:element ref="SharedSecretDynamicPlaintext"/>
              <xs:element ref="AsymmetricDecryption"/>
              <xs:element ref="AsymmetricKeyAgreement"/>
              <xs:element ref="ComplexAuthenticator"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="ComplexAuthenticatorType">
      <xs:complexContent>
        <xs:restriction base="ComplexAuthenticatorType">
          <xs:sequence>
            <xs:choice>
```

```
            <xs:element ref="SharedSecretChallengeResponse"/>
            <xs:element ref="SharedSecretDynamicPlaintext"/>
          </xs:choice>
          <xs:element ref="Password"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="SSL"/>
            <xs:element ref="MobileNetworkNoEncryption"/>
            <xs:element ref="MobileNetworkRadioEncryption"/>
            <xs:element ref="MobileNetworkEndToEndEncryption"/>
            <xs:element ref="WTLS"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="OperationalProtectionType">
    <xs:complexContent>
      <xs:restriction base="OperationalProtectionType">
        <xs:sequence>
          <xs:element ref="SecurityAudit"/>
          <xs:element ref="DeactivationCallCenter"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
            <xs:element ref="SecretKeyProtection"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="SecretKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
```

```
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="MobileDevice"/>
                <xs:enumeration value="MobileAuthCard"/>
                <xs:enumeration value="smartcard"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="SecurityAuditType">
      <xs:complexContent>
        <xs:restriction base="SecurityAuditType">
          <xs:sequence>
            <xs:element ref="SwitchAudit"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="IdentificationType">
      <xs:complexContent>
        <xs:restriction base="IdentificationType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="nym">
            <xs:simpleType>
              <xs:restriction base="nymType">
                <xs:enumeration value="anonymity"/>
                <xs:enumeration value="pseudonymity"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

11.A تخطيطة SAML لسياق الاستيقان NomadTelephony

تحتوي هذه القائمة على تخطيطة SAML لسياق الاستيقان NomadTelephony. والمهاتفة الترحلية تدل على أن الطرف الرئيسي "جوّال" (وربما يستعمل بطاقة هاتفية) ويستيقن ذاته بواسطة خط هاتفي ولاحقة مستعمل وعنصر كلمة سر.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
```

```
<xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

  <xs:annotation>
    <xs:documentation>
      Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony
      Document identifier: saml-schema-authn-context-nomad-telephony-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication_u99 context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:element ref="Password"/>
          <xs:element ref="SubscriberLineNumber"/>
          <xs:element ref="UserSuffix"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorTransportProtocolType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorTransportProtocolType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PSTN"/>
            <xs:element ref="ISDN"/>
            <xs:element ref="ADSL"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:redefine>
```

```
</xs:schema>
```

12.A تخطيطة SAML لسياق الاستيقان PersonalizedTelephony

توفر هذه القائمة تخطيطة SAML للاستيقان من أجل المهاتفة الشخصانية.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalizedTelephony
        Document identifier: saml-schema-authn-context-personal-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SubscriberLineNumber"/>
            <xs:element ref="UserSuffix"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

13.A تخطيطة SAML لسياق الاستيقان من أجل PGP

توفر هذه القائمة تخطيطة SAML للاستيقان من أجل سرية جيدة نوعاً ما (PGP).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
        Document identifier: saml-schema-authn-context-pgp-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
```

```
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:PGP"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

14.A تخطيطة SAML لسياق الاستيقان من أجل PPT

توفر هذه القائمة تخطيطة SAML للاستيقان من أجل نقل تحمية كلمة سر (PPT).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspor
t"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        Document identifier: saml-schema-authn-context-ppt-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
```

```
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="MobileNetworkRadioEncryption"/>
              <xs:element ref="MobileNetworkEndToEndEncryption"/>
              <xs:element ref="WTLS"/>
              <xs:element ref="IPSec"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

15.A تخطيطة SAML لسياق الاستيقان Password

تحتوي هذه القائمة على تخطيطة SAML لسياق الاستيقان بكلمة السر.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Password"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
```

```
  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
        Document identifier: saml-schema-authn-context-pword-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

16.A تخطيطة SAML لسياق الاستيقان PreviousSession

تحتوي هذه القائمة على تخطيطة SAML لسياق الاستيقان PreviousSession. وينطبق صنف الدورة السابقة عندما يكون طرف رئيسي قد استيقن نفسه لدى سلطة استيقان في لحظة ما سابقة مستخدماً أي سياق استيقان تعتمده سلطة الاستيقان تلك.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession"
  finalDefault="extension"
  blockDefault="substitution"
```

```
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
        Document identifier: saml-schema-authn-context-session-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="PreviousSession"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

17.A تخطيطة SAML لسياق الاستيقان Smartcard

هذه هي تخطيطة SAML لسياق الاستيقان بالبطاقة الذكية.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
```

```
    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
        Document identifier: saml-schema-authn-context-smartcard-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="Smartcard"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

18.A تخطيطة SAML لسياق الاستيقان SmartardPKI

هذه هي تخطيطة SAML لسياق الاستيقان ببطاقة ذكية (PKI).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
```

```
  <xs:annotation>
    <xs:documentation>
      Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
      Document identifier: saml-schema-authn-context-smartcardpki-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New authentication_u99 context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:complexContent>
      <xs:restriction base="PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:element ref="Smartcard"/>
          <xs:element ref="ActivationPin"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="AsymmetricDecryption"/>
```

```
            <xs:element ref="AsymmetricKeyAgreement"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:complexContent>
      <xs:restriction base="PrivateKeyProtectionType">
        <xs:sequence>
          <xs:element ref="KeyActivation"/>
          <xs:element ref="KeyStorage"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyActivationType">
    <xs:complexContent>
      <xs:restriction base="KeyActivationType">
        <xs:sequence>
          <xs:element ref="ActivationPin"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="KeyStorageType">
    <xs:complexContent>
      <xs:restriction base="KeyStorageType">
        <xs:attribute name="medium" use="required">
          <xs:simpleType>
            <xs:restriction base="mediumType">
              <xs:enumeration value="smartcard"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

 </xs:redefine>

</xs:schema>
```

19.A تخطيطة SAML لسياق الاستيقان SoftwarePKI

هذه هي تخطيطة SAML لسياق الاستيقان بالبرمجية PKI.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI
        Document identifier: saml-schema-authn-context-softwarepki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
```

```
      V2.0 (March, 2005):
        New authentication_u99 context class schema for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnContextDeclarationBaseType">
        <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TechnicalProtectionBaseType">
    <xs:complexContent>
      <xs:restriction base="TechnicalProtectionBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="PrivateKeyProtection"/>
          </xs:choice>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:complexContent>
      <xs:restriction base="PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:element ref="ActivationPin"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthenticatorBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthenticatorBaseType">
        <xs:sequence>
          <xs:choice>
            <xs:element ref="DigSig"/>
            <xs:element ref="AsymmetricDecryption"/>
            <xs:element ref="AsymmetricKeyAgreement"/>
          </xs:choice>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
    <xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
        <xs:restriction base="PrivateKeyProtectionType">
          <xs:sequence>
            <xs:element ref="KeyActivation"/>
            <xs:element ref="KeyStorage"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyActivationType">
      <xs:complexContent>
        <xs:restriction base="KeyActivationType">
          <xs:sequence>
            <xs:element ref="ActivationPin"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="KeyStorageType">
      <xs:complexContent>
        <xs:restriction base="KeyStorageType">
          <xs:attribute name="medium" use="required">
            <xs:simpleType>
              <xs:restriction base="mediumType">
                <xs:enumeration value="memory"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

20.A تخطيطة SAML لسياق الاستيقان SPKI

هذه هي تخطيطة SAML لسياق الاستيقان بالمفاتيح العمومية. وصنف السياق SPKI يدل على أن الطرف الرئيسي يستيقن ذاته بواسطة توقيع رقمي حيث أقرت صلاحية المفتاح عبر بنية تحتية بسيطة للمفتاح العمومي (SPKI).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
        Document identifier: saml-schema-authn-context-spki-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>
```

```
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

21.A تخطيطة SAML لسياق الاستيقان SRP

هذه هي تخطيطة SAML لسياق الاستيقان بكلمة سر بعيدة مأمونة (SRP) (انظر الطلب RFC 2945 للفريق IETF).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier:
urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
        Document identifier: saml-schema-authn-context-srp-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SharedSecretChallengeResponse"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
```

```
    </xs:complexType>

    <xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
        <xs:restriction base="SharedSecretChallengeResponseType">
          <xs:attribute name="method" type="xs:anyURI"
fixed="urn:ietf:rfc:2945"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

22.A تخطيطة SAML لسياق الاستيقان بالمهاتفة

هذه هي تخطيطة SAML لسياق الاستيقان بالمهاتفة. وهي تستعمل عندما يستيقن الطرف الرئيسي ذاته عبر تقديمه رقم هاتف ثابت، منقول عبر بروتوكول مهاتفة.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony
        Document identifier: saml-schema-authn-context-telephony-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
```

```
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="SubscriberLineNumber"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="PSTN"/>
              <xs:element ref="ISDN"/>
              <xs:element ref="ADSL"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

23.A تخطيطة SAML لسياق الاستيقان TimeSync

هذه هي تخطيطة SAML لسياق الاستيقان TimeSynchToken (إذنة متزامنة). وتنطبق الإذنة المتزامنة عندما يستيقن طرف رئيسي ذاته عبر إذنة متزامنة زمنياً.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken
        Document identifier: saml-schema-authn-context-timesync-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
```

```
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="xs:ID" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="AuthnMethodBaseType">
    <xs:complexContent>
      <xs:restriction base="AuthnMethodBaseType">
        <xs:sequence>
          <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
          <xs:element ref="Authenticator"/>
          <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="PrincipalAuthenticationMechanismType">
    <xs:complexContent>
      <xs:restriction base="PrincipalAuthenticationMechanismType">
        <xs:sequence>
          <xs:element ref="Token"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TokenType">
    <xs:complexContent>
      <xs:restriction base="TokenType">
        <xs:sequence>
          <xs:element ref="TimeSyncToken"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="TimeSyncTokenType">
    <xs:complexContent>
      <xs:restriction base="TimeSyncTokenType">
        <xs:attribute name="DeviceType" use="required">
          <xs:simpleType>
            <xs:restriction base="DeviceTypeType">
              <xs:enumeration value="hardware"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>

        <xs:attribute name="SeedLength" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="64"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>

        <xs:attribute name="DeviceInHand" use="required">
          <xs:simpleType>
            <xs:restriction base="booleanType">
              <xs:enumeration value="true"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
  </xs:redefine>

</xs:schema>
```

24.A تخطيطة SAML لسياق استيقان types

هذه هي تخطيطة SAML لسياق الاستيقان بالأنماط.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
      Document identifier: saml-schema-authn-context-types-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
          V2.0 (March, 2005):
          New core authentication context schema types for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:element name="AuthenticationContextDeclaration"
type="AuthnContextDeclarationBaseType">
    <xs:annotation>
      <xs:documentation>
        A particular assertion_u111 on an identity
        provider's part with respect to the authentication
        context associated with an authentication assertion.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Identification" type="IdentificationType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that describe the
        processes and mechanisms
        the Authentication Authority uses to initially create
        an association between_u97 ? Principal
        and the identity (or name) by which the Principal will
        be known
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PhysicalVerification">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that identification has been
        performed in a physical
        face-to-face meeting with the principal and not in an
        online manner.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:attribute name="credentialLevel">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="primary"/>
            <xs:enumeration value="secondary"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
```

```
</xs:element>

<xs:element name="WrittenConsent" type="ExtensionOnlyType"/>

<xs:element name="TechnicalProtection" type="TechnicalProtectionBaseType">
  <xs:annotation>
    <xs:documentation>
      Refers to those characterstics that describe how the
      'secret' (the knowledge or possession
      of which allows the Principal to authenticate to the
      Authentication Authority) is kept secure
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SecretKeyProtection" type="SecretKeyProtectionType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 the types and strengths of
      facilities
      of a UA used to protect a shared secret key from
      unauthorized access and/or use.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 the types and strengths of
      facilities
      of a UA used to protect a private key from
      unauthorized access and/or use.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="KeyActivation" type="KeyActivationType">
  <xs:annotation>
    <xs:documentation>The actions that must be performed
      before the private key_u99 can be used. </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="KeySharing" type="KeySharingType">
  <xs:annotation>
    <xs:documentation>Whether or not the private key_u105 is shared
      with the certificate authority.</xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="KeyStorage" type="KeyStorageType">
  <xs:annotation>
    <xs:documentation>
      In which medium is the_u107 key stored.
      memory - the key is stored in memory.
      smartcard - the key is_u115 stored in a smartcard.
      token - the key is stored in a hardware token.
      MobileDevice - the key_u105 is stored in a mobile device.
      MobileAuthCard - the key is stored in a mobile
      authentication card.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SubscriberLineNumber" type="ExtensionOnlyType"/>
<xs:element name="UserSuffix" type="ExtensionOnlyType"/>

<xs:element name="Password" type="PasswordType">
  <xs:annotation>
    <xs:documentation>
```

```
      This element indicates_u116 that a password (or passphrase)
      has been used to
      authenticate the Principal to a remote system.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationPin" type="ActivationPinType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that a Pin (Personal
      Identification Number)_u104 has been used to authenticate the Principal
      to some local system in order to activate a key.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Token" type="TokenType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that a hardware or software
      token is used
      as a method of identifying the Principal.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="TimeSyncToken" type="TimeSyncTokenType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that a time synchronization
      token is used to identify the Principal. hardware -
      the time synchonization
      token has been implemented in hardware. software - the
      time synchronization
      token has been implemented in software. SeedLength -
      the length, in bits, of the
      random seed used in the time synchronization token.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Smartcard" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that a smartcard is used to
      identify the Principal.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Length" type="LengthType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 the minimum and/or maximum
      ASCII length of the password which is enforced (by the UA or the
      IdP). In other words, this is the minimum and/or maximum number of
      ASCII characters required to represent a valid password.
      min - the minimum number of ASCII characters required
      in a valid password, as enforced by the UA or the IdP.
      max - the maximum number of ASCII characters required
      in a valid password, as enforced by the UA or the IdP.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimit" type="ActivationLimitType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 the length of time for which an
      PIN-based authentication is valid.
```

```
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Generation">
    <xs:annotation>
      <xs:documentation>
        Indicates whether the password was chosen by the
        Principal or auto-supplied by the Authentication Authority.
        principal chosen - the Principal is allowed to choose
        the value of the password. This is true even if
        the initial password is chosen at random by the UA or
        the IdP and the Principal is then free to change
        the password.
        automatic - the password is chosen by the UA or the
        IdP to be cryptographically strong in some sense,
        or to satisfy certain password rules, and that the
        Principal is not free to change it or to choose a new password.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType>
      <xs:attribute name="mechanism" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="principalchosen"/>
            <xs:enumeration value="automatic"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="AuthnMethod" type="AuthnMethodBaseType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that define the
        mechanisms by which the Principal authenticates to the Authentication
        Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PrincipalAuthenticationMechanism"
type="PrincipalAuthenticationMechanismType">
    <xs:annotation>
      <xs:documentation>
        The method that a Principal employs to perform
        authentication to local system components.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Authenticator" type="AuthenticatorBaseType">
    <xs:annotation>
      <xs:documentation>
        The method applied to validate a principal's
        authentication across a network
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ComplexAuthenticator" type="ComplexAuthenticatorType">
    <xs:annotation>
      <xs:documentation>
        Supports Authenticators with nested combinations of
        additional complexity.
      </xs:documentation>
    </xs:annotation>
  </xs:element>
```

```
  <xs:element name="PreviousSession" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        Indicates that the Principal has been strongly
        authenticated in a previous session during which the IdP has set a
        cookie in the UA. During the present session the Principal has only
        been authenticated by the UA returning the cookie to the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ResumeSession" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        Rather like PreviousSession but using stronger
        security. A secret that was established in a previous session with
        the Authentication Authority has been cached by the local system and
        is now re-used (e.g. a_u77 master Secret is used to derive new session
        keys in TLS, SSL, WTLS).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ZeroKnowledge" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Principal has been
        authenticated by a zero knowledge technique as specified in ISO/IEC
        9798-5.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SharedSecretChallengeResponse"
type="SharedSecretChallengeResponseType"/>

  <xs:complexType name="SharedSecretChallengeResponseType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Principal has been
        authenticated by a challenge-response protocol utilizing shared secret
        keys and symmetric cryptography.
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="method" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="DigSig" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Principal has been
        authenticated by a mechanism which involves the Principal computing a
        digital signature over_u97 at least challenge data provided by the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricDecryption" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a_u112 Private key but it is used
        in decryption mode, rather than signature mode. For example, the
        Authentication Authority generates a secret and encrypts it using the
        local system's public key: the local system then proves it has
        decrypted the secret.
      </xs:documentation>
    </xs:annotation>
  </xs:element>
```

```
  <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a_u112 Private key and uses it for
        shared secret key agreement with the Authentication Authority (e.g.
        via Diffie Helman).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:complexType name="PublicKeyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="keyValidation" use="optional"/>
  </xs:complexType>

  <xs:element name="IPAddress" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Principal has been
        authenticated through connection from a particular IP address.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SharedSecretDynamicPlaintext" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        The local system and Authentication Authority
        share a secret key. The local system uses this to encrypt a
        randomised string to pass to the Authentication Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AuthenticatorTransportProtocol"
type="AuthenticatorTransportProtocolType">
    <xs:annotation>
      <xs:documentation>
        The protocol across which Authenticator information is
        transferred to an Authentication Authority verifier.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="HTTP" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Authenticator has been
        transmitted using bare_u72 HTTP utilizing no additional security
        protocols.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="IPSec" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Authenticator has been
        transmitted using a transport mechanism protected by an IPSEC session.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="WTLS" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates_u116 that the Authenticator has been
        transmitted using a transport mechanism protected by a WTLS session.
```

```
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="MobileNetworkNoEncryption" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that the Authenticator has been
      transmitted solely across a mobile network using no additional
      security mechanism.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="MobileNetworkRadioEncryption" type="ExtensionOnlyType"/>
<xs:element name="MobileNetworkEndToEndEncryption" type="ExtensionOnlyType"/>

<xs:element name="SSL" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that the Authenticator has been
      transmitted using a transport mechnanism protected by an SSL or TLS
      session.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="PSTN" type="ExtensionOnlyType"/>
<xs:element name="ISDN" type="ExtensionOnlyType"/>
<xs:element name="ADSL" type="ExtensionOnlyType"/>

<xs:element name="OperationalProtection" type="OperationalProtectionType">
  <xs:annotation>
    <xs:documentation>
      Refers to those characteristics that describe
      procedural security controls employed by the Authentication Authority.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SecurityAudit" type="SecurityAuditType"/>
<xs:element name="SwitchAudit" type="ExtensionOnlyType"/>
<xs:element name="DeactivationCallCenter" type="ExtensionOnlyType"/>

<xs:element name="GoverningAgreements" type="GoverningAgreementsType">
  <xs:annotation>
    <xs:documentation>
      Provides a mechanism for linking to external (likely
      human readable) documents in which additional business agreements,
      (e.g. liability constraints, obligations, etc.) can be placed.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="GoverningAgreementRef" type="GoverningAgreementRefType"/>

<xs:simpleType name="nymType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="anonymity"/>
    <xs:enumeration value="verinymity"/>
    <xs:enumeration value="pseudonymity"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AuthnContextDeclarationBaseType">
  <xs:sequence>
    <xs:element ref="Identification" minOccurs="0"/>
    <xs:element ref="TechnicalProtection" minOccurs="0"/>
    <xs:element ref="OperationalProtection" minOccurs="0"/>
    <xs:element ref="AuthnMethod" minOccurs="0"/>
    <xs:element ref="GoverningAgreements" minOccurs="0"/>
```

```
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="ID" type="xs:ID" use="optional"/>
</xs:complexType>

<xs:complexType name="IdentificationType">
  <xs:sequence>
    <xs:element ref="PhysicalVerification" minOccurs="0"/>
    <xs:element ref="WrittenConsent" minOccurs="0"/>
    <xs:element ref="GoverningAgreements" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="nym" type="nymType">
    <xs:annotation>
      <xs:documentation>
        This attribute indicates whether or not the
        Identification mechanisms allow the actions of the Principal to be
        linked to an actual end user.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>
</xs:complexType>

<xs:complexType name="TechnicalProtectionBaseType">
  <xs:sequence>
    <xs:choice minOccurs="0">
      <xs:element ref="PrivateKeyProtection"/>
      <xs:element ref="SecretKeyProtection"/>
    </xs:choice>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="OperationalProtectionType">
  <xs:sequence>
    <xs:element ref="SecurityAudit" minOccurs="0"/>
    <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AuthnMethodBaseType">
  <xs:sequence>
    <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
    <xs:element ref="Authenticator" minOccurs="0"/>
    <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="GoverningAgreementsType">
  <xs:sequence>
    <xs:element ref="GoverningAgreementRef" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="GoverningAgreementRefType">
  <xs:attribute name="governingAgreementRef" type="xs:anyURI" use="required"/>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
  <xs:sequence>
    <xs:element ref="Password" minOccurs="0"/>
    <xs:element ref="RestrictedPassword" minOccurs="0"/>
    <xs:element ref="Token" minOccurs="0"/>
    <xs:element ref="Smartcard" minOccurs="0"/>
    <xs:element ref="ActivationPin" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="preauth" type="xs:integer" use="optional"/>
</xs:complexType>
```

```
<xs:group name="AuthenticatorChoiceGroup">
  <xs:choice>
    <xs:element ref="PreviousSession"/>
    <xs:element ref="ResumeSession"/>
    <xs:element ref="DigSig"/>
    <xs:element ref="Password"/>
    <xs:element ref="RestrictedPassword"/>
    <xs:element ref="ZeroKnowledge"/>
    <xs:element ref="SharedSecretChallengeResponse"/>
    <xs:element ref="SharedSecretDynamicPlaintext"/>
    <xs:element ref="IPAddress"/>
    <xs:element ref="AsymmetricDecryption"/>
    <xs:element ref="AsymmetricKeyAgreement"/>
    <xs:element ref="SubscriberLineNumber"/>
    <xs:element ref="UserSuffix"/>
    <xs:element ref="ComplexAuthenticator"/>
  </xs:choice>
</xs:group>

<xs:group name="AuthenticatorSequenceGroup">
  <xs:sequence>
    <xs:element ref="PreviousSession" minOccurs="0"/>
    <xs:element ref="ResumeSession" minOccurs="0"/>
    <xs:element ref="DigSig" minOccurs="0"/>
    <xs:element ref="Password" minOccurs="0"/>
    <xs:element ref="RestrictedPassword" minOccurs="0"/>
    <xs:element ref="ZeroKnowledge" minOccurs="0"/>
    <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
    <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
    <xs:element ref="IPAddress" minOccurs="0"/>
    <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
    <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
    <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
    <xs:element ref="UserSuffix" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:group>

<xs:complexType name="AuthenticatorBaseType">
  <xs:sequence>
    <xs:group ref="AuthenticatorChoiceGroup"/>
    <xs:group ref="AuthenticatorSequenceGroup"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ComplexAuthenticatorType">
  <xs:sequence>
    <xs:group ref="AuthenticatorChoiceGroup"/>
    <xs:group ref="AuthenticatorSequenceGroup"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AuthenticatorTransportProtocolType">
  <xs:sequence>
    <xs:choice minOccurs="0">
      <xs:element ref="HTTP"/>
      <xs:element ref="SSL"/>
      <xs:element ref="MobileNetworkNoEncryption"/>
      <xs:element ref="MobileNetworkRadioEncryption"/>
      <xs:element ref="MobileNetworkEndToEndEncryption"/>
      <xs:element ref="WTLS"/>
      <xs:element ref="IPSec"/>
      <xs:element ref="PSTN"/>
      <xs:element ref="ISDN"/>
      <xs:element ref="ADSL"/>
    </xs:choice>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
```

```
  <xs:complexType name="KeyActivationType">
    <xs:sequence>
      <xs:element ref="ActivationPin" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="KeySharingType">
    <xs:attribute name="sharing" type="xs:boolean" use="required"/>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:sequence>
      <xs:element ref="KeyActivation" minOccurs="0"/>
      <xs:element ref="KeyStorage" minOccurs="0"/>
      <xs:element ref="KeySharing" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="PasswordType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ExternalVerification" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="RestrictedPassword" type="RestrictedPasswordType"/>

  <xs:complexType name="RestrictedPasswordType">
    <xs:complexContent>
      <xs:restriction base="PasswordType">
        <xs:sequence>
          <xs:element name="Length" type="RestrictedLengthType" minOccurs="1"/>
          <xs:element ref="Generation" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ExternalVerification" type="xs:anyURI"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="RestrictedLengthType">
    <xs:complexContent>
      <xs:restriction base="LengthType">
        <xs:attribute name="min" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="3"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="max" type="xs:integer" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="ActivationPinType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="ActivationLimit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
```

```
<xs:element name="Alphabet" type="AlphabetType"/>
<xs:complexType name="AlphabetType">
  <xs:attribute name="requiredChars" type="xs:string" use="required"/>
  <xs:attribute name="excludedChars" type="xs:string" use="optional"/>
  <xs:attribute name="case" type="xs:string" use="optional"/>
</xs:complexType>

<xs:complexType name="TokenType">
  <xs:sequence>
    <xs:element ref="TimeSyncToken"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:simpleType name="DeviceTypeType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="hardware"/>
    <xs:enumeration value="software"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="booleanType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="true"/>
    <xs:enumeration value="false"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="TimeSyncTokenType">
  <xs:attribute name="DeviceType" type="DeviceTypeType" use="required"/>
  <xs:attribute name="SeedLength" type="xs:integer" use="required"/>
  <xs:attribute name="DeviceInHand" type="booleanType" use="required"/>
</xs:complexType>

<xs:complexType name="ActivationLimitType">
  <xs:choice>
    <xs:element ref="ActivationLimitDuration"/>
    <xs:element ref="ActivationLimitUsages"/>
    <xs:element ref="ActivationLimitSession"/>
  </xs:choice>
</xs:complexType>

<xs:element name="ActivationLimitDuration" type="ActivationLimitDurationType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that the Key Activation Limit is
      defined as a specific duration of time.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimitUsages" type="ActivationLimitUsagesType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that the Key Activation Limit is
      defined as a number of_u117 usages.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimitSession" type="ActivationLimitSessionType">
  <xs:annotation>
    <xs:documentation>
      This element indicates_u116 that the Key Activation Limit is
      the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:complexType name="ActivationLimitDurationType">
  <xs:attribute name="duration" type="xs:duration" use="required"/>
```

```
  </xs:complexType>

  <xs:complexType name="ActivationLimitUsagesType">
    <xs:attribute name="number" type="xs:integer" use="required"/>
  </xs:complexType>

  <xs:complexType name="ActivationLimitSessionType"/>

  <xs:complexType name="LengthType">
    <xs:attribute name="min" type="xs:integer" use="required"/>
    <xs:attribute name="max" type="xs:integer" use="optional"/>
  </xs:complexType>

  <xs:simpleType name="mediumType">
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="memory"/>
      <xs:enumeration value="smartcard"/>
      <xs:enumeration value="token"/>
      <xs:enumeration value="MobileDevice"/>
      <xs:enumeration value="MobileAuthCard"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="KeyStorageType">
    <xs:attribute name="medium" type="mediumType" use="required"/>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:sequence>
      <xs:element ref="KeyActivation" minOccurs="0"/>
      <xs:element ref="KeyStorage" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="SecurityAuditType">
    <xs:sequence>
      <xs:element ref="SwitchAudit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ExtensionOnlyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0"  maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="Extension" type="ExtensionType"/>

  <xs:complexType name="ExtensionType">
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
```

25.A تخطيطة SAML لسياق الاستيقان X.509

هذه هي تخطيطة SAML لسياق الاستيقان بالتوصية X.509.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"
  finalDefault="extension"
```

```
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:X509
        Document identifier: saml-schema-authn-context-x509-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
```

```
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

26.A تخطيطة SAML لسياق الاستيقان XMLDSig

هذه هي تخطيطة SAML لسياق الاستيقان بالتوقيع الرقمي في اللغة XML.

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
        Document identifier: saml-schema-authn-context-xmldsig-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
```

```
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
fixed="urn:ietf:rfc:3075"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

27.A تخطيطة SAML للزبون ECP

هذه هي التخطيطة SAML التي تهيئ قائمة جانبية الزبون/الوكيل المفوّض المعزّز (ECP).

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:ecp="urn:oasis:names:tc:SAML:2.0:profiles:SSO:ecp"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
        schemaLocation="saml-schema-protocol-2.0.xsd"/>
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://schemas.xmlsoap.org/soap/envelope/"
        schemaLocation="http://schemas.xmlsoap.org/soap/envelope/"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-ecp-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Custom schema for ECP profile, first published in SAML 2.0.
        </documentation>
    </annotation>

    <element name="Request" type="ecp:RequestType"/>
    <complexType name="RequestType">
        <sequence>
            <element ref="saml:Issuer"/>
            <element ref="samlp:IDPList" minOccurs="0"/>
        </sequence>
        <attribute ref="S:mustUnderstand" use="required"/>
        <attribute ref="S:actor" use="required"/>
        <attribute name="ProviderName" type="string" use="optional"/>
        <attribute name="IsPassive" type="boolean" use="optional"/>
    </complexType>

    <element name="Response" type="ecp:ResponseType"/>
    <complexType name="ResponseType">
        <attribute ref="S:mustUnderstand" use="required"/>
        <attribute ref="S:actor" use="required"/>
```

```
        <attribute name="AssertionConsumerServiceURL" type="anyURI"
use="required"/>
    </complexType>

    <element name="RelayState" type="ecp:RelayStateType"/>
    <complexType name="RelayStateType">
        <simpleContent>
            <extension base="string">
                <attribute ref="S:mustUnderstand" use="required"/>
                <attribute ref="S:actor" use="required"/>
            </extension>
        </simpleContent>
    </complexType>
</schema>
```

28.A تخطيطة SAML للمعطيات الشرحية

هذه هي التخطيطة SAML التي تميئ المعطيات الشرحية.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <import namespace="http://www.w3.org/2001/04/xmlenc#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-
schema.xsd"/>
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://www.w3.org/XML/1998/namespace"
        schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-metadata-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Schema for SAML metadata, first published in SAML 2.0.
        </documentation>
    </annotation>

    <simpleType name="entityIDType">
        <restriction base="anyURI">
            <maxLength value="1024"/>
        </restriction>
    </simpleType>
    <complexType name="localizedNameType">
        <simpleContent>
            <extension base="string">
                <attribute ref="xml:lang" use="required"/>
            </extension>
        </simpleContent>
    </complexType>
    <complexType name="localizedURIType">
        <simpleContent>
            <extension base="anyURI">
                <attribute ref="xml:lang" use="required"/>
            </extension>
```

```
        </simpleContent>
    </complexType>

    <element name="Extensions" type="md:ExtensionsType"/>
    <complexType final="#all" name="ExtensionsType">
        <sequence>
            <any namespace="##other" processContents="lax"
maxOccurs="unbounded"/>
        </sequence>
    </complexType>

    <complexType name="EndpointType">
        <sequence>
            <any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="Binding" type="anyURI" use="required"/>
        <attribute name="Location" type="anyURI" use="required"/>
        <attribute name="ResponseLocation" type="anyURI" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>

    <complexType name="IndexedEndpointType">
        <complexContent>
            <extension base="md:EndpointType">
                <attribute name="index" type="unsignedShort" use="required"/>
                <attribute name="isDefault" type="boolean" use="optional"/>
            </extension>
        </complexContent>
    </complexType>

    <element name="EntitiesDescriptor" type="md:EntitiesDescriptorType"/>
    <complexType name="EntitiesDescriptorType">
        <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <choice minOccurs="1" maxOccurs="unbounded">
                <element ref="md:EntityDescriptor"/>
                <element ref="md:EntitiesDescriptor"/>
            </choice>
        </sequence>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="ID" type="ID" use="optional"/>
        <attribute name="Name" type="string" use="optional"/>
    </complexType>

    <element name="EntityDescriptor" type="md:EntityDescriptorType"/>
    <complexType name="EntityDescriptorType">
        <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <choice>
                <choice maxOccurs="unbounded">
                    <element ref="md:RoleDescriptor"/>
                    <element ref="md:IDPSSODescriptor"/>
                    <element ref="md:SPSSODescriptor"/>
                    <element ref="md:AuthnAuthorityDescriptor"/>
                    <element ref="md:AttributeAuthorityDescriptor"/>
                    <element ref="md:PDPDescriptor"/>
                </choice>
                <element ref="md:AffiliationDescriptor"/>
            </choice>
            <element ref="md:Organization" minOccurs="0"/>
            <element ref="md:ContactPerson" minOccurs="0" maxOccurs="unbounded"/>
            <element ref="md:AdditionalMetadataLocation" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="entityID" type="md:entityIDType" use="required"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
```

```
        <attribute name="ID" type="ID" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>

    <element name="Organization" type="md:OrganizationType"/>
    <complexType name="OrganizationType">
        <sequence>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:OrganizationName" maxOccurs="unbounded"/>
            <element ref="md:OrganizationDisplayName" maxOccurs="unbounded"/>
            <element ref="md:OrganizationURL" maxOccurs="unbounded"/>
        </sequence>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="OrganizationName" type="md:localizedNameType"/>
    <element name="OrganizationDisplayName" type="md:localizedNameType"/>
    <element name="OrganizationURL" type="md:localizedURIType"/>
    <element name="ContactPerson" type="md:ContactType"/>
    <complexType name="ContactType">
        <sequence>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:Company" minOccurs="0"/>
            <element ref="md:GivenName" minOccurs="0"/>
            <element ref="md:SurName" minOccurs="0"/>
            <element ref="md:EmailAddress" minOccurs="0" maxOccurs="unbounded"/>
            <element ref="md:TelephoneNumber" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="contactType" type="md:ContactTypeType" use="required"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="Company" type="string"/>
    <element name="GivenName" type="string"/>
    <element name="SurName" type="string"/>
    <element name="EmailAddress" type="anyURI"/>
    <element name="TelephoneNumber" type="string"/>
    <simpleType name="ContactTypeType">
        <restriction base="string">
            <enumeration value="technical"/>
            <enumeration value="support"/>
            <enumeration value="administrative"/>
            <enumeration value="billing"/>
            <enumeration value="other"/>
        </restriction>
    </simpleType>

    <element name="AdditionalMetadataLocation"
type="md:AdditionalMetadataLocationType"/>
    <complexType name="AdditionalMetadataLocationType">
        <simpleContent>
            <extension base="anyURI">
                <attribute name="namespace" type="anyURI" use="required"/>
            </extension>
        </simpleContent>
    </complexType>

    <element name="RoleDescriptor" type="md:RoleDescriptorType"/>
    <complexType name="RoleDescriptorType" abstract="true">
        <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:KeyDescriptor" minOccurs="0" maxOccurs="unbounded"/>
            <element ref="md:Organization" minOccurs="0"/>
            <element ref="md:ContactPerson" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="ID" type="ID" use="optional"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="protocolSupportEnumeration" type="md:anyURIListType"
use="required"/>
        <attribute name="errorURL" type="anyURI" use="optional"/>
```

```
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <simpleType name="anyURIListType">
        <list itemType="anyURI"/>
    </simpleType>

    <element name="KeyDescriptor" type="md:KeyDescriptorType"/>
    <complexType name="KeyDescriptorType">
        <sequence>
            <element ref="ds:KeyInfo"/>
            <element ref="md:EncryptionMethod" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="use" type="md:KeyTypes" use="optional"/>
    </complexType>
    <simpleType name="KeyTypes">
        <restriction base="string">
            <enumeration value="encryption"/>
            <enumeration value="signing"/>
        </restriction>
    </simpleType>
    <element name="EncryptionMethod" type="xenc:EncryptionMethodType"/>

    <complexType name="SSODescriptorType" abstract="true">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:ArtifactResolutionService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:SingleLogoutService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:ManageNameIDService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="ArtifactResolutionService" type="md:IndexedEndpointType"/>
    <element name="SingleLogoutService" type="md:EndpointType"/>
    <element name="ManageNameIDService" type="md:EndpointType"/>
    <element name="NameIDFormat" type="anyURI"/>

    <element name="IDPSSODescriptor" type="md:IDPSSODescriptorType"/>
    <complexType name="IDPSSODescriptorType">
        <complexContent>
            <extension base="md:SSODescriptorType">
                <sequence>
                    <element ref="md:SingleSignOnService" maxOccurs="unbounded"/>
                    <element ref="md:NameIDMappingService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:AttributeProfile" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
                <attribute name="WantAuthnRequestsSigned" type="boolean"
use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="SingleSignOnService" type="md:EndpointType"/>
    <element name="NameIDMappingService" type="md:EndpointType"/>
    <element name="AssertionIDRequestService" type="md:EndpointType"/>
    <element name="AttributeProfile" type="anyURI"/>

    <element name="SPSSODescriptor" type="md:SPSSODescriptorType"/>
    <complexType name="SPSSODescriptorType">
```

```
        <complexContent>
            <extension base="md:SSODescriptorType">
                <sequence>
                    <element ref="md:AssertionConsumerService"
maxOccurs="unbounded"/>
                    <element ref="md:AttributeConsumingService" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
                <attribute name="AuthnRequestsSigned" type="boolean"
use="optional"/>
                <attribute name="WantAssertionsSigned" type="boolean"
use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="AssertionConsumerService" type="md:IndexedEndpointType"/>
    <element name="AttributeConsumingService"
type="md:AttributeConsumingServiceType"/>
    <complexType name="AttributeConsumingServiceType">
        <sequence>
            <element ref="md:ServiceName" maxOccurs="unbounded"/>
            <element ref="md:ServiceDescription" minOccurs="0"
maxOccurs="unbounded"/>
            <element ref="md:RequestedAttribute" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="index" type="unsignedShort" use="required"/>
        <attribute name="isDefault" type="boolean" use="optional"/>
    </complexType>
    <element name="ServiceName" type="md:localizedNameType"/>
    <element name="ServiceDescription" type="md:localizedNameType"/>
    <element name="RequestedAttribute" type="md:RequestedAttributeType"/>
    <complexType name="RequestedAttributeType">
        <complexContent>
            <extension base="saml:AttributeType">
                <attribute name="isRequired" type="boolean" use="optional"/>
            </extension>
        </complexContent>
    </complexType>

    <element name="AuthnAuthorityDescriptor"
type="md:AuthnAuthorityDescriptorType"/>
    <complexType name="AuthnAuthorityDescriptorType">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:AuthnQueryService" maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="AuthnQueryService" type="md:EndpointType"/>

    <element name="PDPDescriptor" type="md:PDPDescriptorType"/>
    <complexType name="PDPDescriptorType">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:AuthzService" maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="AuthzService" type="md:EndpointType"/>
```

```
    <element name="AttributeAuthorityDescriptor"
type="md:AttributeAuthorityDescriptorType"/>
    <complexType name="AttributeAuthorityDescriptorType">
        <complexContent>
            <extension base="md:RoleDescriptorType">
                <sequence>
                    <element ref="md:AttributeService" maxOccurs="unbounded"/>
                    <element ref="md:AssertionIDRequestService" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:NameIDFormat" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="md:AttributeProfile" minOccurs="0"
maxOccurs="unbounded"/>
                    <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="AttributeService" type="md:EndpointType"/>

    <element name="AffiliationDescriptor" type="md:AffiliationDescriptorType"/>
    <complexType name="AffiliationDescriptorType">
        <sequence>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="md:Extensions" minOccurs="0"/>
            <element ref="md:AffiliateMember" maxOccurs="unbounded"/>
            <element ref="md:KeyDescriptor" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="affiliationOwnerID" type="md:entityIDType"
use="required"/>
        <attribute name="validUntil" type="dateTime" use="optional"/>
        <attribute name="cacheDuration" type="duration" use="optional"/>
        <attribute name="ID" type="ID" use="optional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
    </complexType>
    <element name="AffiliateMember" type="md:entityIDType"/>
</schema>
```

29.A تخطيطة البروتوكول SAML

هذه هي قائمة التخطيطة للبروتوكول SAML.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <import namespace="urn:oasis:names:tc:SAML:2.0:assertion"
        schemaLocation="saml-schema-assertion-2.0.xsd"/>
    <import namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"/>
    <annotation>
        <documentation>
            Document identifier: saml-schema-protocol-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V1.0 (November, 2002):
              Initial Standard_u83 schema.
            V1.1 (September, 2003):
              Updates within the same V1.0 namespace.
```

```
            V2.0 (March, 2005):
              New protocol schema based in a SAML V2.0 namespace.
     </documentation>
    </annotation>
    <complexType name="RequestAbstractType" abstract="true">
        <sequence>
            <element ref="saml:Issuer" minOccurs="0"/>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="samlp:Extensions" minOccurs="0"/>
        </sequence>
        <attribute name="ID" type="ID" use="required"/>
        <attribute name="Version" type="string" use="required"/>
        <attribute name="IssueInstant" type="dateTime" use="required"/>
        <attribute name="Destination" type="anyURI" use="optional"/>
          <attribute name="Consent" type="anyURI" use="optional"/>
    </complexType>
    <element name="Extensions" type="samlp:ExtensionsType"/>
    <complexType name="ExtensionsType">
        <sequence>
            <any namespace="##other" processContents="lax"
maxOccurs="unbounded"/>
        </sequence>
    </complexType>
    <complexType name="StatusResponseType">
          <sequence>
            <element ref="saml:Issuer" minOccurs="0"/>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="samlp:Extensions" minOccurs="0"/>
            <element ref="samlp:Status"/>
          </sequence>
          <attribute name="ID" type="ID" use="required"/>
          <attribute name="InResponseTo" type="NCName" use="optional"/>
          <attribute name="Version" type="string" use="required"/>
          <attribute name="IssueInstant" type="dateTime" use="required"/>
          <attribute name="Destination" type="anyURI" use="optional"/>
          <attribute name="Consent" type="anyURI" use="optional"/>
    </complexType>
    <element name="Status" type="samlp:StatusType"/>
    <complexType name="StatusType">
        <sequence>
            <element ref="samlp:StatusCode"/>
            <element ref="samlp:StatusMessage" minOccurs="0"/>
            <element ref="samlp:StatusDetail" minOccurs="0"/>
        </sequence>
    </complexType>
    <element name="StatusCode" type="samlp:StatusCodeType"/>
    <complexType name="StatusCodeType">
        <sequence>
            <element ref="samlp:StatusCode" minOccurs="0"/>
        </sequence>
        <attribute name="Value" type="anyURI" use="required"/>
    </complexType>
    <element name="StatusMessage" type="string"/>
    <element name="StatusDetail" type="samlp:StatusDetailType"/>
    <complexType name="StatusDetailType">
        <sequence>
            <any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
    </complexType>
    <element name="AssertionIDRequest" type="samlp:AssertionIDRequestType"/>
    <complexType name="AssertionIDRequestType">
          <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <element ref="saml:AssertionIDRef" maxOccurs="unbounded"/>
                </sequence>
            </extension>
          </complexContent>
    </complexType>
    <element name="SubjectQuery" type="samlp:SubjectQueryAbstractType"/>
```

```
    <complexType name="SubjectQueryAbstractType" abstract="true">
          <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <element ref="saml:Subject"/>
                </sequence>
            </extension>
          </complexContent>
    </complexType>
    <element name="AuthnQuery" type="samlp:AuthnQueryType"/>
    <complexType name="AuthnQueryType">
        <complexContent>
            <extension base="samlp:SubjectQueryAbstractType">
                <sequence>
                    <element ref="samlp:RequestedAuthnContext" minOccurs="0"/>
                </sequence>
                <attribute name="SessionIndex" type="string" use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="RequestedAuthnContext"
type="samlp:RequestedAuthnContextType"/>
    <complexType name="RequestedAuthnContextType">
        <choice>
            <element ref="saml:AuthnContextClassRef" maxOccurs="unbounded"/>
            <element ref="saml:AuthnContextDeclRef" maxOccurs="unbounded"/>
        </choice>
        <attribute name="Comparison" type="samlp:AuthnContextComparisonType"
use="optional"/>
    </complexType>
    <simpleType name="AuthnContextComparisonType">
        <restriction base="string">
            <enumeration value="exact"/>
            <enumeration value="minimum"/>
            <enumeration value="maximum"/>
            <enumeration value="better"/>
        </restriction>
    </simpleType>
    <element name="AttributeQuery" type="samlp:AttributeQueryType"/>
    <complexType name="AttributeQueryType">
        <complexContent>
            <extension base="samlp:SubjectQueryAbstractType">
                <sequence>
                    <element ref="saml:Attribute" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="AuthzDecisionQuery" type="samlp:AuthzDecisionQueryType"/>
    <complexType name="AuthzDecisionQueryType">
        <complexContent>
            <extension base="samlp:SubjectQueryAbstractType">
                <sequence>
                    <element ref="saml:Action" maxOccurs="unbounded"/>
                    <element ref="saml:Evidence" minOccurs="0"/>
                </sequence>
                <attribute name="Resource" type="anyURI" use="required"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="AuthnRequest" type="samlp:AuthnRequestType"/>
    <complexType name="AuthnRequestType">
        <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <element ref="saml:Subject" minOccurs="0"/>
                    <element ref="samlp:NameIDPolicy" minOccurs="0"/>
                    <element ref="saml:Conditions" minOccurs="0"/>
                    <element ref="samlp:RequestedAuthnContext" minOccurs="0"/>
                    <element ref="samlp:Scoping" minOccurs="0"/>
```

```
                </sequence>
                <attribute name="ForceAuthn" type="boolean" use="optional"/>
                <attribute name="IsPassive" type="boolean" use="optional"/>
                <attribute name="ProtocolBinding" type="anyURI" use="optional"/>
                <attribute name="AssertionConsumerServiceIndex"
type="unsignedShort" use="optional"/>
                <attribute name="AssertionConsumerServiceURL" type="anyURI"
use="optional"/>
                <attribute name="AttributeConsumingServiceIndex"
type="unsignedShort" use="optional"/>
                <attribute name="ProviderName" type="string" use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="NameIDPolicy" type="samlp:NameIDPolicyType"/>
    <complexType name="NameIDPolicyType">
        <attribute name="Format" type="anyURI" use="optional"/>
        <attribute name="SPNameQualifier" type="string" use="optional"/>
        <attribute name="AllowCreate" type="boolean" use="optional"/>
    </complexType>
    <element name="Scoping" type="samlp:ScopingType"/>
    <complexType name="ScopingType">
        <sequence>
            <element ref="samlp:IDPList" minOccurs="0"/>
            <element ref="samlp:RequesterID" minOccurs="0"
maxOccurs="unbounded"/>
        </sequence>
        <attribute name="ProxyCount" type="nonNegativeInteger" use="optional"/>
    </complexType>
    <element name="RequesterID" type="anyURI"/>
    <element name="IDPList" type="samlp:IDPListType"/>
    <complexType name="IDPListType">
        <sequence>
            <element ref="samlp:IDPEntry" maxOccurs="unbounded"/>
            <element ref="samlp:GetComplete" minOccurs="0"/>
        </sequence>
    </complexType>
    <element name="IDPEntry" type="samlp:IDPEntryType"/>
    <complexType name="IDPEntryType">
        <attribute name="ProviderID" type="anyURI" use="required"/>
        <attribute name="Name" type="string" use="optional"/>
        <attribute name="Loc" type="anyURI" use="optional"/>
    </complexType>
    <element name="GetComplete" type="anyURI"/>
    <element name="Response" type="samlp:ResponseType"/>
    <complexType name="ResponseType">
          <complexContent>
            <extension base="samlp:StatusResponseType">
                <choice minOccurs="0" maxOccurs="unbounded">
                    <element ref="saml:Assertion"/>
                    <element ref="saml:EncryptedAssertion"/>
                </choice>
            </extension>
          </complexContent>
    </complexType>
    <element name="ArtifactResolve" type="samlp:ArtifactResolveType"/>
    <complexType name="ArtifactResolveType">
          <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <element ref="samlp:Artifact"/>
                </sequence>
            </extension>
          </complexContent>
    </complexType>
    <element name="Artifact" type="string"/>
    <element name="ArtifactResponse" type="samlp:ArtifactResponseType"/>
    <complexType name="ArtifactResponseType">
          <complexContent>
            <extension base="samlp:StatusResponseType">
                <sequence>
```

```
                    <any namespace="##any" processContents="lax" minOccurs="0"/>
                </sequence>
             </extension>
           </complexContent>
    </complexType>
    <element name="ManageNameIDRequest" type="samlp:ManageNameIDRequestType"/>
    <complexType name="ManageNameIDRequestType">
           <complexContent>
             <extension base="samlp:RequestAbstractType">
                <sequence>
                    <choice>
                        <element ref="saml:NameID"/>
                        <element ref="saml:EncryptedID"/>
                    </choice>
                    <choice>
                        <element ref="samlp:NewID"/>
                        <element ref="samlp:NewEncryptedID"/>
                        <element ref="samlp:Terminate"/>
                    </choice>
                </sequence>
             </extension>
           </complexContent>
    </complexType>
    <element name="NewID" type="string"/>
    <element name="NewEncryptedID" type="saml:EncryptedElementType"/>
    <element name="Terminate" type="samlp:TerminateType"/>
    <complexType name="TerminateType"/>
    <element name="ManageNameIDResponse" type="samlp:StatusResponseType"/>
    <element name="LogoutRequest" type="samlp:LogoutRequestType"/>
    <complexType name="LogoutRequestType">
        <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <choice>
                        <element ref="saml:BaseID"/>
                        <element ref="saml:NameID"/>
                        <element ref="saml:EncryptedID"/>
                    </choice>
                    <element ref="samlp:SessionIndex" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
                <attribute name="Reason" type="string" use="optional"/>
                <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
            </extension>
        </complexContent>
    </complexType>
    <element name="SessionIndex" type="string"/>
    <element name="LogoutResponse" type="samlp:StatusResponseType"/>
    <element name="NameIDMappingRequest" type="samlp:NameIDMappingRequestType"/>
    <complexType name="NameIDMappingRequestType">
        <complexContent>
            <extension base="samlp:RequestAbstractType">
                <sequence>
                    <choice>
                        <element ref="saml:BaseID"/>
                        <element ref="saml:NameID"/>
                        <element ref="saml:EncryptedID"/>
                    </choice>
                    <element ref="samlp:NameIDPolicy"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>
    <element name="NameIDMappingResponse"
type="samlp:NameIDMappingResponseType"/>
    <complexType name="NameIDMappingResponseType">
        <complexContent>
            <extension base="samlp:StatusResponseType">
                <choice>
                    <element ref="saml:NameID"/>
                    <element ref="saml:EncryptedID"/>
```

```
                </choice>
            </extension>
        </complexContent>
    </complexType>
</schema>
```

30.A تخطيطة SAML للتوصية X.500

هذه هي قائمة التوصية X.500 في SAML.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <annotation>
        <documentation>
            Document identifier: saml-schema-x500-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
              V2.0 (March, 2005):
                Custom schema for X.500 attribute profile, first published in SAML 2.0.
        </documentation>
    </annotation>
    <attribute name="Encoding" type="string"/>
</schema>
```

31.A تخطيطة SAML للغة XACML

هذه هي قائمة اللغة التأشيرية التوسّعية للتحكم في النفاذ (XACML) في SAML

```
<?xml version="1.0" encoding="UTF-8"?>
<schema
    targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <annotation>
        <documentation>
            Document identifier: saml-schema-xacml-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V2.0 (March, 2005):
              Custom schema for XACML attribute profile, first published in SAML 2.0.
        </documentation>
    </annotation>
    <attribute name="DataType" type="anyURI"/>
</schema>
```

التذييل I
اعتبارات الأمن والسرية

يجب التطرّق إلى الأمن والسرية بصورة نظامية منتظمة، مع النظر إلى العوامل البشرية مثل التهجمات الهندسية الاجتماعية، والمسائل السياسية، وإدارة المفاتيح، وإدارة الثقة، وعمليات التنفيذ المأمونة، وغيرها من العوامل التي لا تقع في نطاق هذا التذييل. وهناك ثمن لحلول الأمن التقنية، إذ يتعين أن تؤخذ في الاعتبار المتطلبات والسياسات البديلة بمثل ما تعبر به المتطلبات القانونية والتنظيمية.

ويلخص هذا التذييل المسائل والنهوج العامة الأمنية، وكذلك التهديدات الخاصة والتدابير المضادة من أجل استخدام التأكيدات والبروتوكولات والروابط والجانبيات في اللغة SAML بطريقة مأمونة تحفظ سريتها. يشرح هذا التذييل ويحلل صفات اللغة SAML من حيث الأمن والسرية. والغاية من كل ذلك توفير المعلومات للمهندسين المعماريين ورجال التنفيذ عن الأنظمة المعتمدة على اللغة SAML بشأن ما يلي:

- مسائل السرية المطلوب اعتبارها، وكيف تعالج معمارية اللغة SAML هذه المسائل.
- التهديدات وبالتالي المخاطر الأمنية التي يتعرض لها النظام القائم على اللغة SAML.
- المخاطر الأمنية التي تتطرق إليها معمارية اللغة SAML، وكيف تقوم بذلك.
- المخاطر الأمنية التي لا تتطرق إليها.
- التوصيات الخاصة بالتدابير المضادة التي تخفف من هذه المخاطر الأمنية.

1.I السرية

تشتمل اللغة SAML على القدرة على إصدار الإعلانات عن نعوت الكيانات المستيقنة وتراخيصها. هناك الكثير جداً من الحالات العامة التي تكون فيها المعلومات المحمولة في هذه الإعلانات شيئاً يرغب واحد أو عدة من الأطراف المشتركة في اتصال ما، في قصر النفاذ إليها على مجموعة من الكيانات محدودة العدد قدر الإمكان. والإعلانات عن النعوت الطبية أو المالية هي أمثلة بسيطة عن هذه الحالات.

وتوجد في بلدان عديدة وفي مناطق قضائية متعددة قوانين وتنظيمات بشأن السرية، وينبغي مراعاتها عند نشر نظام قائم على اللغة SAML. والأطراف التي تصدر الإعلانات، وتصدر التأكيدات، وتحمل التأكيدات، وتستهلك التأكيدات يجب أن تكون واعية لهذه المسائل المحتملة الخاصة بالسرية، وأن تسعى إلى التطرق إليها عند أعمال تنفيذها الأنظمة القائمة على اللغة SAML.

2.I الائتمانية

لعل أهم جانب يهم ضمان السرية للأطراف المشتركة في تعامل مبني على اللغة SAML هو القدرة على إنهاء التعامل بضمان الائتمانية. وبعبارة أخرى، هل يمكن نقل المعلومات الواردة في تأكيد، من مُصْدره إلى الجماعة المقصودة، وفقط إلى الجماعة المقصودة، من دون أن تتمكن أطراف أخرى من النفاذ إليه.

من الناحية التقنية، يمكن نقل المعلومات بائتمان. وعلى جميع الأطراف المشتركة في التعاملات القائمة على اللغة SAML أن تحلل كل واحدة من خطواتها أثناء التعامل (ولدى كل استعمال لاحق لمعطيات حاصلة من المعاملات) لكي تتأكد من أن المعلومات المطلوب الحفاظ على ائتمانها قد احتفظ لها بالفعل على ائتمانها.

وتجدر الملاحظة أيضاً أن مجرد تعمية محتويات التأكيدات قد لا تضمن حماية السرية حماية كافية. فهناك حالات عديدة، شكّل فيها مجرد تيسر المعلومات لأحد المستعملين (أو لعنوان IP) الذي نفذ إلى خدمة معينة، انتهاكاً للسرية (كما في حالة المعلومات التي ينفذ إليها مستعمل في منشأة عيادة طبية من أجل تأكيد، فقد يكون ذلك كافياً لتشكيل خرق للسرية من دون

معرفة محتويات التأكيد). ويمكن تقديم حلول جزئية لهذه المسائل عن طريق تقنيات مختلفة منها التعامل المغفل الاسم، كما هو مشروح في الفقرات التالية.

3.I استعارة الأسماء وإغفالها

لا توجد تعريفات لإغفال الاسم تلبي جميع الحالات. والعديد من التعريفات تتعامل مع الحالة البسيطة التي تكمن في مرسل ورسالة، وتناقش "إغفال الاسم" من حيث عدم المقدرة على ربط مرسل معين رسالة مرسلة، أو المقدرة على ترجيع رسالة إلى مرسلها. وبينما يكون هذا التعريف وافياً للحالة الاستثنائية، إلا أنه يتجاهل تجمّع المعلومات على مرّ الزمن استناداً إلى السلوك بدلاً من معرّف الهوية.

ومن المفيد في اللغة SAML التفكير بإغفال الاسم باعتباره موجوداً "داخل مجموعة". وهذه الفكرة ذات صلة باللغة SAML بسبب استعمال السلطات. وحتى إذا كان الصاحب "مغفل الاسم"، إلا أنه يبقى قابلاً للتعرّف إليه كعضو في مجموعة الأصحاب داخل ميدان السلطة المعنية. وتقتصر الأنظمة القادرة في اللغة SAML على "إغفال جزئي للاسم" في أحسن الأحوال بسبب استعمال السلطات. والكيان الذي صدر تأكيد حوله، هو بالفعل قابل للتعرّف إليه كواحد من فريق الكيانات التي لها علاقة بالسلطة المُصْدرة.

والاقتصار على إغفال الاسم قد يكون أسوأ بكثير من مجرّد تجمّع سلطات، تبعاً للطريقة التي تستعمل بها معرّفات الهوية، لأن إعادة استخدام أسماء مستعارة لتعريف الهوية تؤدي إلى تزايد المعلومات المحتملة للتعريف بالهوية. ويضاف إلى ذلك أن مستعملي الأنظمة القادرة في اللغة SAML يستطيعون أن يجعلوا انتهاك إغفال الاسم أسوأ بأفعالهم.

وبغض النظر عن الهوية القانونية، فإن كل معرف هوية لصاحب يمكن اعتباره اسماً مستعاراً له. وكذلك فإن فكرة "حامل المفتاح" يمكن اعتبارها هي الأخرى صالحة كمثيلاتها لتكون مكافئة لاسم مستعار، يربط عملاً (أو مجموعة أعمال) بصاحب. وحتى الوصف الذي من قبيل "المستعمل طلب النفاذ للتو إلى الشيء XYZ في الساعة 23:34" يمكن اعتباره صالحاً كمكافئ لاسم مستعار.

وهكذا فلا فرق، فيما يخص "المقدرة على الأذيّة"، بين أن يوصف المستعمل عن طريف معرف هوية أو عن طريق سلوك (مثل استعمال مفتاح أو أداء عمل).

والذي يظهر الفرق هو عدد المرات التي يستعمل فيها المكافئ الخاص لاسم مستعار. فإغفال الاسم يولد نوعاً من تصنيف الأسماء المستعارة بدءاً من الأسماء المستعارة الشخصية (مثل اللقب) التي تستعمل كل الوقت ومروراً بأنماط مختلفة من الأسماء المستعارة الوظيفية (مثل وزير الدفاع) وانتهاءً بالأسماء المستعارة التي "تستعمل لمرة واحدة فقط".

والأسماء المستعارة التي تستعمل لمرة واحدة فقط هي وحدها التي تحقق لك إغفال الاسم (ففي اللغة SAML، يعتبر هذا "إغفال اسم في مجموعة"). ومع ذلك فكلما ازداد استعمال الاسم المستعار أكثر، كانت هناك خطورة أكبر على إغفال الاسم. وبعبارة أخرى، إن إعادة استعمال اسم مستعار يتيح توفر معلومات إضافية محتملة للتعريف بالهوية، مرتبطة بالاسم المستعار. ومع مرور الزمن، قد يؤدي ذلك إلى تنامٍ يصبح وحده المعرف للهوية المصاحبة للاسم المستعار.

وتستطيع سلطات الموقع الأصلي (مثل سلطات الاستيقان وسلطات النعت) أن توفر درجة من "إغفال الاسم الجزئي" باستعمالها معرفات الهوية أو المفاتيح التي تستعمل لمرة واحدة فقط (كما في حالة "حامل المفتاح"). وإغفال الاسم هذا "جزئي" في أحسن الأحوال، لأن الصاحب هو محصور بالضرورة ضمن مجموعة الأصحاب التي هي على علاقة مع السلطة. وقد تنخفض هذه المجموعة في المستقبل (مما يخفض أيضاً مرتبة إغفال الاسم) عند استعمال نعوت تجميعية تقوم بتجزئة جماعة المستعملين في الموقع الأصلي. والمستعملون الذين يهتمون حقيقة بالاسم المستعار يتعين عليهم أن يهتموا بالتنكر أو باجتناب المخططات السلوكية غير الاعتيادية التي قد تصلح "لإزالة إغفال الاسم" عنهم مع مرور الزمن.

4.I الأمـــن

تدرس الفقرات التالية الاعتبارات الأمنية.

1.4.I المعلومات الأساسية

الاتصال ما بين الأنظمة المستندة إلى الحاسوب، عرضة لتهديدات متنوعة، وهذه التهديدات تحمل معها مستوى معيناً من المخاطرة. وتتوقف طبيعة المخاطرة على مجموعة من العوامل منها طبيعة الاتصال، وطبيعة أنظمة الاتصال، وأوساط حمل الاتصال، وبيئة الاتصال، وبيئات النظام النهائي وغيرها.

واللغة SAML أعدّت لتساعد المطورين على إقرار سياقات أمنية للاتصالات من سوية التطبيق المستندة إلى الحاسوب داخل الميادين الأمنية أو ما بينها. وفي هذا الدور تقوم SAML بتحويل معطيات الاستيقان لدعم مقدرة الأنظمة النهائية على الحماية من الاستعمالات غير المرخص بها. وينطبق أمن الاتصالات مباشرة على تصميم اللغة SAML. وينظر باهتمام إلى أمن الأنظمة خاصة في سياق نموجات التهديدات التي تتعرض لها SAML.

2.4.I مجال التطبيق

بعض المجالات التي تؤثر تأثيراً واسعاً في الأمن الإجمالي لنظام يستخدم اللغة SAML تقع صراحة خارج نطاق SAML. وفي الوقت الذي لا تتطرق فيه هذه التوصية إلى هذه المجالات، ينبغي أن تؤخذ بالحسبان دائماً عند مراجعة أمن أحد الأنظمة. وهذه القضايا مهمة بشكل خاص، غير أنها تقع حالياً خارج نطاق SAML:

- الاستيقان الأولي: تسمح اللغة SAML بإصدار إعلانات حول أفعال الاستيقان التي حدثت، ولكنها لا تورد متطلبات أو مواصفات حول أفعال الاستيقان هذه. وينبغي لمستهلكي تأكيدات الاستيقان أن يكونوا حذرين من منح الثقة العمياء لهذه التأكيدات، ما لم يكونوا وحتى يكونوا على معرفة بالأسس التي بنيت عليها هذه التأكيدات. ويجب ألا تزيد الثقة بهذه التأكيدات أبداً على الثقة بالطرف المؤكد الذي توصّل بشكل سليم إلى النتائج المؤكدة.
- نموذج الثقة: تتوقف الثقة بمحادثة في اللغة SAML في كثير من الأحيان على نموذج الثقة التحتي الذي يكون مبنياً في العادة على البنية التحتية لإدارة المفاتيح (مثل PKI أو المفتاح السري). فمثلاً رسائل SOAP المأمونة عن طريق التوقيع XML، لا تكون مأمونة إلا إلى الحد الذي تكون فيه المفاتيح المستعملة موثوقة. فالمفاتيح المشبوهة غير المكتشفة أو الشهادة المبطلة مثلاً يمكن أن تسمح باختراق أمني. وحتى الإخفاق في طلب شهادة يفتح الباب أمام تهجمات بتقمّص الشخصية. إن وضع البنية التحتية PKI ليس أمراً تافهاً بل لا بد من تنفيذ مناسب للبروتوكولات الأمنية للحفاظ على أمن نظام ما، بما في ذلك توليد الأرقام العشوائية أو شبه العشوائية ووضع المفاتيح في ذاكرات مأمونة.

3.4.I نموذج تهديدات اللغة SAML

إن النموذج العام لتهديدات الإنترنت في الخطوط التوجيهية للفريق IETF بشأن الاعتبارات الأمنية، هو أساس نموذج تهديدات اللغة SAML. ونفترض هنا أن النقطتين النهائيتين (أو أكثر) في معاملة SAML تكونات غير مشبوهتين، ولكن المتهجم يتحكم تحكماً كاملاً في قناة الاتصال.

وإضافة إلى ذلك، ونظراً إلى طبيعة اللغة SAML باعتبارها بروتوكولاً متعدد الأطراف لإعلانات الاستيقان والترخيص، يتعين النظر في الحالات التي يكون فيها طرف (أو أكثر) مشتركاً في معاملة SAML مشروعة – يعمل بصورة مشروعة حسب دوره في هذا التعامل – يحاول استخدام معلومة مكتسبة من تعامل سابق في تعامل لاحق بطريقة خبيثة.
والسيناريوهات التالية تشرح بعض التهجمات المحتملة:

- **التواطؤ**: التعاون السري بين كيانين أو أكثر في نظام لإطلاق تهجم، مثل:
  - التواطؤ بين طرف رئيسي ومزوّد خدمة؛
  - التواطؤ بين طرف رئيسي ومزوّد هوية؛
  - التواطؤ بين مزوّد هوية ومزوّد خدمة؛

- التواطؤ بين طرفين رئيسيين أو أكثر؛
- التواطؤ بين مزوّدَيْ خدمة اثنين أو أكثر؛
- التواطؤ بين مزوّدَيْ هوية اثنين أو أكثر.

- **تهجمات إنكار الخدمة:** منع النفاذ المرخص إلى مورد في نظام أو تأخير عمليات نظام ووظائفه.
- **تهجمات اقتحام بشري:** شكل من التهجم بالتنصّت الفعلي على الأسلاك، يقوم المتهجم فيه باعتراض معطيات الاتصال وتعديلها انتقائياً لكي يتنكّر كواحد أو أكثر من الكيانات المشتركة في جمعية اتصالات.
- **تهجمات إعادة الإرسال التكراري:** تهجم تكرر فيه معطيات الإرسال بطريقة خبيثة أو احتيالية، سواء قام به المُصْدر أم خصم يعترض المعطيات ويعيد إرسالها، وربما كجزء من تهجم تنكري.
- **أسرار دورة:** شكل من التنصّت الفعلي على الأسلاك، يلتقط المتهجم فيه التحكم في جمعية اتصالات منشأة سابقاً.

وفي جميع الحالات، تقع خارج تطبيق هذه الوثيقة، الآليات المحلية التي تستخدمها الأنظمة لتقرر ما إذا كانت ستولد تأكيدات أم لا. وهكذا فالتهديدات التي تبرز من تفاصيل الافتتاح الأصلي لدى سلطة الاستيقان، تقع هي الأخرى خارج هذا النطاق. وإذا أصدرت سلطة ما تأكيداً كاذباً، تصبح عندئذ التهديدات التي تبرز من استهلاك هذا التأكيد في الأنظمة البُعْدية واقعة خارج هذا النطاق صراحة.

والنتيجة المباشرة لمثل هذه الرؤية هي أن أمن نظام قائم على تأكيدات داخلة هو جيد فقط بقدر جودة أمن النطا المستعمل لتوليد هذه التأكيدات، وجودة صحة المعطيات والمعالجة التي بني عليها توليد التأكيدات. وعند تحديد المُصْدرين الذين تجب الثقة بهم، وخاصة في الحالات التي ستستخدم التأكيدات فيها كدخل في الاستيقان وفي قرارات الترخيص، تبقى المخاطرة الكامنة في إساءة الأمن الناجمة عن استهلاك تأكيدات صادرة كاذبة ولكنها صالحة، من الأمور الهامة. وينبغي أن تكون سياسات الثقة بين الأطراف المؤكدة والأطراف الواثقة مكتوبة دوماً، لكي تتضمن اعتبارات مهمة من الاعتمادية، وينبغي لعمليات التنفيذ أن تقدم وسائل تدقيق مناسبة.

5.I التقنيات الأمنية

تشرح الفقرات التالية التقنيات الأمنية ومختلف تقانات التخزين المتيسرة لتنفيذها في تطورات اللغة SAML.

1.5.I الاستيقان

الاستيقان يعني هنا مقدرة طرف في تعامل على تحديد هوية الطرف الآخر في هذا التعامل. ويمكن أن يكون هذا الاستيقان وحيد الاتجاه أو أن يكون ثنائي الاتجاهات.

- **الدورة النشيطة:** يتوفر الاستيقان غير الدائم بواسطة قناة الاتصال المستعملة لنقل رسالة في اللغة SAML. ويمكن أن يكون هذا الاستيقان وحيد الاتجاه – من مبتدر الدورة إلى المستلم – أو ثنائي الاتجاهات. ويحدد بروتوكول الاتصال المستعمل الطريقة الخاصة. فمثلاً يوفر استعمال بروتوكول شبكة مأمونة، مثل البروتوكول TLS أو بروتوكول أمن IP، المقدرة لمرسل رسالة SAML على استيقان المقصد لبيئة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP).
- **سوية الرسالة:** يوفر التوقيع XML التابع للتجمع W3C وOASIS WSS الطرائق اللازمة لإحداث "استيقان" دائم يكون وثيق الاقتران بالوثيقة. ولا تضمن هذه الطريقة لوحدها أن يكون مرسل الرسالة هو في الواقع موقّعها (ولا شك أن هذه الحالة لا تكون هي إحدى الحالات التي يشترك فيها وسطاء). وكل طريقة تسمح بالتأكيد الدائم على اشتراك كيان يستبان استبانة وحيدة التقابل مع مجموعة فرعية معطاة من رسالة XML، تكون كافية لتلبية هذا المطلب.

2.5.I الائتمانية

الائتمانية تعني أن محتويات رسالة ما لا يمكن أن يقرأها إلا المستلمون المرغوب فيهم، وليس أحد غيرهم ممن يصادفوه هذه الرسالة.

- **أثناء العبور:** يوفر استعمال بروتوكول شبكة مأمونة، مثل البروتوكول TLS أو بروتوكول أمن IP، ائتمانية عابرة للرسالة، لأنها محوّلة بين عقدتين.
- **سوية الرسالة:** يوفر تجفير اللغة XML تجفيراً انتقائياً لوثائق اللغة XML. وتوفر هذه الطريقة في التجفير الائتمانية الدائمة والانتقائية للعناصر داخل الرسالة XML.

3.5.I سلامة المعطيات

سلامة المعطيات هي القدرة على التأكيد بأن الرسالة بالشكل الذي استلمت به هي غير معدّلة عن الصيغة التي أرسلت بها.

- **أثناء العبور:** استعمال بروتوكول شبكة مأمونة، مثل البروتوكول TLS أو بروتوكول أمن IP يمكن تشكيله ليوفر حماية السلامة في الرزم المرسلة عبر توصيل الشبكة.
- **سوية الرسالة:** يوفر توقيع اللغة XML طريقة تولد ضمانة دائمة لغياب التعديل في طبيعة الرسالة المقترنة اقتراناً وثيقاً بهذه الرسالة. وكل طريقة تسمح بالتأكيد الدائم على اشتراك كيان يستبان استبانة وحيدة التقابل مع مجموعة فرعية معطاة من رسالة XML، تكون كافية لتلبية هذا المطلب.

4.5.I ملاحظات حول إدارة المفتاح

في عدة نقاط من هذا التذييل يشار إلى مقدرة الأنظمة على توفير الاستيقان وسلامة المعطيات والائتمانية عبر تخطيطات متنوعة يشترك فيها التوقيع الرقمي والتجفير. وفي جميع هذه التخطيطات، يكون توفير التخطيطة للأمن مقيداً حسب أنظمة إدارة المفتاح الموجودة. ويأتي فيما يلي تفصيل بعض التقييدات المعينة.

1) **النفاذ إلى المفتاح:** من المفترض، عندما تستعمل الأنظمة القائمة على المفاتيح من أجل الاستيقان وسلامة المعطيات وعدم الرفض، أن يتحقق الأمن الذي يضمن ألا يتيسر النفاذ إلى مفتاح خاص أو سري يمثل طرفاً رئيسياً، "لأطراف غير مناسبة. فيكون مثلاً التوقيع الرقمي الذي يخلقه "بوب" بالمفتاح الخاص هو البرهان الوحيد على تدخل "بوب"، طالما أن "بوب" هو الوحيد الذي يمتلك النفاذ إلى المفتاح. وينبغي قصر النفاذ إلى المفتاح عموماً على أصغر مجموعة ممكنة من الكيانات (وهذا مهم بصورة خاصة لمفاتيح الشركات أو المنظمات)، كما ينبغي حمايته بجمل سرية أو بوسائل أخرى. وتطبق الاحتياطات الأمنية الشائعة (لا تكتب الجملة السرية ولا تترك نافذة مفتوحة مع النفاذ إلى المفتاح، عندما تكون غائباً عن الحاسوب، وهكذا).

2) **ربط الهوية بالمفتاح:** في الأنظمة القائمة على المفاتيح التي تستعمل للاستيقان، يتعين أن يكون هناك نوع من الارتباط الموثوق بين الهوية والمفتاح. فالتحقيق من توقيع رقمي على وثيقة يمكنه أن يحدد إن كانت الوثيقة لم تعدّل منذ التوقيع عليها، وأنها كانت موقّعة فعلاً بمفتاح معين. ومع ذلك فإن هذا لا يؤكد أن المفتاح المستعمل هو فعلاً لفرد معين يناسب اللحظة والغرض. والتحقق من ربط المفتاح بأحد الأطراف يتطلب إقراراً إضافياً بالصلاحية.

يجب إقامة هذه الرابطة بين المفتاح والفرد. والحلول الشائعة تشتمل على أدلّة محلّية تختزن بنفس الوقت معرفات الهوية والمفاتيح – وهو أمر يسهل فهمه ويصعب الحفاظ عليه – أو على استخدام الشهادات. واستخدام الشهادات يوفر وسائل قابلة للقياس للجمع بين المفتاح والهوية، ولكنه يتطلب آليات لإدارة عمر الشهادة، ويغير الوضع القانوني للرابطة (فمثلاً عندما يترك أحد الموظفين الشركة لا يعود يمتلك هوية الشركة). وأحد النهوج الشائعة استخدام البنية التحتية لمفتاح عمومي (PIK).

وفي هذه الحالة تعرف هوية مجموعة جذرية موثوقة من سلطات إصدار الشهادات (CA) لكل مستهلك توقيعات – تجيب عن السؤال "بمن أثق لإصدار إعلانات عن ربط الهوية بالمفتاح؟". وعندئذ يصبح التحقق من توقيع، عملية يأتي في أولها التحقق من التوقيع (لتحديد أن التوقيع كان قد جرى بالمفتاح موضوع البحث، وأن الرسالة لم يصبها أي تغيير)، ثم إقرار صلاحية سلسلة الشهادات (لتحديد أن المفتاح مرتبط بالهوية الصحيحة)، ثم إقرار صلاحية أن الربط مازال مناسباً. وإقرار صلاحية الربط يتطلب اتخاذ خطوات لضمان كون الربط مازال صالحاً – ويكون للشهادة "عمر حياة" مدمج فيها، ولكن إذا حدث أن تعرض المفتاح للتشويه أثناء عمر حياة الشهادة، يصبح عندئذ ربط المفتاح بالهوية الموجودة في الشهادة غير صالح، ولكن الشهادة تبقى صالحة في الظاهر. وكثيراً ما تتوقف الشهادات على تصاحبات قد ينتهي أجلها قبل انقضاء عمر هذه الشهادات (مثل الحالة التي تصبح الشهادات فيها غير صالحة، عندما يغير أحدهم موظفيه، إلخ). إذاً فإن النظام الجيّد لإدارة المفاتيح يكون قوياً جداً إلا أنه معقد جداً أيضاً. فالتحقق من توقيع ينتهي بأن يكون عملية تحقق من ارتباط الوثيقة بالمفتاح، ثم التحقق من ارتباط المفتاح بالهوية، وكذلك التحقق من الصلاحية الجارية للمفتاح والشهادة.

5.5.I متتابعات التجفير TLS

تشدد التوصية في مواضع كثيرة من هذه التوصية باستعمال البروتوكول HTTP فوق الصيغة 3.0 من طبقة التوصيل المأمون (SSL) (انظر التذييل IV) أو الصيغة 1.0 من البروتوكول TLS أو باستعمال محددات المواقع URL مع تخطيطات HTTPS URL.

وفي أي استعمال للصيغة SSL 3.0 أو الصيغة TLS 1.0 لرابطة في SAML، يتعين على المخدّمات أن تستيقن ذاتها لدى الزبائن باستعمال الشهادة X.509 v3. ويتعين على الزبون أن ينشئ هوية المخدّم استناداً إلى محتويات الشهادة (عادة عبر تفحص الحقل DN للصاحب في الشهادة).

ويمكن تشكيل SSL/TLS لاستخدام عدة متتابعات تجفير مختلفة، ليست كلها وافية لتأمين "أفضل ممارسات" أمنية. وتجمع متتابعة التجفير أربعة أنواع من الميزات الأمنية، وتعطى اسماً في [SSL]. وقبل أن تتدفق المعطيات على توصيل SSLن تسعى النهايتان للتفاوض بشأن متتابعة تجفير. مما يسمح لهما بتوفير نوعية مناسبة من الحماية لاتصالاتهما، ضمن تجمعيات من الآليات الخاصة المتيسرة. والميزات التي تتصاحب مع تجفير هي:

تحدّد الطبقة SSL عدة خوارزميات لتبادل المفاتيح. وتقدم بعض الآليات استيقان المخدّم. وتُعتمد أيضاً آليات مغفلة الأسماء لتبادل المفتاح. (الخوارزميات المغفلة الأسماء لتبادل المفاتيح معرضة لتهجمات اقتحامية بشرية، ولا يوصى بها في سياق اللغة SAML). والخوارزمية RSA لتبادل المفتاح المستيقن هي حالياً أكثر خوارزمية قابلة للتشغيل البيني (لقد انقضت صلاحية براءة الخوارزمية RSA). وهناك خوارزمية أخرى مهمة لتبادل المفتاح هي تبادل المفتاح المستيقن Diffie-Hellman "DHE_DSS"، التي ليس لها قيود تنفيذ مرتبطة ببراءة.

معرفة هل خوارزمية تبادل المفتاح مسموح بتصديرها من الولايات المتحدة الأمريكية. يجب على الخوارزميات التي يمكن تصديرها أن تستخدم المفاتيح العمومية القصيرة (512 بتة) لتبادل المفتاح، والمفاتيح المتناظرة القصيرة (40 بتة) للتجفير. والمفاتيح التي لها هذه الأطوال تعرضت إلى تهجمات ناجحة، ولا يوصى باستعمالها.

وأسرع خيار لخوارزمية التجفير هو تدفق التجفير RC4، كما يعتمد DES وأشكاله الأخرى (DES40 و3DES-EDE) وكذلك AES في الأسلوب "سَلْسَلَة فِدر التجفير" (CBC). وهناك أساليب أخرى مقبولة، يرجى الرجوع إلى وثائقيات TLS.

التجفير المعدوم هو أحد الخيارات في بعض متتابعات التشفير. والتجفير المعدوم لا يقوم بأي تجفير، وفي مثل هذه الحالات، لا يستعمل SSL أو TLS إلا للاستيقان ولتأمين حماية السلامة. متتابعات التجفير مع التجفير المعدوم لا توفر الائتمانية، ويتعين ألا تستعمل في الحالات التي لا تكون الائتمانية إحدى متطلباتها، ولا يمكن الحصول عليها بوسائط أخرى غير SSL/TLS.

وتستعمل الخوارزمية المختصرة (digest algorithm) في شفرة استيقان الرسالة. وقد أوصت لجنة الاتصالات الاتحادية (FCC) في الولايات المتحدة الأمريكية باستخدام الخوارزمية SHA-256، وقرر فريق المهام الهندسية في الإنترنت (IETF) أن يتّبعها.

6.I اعتبارات أمنية عامة في اللغة SAML

تحلل الفقرات التالية المخاطر الأمنية لدى استعمال اللغة SAML وتنفيذها، كما تشرح التدابير المضادة التي تخفف من المخاطر.

1.6.I التأكيدات في اللغة SAML

يوجد القليل الذي يمكن قوله حول الشؤون الأمنية، على صعيد التأكيد SAML بالذات – وتبرز أكثر هذه الشؤون في بروتوكول الطلب والاستجابة، أو أثناء محاولة استعمال اللغة SAML بواسطة واحدة من الروابط. ولا شك أن يتوقع من المستهلك أن يحترم دوماً فترة صلاحية التأكيد، وكل عنصر <OneTimeUse> موجود في هذا التأكيد.

ومع ذلك فهناك شأن يستحق التحليل على صعيد التأكيد هو أن التأكيد بمجرد إصداره يصبح غير خاضع لتحكم المُصْدر. ولهذا الأمر عدد من التفرعات. فالمُصْدر مثلاً لا يستطيع التحكم في المدة التي سيدوم التأكيد فيها داخل أنظمة المستهلك، ولا إن كان المُصْدر يملك التحكم في الأجزاء التي سيتقاسمها المستهلك معه من معلومات التأكيد. وتأتي هذه الشؤون إضافة إلى شؤون متهجم خبيث، يستطيع أن يرى محتويات التأكيدات التي تمر في الشبكة غير مجفّرة (أو بما لا يكفي من التجفير).

وعلى الرغم من الجهود التي بذلت لحل هذه الشؤون داخل توصية اللغة SAML، إلا أن هذه التوصية لا تتضمن أي شيء يلغي الحاجة إلى التعبير باهتمام عما يمكن أن يحتويه التأكيد. وينبغي للمُصْدرين في جميع الأوقات أن يأخذوا بعين الاعتبار النتائج المحتملة التي تأتي من تخزين معلومات تأكيد في مكان بعيد، حيث يمكن إساءة استعماله مباشرة، أو يمكن تعرضه لهواة حاسوب متسللين، أو يمكن تخزينه لاستعمال احتياطي خلاق. وينبغي للمُصْدرين أيضاً أن ينظروا في احتمال تقاسم معلومات التأكيد مع أطراف أخرى أو حتى نشرها على الجمهور العام سواء بقصد أم سهواً بغير قصد.

2.6.I بروتوكول اللغة SAML

تشرح هذه الفقرة الاعتبارات الأمنية الخاصة ببروتوكول الطلب والاستجابة في اللغة SAML بالذات، بعيداً عن أي تهديد ينتج عن استعمال رابطة بروتوكول خاصة.

– **إنكار الخدمة:**

بروتوكول اللغة SAML معرّض لتهجم إنكار الخدمة (DoS). فمعالجة طلب في اللغة SAML هو عملية باهظة جداً، يشمل تحليل رسالة الطلب (يقتضي عادة إنشاء شجرة DOM)، والبحث عن تخزين قاعدة معطيات أو تأكيد (يحتمل أن يكون دون فهرسة)، وبناء رسالة استجابة، وعمليات توقيع رقمي محتملة واحدة أو أكثر. وعليه فإن الجهد المطلوب من متهجم ليولد الطلبات هو أقل بكثير من الجهد الذي تحتاجه معاملة هذه الطلبات.

1) تطلّب استيقان زبون في سوية أدنى

التطلب من الزبائن أن يستيقنوا أنفسهم في سوية أدنى من سوية بروتوكول اللغة SAML (مثل استعمال الرابطة SOAP فوق HTTP، ومع HTTP فوق TLS/SSL، مع مطلب لأن تكون للشهادات في جانب الزبون سلطة موثوقة لإصدار الشهادات عند جذورها)، مما يوفر تقفّي الأثر في حالة التهجم لإنكار الخدمة (Dos).

إذا كان الاستيقان مستعملاً فقط لتوفير تقفّي الأثر، فهو لا يقي بذاته من حدوث التهجم، لكنه يؤثر كعامل ردع.

وإذا كان الاستيقان مقترناً بنظام تحكّم في النفاذ، فإن التهجمات لإنكار الخدمة من أطراف خارجية تتوقف فعلاً. (يحتمل أن تبقى زيادة الحمولة في تخطيطة استيقان الزبون تعمل كتهجم لإنكار الخدمة على خدمة اللغة SAML، ولكن هذا التهجم يحتاج أن يكون التعامل معه في سياق تخطيطة استيقان الزبون المختارة).

مهما يكن النظام المستعمل لاستيقان الزبون، ينبغي له أن يوفر الإمكانية لاستبانة مصدر واحد لكل طلب، وينبغي أن يكون غير قابل للتزوير. (وفي حالة تقفّي الأثر فقط، يكون إدخال عنوان بروتوكول الإنترنت (IP) غير كافٍ، نظراً إلى أن هذه المعلومة يمكن تحريفها بسهولة).

2) تطلّب توقيع الطلبات

مطلب توقيع الطلبات يقلل من رتبة اللاتناظر بين العمل الذي يقوم به الطالب وعمل المتسجيب. فالعمل الإضافي المطلوب من المستجيب ليتحقق من التوقيع يشكل نسبة مئوية صغيرة نسبياً من العمل الكلي المطلوب من المستجيب، في حين أن عملية حساب التوقيع الرقمي تمثل قدراً كبيراً نسبياً من عمل الطالب. فتضييق هذا اللاتناظر يخفّض من المخاطرة التي تصحب التهجم لإنكار الخدمة.

ومع ذلك، يستطيع نظرياً أي متهجم أن يأسر رسالة موقّعة، ثم يعيد إرسالها باستمرار، ملتفاً بذلك حول هذا المطلب. ويمكن اجتناب مثل هذه الحالة بتطلب استعمال عنصر التوقيع XML `<ds:SignatureProperties>` الذي يحتوي على خاتم توقيت. ويمكن بعد ذلك استعمال خاتم التوقيت لتحديد ما إذا كان التوقيع حديثاً. وفي هذه الحالة، كلما كانت الفجوة الزمنية بعد الإصدار التي يعامل التوقيع أثناءها بصفته صالحاً، فجوة أضيق، كان الأمان الذي تحصل عليه من التهجمات التكرارية لإنكار الخدمة، أعلى.

3) تقييد النفاذ إلى المحدّد URL في التفاعل

الحدّ إلى مستوى منخفض جداً من إمكانية إصدار طلب خدمة في اللغة SAML من مجموعة من الأطراف المعروفة يخفض من خطورة التهجم لإنكار الخدمة بنسبة جسيمة. وفي هذه الحالة، لا يمكن حصول تهجمات إلا التهجمات الصادرة عن المجموعة المنتهية من الأطراف المعروفة، وبذلك ينخفض إلى حدّ كبير التعرض لهجمات من الزبائن الخبثاء ولتهجمات إنكار الخدمة التي تستعمل آلات مشبوهة مثل الأخيلة المخمورة.

وهناك طرائق عديدة للحدّ من النفاذ، مثل وضع المستجيب في اللغة SAML داخل شبكة داخلية مأمونة، وتنفيذ قواعد النفاذ على صعيد المسيّر.

7.I الاعتبارات الأمنية في روابط اللغة SAML

الاعتبارات الأمنية في تصميم بروتوكول الطلب والاستجابة في اللغة SAML، تتوقف إلى حدّ بعيد على رابطة البروتوكول الخاصة المستعملة. والروابط المعتمدة هي رابطة SOAP، ورابطة SOAP المقلوب (PAOS)، ورابطة HTTP Redirect، ورابطة HTTP Redirect/POST، ورابطة HTTP Artifact ورابطة SAML URI.

1.7.I الرابطة SAML SOAP

لما كانت الرابطة SAML SOAP لا تتطلب أي استيقان، وليس لها متطلبات لا بشأن الائتمانية أثناء العبور ولا بسلامة الرسالة، فهي مفتوحة أمام تهجمات شائعة واسعة التنوع. وتناقش الاعتبارات العامة منفصلة عن الاعتبارات المتعلقة بحالة SOAP فوق HTTP.

1) التنصت

التهديد: لما كان مطلب الائتمانية أثناء العبور غير موجود، يمكن لطرف متنصت الحصول على الرسالة SOAP المتضمنة طلباً، وعلى الرسالة SOAP المتضمنة الاستجابة المقابلة لهذا الطلب. وهذه الحيازة تعرض في نفس الوقت طبيعة الطلب وتفاصيل الاستجابة، وقد تحتوي على تأكيد واحد أو أكثر.

وعرض تفاصيل الطلب يضعف في بعض الحالات أمن الطرف الطالب، بالكشف عن تفاصيل أنواع التأكيدات التي يطلبها أو عن الذين تطلب منهم هذه التأكيدات. فإذا كان مثلاً باستطاعة متنصّتٍ أن يحدّد أن الموقع X يتواتر طلبه على تأكيدات استيقانية من موقع Y مع طريقة تثبيت معينة، فإنه يصبح قادراً على استخدام هذه المعلومات في تشويه الموقع X.

وكذلك يخلق التنصّت على سلسلة من الاستفهامات عن الاستيقان، "خريطة" للموراد الموجودة تحت تحكم سلطة ترخيص معينة.

وإضافة إلى ذلك فإن عرض الطلب نفسه يشكل في بعض الحالات انتهاكاً للسرية. فالتنصت مثلاً على استفهام وعلى الإجابة عنه، يمكنه أن يعرض كون مستعمل معين نشيطاً في موقع الاستفهام، مما قد يشكل معلومة ينبغي عدم إفشائها في حالات مختلفة مثل مواقع المعلومات الطبية أو المواقع السياسة وما إلى ذلك. وكذلك قد تشكل تفاصيل أي تأكيدات تحملها الاستجابة معلومة يجب الاحتفاظ بها مؤتمنة. ويصح هذا خاصة في الاستجابات التي تتضمن تأكيدات نعوت، فإذا كانت هذه النعوت تمثل معلومات يجب ألا تتيسر لكيانات ليست أطرافاً في تعامل ما (مثل أسعار الفائدة والنعوت الطبية وما إلى ذلك)، عندها تكون خطورة التنصت عالية.

التدابير المضادة: في الحالات التي يشكل فيها أي واحد من هذه المخاطر قضية، يكون على التدبير المضاد لتهجمات التنصّت أن يقدم شكلاً من ائتمانية الرسالة أثناء العبور. وفي الرسائل SOAP، يمكن أن توضع هذه الائتمانية موضع التنفيذ إما على صعيد البروتوكول SOAP وإما على صعيد طبقة النقل في البروتوكول SOAP (أو على أصعدة أخفض من ذلك).

وإضافة الائتمانية أثناء العبور على صعيد البروتوكول SOAP تعني إنشاء رسالة البروتوكول SOAP بحيث لا يتمكن أي كان، سوى الطرف المقصود، من النفاذ إلى الرسالة، بصرف النظر عن طبقة النقل في البروتوكول SOAP. والحلّ العام لهذه المسألة يكون في التجفير XML. وتسمح هذه التوصية بتجفير الرسالة SOAP نفسها، مما يزيل خطورة التنصت، ما لم يكن المفتاح المستعمل في التجفير مشبوهاً. ويمكن للمطورين أن يعتمدوا، كحل بديل، على طبقة النقل، أو على طبقة أخفض، في البروتوكول SOAP لتوفير الائتمانية أثناء العبور.

وتتوقف تفاصيل توفير هذه الائتمانية على النقل الخاص المختار في البروتوكول SOAP. وإحدى هذه الطرائق هي استخدام HTTP فوق TLS/SSL. وقد تتطلب أساليب النقل الأخرى تقنيات أخرى للائتمانية أثناء العبور، فقد يستعمل البروتوكول نقل بريد بسيط (SMTP) في التوسّعات S/MIME.

وقد توفر طبقة أخفض من طبقة النقل في SOAP الائتمانية أثناء العبور في بعض الحالات. فإذا كان التفاعل طلب–استجابة مثلاً منفذاً فوق نفق IPSec، فإن النفق نفسه يمكنه أن يوفر ائتمانية وافية أثناء العبور.

2) إعادة الإرسال التكراري

التهديد: توجد قابلية تأثر صغيرة بالتهجمات على إعادة الإرسال، على صعيد الرابطة SOAP. إن إعادة الإرسال هي أكثر من قضية في مختلف الجانبيات. وأول مسألة تنشأ من إعادة الإرسال على صعيد الرابطة SOAP هي احتمال استخدام إعادة الإرسال كطريقة تهجم لإنكار الخدمة.

التدابير المضادة: أفضل وسيلة لاتقاء تهجمات إعادة الإرسال هي منع أسر الرسالة في المقام الأول. وتستطيع بعض تخطيطات صعيد النقل المستعملة لتوفير الائتمانية أثناء العبور أن تؤدي هذا الهدف. فإذا حدث التحاور طلب–استجابة مثلاً في اللغة SAML، على البروتوكول SOAP فوق HTTP/TLS، يمتنع أسر الرسائل على أطراف ثالثة.

ولما كان معيد الإرسال المحتمل لا يحتاج أن يفهم الرسالة لكي يعد إرسالها، فإن التخطيطات مثل التجفير XML لا توفر حماية من إعادة الإرسال. فإذا استطاع متهجم أسر طلب SAML كان الطالب قد وقّعه وجرى تجفيره للمتسحيب، يستطيع المتهجم إعادة إرسال هذا الطلب في أي وقت يشاء، دو حاجته إلى فك التجفير. ويشتمل الطلب SAML على معلومات عن وقت إصدار الطلب، مما يتيح تحديد ما إذا كانت قد حصلت إعادة إرسال. ومن ناحية أخرى يمكن استعمال المفتاح الوحيد للطلب (معرف هويته) لتحديد كونه طلباً معاداً إرساله أم لا.

ومن التهديدات الأخرى لتهجم إعادة الإرسال حالات يكون فيها نموذج "الدفع على القطعة" هو السائد. فيمكن استخدام إعادة الإرسال لتحميل مبالغ ضخمة على حساب معين.

وبالمثل هناك نموذجات يكون فيها الزبون قد مُنح (أو قد اشترى) من نظام ما عدداً ثابتاً من التفاعلات، فيأتي التهجم لإعادة الإرسال ويستنفذ جميع هذه الاستعمالات، ما لم يكن المصدر حريصاً على الاحتفاظ بأثر المفتاح الوحيد لكل طلب.

3) إدراج رسالة

التهديد: يدرج طلب أو استجابة مستصطنعان (مُفَبْركان) في تدفق الرسائل. فقد تولد استجابة خاطئة لدى المستلم فعلاً غير مناسب، كما في حالة الإجابة "بنغم" مزيفة عن استفهام بشأن قرار ترخيص أو في حالة إعادة معلومات نعت خاطئة في إجابة على استفهام عن نعت.

التدابير المضادة: إمكانية إدراج طلب لا تشكل تهديداً على صعيد الرابطة SOAP. فالتهديد بإدراج استجابة خاطئة يمكن اعتباره تهجماً لإنكار خدمة، كأن ترجّع أخطاء SOAP كاستجابات، ولكن مثل هذا التهجم يصبح واضحاً بسرعة كبيرة. ويتطرق البروتوكول في اللغة SAML إلى التهجم الأكثر حذفاً الذي يكمن في ترجيع استجابات مستصطنعة، وهو مناسب لهذا الغرض، لأن كل استجابة SOAP، حسب تعريف الرابطة SOAP، يتعين عليها أن تحتوي على استجابة بروتوكول SAML وحيدة، ما لم تكن تحتوي على خطأ. ويعالج البروتوكول SAML هذا الأمر بآليتين: ترابط الاستجابات مع الطلبات باستخدام النعت المطلوب `InResponseTo`، مما يجعل التهجم أصعب لأن الطلبات موقّعة وإما عبر توصيل نقل مأمون مثل SSL/TLS.

4) إلغاء رسالة

التهديد: التهجم لإلغاء رسالة إما أن يمنع طلباً من الوصول إلى مستجيب وإما أن يمنع استجابة من الوصول إلى طالب.

التدابير المضادة: في كلتا الحالين لا تتطرق رابطة البروتوكول SOAP إلى هذا التهديد. والترابط بين رسالتي الطلب والاستجابة قد يردع مثل هذا التهجم، كأن يستخدم النعت `InResponseTo` في النمط **StatusResponseType**.

5) تعديل رسالة

التهديد: تعديل الرسالة هو تهديد للرابطة SOAP في كلا الاتجاهين.

يمكن أن ينتج عن تعديل رسالة لتشويه تفاصيل الطلب، ترجيع اختلافات كبيرة في النتائج، ويستطيع متهجم ماكر استخدامها بدوره لتخريب أنظمة تتوقف على التأكيدات الراجعة. فمثلاً يمكن لتحريف قائمة النعوت المطلوبة في العناصر `<Attribute>` أن يؤدي إلى نتائج تضطر المستجيب إلى تشويه الطلب أو رفضه.

كما يمكن أن ينتج عن تعديل رسالة لتشويه المُصْدر الظاهري للطلب، إنكار للخدمة أو تسيير خاطئ للاستجابة. وقد يحتاج أن يحدث هذا التشويه تحت مستوى اللغة SAML، وهو يقع بذلك خارج نطاق تطبيقها.

وقد ينتج عن تعديل الاستجابة لتشويه تفاصيل التأكيدات الموجودة فيها درجات كبيرة من التخريب. وأبسط الأمثلة على تشويه التفاصيل في استيقان أو في قرار ترخيص، قد تؤدي إلى صنوف من المسّ الجدّي جداً بالأمن.

التدابير المضادة: بغية معالجة هذه التهديدات المحتملة، لا بد من استعمال نظام يضمن سلامة الرسالة أثناء العبور، ولكن نظراً إلى هذا التهديد الواسع، يشدّد على التوصية باستخدام مثل هذا النظام. وعلى صعيد الرابطة SOAP يمكن تحقيق ذلك بالتوقيع رقمياً على الطلبات والاستجابات باستخدام نظام مثل توقيع اللغة XML.

وعندما تكون الرسائل موقّعة رقمياً، يكون لدى المستلم ضمان بأن الرسالة لم تتشوه أثناء العبور، إلا إذا كان المفتاح المستعمل قد تخرّب.

ويمكن أيضاً تحقيق هدف سلامة الرسالة أثناء العبور على صعيد أخفض باستخدام نقل SOAP يوفر صفة السلامة المضمونة، أو إذا كان مبنياً على بروتوكول يوفر مثل هذه الصفة. والنقل SOAP فوق HTTP فوق TLS/SSL هو نقل يوفر مثل هذه الضمانة.

والتجفير لوحده لا يوفر هذه الحماية لأنه حتى إذا كانت الرسالة المعترضة لا يمكن أن تتشوه *من ذاتها*، إلا أنه يمكن الاستعاضة عنها برسالة تولّد من جديد.

6) الاقتحام البشري

التهديد: رابطة البروتوكول SOAP عرضة لتهجمات بالاقتحام البشري (MITM). ولكي تمنع الكيانات الخبيثة من القيام باقتحامات (مع كل الأخطار المناقشة في فقرتي التنصت وتعديل رسالة)، يلزم نوع من الاستيقان الثنائي الأطراف.

التدابير المضادة: يمكن أن يسمح نظام الاستيقان ثنائي الأطراف للطرفين كلهما أن يحددا أن ما يشاهدانه في المحاورة هو ما يأتي فعلاً من الطرف الآخر في المحاورة.

وعلى صعيد الرابطة SOAP، يمكن بلوغ هذا الهدف بالتوقيع الرقمي على الطلب والاستجابة كليهما. ولا تمنع هذه الطريقة متنصتاً من الوقوف في المنتصف ويعيد الإرسال في الاتجاهين، ولكنها تمنعه من تشويه المحاورة في أي من الاتجاهين من دون أن يكتشف أمره.

لما كان العديد من تطبيقات البروتوكول SOAP لا تستخدم الدورات، فإن هذا النوع من استيقان المؤلف (بالتقابل مع استيقان المرسل) قد يحتاج إلى أن يدمج مع معلومات قادمة من طبقة النقل لكي يؤكد أن المرسل والمؤلف هما نفس الطرف، وذلك في سبيل اتّقاء شكل أضعف من "الاقتحام المتنصّت".

وهناك تنفيذ آخر قد يتوقف على نقل SOAP يوفر الاستيقان الثنائي الأطراف، أو على نقل منفذ عند مستوى أخفض ويوفر هذا الاستيقان. ومثال على هذا هو SOAP فوق HTTP على TLS/SSL للمرة الثانية، مع شهادات مطلوبة في جانبي الزبون والمخدّم كليهما.

وفوق ذلك فإن فترة صلاحية التأكيدات المرجّعة تعمل كضابط لدرجة أن المخاطرة القادمة من تهجمات الاقتحام (MITM). وكلما كانت فترة صلاحية التأكيد أقصر، كان الضرر أقل في حالة الاعتراض.

7) استخدام SOAP فوق HTTP

لما كانت الرابطة SOAP تتطلب من تطبيقات مطابقة، أن تعتمد HTTP فوق TLS/SSL مع عدد من الطرائق المختلفة للاستيقان ثنائي الأطراف، مثل بيزك (Basic) فوق SSL في جانب المخدّم، والاستيقان المدعوم بالشهادات فوق SSL في جانب المخدّم، فإن هذه الطرائق تكون دوماً متيسرة للتخفيف من التهديدات، حيث لا تكون أنظمة المستوى المنخفض متيسرة، وحيث تعتبر التهجمات المعددة أعلاه كتهديدات ذات معنى.

وهذا لا يعني أن استخدام HTTP فوق TLS، مع شكل ما من الاستيقان ثنائي الأطراف، هو أمر إلزامي. فإذا كان للحماية بسوية مقبولة من مختلف المخاطر، أن تحصل بوسائل أخرى (بواسطة النفق IPSec مثلاً)، لن تكون هناك حاجة إلى كامل TLS مع الشهادات. ومع ذلك ففي أغلب حالات SOAP فوق HTTP، يكون استعمال HTTP فوق TLS مع الاستيقان ثنائي الأطراف هو الاختيار المناسب.

ويشرح الطلب RFC بشأن الاستيقان HTTP (الطلب RFC 2617 للفريق IETF) التهجمات المحتملة في بيئة البروتوكول HTTP عند استعمال تخطيطات الاستيقان الأساسي أو لموجز الرسائل.

ويلاحظ مع ذلك أن استخدام الأمن على صعيد النقل (مثل بروتوكول SSL أو TLS تحت HTTP) يوفر فقط الائتمانية و/أو السلامة و/أو الاستيقان "لقفزة واحدة". وفي النموذجات التي يوجد فيها وسطاء أو التي تحتاج التأكيدات موضوع البحث فيها أن تعيش لأكثر من قفزة واحدة، لا يوفر استعمال HTTP مع TLS/SSL الأمن الوافي.

2.7.I جانبيات المتصفح على شبكة الويب بتوقيع وحيد (SSO)

إن استيقان المستعمل في موقع المُصْدر يقع صراحة خارج النطاق، مثلما هي المسائل المتعلقة باستيقان هذا الموقع المصدر. ويعني مفهوم المفتاح أن كيان النظام المصدر أن يكون قادراً على التأكيد بأن كيان النظام للزبون المستيقن الذي يتعامل معه هو نفس الكيان الذي سيكون في الخطوة التالية من التعامل. ومن الطرائق التي تحقق ذلك أن يجري أداء هذه الخطوات الأولية باستخدام TLS كطبقة دورة تحتية في البروتوكول المستعمل لهذا التعامل الأولي (من المعقول أن يكون HTTP).

1.2.7.I جانبية التوقيع الوحيد (SSO)

1) التنصت

التهديد: احتمال التنصّت موجود في جميع حالات المتصفح على شبكة الويب.

التدابير المضادة: في الحالات التي تطلب فيها الائتمانية (ينبغي ألا يغرب عن البال أن أي تأكيد لا يرسل بطريقة مأمونة، ومعه الطلبات التي تصحبه، يكون عرضة للمتنصت الخبيث)، تحتاج الحركة في البروتوكول HTTP أن تحدث فوق نقل يضمن الائتمانية. والبروتوكول HTTP فوق TLS/SSL وبروتوكول أمن IP يلبيان هذا المطلب.

2) سرقة معلومات استيقان المستعمل

التهديد: في الحالة التي يستيقن فيها صاحب نفسه لدى الموقع المصدر بكشفه عن معلومات استيقان يعاد استعمالها، وهي بشكل كلمة سر مثلاً، فإن سرقة معلومات الاستيقان ستمكّن خصماً من أن يتقمص شخصية الصاحب.

التدابير المضادة: وفي سبيل اجتناب هذه المسألة، يتعين على التوصيل بين متصفح الصاحب والموقع المصدر أن يقيم حافظاً للائتمانية. وفوق ذلك يجب اتخاذ خطوات يقوم بها الصاحب أو الموقع المقصد للتأكد من أن الموقع المصدر هو الموقع المصدر الأصلي المتوقع والموثوق قبل الكشف عن معلومات الاستيقان. ويمكن استعمال HTTP فوق TLS لمعالجة هذا الشاغل.

3) **سرقة إذنة الحامل**

التهديد: في الحالة التي يحتوي فيها تأكيد الاستيقان على معرف هوية بروتوكول الاستيقان لحامل التأكيد، فإن سرقة الشيء المصطنع ستمكّن خصماً من أن يتقمّص شخصية الصاحب.

التدابير المضادة: كل واحدة من الطرائق التالية تخفّض من أرجحية حدوث ذلك:

يقيم الموق المقصد حافظاً للائتمانية على توصيله مع متصفح الصاحب.

يتأكد (خارج النطاق) الصاحب أو الموقع المقصد من أن الموقع المصدر يقيم حافظاً للائتمانية على توصيله متصفح الصاحب.

يتحقق الموقع المقصد من أن متصفح الصاحب قد أعاد توجيهه الموقع المصدر مباشرة، هذا الموقع الذي استيقن الصاحب مباشرة.

يرفض الموقع المصدر أن يستجيب لأكثر من طلب واحد يخص تأكيداً مقابلاً لنفس معرف هوية التأكيد.

إذا كان التأكيد يتضمن عنصر شرط من النمط **AudienceRestrictionType**، يعرف هوية ميدان معين، عندئذ يتحقق الموقع المقصد من أنه عضو في هذا الميدان.

التوصيل بين الموقع المقصد والموقع المصدر، الذي مرّ فوقه معرف هوية التأكيد، مقام مع حافظ للائتمانية.

يتعين على الموقع المقصد، أثناء اتصاله بالموقع المصدر الذي مرّ فوقه معرف هوية التأكيد، أن يتأكد من أن هذا الموقع المصدر هو الموقع المصدر الأصلي المتوقع والموثوق.

4) **إعادة الإرسال التكراري**

احتمال حدوث تهجم لإعادة الإرسال التكراري موجود لهذه المجموعة من الجانبيات. ويمكن أن يستعمل التهجم لإعادة الإرسال لمحاولة إنكار الخدمة أو للحصول على المعلومات بالاحتيال. وتتوقف التدابير المضادة المناسبة، على أي رابطة معينة تستعمل، وهي معروضة أعلاه.

5) **إدراج رسالة**

تهجمات إدراج الرسالة معروضة في الفقرة I.1.7.

6) **إلغاء رسالة**

التهديد: إلغاء رسالة أثناء أي مرحلة من التعاملات بين المتصفح ومُصْدر التأكيد SAML ومستهلك التأكيد SAML، يتسبب في فشل التعامل. وينتج إنكاراً لخدمة ما، ولكنه لا يزيد تعرض أي معلومات.

التدابير المضادة: إن استخدام قناة نقل محمية السلامة يعالج تهديد إلغاء الرسالة، في حالة عدم وجود أي وسيط.

7) **تعديل رسالة**

التهديد: احتمال تشويه الرسائل في التدفق موجود بالنسبة إلى هذه المجموعة من الجانبيات. وبعض النتائج المحتملة غير المرغوب فيها هي كالتالي:

قد ينتج تشويه الطلب الأولي رفض لدى المُصْدر SAML أو خلق شيء مصطنع يستهدف مورداً مختلفاً غير المورد المطلوب.

وقد ينتج عن تشويه الشيء المصطنع إنكار الخدمة لدى المستهلك SAML.

وقد ينتج تشويه التأكيدات بالذات عندما تكون عابرة، جميع أنواع النتائج السيئة (إأن لم تكن موقعة) أو إنكار الخدمة (إن كانت موقّعة والمستهلك يرفضها).

التدابير المضادة: لاجتناب تعديل الرسائل، يجب أن تنقل الحركة بوسائل نظام يضمن سلامة الرسالة من نقطة نهائية إلى نقطة نهائية.

وفيما يخص الجانبيات القائمة على متصفح شبكة الويب، تكون الطريقة التي يوصى بها لتوفير سلامة الرسالة أثناء العبور هي استخدام HTTP فوق TLS/SSL، مع متتابعة تجفير توفر التحقق من سلامة المعطيات.

8) الاقتحام البشري

التهديد: تكون التهجمات الاقتحامية البشرية مؤذية بشكل خاص لهذه المجموعة من الجانبيات. يمكن للاقتحام البشري أن يرحّل الطلبات، وأن يأسر التأكيد المرجّع (أو الشيء المصطنع)، وأن يعيد ترحيل المزيف منها إلى الخلف. وبعد ذلك لا يستطيع المستعمل الأصلي النفاذ إلى المورد موضوع البحث، ولكن المقتحم البشري يستطيع فعل ذلك باستخدام المورد المأسور.

التدابير المضادة: يتطلب تجنب هذا التهديد عدداً من التدابير المضادة. تكون البداية باستعمال نظام يوفر استيقاناً معمقاً ثنائي الأطراف يجعل من الصعب جداً على الاقتحام البشري أن يندرج بنفسه في المحاورة.

ومع ذلك يبقى الاحتمال وارداً في أن يعمل مقتحم بشري فقط كمرسل منفذ ثنائي الاتجاهات، وأن يتنصت على المعلومات، بنيّة أسر التأكيد المرجّع أو معاملته (أو ربما تشويه الترجيع الأخير إلى الطالب). وإقامة نظام للائتمانية سوف يمنع التنصت. بينما إقامة نظام لسلامة المعطيات سوف يمنع تشويه الرسالة أثناء إرسال منفذ إلى الأمام.

وفيما يخص هذه المجموعة من الجانبيات، يمكن تلبية جميع المتطلبات الخاصة باستيقان الدورة المعمق ثنائي الأطراف، وبالائتمانية وسلامة المعطيات باستعمال HTTP فوق TLS/SSL، إذا كانت الطبقة TLS/SSL تستخدم متتابعة تجفير مناسبة (تجفير معمق بما يكفي لتوفير الائتمانية ودعم سلامة المعطيات)، وتتطلب شهادات الصيغة X.509 v3 للاستيقان.

9) تقمّص شخصية من دون إعادة استيقان

التهديد: محاولات مستعمل نصّاب تقمّص شخصية طرف رئيسي مكتتب حالياً في دورة، فيكسب بذلك النفاذ إلى موارد محمية.

بمجرد نجاح طرف رئيسي في أن يكتتب لدى مزوّد هوية، لا تعود الرسائل <AuthnRequest> اللاحقة القادمة من مزودي خدمة مختلفين والتي تخص هذا الطرف الرئيسي، تتسبب بالضرورة في إعادة استيقان الطرف الرئيسي. ومع ذلك يجب استيقان الأطراف الرئيسية، ما لم يكن مزوّد الهوية قادراً على تحديد أن الرسالة <AuthnRequest> لا ترتبط فقط بهوية الطرف الرئيسي، بل ترتبط أيضاً بدورة مزوّد هوية صالحة الاستيقان بالنسبة إلى هذا الطرف الرئيسي.

التدابير المضادة: في عمليات التنفيذ التي يكون فيها هذا التهديد أحد الشواغل، يتعين على مزوّدي الهوية أن يحتفظوا بمعلومات الحالة الخاصة بالدورات النشيطة، ويتعين عليهم أيضاً أن يقروّا صلاحية التقابل بين رسالة <AuthnRequest> وإحدى الدورات النشيطة قبل إصدار استجابة <Response> من دون استيقان الطرف الرئيسي أولاً. ويمكن إرسال الكعكات بالبريد إلى مزوّدي الهوية لدعم هذه العملية الخاصة بإقرار الصلاحية، وإن كانت Liberty لا تلزم بالنهج المبني على الكعكة.

2.2.7.I جانبية الزبون أو الوكيل المفوّض المعزّز

1) الاقتحام البشري

التهديد: اعتراض الرسائل SOAP التي هي AuthnRequest وResponse، سيؤدي لاحقاً إلى تقمّص شخصية الطرف الرئيسي.

يستطيع كيان طفيلي في نظام، أن يجعل من نفسه مقتحماً بشرياً (MITM) بين الزبون المعزّز ومزوّد خدمة شرعي، حيث يقوم بدور مزوّد الخدمة في التفاعلات مع الزبون المعزّز، وبدور الزبون المعزّز في التفاعلات مع مزوّد الخدمة الشرعي. وبهذه الطريقة، يتمكن المقتحم البشري كخطوة أولى أن يعترض الرسالة AuthnRequest لمزوّد الخدمة، وأن يبدّل أي محدد موقع URL بالقيمة التي يختارها من responseConsumerServiceURL في فِدرة الرأسية من PAOS، قبل أن يقوم بإرسال AuthnRequest إلى الأمام إلى الزبون المعزّز. ويقوم المقتحم عادة بإدراج قيمة للمحدد URL تحيل إلى ذاته. وبعد ذلك إذا استلم الزبون المعزز لاحقاً استجابة Response من مزوّد الهوية، وأرسل بعد ذلك الاستجابة المحتواة إلى responseConsumerServiceURL المستلمة من المقتحم، يصبح المقتحم MITM قادراً على التنكّر كطرف رئيسي لدى مزوّد الخدمة الشرعي.

التدابير المضادة: يعيّن مزوّد الهوية للزبون المعزّز، العنوان الذي يتوجب على الزبون المعزز أن يرسل إليه الاستجابة Response. ولا تستعمل الرأسية في PAOS التي هي responseConsumerServiceURL إلا لاستجابات الخطأ من الزبون المعزز كما هو محدد في الجانبية.

2) إنكار الخدمة

التهديد: تغيير الطلب AuthnRequest SOAP، بحيث لا تعود معالجته ممكنة، كأن تغير مثلاً قيمة نعت الخدمة في فِدرة الرأسية من البروتوكول PAOS إلى قيمة غير معروفة، أو كأن تغير فِدرة الرأسية للزبون ECP ProviderID أو IDPList بحيث يتم إفشال الطلب.

التدابير المضادة: توفير حماية السلامة للرسالة SOAP، باستخدام أمن الرسالة SOAP أو SSL/TLS.

3.2.7.I جانبية اكتشاف مزوّد الهوية

التهديد: تهجم لتسميم الكعكة، حيث يجري تعديل المعلمات داخل الكعكة، حتى يكتشف مزوّد هوية محتال مثلاً.

التدابير المضادة: الآلية الخاصة باستخدام ميدان مشترك تحدّ من جدوى هذا التهديد.

4.2.7.I جانبية اختتام الدورة الوحيد

التهديد: تهجم منفعل للحصول على معرف الهوية لاسم طرف رئيسي.

يستطيع المتهجم المنفعل أثناء المراحل الأولى أن يحصل على المعلومات <LogoutRequest> عند إصدارها في اتجاه الترجيع. وعرض هذه المعطيات بشكل تهديداً للسرية.

التدابير المضادة: ينبغي أن تجري جميع التبادلات على طريق نقل مأمون مثل طبقة التوصيل المأمون (SSL) أو أمن طبقة النقل (TLS).

التهديد: رسالة <LogoutRequest> غير موقّعة

يمكن أن يحقن كيان طفيلي في نظام رسالة غير موقعة <LogoutRequest>، حتى ينكر الخدمة على طرف رئيسي. وبافتراض أن NameID يمكن استنتاجه أو اشتقاقه، يمكن عندئذ التصور بأن يضطر وكيل المستعمل إلى تسليم رسالة <LogoutRequest> مستصنعة (مفبركة).

التدابير المضادة: توقع الرسالة <LogoutRequest>. ويستطيع مزوّد الهوية أن يتحقق عندئذ من هوية طرف رئيسي في غياب طلب موقع.

5.2.7.I جانبيات إدارة معرف هوية الاسم

التهديد: السماح لكيانات النظام أن تربط المعلومات أو أن تعرض معلومات الهوية بطريقة غير مناسبة فتتسبب في الإساءة إلى السرية.

التدابير المضادة: يتعين على مزوّد الهوية أن يهتم باستعمال معرفات هوية أسماء مختلفة مع مزوّدي الخدمة المختلفين إلى نفس الطرف الرئيسي. وينبغي لمزوّد الهوية أن يجفّر معرف هوية الاسم الذي يرجعه إلى مزوّد الخدمة، مما يساعد التفاعلات لاحقاً على استخدام معرف هوية عاتم.

6.2.7.I جانبيات النعت

جرت أعلاه مناقشة التهديدات المتعلقة بالروابط المصاحبة لجانبيات النعت. ولا توجد تهديدات إضافية معروفة خاصة بالجانبية.

التذييل II

تسجيل نمط الوسط الحامل للتوسّعات application/samlassertion+xml MIME

يحتوي هذا التذييل على تسجيل نمط الوسط الحامل للتوسّعات Application/Assertion MIME في اللغة SAML.

اسم نمط الوسط الحامل للتوسّعات MIME

- application

اسم النمط الفرعي MIME

- samlassertion+xml

المعلمات المطلوبة

- لا يوجد

المعلمات الاختيارية

- charset
- مماثلة للمعلمة charset من application/xml الواردة في الطلب RFC 3923 للفريق IETF.

اعتبارات التشفير

- مماثلة للاعتبارات الخاصة بالتطبيق application/xml الواردة في الطلب RFC 3923 للفريق IETF.

الاعتبارات الأمنية

لا تحتوي الأشياء التي من النمط samlassertion+xml على أي محتوى قابل للتنفيذ. ومع ذلك فإن التأكيدات SAML هي أشياء مبنية على اللغة SAML، وبصفتها هذه فهي تمتلك جميع الاعتبارات الأمنية العامة الواردة في البند 10 من الطلب RFC 3923 للفريق IETF، ومعها أيضاً الاعتبارات الإضافية، طالما أنها أشياء أمنية صريحة. فالأشياء التي من النمط

samlassertion+xml تحتوي في الغالب على معطيات، يمكنها أن تعرف هوية شخص طبيعي أو تنتمي إليه، كما يمكن استعمالها أيضاً كقرارات دورات أو تحكّم في النفاذات.

ولمعاكسة القضايا المحتملة، تحتوي الأشياء التي من النمط samlassertion+xml على معطيات ينبغي أن يكون المُصْدر موقّعاً عليها بالشكل المناسب. وأي توقيع من هذه الشاكلة يتعين على مستلم المعطيات أن يتحقق منه لأمرين معاً هما كونه توقيعاً صالحاً، وكونه توقيع المُصدر بنفس الوقت. ويمكن أيضاً لمُصْدري الأشياء التي من النمط samlassertion+xml والحاوية على التأكيدات SAML، أن يجفّروا جميع التأكيدات أو جزءاً منها.

وفوق ذلك تعين جانبيات اللغة SAML وروابط البروتوكول فيها استعمال القنوات المأمونة حسب المقتضى.

وتدرج هذه التوصية (الصيغة 2.0 للغة SAML) في تصميمها تقنيات متنوعة لحماية السرية. مثل المشغّلات العائمة الخاصة بالتفاعلات بين كيانات نظام خاصة التي يمكن إسنادها إلى الأصحاب. والمشغلات يمكن أن تتقابل مع معرفات الهوية في سياقات واسعة (مثل عناوين البريد الإلكتروني ومعرفات هوية الحسابات إلخ) عن طريق الأطراف المعينة فقط.

اعتبارات قابلية التشغيل البيني

يكون لتأكيدات اللغة SAML أرقام صريحة تبين صيغتها. لذلك ينبغي للأطراف الواثقة أن تتأكد من تقيدها بمعلومات صيغة التأكيد. وأن تتصرف بموجب ذلك.

مواصفة منشورة

تحدد الصيغة 2.0 للغة SAML (هذه التوصية) صراحة استخدام نمط الوسط الحامل للتوسّعات MIME application/samlassertion+xml. ومع ذلك فإن من المفهوم أن التأكيدات غير التابعة للغة SAML (أي SAML v1 و/أو SAML v1.1) ينبغي في الواقع نقلها باستخدام الروابط SAML.

التطبيقات التي تستخدم هذا النمط من الأوساط الحاملة

احتمالياً، كل تطبيق ينفذ SAML، وكذلك تلك التطبيقات التي تنفذ مواصفات مبنية على اللغة SAML.

المعلومات الإضافية

الرقم أو الأرقام السحرية

كما في application/xml بصورة عامة. وبصورة خاصة سيكون للعنصر الجذر في اللغة XML من الشيء المرجّع اسم يوصف بمكان الاسم مع:

- اسم محلي هو: Assertion
- معرف URI لمكان الاسم: واحد من المعرفات URI لمكان الاسم في اللغة XML من التأكيد SAML الخاص بالصيغة، كما تعرفه التوصية "المركزية" SAML المناسبة للصيغة.

وفي اللغة SAML خصوصاً، يمكن للعنصر الجذر من الشيء المرجّع أن يكون <saml:Assertion> أو <saml:EncryptedAssertion>، حيث "saml" يمثل أي سابقة لمكان الاسم في اللغة XML، تتقابل مع URI لمكان اسم التأكيد SAML:

urn:oasis:names:tc:SAML:2.0:assertion

توسّع الملف (أو توسّعاته)

لا يوجد

شفرة نمط الملفّ ماكنتوش (أو شفراته)

لا يوجد

عنوان الشخص أو البريد الإلكتروني للاتصال به من أجل مزيد من المعلومات

جرى هذا التسجيل باسم اللجنة التقنية للخدمات الأمنية (Security Services Technical Committee) (SSTC) التابعة للمنظمة المعنية بتقديم معايير المعلومات المهيكلة (OASIS).

الاستعمال المقصود

عمومي

III التذييل

تسجيل نمط الوسط الحامل للتوسّعات application/samlmetadata+xml MIME

يعرّف هذا التذييل نمط الوسط الحامل للتوسّعات MIME – `application/samlmetadata+xml` – لاستعماله مع الوضع التسلسلي للمعطيات الشرحية في اللغة الإرشادية للتدعيم الأمني (SAML).

1) اسم نمط الوسط الحامل للتوسّعات MIME

– `application`

2) اسم النمط الفرعي MIME

– `samlmetadata+xml`

3) المعلمات المطلوبة

– لا يوجد.

4) المعلمات الاختيارية

– `charset`

– مماثلة للمعلمة `charset` من application/xml (انظر الطلب RFC 3023 للفريق IETF).

5) اعتبارات التشفير

– مماثلة للاعتبارات الخاصة بالتطبيق `application/xml` (الواردة في الطلب RFC 3023 للفريق IETF).

6) الاعتبارات الأمنية

لا تحتوي الأشياء التي من النمط `samlmetadata+xml` على أي محتوى قابل للتنفيذ. ومع ذلك فإن هذه الأشياء هي أشياء مبنية على اللغة XML، وبصفتها هذه فهي تمتلك جميع الاعتبارات الأمنية العامة الواردة في البند 10 من الطلب RFC 3023 للفريق IETF.

ولمعاكسة القضايا المحتملة، يمكن للناشر أن يوقع على الأشياء التي من النمط `samlmetadata+xml`. وأي توقيع من هذه الشاكلة يتعين على مستلم المعطيات أن يتحقق منه لأمرين معاً هما كونه توقيعاً صالحاً وأيضاً كونه موقعاً من الناشر.

7) اعتبارات قابلية التشغيل البيني

تعتمد المعطيات الشرحية في اللغة SAML صراحة التعريف بهوية البروتوكولات والصيغ المعتمدة من الكيانات المعرفة الهوية. فيمكن مثلاً الإشارة إلى كيان مزوّد الهوية كمعتمد على الصيغة SAML v2.0

وعلى غيرها من البروتوكولات، إذا كانت هوياتها معرفة بلا لبس عبر معرف URI. ويؤيد هذا البروتوكول أن تنقل المعلومات عبر النعت protocolSupportEnumeration لأشياء المعطيات الشرحية التي هي من النمط **RoleDescriptorType**.

8) توصية منشورة

تحدد المعطيات الشرحية في اللغة SAML صراحة استخدام نمط الوسط الحامل للتوسّعات MIME application/samlmetadata+xml.

والتطبيقات التي يستخدمها هذا النمط من الأوساط هي:

احتمالياً، كل تطبيق ينفّذ الصيغة SAML v2.0، وكذلك تلك التطبيقات التي تنفّذ مواصفات مبنية على اللغة SAML.

9) معلومات إضافية

1) الرقم أو الأرقام السحرية

كما في application/xml بصورة عامة (انظر الطلب RFC 3023 للفريق IETF). وبصورة خاصة سيكون العنصر الجذر في اللغة XML من الشيء المرجّع اسم يوصف بمكان الاسم مع:

- اسم محلي هو EntityDescriptor أو AffiliationDescriptor أو EntitiesDescriptor.
- معرف URI لمكان الاسم: urn:oasis:names:tc:SAML:2.0:metadata (مكان الاسم للمعطيات الشرحية في الصيغة SAML v2.0).

10) توسّع الملف (أو توسّعاته)

لا يوجد.

11) شفرة نمط الملف ماكنتوش (أو شفراته)

لا يوجد.

12) عنوان الشخص أو البريد الإلكتروني للاتصال به من أجل مزيد من المعلومات

جرى هذا التسجيل باسم اللجنة التقنية للخدمات الأمنية (Security Services Technical Committee) (SSTC) التابعة للمنظمة المعنية بتقديم معايير المعلومات المهيكلة (OASIS).

13) الاستعمال المقصود

عمومي.

التذييل IV

استعمال طبقة التوصيل المأمون (SSL)

يمكن لبعض عمليات التنفيذ في اللغة SAML أن تقبل استعماله الصيغة SSL 3.1 بالإضافة إلى الصيغة TLS 1.0 أو كبديل منها (TLS: أمن طبقة النقل). وعمليات التنفيذ التي تستعمل الصيغة SSL 3.0 ينبغي لها أن تتأكد من أن الأمن الكلي للتنفيذ متّسق مع التقييدات المفروضة على استخدام التجفيرات في TLS. مثل المطلب القائل باستخدام متتابعة التشفير TLS_RSA_WITH_3DES_EDE_CBC_SHA المترجم إلى استعمال متتابعة التشفير SSL_RSA_WITH_3DES_EDE_CBC_SHA. وعمليات التنفيذ FIPS ذات المقدرة SSL تستخدم متتابعة التجفير FIPS المقابلة لمتتابعة التشفير SSL: SSL_RSA_WITH_3DES_EDE_CBC_SHA.

وعمليات التنفيذ TLS لجانبية التوقيع الوحيد للمتصفح على الويب في اللغة SAML التي تدعم متتابعة التشفير TLS_RSA_WITH_3DES_EDE_CBC_SHA، عليها أن تستعمل متتابعة التجفير SSL_RSA_WITH_3DES_EDE_CBC_SHA.

التذييل V

تخطيطة SAML لسياق الاستيقان

يحتوي هذا التذييل على تخطيطة SAML لسياق الاستيقان من أجل شهادة SSL (sslcert).

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
      <xs:documentation>
        Class identifier: urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
        Document identifier: saml-schema-authn-context-sslcert-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
          V2.0 (March, 2005):
            New authentication_u99 context class schema for SAML V2.0.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
            <xs:element ref="GoverningAgreements" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
```

```
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnMethodBaseType">
          <xs:sequence>
            <xs:element ref="PrincipalAuthenticationMechanism"/>
            <xs:element ref="Authenticator"/>
            <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
        <xs:restriction base="PrincipalAuthenticationMechanismType">
          <xs:sequence>
            <xs:element ref="RestrictedPassword"/>
          </xs:sequence>
          <xs:attribute name="preauth" type="xs:integer" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorBaseType">
          <xs:sequence>
            <xs:element ref="DigSig"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="PublicKeyType">
      <xs:complexContent>
        <xs:restriction base="PublicKeyType">
          <xs:attribute name="keyValidation" type="xs:anyURI"
fixed="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
        <xs:restriction base="AuthenticatorTransportProtocolType">
          <xs:sequence>
            <xs:choice>
              <xs:element ref="SSL"/>
              <xs:element ref="WTLS"/>
            </xs:choice>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

  </xs:redefine>

</xs:schema>
```

التذييل VI

تخطيطة XML لأنماط سياق الاستيقان

يعطي هذا التذييل القائمة الكاملة بتخطيطة XML لأنماط سياق الاستيقان، كما يعطي تخطيطة XML لسياق الاستيقان بذاتها، والمستعملة لإقرار صلاحية الإعلانات المعممة الفردية. وليس لتخطيطة الأنماط مكان اسم هدف بحد ذاته، لذلك فهو متضمن في التذييل V.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
      Document identifier: saml-schema-authn-context-types-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
          V2.0 (March, 2005):
          New core authentication context schema types for SAML V2.0.
    </xs:documentation>
  </xs:annotation>

  <xs:element name="AuthenticationContextDeclaration"
type="AuthnContextDeclarationBaseType">
    <xs:annotation>
      <xs:documentation>
        A particular assertion on an identity
        provider's part with respect to the authentication
        context associated with an authentication assertion.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Identification" type="IdentificationType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that describe the
        processes and mechanisms
        the Authentication Authority uses to initially create
        an association between a Principal
        and the identity (or name) by which the Principal will
        be known
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PhysicalVerification">
    <xs:annotation>
      <xs:documentation>
        This element indicates that identification has been
        performed in a physical
        face-to-face meeting with the principal and not in an
        online manner.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:attribute name="credentialLevel">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="primary"/>
            <xs:enumeration value="secondary"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
```

```
  </xs:complexType>
</xs:element>

<xs:element name="WrittenConsent" type="ExtensionOnlyType"/>

<xs:element name="TechnicalProtection" type="TechnicalProtectionBaseType">
  <xs:annotation>
    <xs:documentation>
      Refers to those characterstics that describe how the
      'secret' (the knowledge or possession
      of which allows the Principal to authenticate to the
      Authentication Authority) is kept secure
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SecretKeyProtection" type="SecretKeyProtectionType">
  <xs:annotation>
    <xs:documentation>
      This element indicates the types and strengths of
      facilities
      of a UA used to protect a shared secret key from
      unauthorized access and/or use.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="PrivateKeyProtection" type="PrivateKeyProtectionType">
  <xs:annotation>
    <xs:documentation>
      This element indicates the types and strengths of
      facilities
      of a UA used to protect a private key from
      unauthorized access and/or use.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="KeyActivation" type="KeyActivationType">
  <xs:annotation>
    <xs:documentation>The actions that must be performed
      before the private key can be used. </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="KeySharing" type="KeySharingType">
  <xs:annotation>
    <xs:documentation>Whether or not the private key is shared
      with the certificate authority.</xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="KeyStorage" type="KeyStorageType">
  <xs:annotation>
    <xs:documentation>
      In which medium is the key stored.
      memory - the key is stored in memory.
      smartcard - the key is stored in a smartcard.
      token - the key is stored in a hardware token.
      MobileDevice - the key is stored in a mobile device.
      MobileAuthCard - the key is stored in a mobile
      authentication card.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SubscriberLineNumber" type="ExtensionOnlyType"/>
<xs:element name="UserSuffix" type="ExtensionOnlyType"/>

<xs:element name="Password" type="PasswordType">
  <xs:annotation>
```

```
    <xs:documentation>
      This element indicates that a password (or passphrase)
      has been used to
      authenticate the Principal to a remote system.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationPin" type="ActivationPinType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that a Pin (Personal
      Identification Number) has been used to authenticate the Principal
      to some local system in order to activate a key.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Token" type="TokenType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that a hardware or software
      token is used
      as a method of identifying the Principal.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="TimeSyncToken" type="TimeSyncTokenType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that a time synchronization
      token is used to identify the Principal. hardware -
      the time synchonization
      token has been implemented in hardware. software - the
      time synchronization
      token has been implemented in software. SeedLength -
      the length, in bits, of the
      random seed used in the time synchronization token.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Smartcard" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that a smartcard is used to
      identify the Principal.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="Length" type="LengthType">
  <xs:annotation>
    <xs:documentation>
      This element indicates the minimum and/or maximum
      ASCII length of the password which is enforced (by the UA or the
      IdP). In other words, this is the minimum and/or maximum number of
      ASCII characters required to represent a valid password.
      min - the minimum number of ASCII characters required
      in a valid password, as enforced by the UA or the IdP.
      max - the maximum number of ASCII characters required
      in a valid password, as enforced by the UA or the IdP.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimit" type="ActivationLimitType">
  <xs:annotation>
    <xs:documentation>
      This element indicates the length of time for which an
```

```
        PIN-based authentication is valid.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Generation">
    <xs:annotation>
      <xs:documentation>
        Indicates whether the password was chosen by the
        Principal or auto-supplied by the Authentication Authority.
        principalchosen - the Principal is allowed to choose
        the value of the password. This is true even if
        the initial password is chosen at random by the UA or
        the IdP and the Principal is then free to change
        the password.
        automatic - the password is chosen by the UA or the
        IdP to be cryptographically strong in some sense,
        or to satisfy certain password rules, and that the
        Principal is not free to change it or to choose a new password.
      </xs:documentation>
    </xs:annotation>

    <xs:complexType>
      <xs:attribute name="mechanism" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="principalchosen"/>
            <xs:enumeration value="automatic"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>

  <xs:element name="AuthnMethod" type="AuthnMethodBaseType">
    <xs:annotation>
      <xs:documentation>
        Refers to those characteristics that define the
        mechanisms by which the Principal authenticates to the
        Authentication Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="PrincipalAuthenticationMechanism"
type="PrincipalAuthenticationMechanismType">
    <xs:annotation>
      <xs:documentation>
        The method that a Principal employs to perform
        authentication to local system components.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="Authenticator" type="AuthenticatorBaseType">
    <xs:annotation>
      <xs:documentation>
        The method applied to validate a principal's
        authentication across a network
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ComplexAuthenticator" type="ComplexAuthenticatorType">
    <xs:annotation>
      <xs:documentation>
        Supports Authenticators with nested combinations of
        additional complexity.
      </xs:documentation>
    </xs:annotation>
  </xs:element>
```

```
  <xs:element name="PreviousSession" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        Indicates that the Principal has been strongly
        authenticated in a previous session during which the IdP has set a
        cookie in the UA. During the present session the Principal has only
        been authenticated by the UA returning the cookie to the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ResumeSession" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        Rather like PreviousSession but using stronger
        security. A secret that was established in a previous session with
        the Authentication Authority has been cached by the local system
        and is now re-used (e.g. a Master Secret is used to derive new
        session keys in TLS, WTLS).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="ZeroKnowledge" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a zero knowledge technique as specified in ISO/IEC
        9798-5.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SharedSecretChallengeResponse"
type="SharedSecretChallengeResponseType"/>

  <xs:complexType name="SharedSecretChallengeResponseType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a challenge-response protocol utilizing shared
        secret keys and symmetric cryptography.
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="method" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="DigSig" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated by a mechanism which involves the Principal computing
        a digital signature over at least challenge data provided
        by the IdP.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricDecryption" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a private key but it is used
        in decryption mode, rather than signature mode. For example, the
        Authentication Authority generates a secret and encrypts it using
        the local system's public key: the local system then proves it has
        decrypted the secret.
      </xs:documentation>
```

```
    </xs:annotation>
  </xs:element>

  <xs:element name="AsymmetricKeyAgreement" type="PublicKeyType">
    <xs:annotation>
      <xs:documentation>
        The local system has a private key and uses it for
        shared secret key agreement with the Authentication Authority
        (e.g., via Diffie Helman).
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:complexType name="PublicKeyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="keyValidation" use="optional"/>
  </xs:complexType>

  <xs:element name="IPAddress" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Principal has been
        authenticated through connection from a particular IP address.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="SharedSecretDynamicPlaintext" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        The local system and Authentication Authority
        share a secret key. The local system uses this to encrypt a
        randomised string to pass to the Authentication Authority.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="AuthenticatorTransportProtocol"
type="AuthenticatorTransportProtocolType">
    <xs:annotation>
      <xs:documentation>
        The protocol across which Authenticator information is
        transferred to an Authentication Authority verifier.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="HTTP" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using bare HTTP utilizing no additional security
        protocols.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="IPSec" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
        This element indicates that the Authenticator has been
        transmitted using a transport mechanism protected by an IPSEC session.
      </xs:documentation>
    </xs:annotation>
  </xs:element>

  <xs:element name="WTLS" type="ExtensionOnlyType">
    <xs:annotation>
      <xs:documentation>
```

```
      This element indicates that the Authenticator has been
      transmitted using a transport mechanism protected by a WTLS session.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="MobileNetworkNoEncryption" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Authenticator has been
      transmitted solely across a mobile network using no additional
      security mechanism.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="MobileNetworkRadioEncryption" type="ExtensionOnlyType"/>
<xs:element name="MobileNetworkEndToEndEncryption" type="ExtensionOnlyType"/>

<xs:element name="SSL" type="ExtensionOnlyType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Authenticator has been
      transmitted using a transport mechanism protected by an SSL or TLS
      session.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="PSTN" type="ExtensionOnlyType"/>
<xs:element name="ISDN" type="ExtensionOnlyType"/>
<xs:element name="ADSL" type="ExtensionOnlyType"/>

<xs:element name="OperationalProtection" type="OperationalProtectionType">
  <xs:annotation>
    <xs:documentation>
      Refers to those characteristics that describe
      procedural security controls employed by the Authentication Authority.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="SecurityAudit" type="SecurityAuditType"/>
<xs:element name="SwitchAudit" type="ExtensionOnlyType"/>
<xs:element name="DeactivationCallCenter" type="ExtensionOnlyType"/>

<xs:element name="GoverningAgreements" type="GoverningAgreementsType">
  <xs:annotation>
    <xs:documentation>
      Provides a mechanism for linking to external (likely
      human readable) documents in which additional business agreements,
      (e.g., liability constraints, obligations, etc.) can be placed.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="GoverningAgreementRef" type="GoverningAgreementRefType"/>

<xs:simpleType name="nymType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="anonymity"/>
    <xs:enumeration value="verinymity"/>
    <xs:enumeration value="pseudonymity"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AuthnContextDeclarationBaseType">
  <xs:sequence>
    <xs:element ref="Identification" minOccurs="0"/>
    <xs:element ref="TechnicalProtection" minOccurs="0"/>
    <xs:element ref="OperationalProtection" minOccurs="0"/>
```

```
    <xs:element ref="AuthnMethod" minOccurs="0"/>
    <xs:element ref="GoverningAgreements" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="ID" type="xs:ID" use="optional"/>
</xs:complexType>

<xs:complexType name="IdentificationType">
  <xs:sequence>
    <xs:element ref="PhysicalVerification" minOccurs="0"/>
    <xs:element ref="WrittenConsent" minOccurs="0"/>
    <xs:element ref="GoverningAgreements" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="nym" type="nymType">
    <xs:annotation>
      <xs:documentation>
        This attribute indicates whether or not the
        Identification mechanisms allow the actions of the Principal to
        be linked to an actual end user.
      </xs:documentation>
    </xs:annotation>
  </xs:attribute>
</xs:complexType>

<xs:complexType name="TechnicalProtectionBaseType">
  <xs:sequence>
    <xs:choice minOccurs="0">
      <xs:element ref="PrivateKeyProtection"/>
      <xs:element ref="SecretKeyProtection"/>
    </xs:choice>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="OperationalProtectionType">
  <xs:sequence>
    <xs:element ref="SecurityAudit" minOccurs="0"/>
    <xs:element ref="DeactivationCallCenter" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AuthnMethodBaseType">
  <xs:sequence>
    <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
    <xs:element ref="Authenticator" minOccurs="0"/>
    <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="GoverningAgreementsType">
  <xs:sequence>
    <xs:element ref="GoverningAgreementRef" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="GoverningAgreementRefType">
  <xs:attribute name="governingAgreementRef" type="xs:anyURI" use="required"/>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
  <xs:sequence>
    <xs:element ref="Password" minOccurs="0"/>
    <xs:element ref="RestrictedPassword" minOccurs="0"/>
    <xs:element ref="Token" minOccurs="0"/>
    <xs:element ref="Smartcard" minOccurs="0"/>
    <xs:element ref="ActivationPin" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
```

```
  <xs:attribute name="preauth" type="xs:integer" use="optional"/>
</xs:complexType>

<xs:group name="AuthenticatorChoiceGroup">
  <xs:choice>
    <xs:element ref="PreviousSession"/>
    <xs:element ref="ResumeSession"/>
    <xs:element ref="DigSig"/>
    <xs:element ref="Password"/>
    <xs:element ref="RestrictedPassword"/>
    <xs:element ref="ZeroKnowledge"/>
    <xs:element ref="SharedSecretChallengeResponse"/>
    <xs:element ref="SharedSecretDynamicPlaintext"/>
    <xs:element ref="IPAddress"/>
    <xs:element ref="AsymmetricDecryption"/>
    <xs:element ref="AsymmetricKeyAgreement"/>
    <xs:element ref="SubscriberLineNumber"/>
    <xs:element ref="UserSuffix"/>
    <xs:element ref="ComplexAuthenticator"/>
  </xs:choice>
</xs:group>

<xs:group name="AuthenticatorSequenceGroup">
  <xs:sequence>
    <xs:element ref="PreviousSession" minOccurs="0"/>
    <xs:element ref="ResumeSession" minOccurs="0"/>
    <xs:element ref="DigSig" minOccurs="0"/>
    <xs:element ref="Password" minOccurs="0"/>
    <xs:element ref="RestrictedPassword" minOccurs="0"/>
    <xs:element ref="ZeroKnowledge" minOccurs="0"/>
    <xs:element ref="SharedSecretChallengeResponse" minOccurs="0"/>
    <xs:element ref="SharedSecretDynamicPlaintext" minOccurs="0"/>
    <xs:element ref="IPAddress" minOccurs="0"/>
    <xs:element ref="AsymmetricDecryption" minOccurs="0"/>
    <xs:element ref="AsymmetricKeyAgreement" minOccurs="0"/>
    <xs:element ref="SubscriberLineNumber" minOccurs="0"/>
    <xs:element ref="UserSuffix" minOccurs="0"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:group>

<xs:complexType name="AuthenticatorBaseType">
  <xs:sequence>
    <xs:group ref="AuthenticatorChoiceGroup"/>
    <xs:group ref="AuthenticatorSequenceGroup"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ComplexAuthenticatorType">
  <xs:sequence>
    <xs:group ref="AuthenticatorChoiceGroup"/>
    <xs:group ref="AuthenticatorSequenceGroup"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AuthenticatorTransportProtocolType">
  <xs:sequence>
    <xs:choice minOccurs="0">
      <xs:element ref="HTTP"/>
      <xs:element ref="SSL"/>
      <xs:element ref="MobileNetworkNoEncryption"/>
      <xs:element ref="MobileNetworkRadioEncryption"/>
      <xs:element ref="MobileNetworkEndToEndEncryption"/>
      <xs:element ref="WTLS"/>
      <xs:element ref="IPSec"/>
      <xs:element ref="PSTN"/>
      <xs:element ref="ISDN"/>
      <xs:element ref="ADSL"/>
    </xs:choice>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
```

```
  </xs:complexType>

  <xs:complexType name="KeyActivationType">
    <xs:sequence>
      <xs:element ref="ActivationPin" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="KeySharingType">
    <xs:attribute name="sharing" type="xs:boolean" use="required"/>
  </xs:complexType>

  <xs:complexType name="PrivateKeyProtectionType">
    <xs:sequence>
      <xs:element ref="KeyActivation" minOccurs="0"/>
      <xs:element ref="KeyStorage" minOccurs="0"/>
      <xs:element ref="KeySharing" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="PasswordType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="ExternalVerification" type="xs:anyURI" use="optional"/>
  </xs:complexType>

  <xs:element name="RestrictedPassword" type="RestrictedPasswordType"/>

  <xs:complexType name="RestrictedPasswordType">
    <xs:complexContent>
      <xs:restriction base="PasswordType">
        <xs:sequence>
          <xs:element name="Length" type="RestrictedLengthType" minOccurs="1"/>
          <xs:element ref="Generation" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ExternalVerification" type="xs:anyURI"
use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="RestrictedLengthType">
    <xs:complexContent>
      <xs:restriction base="LengthType">
        <xs:attribute name="min" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:integer">
              <xs:minInclusive value="3"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
        <xs:attribute name="max" type="xs:integer" use="optional"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="ActivationPinType">
    <xs:sequence>
      <xs:element ref="Length" minOccurs="0"/>
      <xs:element ref="Alphabet" minOccurs="0"/>
      <xs:element ref="Generation" minOccurs="0"/>
      <xs:element ref="ActivationLimit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
```

```
</xs:complexType>

<xs:element name="Alphabet" type="AlphabetType"/>
<xs:complexType name="AlphabetType">
  <xs:attribute name="requiredChars" type="xs:string" use="required"/>
  <xs:attribute name="excludedChars" type="xs:string" use="optional"/>
  <xs:attribute name="case" type="xs:string" use="optional"/>
</xs:complexType>

<xs:complexType name="TokenType">
  <xs:sequence>
    <xs:element ref="TimeSyncToken"/>
    <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:simpleType name="DeviceTypeType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="hardware"/>
    <xs:enumeration value="software"/>
  </xs:restriction>
</xs:simpleType>

<xs:simpleType name="booleanType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="true"/>
    <xs:enumeration value="false"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="TimeSyncTokenType">
  <xs:attribute name="DeviceType" type="DeviceTypeType" use="required"/>
  <xs:attribute name="SeedLength" type="xs:integer" use="required"/>
  <xs:attribute name="DeviceInHand" type="booleanType" use="required"/>
</xs:complexType>

<xs:complexType name="ActivationLimitType">
  <xs:choice>
    <xs:element ref="ActivationLimitDuration"/>
    <xs:element ref="ActivationLimitUsages"/>
    <xs:element ref="ActivationLimitSession"/>
  </xs:choice>
</xs:complexType>

<xs:element name="ActivationLimitDuration" type="ActivationLimitDurationType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Key Activation Limit is
      defined as a specific duration of time.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimitUsages" type="ActivationLimitUsagesType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Key Activation Limit is
      defined as a number of usages.
    </xs:documentation>
  </xs:annotation>
</xs:element>

<xs:element name="ActivationLimitSession" type="ActivationLimitSessionType">
  <xs:annotation>
    <xs:documentation>
      This element indicates that the Key Activation Limit is
      the session.
    </xs:documentation>
  </xs:annotation>
</xs:element>
```

```
  <xs:complexType name="ActivationLimitDurationType">
    <xs:attribute name="duration" type="xs:duration" use="required"/>
  </xs:complexType>

  <xs:complexType name="ActivationLimitUsagesType">
    <xs:attribute name="number" type="xs:integer" use="required"/>
  </xs:complexType>

  <xs:complexType name="ActivationLimitSessionType"/>

  <xs:complexType name="LengthType">
    <xs:attribute name="min" type="xs:integer" use="required"/>
    <xs:attribute name="max" type="xs:integer" use="optional"/>
  </xs:complexType>

  <xs:simpleType name="mediumType">
    <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="memory"/>
      <xs:enumeration value="smartcard"/>
      <xs:enumeration value="token"/>
      <xs:enumeration value="MobileDevice"/>
      <xs:enumeration value="MobileAuthCard"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="KeyStorageType">
    <xs:attribute name="medium" type="mediumType" use="required"/>
  </xs:complexType>

  <xs:complexType name="SecretKeyProtectionType">
    <xs:sequence>
      <xs:element ref="KeyActivation" minOccurs="0"/>
      <xs:element ref="KeyStorage" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="SecurityAuditType">
    <xs:sequence>
      <xs:element ref="SwitchAudit" minOccurs="0"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ExtensionOnlyType">
    <xs:sequence>
      <xs:element ref="Extension" minOccurs="0"  maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="Extension" type="ExtensionType"/>

  <xs:complexType name="ExtensionType">
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>


<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:oasis:names:tc:SAML:2.0:ac"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac"
  blockDefault="substitution"
  version="2.0">

  <xs:annotation>
    <xs:documentation>
```

```
      Document identifier: saml-schema-authn-context-2.0
      Location: http://docs.oasis-open.org/security/saml/v2.0/
      Revision history:
        V2.0 (March, 2005):
          New core authentication context schema for SAML V2.0.
          This is just an include of all types from the schema
          referred to in the include statement below.
    </xs:documentation>
  </xs:annotation>

  <xs:include schemaLocation="saml-schema-authn-context-types-2.0.xsd"/>

</xs:schema>
```

التذييل VII

جانبية النعت PAC من DCE من اللغة SAML

يدرس هذا التذييل جانبية الرابطة SAML لشهادات النعت الخاص (PAC) من بيئة الحساب الموزع (DCE) (انظر opensource DCE).

1.VII جانبية النعت PAC من DCE

تعرف جانبية النعت PAC من DCE التعبير عن معلومات PAC من DCE بصفتها أسماء وقيم نعت في SAML. وتستعمل لتقييس الوضع على تقابل بين المعلومات الأولية التي تكون هوية طرف رئيسي في البيئة DCE وبين مجموعة من نعوت اللغة SAML. وهذه الجانبية مبنية على جانبية النعت UUID (معرف هوية وحيد عالمي) المعرف في الفقرة الفرعية 3.9.4.11.

1) المعلومات المطلوبة

- **تعريف الهوية:** `urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE` (وهذا هو أيضاً مكان الاسم الهدف المسند في تخطيطة جانبية النعت PAC من DCE في الملحق A)
- **معلومات الاتصال:** security-services-comment@lists.oasis-open.org
- **الوصف:** وارد أدناه.
- **التحيينات:** لا يوجد.

2) وصف الشهادات PAC

إن الشهادات PAC من البيئة DCE هي بنية قابلة للتوسّع يمكنها أن تحمل نعوتاً من سجل البيئة DCE، ولكن مجموعة مركزية من المعلومات هي مشتركة بين الأطراف الرئيسية وتشكل لحمة الهوية في البيئة DCE:

- "عِزْبة" أو "خلية" الطرف الرئيسي في البيئة DCE.
- معرف الهوية الوحيد للطرف الرئيسي.
- الطرف المحلي الأولي في البيئة DCE الذي يكون الطرف الرئيسي عضواً فيها.
- مجموعة الأفرقة المحلية في البيئة DCE التي يكون الطرف الرئيسي عضواً فيها (قيم متعددة).
- مجموعة الأفرقة الأجنبية في البيئة DCE التي يكون الطرف الرئيسي عضواً فيها (قيم متعددة).

القيمة أو القيم الأساسية لكل واحد من هذه النعوت هي من معرفات الهوية UUID.

3) تسمية النعت في اللغة SAML

تعرّف هذه الجانبية وضع معلومات البيئة DCE على تقابل مع نعوت اللغة SAML، وبذلك تعرّف أسماء النعوت الخاصة الحقيقية، بدلاً من اصطلاح على التسمية.

وفي جميع النعوت التي تعرّفها هذه الجانبية، يجب أن يأخذ نعت اللغة XML NameFormat في العناصر <Attribute> القيمة: urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

ولتمكين الإنسان من قراءة الأسماء، ربما تحتاج بعض التطبيقات إلى مطلب أيضاً هو أن تحمل سلسلة اختيارية من الأسماء، إلى جانب المعرّف الموحّد URI. ويمكن استخدام النعت XML الاختياري FriendlyName لتحقيق هذا الغرض.

4) مقارنة اسم النعت

يعود عنصران من <Attribute> إلى النعت نفسه من SAML إذا، وفقط إذا، كانت قيمتا النعت Name XML متساويتين بمعنى التوصية ITU-T X.667. وليس للنعت FriendlyName أي دور يلعبه في هذه المقارنة.

5) نعوت اللغة XML الخاصة بالجانبية

لا توجد نعوت إضافية XML معرفة لاستعمالها مع العنصر <Attribute>.

6) قيم النعت في SAML

القيمة أو القيم الأساسية لكل واحد من النعوت التي تعرّفها هذه الجانبية هي من معرفات الهوية UUID. وقواعد تركيب الاسم URN المشروحة في الفقرة الفرعية 3.9.4.11 تستخدم لتمثيل مثل هذه القيم.

ومع ذلك فإن هذه الجانبية تسمح لمعلومات إضافية بأن تصحب قيمة المعرّف UUID، وهي تتكون من سلسلة سهلة على الإنسان قراءتها، ومن معرّف UUID إضافي يمثل خلية أو عِزْبة في البيئة DCE. وتحمل المعلومات الإضافية في العنصر <AttributeValue> داخل نعتي اللغة XML FriendlyName وRealm (العِزْبة) المعرّفين في مكان الاسم XML urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE. وهذا ليس مماثلاً للنعت XML FriendlyName المعرّف في البند 8. وإن كان لهما نفس الغرض الأساسي.

وقائمة التخطيطة التالية تبين كيف تستعمل النعوت والأنماط المعقدة XML الخاصة بالجانبية في النمط xsi:type (الملحق A)

```
<schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE"
    xmlns:dce="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <annotation>
        <documentation>
            Document identifier: saml-schema-dce-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V2.0 (March, 2005):
                Custom schema for DCE attribute profile, first published in
SAML 2.0.
        </documentation>
    </annotation>
    <complexType name="DCEValueType">
        <simpleContent>
            <extension base="anyURI">
```

```
                <attribute ref="dce:Realm" use="optional"/>
                <attribute ref="dce:FriendlyName" use="optional"/>
            </extension>
        </simpleContent>
    </complexType>
    <attribute name="Realm" type="anyURI"/>
    <attribute name="FriendlyName" type="string"/>
</schema>
```

7) تعريفات النعت

فيما يلي مجموعة من النعوت SAML تعرّفها هذه الجانبية. وفي كل حالة يمكن إدراج النعت XML xsi:type في العنصر <AttributeValue>، ولكنه يجب أن يأخذ القيمة **dce:DCEValueType**، حيث تكون السابقة DCE اختيارية ويتعين أن تكون مرتبطة بمكان الاسم XML.

ومثل هذا الاستعمال للنمط xsi:type يتطلب من مستهلكي النعت إقرار صلاحيته، لإدراج تخطيطة التوسّع التي تعرفها هذه الجانبية.

أ) Realm (العِزْبة)

يمثل هذا النعت الوحيد القيمة العزبة أو الخلية من البيئة DCE التابعة لصاحب التأكيد SAML.

الاسم: urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:realm

ويحتوي العنصر الوحيد <AttributeValue> على معرّف UUID بشكل الاسم URN الذي يعرّف هوية العزبة أو الخلية من البيئة DCE التابعة لصاحب التأكيد SAML مع نعت XML FriendlyName اختياري خاص بالجانبية يحتوي على اسم سلسلة المنطقة.

ب) Principal (الطرف الرئيسي)

يمثل هذا النعت الوحيد القيمة الهوية الرئيسية في البيئة DCE التابعة لصاحب التاكيد SAML.

الاسم: urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:principal

ويحتوي العنصر الوحيد <AttributeValue> على معرّف UUID بشكل الاسم URN الذي يعرّف الهوية الرئيسية في البيئة DCE التابعة لصاحب التأكيد SAML، مع نعت XML FriendlyName اختياري خاص الجانبية يحتوي على اسم سلسلة الطرف الرئيسي.

ويمكن للنعت XML Realm الخاص الجانبية أن يكون مدرجاً، ويتعين أن يحتوي على معرّف UUID بشكل الاسم URN الذي يعرّف هوية العِزْبة أو الخلية من البيئة DCE التابعة لصاحب التأكيد SAML.

ج) Primary group (الفريق الأولي)

يمثل هذا النعت الوحيد القيمة الفريق الأولي DCE الذي يكون صاحب التأكيد SAML عضواً فيه.

الاسم: urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:primary-group

ويحتوي العنصر الوحيد <AttributeValue> على معرّف UUID بشكل الاسم URN الذي يعرّف هوية الفريق الأولي DCE لصاحب التأكيد SAML، مع نعت XML FriendlyName اختياري خاص بالجانبية يحتوي على اسم سلسلة الفريق.

ويمكن للنعت XML Realm الخاص بالجانبية أن يكون مدرجاً، ويتعين أن يحتوي على معرّف UUID بشكل الاسم URN يعرف هوية العِزْبة أو الخلية من البيئة DCE التابعة لصاحب التأكيد SAML.

د) **Groups (الأفرقة)**

يمثل هذا النعت المتعدد القيم الأفرقة المحلية في البيئة DCE التي يكون صاحب التأكيد SAML عضواً فيها.

الاسم: `urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:groups`

ويحتوي كل عنصر `<AttributeValue>` على معرف UUID بشكل الاسم URN الذي يعرّف هوية عضو من فريق البيئة DCE التابع لصاحب التأكيد SAML، مع نعت XML `FriendlyName` اختياري خاص بالجانبية يحتوي على اسم سلسلة الفريق.

ويمكن للنعت Realm XML أن يكون مدرجاً، ويتعين أن يحتوي على معرّف UUID بشكل الاسم URN يعرّف هوية العِزْبة أو الخلية من البيئة DCE التابعة لصاحب التأكيد SAML.

هـ) **Foreign groups (الأفرقة الأجنبية)**

يمثل هذا النعت المتعدد القيم الأفرقة الأجنبية في البيئة DCE التي يكون صاحب التأكيد SAML عضواً فيها.

الاسم: `urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:foreign-groups`

ويحتوي كل عنصر `<AttributeValue>` على معرّف UUID بشكل الاسم URN الذي يعرّف هوية عضو من الفريق الأجنبي في البيئة DCE التابع لصاحب التأكيد SAML، مع نعت XML `FriendlyName` اختياري خاص بالجانبية يحتوي على اسم سلسلة الفريق.

ويمكن للنعت Realm XML أن يكون مدرجاً، ويتعين أن يحتوي على معرّف UUID بشكل الاسم URN يعرّف هوية العِزْبة أو الخلية من البيئة DCE التابعة للفريق الأجنبي.

2.VII تخطيطة البيئة DEC في اللغة SAML

هذه هي تخطيطة سياق الاستيقان SAML لبيئة الحساب الموزع (DCE).

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE"
    xmlns:dce="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE"
    xmlns="http://www.w3.org/2001/XMLSchema"
    elementFormDefault="unqualified"
    attributeFormDefault="unqualified"
    blockDefault="substitution"
    version="2.0">
    <annotation>
        <documentation>
            Document identifier: saml-schema-dce-2.0
            Location: http://docs.oasis-open.org/security/saml/v2.0/
            Revision history:
            V2.0 (March, 2005):
                Custom schema for DCE attribute profile, first published in SAML 2.0.
        </documentation>
    </annotation>
    <complexType name="DCEValueType">
        <simpleContent>
            <extension base="anyURI">
                <attribute ref="dce:Realm" use="optional"/>
                <attribute ref="dce:FriendlyName" use="optional"/>
            </extension>
        </simpleContent>
    </complexType>
    <attribute name="Realm" type="anyURI"/>
    <attribute name="FriendlyName" type="string"/>
</schema>
```

3.VII مثـــال

فيما يلي مثال على تحويل معطيات الشهادات PAC إلى نعوت اللغة SAML تنتمي إلى طرف رئيسي في البيئة DCE اسمه "jdoe" في العِزْبة "example.com"، وعضو في الفريقين المحليين "cubicle-dwellers" و"underpaid" وفي فريق أجنبي "engineers".

```
<saml:Assertion
xmlns:dce="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE" ...>
  <saml:Issuer>...</saml:Issuer>
  <saml:Subject>...</saml:Subject>
  <saml:AttributeStatement>
  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
 Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:realm">
    <saml:AttributeValue xsi:type="dce:DCEValueType"
dce:FriendlyName="example.com">
    urn:uuid:003c6cc1-9ff8-10f9-990f-004005b13a2b
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
 Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:principal">
    <saml:AttributeValue xsi:type="dce:DCEValueType"
dce:FriendlyName="jdoe">
    urn:uuid:00305ed1-a1bd-10f9-a2d0-004005b13a2b
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
 Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:primary-group">
    <saml:AttributeValue xsi:type="dce:DCEValueType"
 dce:FriendlyName="cubicle-dwellers">
    urn:uuid:008c6181-a288-10f9-b6d6-004005b13a2b
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
 Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:groups">
    <saml:AttributeValue xsi:type="dce:DCEValueType"
 dce:FriendlyName="cubicle-dwellers">
    urn:uuid:008c6181-a288-10f9-b6d6-004005b13a2b
    </saml:AttributeValue>
    <saml:AttributeValue xsi:type="dce:DCEValueType"
dce:FriendlyName="underpaid">
    urn:uuid:006a5a91-a2b7-10f9-824d-004005b13a2b
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
 Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:DCE:foreign-groups">
    <saml:AttributeValue xsi:type="dce:DCEValueType"
dce:FriendlyName="engineers"
 dce:Realm="urn:uuid:00583221-a35f-10f9-8b6e-004005b13a2b">
    urn:uuid:00099cf1-a355-10f9-9e95-004005b13a2b
    </saml:AttributeValue>
  </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

التذييل VIII

توضيحات المنظمة OASIS حول اللغة SAML

يضيف هذا التذييل المراجعات التي جرت على الصيغة SAML v2.0 داخل المنظمة OASIS. لقد قرر فريق اللغة SAML في المنظمة OASIS أن ينشر هذه التعليقات التوضيحية كوثيقة منفصلة (انظر OASIS PE:2006). إن هذه التوضيحات ليست معيارية، ولم تدمج في الصيغة 2.0 للغة SAML من المنظمة OASIS. وفي هذه التوصية جرى إيراد هذه المراجعات في هذا التذييل لضمان أن يكون الذين ينفذون اللغة SAML على اطّلاع على المناقشات التي جرت بعد إصدار صيغة اللغة SAML v2.0 من المنظمة OASIS بصفتها أحد معايير المنظمة OASIS.

1.VIII تصويت خطأ محتمل: PE14

الوصف: يحتاج النعت Allowcreate إلى تعريف أكثر وضوحاً

قابلية الانطباق في هذه التوصية

يرجى الرجوع إلى الملاحظات المناسبة في الفقرتين الفرعيتين 1.4.2.8 و6.2.8. وعلاوة على ذلك نقدم أدناه توضيحاً يخص المقطع الثاني من الفقرة الفرعية 3.6.2.8:

إذا كان الطلب يتضمن العنصر <Terminate>، يكون المزوّد الطالب يشير إلى (في حالة مزوّد خدمة) أنه لن يقبل تأكيدات بعد الآن من هذا المزوّد للخدمة حول الطرف الرئيسي.

وإذا كان المزوّد المستلم يحتفظ بحالة متصاحبة مع معرف هوية الاسم، مثل قيمة معرّف الهوية بالذات (في حالة معرّف هوية بشكل زوج)، أو قيمة SPProvidedID، أو موافقة المرسل على خلق أو استعمال معرف الهوية إلخ، يستطيع المستلم أن يقوم بأي عملية صيانة مع معرفته أن العلاقة التي يمثلها معرف هوية الاسم قد انتهت.

وأي عمليات لاحقة يؤديها المستلم باسم المرسل وتخص الطرف الرئيسي (مثل <AuthnRequest> لاحق)، ينبغي تنفيذها بطريقة تتّسق مع غياب أي حالة سابقة.

والانتهاء هو ضمناً خطوة تنظيف كل سلوك إدارة حالة، أطلقه استعمال النعت AllowCreate في بروتوكول طلب الاستيقان الموجود في الفقرة 4.2.8. والتطويرات التي لا تستخدم هذا النعت، يكون من المعقول لها أن تتحاشى استعمال العنصر <Terminate>، أو أن تتعامل معه كعنصر استشاري للاطّلاع فقط.

وتجدر الإشارة أن في أغلب الحالات (وأحد الاستثناءات المهمة هو القواعد التي تحيط بالنعت SPProvidedID) لا توجد أي متطلبات من مزوّدي الهوية أو مزوّدي الخدمة، فيما يخص خلق حالة دائمة أو استعمالها. إذ لا يوجد أي سلوك صريح يكون إلزامياً، عندما يُستلم العنصر <Terminate> وهو يساوي 450. ومع ذلك، إذا كانت الحالة الدائمة موجودة، وتتعلق باستعمال معرف هوية (كما في حالة كون النعت SPProvidedID مرفقاً)، فإن العنصر <Terminate> يوفر دلالة واضحة على أن هذه الحالة ينبغي إلغاؤها (أو توسم بأنها بالية بطريقة ما).

2.VIII تصويت خطأ محتمل: PE26

الوصف: يجب توضيح جانبية التوقيع (SSO)

قابلية الانطباق في هذه التوصية: تُوَضَّح الفقرات الفرعية التالية كما يلي:

2.4.1.4.11 استعمال <Response>

إذا كان مزوّد الهوية يرغب في ترجيع خطأ، يتعين عليه ألا يدرج أي تأكيدات في الرسالة <Response> وإلا فإذا كان الطلب ناجحاً (أو إذا كانت الاستجابة غير مترافقة مع طلب)، يتعين على العنصر <Response> أن يتطابق مع ما يلي:

- إذا كانت الاستجابة غير موقّعة، يمكن أن يكون العنصر <Issuer> محذوفاً، أما إذا كان موجوداً (أو إذا كانت الاستجابة موقّعة) فيتعين عليه أن يحتوي على معرف الهوية الوحيد لمزوّد الهوية المُصْدر. والنعت Format يتعين أن يكون محذوفاً أو له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
- يتعين أن يحتوي على الأقل <Assertion> واحداً. ويتعين على كل عنصر <Issuer> من تأكيد أن يحتوي على معرّف الهوية الوحيد لمزوّد الهوية المستجيب. ويتعين أن يكون النعت Format محذوفاً أو له قيمة من urn:oasis:names:tc:SAML:2.0:nameid-format:entity. ويلاحظ أن هذه الجانبية تفترض مزود هوية مستجيباً واحداً، وجميع التأكيدات الموجودة في استجابة يتعين أن تكون صادرة عن الكيان نفسه.
- إذا كانت توجد عدة تأكيدات، يتعين عندئذ على العنصر <Subject> من كل تأكيد أن يعود إلى نفس الطرف الرئيسي. ومسموح باختلاف محتويات العناصر <Subject> (أي تستخدم عناصر <NameID> مختلفة أو بديلتها العناصر <SubjectConfirmation>).
- يتعين على كل تأكيد صادر للاستهلاك باستخدام هذه الجانبية، أن يحتوي على العنصر <Subject> مع عنصر واحد على الأقل <SubjectConfirmation> يحتوي على Method من: urn:oasis:names:tc:SAML:2.0:cm:bearer. ويسمى مثل هذا التأكيد تأكيد الحامل. ويمكن أن تحتوي تأكيدات الحامل على عناصر إضافية من <SubjectConfirmation>.
- ويمكن أن توجد أيضاً تأكيدات من دون عنصر <SubjectConfirmation> من الحامل. ومعالجة التأكيدات الإضافية أو العناصر <SubjectConfirmation> تقع خارج نطاق هذه الجانبية.
- يتعين على عنصر واحد على الأقل <SubjectConfirmation> من الحامل، أن يحتوي على عنصر <SubjectConfirmationData> يجب أن يحتوي هو نفسه على النعت Recipient الذي يحتوي على المحدّد URL لخدمة مستهلك التأكيد التابعة لمزوّد الخدمة، كما يتعين عليه أن يحتوي على النعت NotOnOrAfter الذي يحدّ النافذة التي يمكن أثناءها تسليم التأكيد. ويمكنه أن يحتوي أيضاً على النعت Address الذي يحدّ عنوان الزبون الذي يمكن تسليم التأكيد اعتباراً منه. ويجب ألا يحتوي على النعت NotBefore. وإذا كانت الرسالة الحاوية هي استجابة للعنصر <AuthnRequest>، يتعين عندئذ أن يتواءم النعت InResponseTo مع معرف هوية الطلب.
- يتعين على مجموعة من تأكيد واحد أو من تأكيدات أن تحتوي على الأقل عنصراً واحداً <AuthnStatement> يعكس استيقان الطرف الرئيسي لدى مزوّد الهوية. ويمكن إدراج عدة عناصر <AuthnStatement>، ولكن علم الدلالات لتأكيدات متعددة ليس معرفاً في هذه الجانبية.

- إذا كان مزوّد الهوية يقبل الجانبية Single Logout المعرفة في الفقرة الفرعية 5.4.1.4.11، يتعين على الإعلانات الاستيقانية أن تحتوي على النعت SessionIndex لكي تنشط طلبات اختتام الدورة لكل دورة الصادرة عن مزوّد الخدمة.
- يمكن إدراج إعلانات أخرى في تأكيد (أو تأكيدات) الحامل، حسب تقدير مزوّد الخدمة. ويمكن بصورة خاصة إدراج العناصر <AttributeStatement>. ويمكن أن يحتوي الطلب <AuthnRequest> على نعت في اللغة XML هو AttributeConsumingServiceIndex محيلاً المعلومات عن النعوت المرغوبة أو المطلوبة كما في البند 9. ويمكن أن يتجاهل ذلك مزوّد الهوية، كما يمكنه إرسال نعوت أخرى، حسب تقديره.
- يتعين على كل تأكيد حامل أن يحتوي على <AudienceRestriction> الذي يحتوي على معرف الهوية الوحيد لمزوّد الخدمة وكأنه العنصر <Audience>.
- يمكن إدراج شروط أخرى (وعناصر <Audience> أخرى) حسب طلب مزوّد الخدمة أو حسب تقدير مزوّد الهوية. (لا شك أن جميع هذه الشروط يجب أن تكون مفهومة ومقبولة من قبل مزوّد الخدمة، بغية اعتبار التأكيد صالحاً).
- وليس مزوّد الهوية ملزماً بتكريم المجموعة المطلوبة من <Conditions> في الرسالة <AuthnRequest>، إن وجدت.

3.4.1.4.11 قواعد معالجة الرسالة <Response>

بصرف النظر عن رابطة اللغة SAML المستعملة، يتعين على مزوّد الخدمة أن يفعل التالي:

- التحقق من أي توقيعات موجودة على التأكيد (التأكيدات) أو على الاستجابة.
- التحقق من أن النعت Recipient الموجود في العنصر <SubjectConfirmationData> من الحامل يتواءم مع المحدّد URL لخدمة مستهلك التأكيدات التي سلمت لها الاستجابة <Response> أو الشيء المصطنع.
- التحقق من أن النعت NotOnOrAfter الموجود في العنصر <SubjectConfirmationData> من الحامل لم يمر، مع مراعاة انحراف الميقاتيات المسموح به بين المزوّدين.
- التحقق من أن النعت InResponseTo الموجود في العنصر <SubjectConfirmationData> من الحامل يساوي معرّف الهوية لرسالته الأصلية <AuthnRequest>، ما لم تكن الاستجابة غير مطلوبة، وهي الحالة التي يتعين ألا يكون النعت موجوداً فيها.
- التحقق من أي تأكيد يُعتمد عليه هو صالح بالنسبة إلى الجوانب الأخرى. ويلاحظ أنه بينما يسمح بوجود عدة عناصر <SubjectConfirmation> من الحامل، فإن نجاح تقدير عنصر واحد من هذا النوع، ومتفق مع هذه الجانبية، يكون كافياً لتثبيت التأكيد. وعلى كل حال يجب تقدير كل تأكيد على حدة، إن كان يوجد أكثر من تأكيد واحد.
- إذا كانت العنصر <SubjectConfirmationData> من الحامل يشتمل على نعت Address، يمكن أن يتحقق مزوّد الخدمة من عنوان زبون وكيل المستعمل بمقابلته بهذا النعت.
- كل تأكيد ليس صالحاً، أو لا يمكن تلبية متطلباته الخاصة بتثبيت الصاحب، ينبغي استبعاده وعدم استعماله لإنشاء السياق الأمني للطرف الرئيسي.

- إذا كان العنصر <AuthnStatement> المستعمل لإنشاء سياق أمني للطرف الرئيسي، يحتوي على النعت SessionNotOnOrAfter، ينبغي استبعاد السياق الأمني، بمجرد بلوغ هذا الوقت، إلا إذا كان مزوّد الخدمة يعيد تكوين هوية الطرف الرئيسي بتكراره استعمال هذه الجانبية. ويلاحظ أنه إذا كانت عدة عناصر <AuthnStatement> موجودة، ينبغي تكريم قيمة SessionNotOnOrAfter الأقرب إلى الوقت الحاضر.

4.4.1.4.11 قواعد المعالجة الخاصة بالرابطة POST

إذا كانت الرابطة HTTP POST هي المستعملة لتسليم الرسالة <Response>، تتعين حماية كل تأكيد بواسطة توقيع رقمي. ويمكن تحقيق ذلك بتوقيع كل عنصر <Assertion> منفرد، أو بتوقيع العنصر <Response>.

ويتعين على مزوّد الخدمة أن يتأكد من أن تأكيدات الحامل ليست مكررة، باحتفاظه بمجموعة قيم معرفات الهوية المستعملة طوال الوقت الذي يمكن اعتبار التأكيد فيه صالحاً، استناداً إلى النعت NotOnOrAfter في <SubjectConfirmationData>.

المصـــادر

– **FIPS-197** (2001), *Advanced Encryption Standard* (AES).

– **IETF RFC 1738** (1994), *Uniform Resource Locators (URL)*.

– **IETF RFC 2256** (1997), *A Summary of the X.500 (96) User Schema for use with LDAPv3*.

– **IETF RFC 2279** (1998), *UTF-8, a transformation format of ISO 10646*.

– **IETF RFC 2743** (2000), *Generic Security Service Application Program Interface Version 2, Update 1*.

– **DCE**, *Distributed Computing Environment (DCE)*, Open Source. See http://www.opengroup.org/dce.

– **OASIS Authentication Context 2.0**, *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Bindings 1**, *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML),* 5 November 2002, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Bindings 1.1**, *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML),* 22 September 2003, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Bindings 2.0**, *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Conformance 2.0**, *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.00*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Glossary 2.0**, *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Metadata 2.0**, *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Errata Document 24**, *Revision 24 draft of the non-normative SAML V2.0 Errata document*, 27 February 2006, http://www.oasis-open.org/committees/download.php/16935/sstc-saml-errata-2.0-draft-24.pdf.

– **OASIS Protocol 1.0**, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML),* 5 November 2002, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Protocol 1.1**, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML),* 22 September 2003, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Protocol 2.0**, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS SAML 1.0**, *Security Assertion Markup Language (SAML) Version 1.0 Specification Set,* 5 November 2002, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS SAML 1.1**, *Security Assertion Markup Language (SAML) Version 1.1 Specification Set,* 22 September 2003, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Security 1**, *Security Considerations for the OASIS Security Assertion Markup Language (SAML),* 5 November 2002, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Security 1.1**, *Security Considerations for the OASIS Security Assertion Markup Language (SAML),* 22 September 2003, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS Security 2.0**, *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*, 15 March 2005, http://www.oasis-open.org/apps/org/workgroup/security/.

– **OASIS XACML1-1**, *eXtensible Access Control Markup Language (XACML) V1.1,* 24 July 2003, http://www.oasis-open.org/apps/org/workgroup/xacml/.

– **OASIS XACML1-1**, *eXtensible Access Control Markup Language (XACML) V1.0,* 18 February 2003, http://www.oasis-open.org/apps/org/workgroup/xacml/.

– **OASIS XACML 2.0**, *eXtensible Access Control Markup Language (XACML) V2.0,* 1 February 2005, http://www.oasis-open.org/apps/org/workgroup/xacml/.

– **SSL3**, *The SSL Protocol Version 3.0*. See http://wp.netscape.com/eng/ssl3/draft302.txt.

– **W3C Character Model** (2004), Working draft, 27 October 2005, *Character Model for the World Wide Web 1.0: Normalization.*

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات المعطيات على الشبكة الهاتفية
السلسلة X	**شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2007