الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2722

(2011/01)

السلسلة Y: البُنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

شبكات الجيل التالي – الأمـــن

آليات إدارة الهوية في شبكات الجيل التالي

التوصيـــة ITU-T Y.2722

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
نوعية الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الشبكات الذكية الشمولية	Y.2699-Y.2600
الأمـــن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3099-Y.3000

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

التوصيـــة ITU-T Y.2722

آليات إدارة الهوية في شبكات الجيل التالي

ملخص

توصِّف التوصية ITU-T Y.2722 الآليات التي يمكن استعمالها لاستيفاء متطلبات إدارة الهوية واحتياجات نشر شبكات الجيل التالي (NGN).

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2722	2011.01.28	13

المصطلحات الرئيسية

هوية موحَّدة، إدارة الهوية، آليات إدارة الهوية، شبكة الجيل التالي، الأمن.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). 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).

ملاحظـــة

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، كان الاتحاد قد تلقّى 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/.

جـــدول المحتـــويات

الصفحة

التوصيـــة ITU-T Y.2722

آليات إدارة الهوية في شبكات الجيل التالي

1 مجال التطبيق

تحدد توصية قطاع تقييس الاتصالات، *متطلبات إدارة الهوية في شبكات الجيل التالي وحالات استعمالها* [ITU-T Y.2721]، متطلبات إدارة الهوية في شبكات الجيل التالي. وتوصّف هذه التوصية آليات إدارة الهوية IdM المحددة ومجموعة من الخيارات التي ينبغي استعمالها للوفاء بمتطلبات شبكات الجيل التالي الواردة في التوصية [ITU-T Y.2721]. كما تقدم أفضل الممارسات والمبادئ التوجيهية التي تدعم قابلية التشغيل البيني وغيرها من الاحتياجات.

يُراد لهذه التوصية أن تُستخدم، جنباً إلى جنب، مع التوصيتين [ITU-T Y.2720] و[ITU-T Y.2721]، إذ إن المفاهيم الأساسية من حيث المعمارية والمتطلبات وحالات الاستخدام لا تتكرر في هذه التوصية.

ملاحظة – على المستفيدين من الآليات المذكورة ومستخدميها الالتزام بجميع القوانين واللوائح والسياسات المعمول بها على الصعيدين الوطني والإقليمي. وقد تتطلب بعض اللوائح والتشريعات الخاصة تنفيذ آليات لحماية المعلومات التي تعرِّف بصاحبها شخصياً.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.509] التوصية ITU-T X.509 (2005) | ISO/IEC 9594-8:2005، *تِقانة (تكنولوجيا) المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: الأطر العامة لشهادات المفتاح العمومي والنعت*

[ITU-T X.1035] التوصية ITU-T X.1035 (2007)، *بروتوكول تبادل المفاتيح (PAK) المستيقَن منه بكلمة مرور.*

[ITU-T X.1141] التوصية ITU-T X.1141 (2006)، *اللغة الشرحية لتوكيد الأمن (SAML 2.0).*

[ITU-T X.1252] التوصية ITU-T X.1252 (2010)، *مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية.*

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2006)، المتطلبات الوظيفية لشبكة الجيل التالي ومعماريتها، الإصدار 1.

[ITU-T Y.2701] التوصية ITU-T Y.2701 (2007)، *متطلبات الأمن لشبكة الجيل التالي (NGN)، الإصدار 1.*

[ITU-T Y.2702] التوصية ITU-T Y.2702 (2008)، *متطلبات الاستيقان والترخيص في الإصدار 1 من شبكات الجيل التالي.*

[ITU-T Y.2704] التوصية ITU-T Y.2704 (2010)، *آليات وإجراءات الأمن لشبكات الجيل التالي (NGN).*

[ITU-T Y.2720] التوصية ITU-T Y.2720 (2009)، *إطار إدارة الهوية في شبكات الجيل التالي.*

[ITU-T Y.2721] التوصية ITU-T Y.2721 (2010)، *متطلبات إدارة الهوية في شبكات الجيل التالي وحالات الاستعمال.*

[3GPP TS 23.228] 3GPP TS 23.228 (ساري المفعول)، *IP Multimedia Subsystem (IMS); Stage 2.*

[ATIS 33102] ATIS.3GPP.33.102V710-2007، *Security Architecture.*

[IETF RFC 2289] IETF RFC 2289 (1998)، *A One-Time Password System.*

3 التعاريف

تعتمد هذه التوصية على مصطلحات محددة في التوصيتين [ITU-T Y.2720] و[ITU-T X.1252].

وقد اعتمدت، على وجه التحديد، التعريفين التاليين الواردين في التوصية [ITU-T X.1252]:

1.3 مورّد الهوية (IdP): انظر مورّد خدمة الهوية (IdSP).

2.3 مورّد خدمة الهوية (IdSP): كيان يقوم بالتحقق من معلومات هويات الكيانات الأخرى مع الحفاظ عليها وإدارتها، ويمكن أن يستحدثها ويخصصها.

4 المختصرات

تستعمل هذه التوصية المختصرات والتسميات التالية:

AKA الاستيقان واتفاق المفاتيح (*Authentication and Key Agreement*)

ASP مورد خدمة التطبيقات (*Application Service Provider*)

AuC مركز الاستيقان (*Authentication Centre*)

AV متجه الاستيقان (*Authentication Vector*)

BSF وظيفة مخدم الدعم (*Bootstrapping Server Function*)

CK مفتاح الشفرة (*Ciphering Key*)

GBA معمارية عامة للدعم (*Generic Bootstrapping Architecture*)

HSS نظام مشترك منزلي (*Home Subscriber System*)

IdM إدارة الهوية (*Identity Management*)

IdP مورد الهوية (*Identity Provider*)

IdSP مورد خدمة الهوية (*Identity Service Provider*)

IK مفتاح التكاملية (*Integrity Key*)

IMPI هوية مستعمل خاص للوسائط المتعددة العاملة ببروتوكول الإنترنت (*IP Multimedia Private user Identity*)

IMPU هوية مستعمل عام للوسائط المتعددة العاملة ببروتوكول الإنترنت (*IP Multimedia Public User identity*)

IMS نظام فرعي متعدد الوسائط يستعمل ببروتوكول الإنترنت (*IP Multimedia Subsystem*)

IMSI هوية مشترك في الخدمة المتنقلة الدولية (*International Mobile Subscriber Identity*)

IPTV تلفزيون يعمل ببروتوكول الإنترنت (*Internet Protocol Television*)

ISIM وحدة هوية مشترك في النظام (*IMS Subscriber Identity Module*)

LDAP بروتوكول خفيف للنفاذ إلى الدليل (*Lightweight Directory Access Protocol*)

MS محطة متنقل (*Mobile Station*)

NAF وظيفة تطبيقات الشبكة (*Network Application Function*)

NGN شبكات الجيل التالي (*Next Generation Networks*)

OASIS منظمة تطوير معايير المعلومات المنظمة (*Organization for the Advancement of Structured Information Standards*)

OTP كلمة مرور لمرة واحدة (*One Time Password*)

PII المعلومات التي يمكن التعرف على أصحابها شخصياً (*Personally Identifiable Information (PII)*)

PKI بنية تحتية رئيسية عمومية (*Public Key Infrastructure*)

RP الطرف المعوّل (*Relying Party*)

SAML اللغة الشرحية لتوكيد الأمن (*Security Assertion Markup Language*)

SIP بروتوكول بدء الجلسة (*Session Initiation Protocol*)

SLF وظيفة محدد موقع المشترك (*Subscriber Locator Function*)

SOAP بروتوكول بسيط للنفاذ إلى الأغراض (*Simple Object Access Protocol*)

SQL لغة منظمة للاستفسار (*Structured Query Language*)

SSO تسجيل الدخول لمرة واحدة (*Single Sign-On*)

UE تجهيزات المستعمل (*User Equipment*)

UICC بطاقة دارة عالمية متكاملة (*Universal Integrated Circuit Card*)

UMTS نظام عالمي للاتصالات المتنقلة (*Universal Mobile Telecommunications System*)

USIM وحدة هوية عالمية للمشترك (*Universal Subscriber Identifier Module*)

WAP بروتوكول التطبيق اللاسلكي (*Wireless Application Protocol*)

WSS أمن خدمات شبكة الويب (*Web Services Security*)

XML اللغة الشرحية التوسعية (*eXtensible Markup Language*)

XRDS تتابع واصف الموارد التوسعي (*eXtensible Resource Descriptor Sequence*)

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"يجب" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"يوصى" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

"يحظر" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"من الجائز": تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

وفي متن هذه التوصية وتذييلاتها، تصادف أحياناً عبارات "*يتعين*" و"*يتعين ألا*" و"*ينبغي*" و"*يمكن*"، وينبغي تأويلها لتفيد بالمعاني الآتية على التوالي: "*يتعين*" و"*يحظر*" و"*يوصى*" و"*من الجائز*". وإذ تظهر مثل هذه العبارات أو المصطلحات الرئيسية في تذييل أو في مادة محددة صراحة على أنها "*إعلامية*"، تفسَّر على أنه ليس وراءها أي قصد معياري.

6 الآليات والإجراءات الداعمة لوظائف إدارة الهوية

1.6 إدارة دورة الحياة

يرجى الرجوع إلى التوصية [ITU-T Y.2720]، *إطار إدارة الهوية في شبكات الجيل التالي*، للحصول على معلومات عن إدارة دورة حياة الهوية.

2.6 الاستيقان وضمان الاستيقان

تصف هذه الفقرة آليات الاستيقان والتأكد من الهويات ومعلوماتها. وتحيل إلى آليات استيقان محددة في أماكن أخرى.

ويمكن لمورد خدمة الهوية أن يستخدم آليات استيقان، مثل الاستيقان القائم على أوصاف اللغة الشرحية لتوكيد الأمن (SAML) بخدمات شبكة الويب (WS) أو الاستيقان استناداً إلى الشهادات أو الاستيقان استناداً إلى كلمة المرور (بما في ذلك كلمة المرور لمرة واحدة)، لتطبيقات أو خدمات معينة حسب السياق ومستوى الضمان اللازم. وتنتقى طريقة الاستيقان استناداً إلى مقتضيات مستوى الأمن. وقد يطلب مزود خدمة الهوية معلومات مستوى الأمن كي يعثر على طرائق الاستيقان التي تفي بمتطلبات مستوى الأمن التي يضعها مورد الخدمة.

1.2.6 الاستيقان القائم على أوصاف اللغة الشرحية لتوكيد الأمن (SAML) لخدمات شبكة الويب (WS)

1.1.2.6 الاستيقان القائم على أوصاف اللغة الشرحية لتوكيد الأمن (SAML)

الاستيقان القائم على أوصاف اللغة الشرحية لتوكيد الأمن (SAML) [المرجع ITU-T X.1141] نسق التوكيدات الممكن استخدامها لأغراض تبادل معلومات الأمن في إدارة الهوية. ومن بين وظائف إدارة الهوية التي يمكن استخدامها مع اللغة SAML وظائف الاستيقان وتقاسم النعوت والترخيص التي تقابل ثلاثة أنماط لبيانات موضوع توكيد لغة SAML:

- بيان الاستيقان – يرسل معلومات تفيد باستيقان موضوع التوكيد من خلال وسائل خاصة وفي وقت خاص.
- بيان النعوت – يرسل معلومات تفيد بارتباط موضوع التوكيد مع النعوت المعددة في القائمة.
- بيان قرار الترخيص – يرسل معلومات تفيد بضمان نفاذ موضوع التوكيد إلى موارد محددة أو برفض هذا النفاذ له.

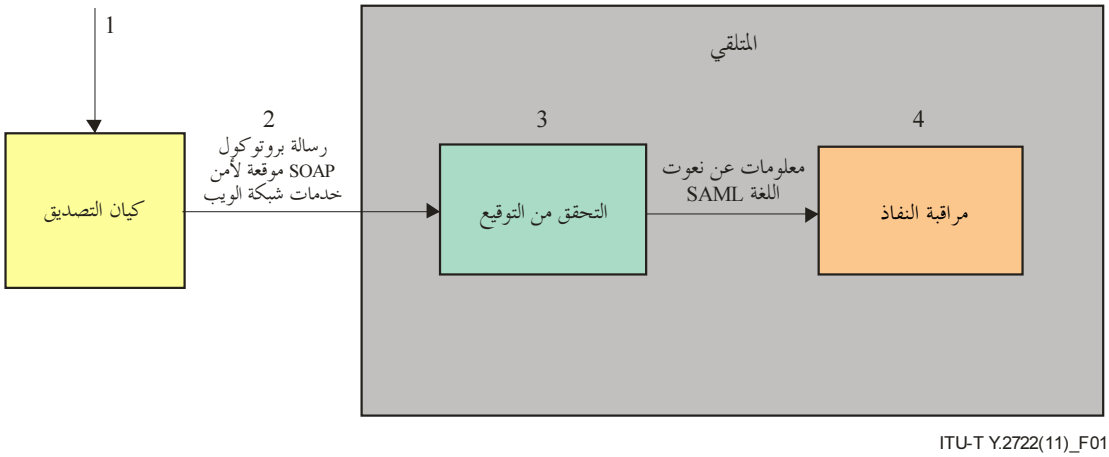
ويمكن وصف محتوى توكيد اللغة SAML على مستوى عام كالتالي: صدر التوكيد **A** في الوقت **t** عن الجهة المصدر **R** بخصوص الموضوع **S** والشروط **C** المتوفرة صالحة.

وتُستخدم توكيدات اللغة SAML لإبلاغ معلومات الاستيقان والنعوت والترخيص المنقولة في رسائل البروتوكول البسيط للنفاذ إلى الغرض (SOAP). وعند تبادل رسائل البروتوكول SOAP عبر قنوات نقل غير محمية، يوصى بشدة باستعمال توقيع اللغة XML [المرجع b-W3C XML] من أجل التحقق من العلاقة وفي القائمة بين رسالة البروتوكول SOAP وبيانات التوكيدات التي تحملها الرسالة. وفي *أمن خدمات شبكة الويب (WSS)*: يصف المعيار *أوصاف أذنات اللغة SAML* [المرجع b-OASIS SAML token] كيفية:

- نقل توكيدات اللغة SAML (تسمى أيضاً أذنات اللغة SAML) في رسالة SOAP وتؤول إليها.
- استعمال توقيع اللغة XML لضم موضوع توكيد لغة SAML وبياناتها إلى رسالة بروتوكول SOAP.

أما الاستعمال المعتاد لأذنة اللغة SAML مع رسالة البروتوكول SOAP وفقاً لهذه التوصية فيظهر في الشكل 1 ويرد وصفه أدناه.

وتتضمن رسالة البروتوكول SOAP الموقعة في هذا المثال توكيد اللغة SAML وبيان النعوت. واستناداً إلى المعلومات الواردة في هذا البيان يستطيع متلقي الرسالة اتخاذ قرارات التحكّم في النفاذ إلى المورد المطلوب.



الشكل 1 – الخطوات المعتادة لإنشاء رسالة بروتوكول SOAP مع إذنة اللغة SAML ومعالجتها

1) يحصل كيان التصديق على توكيد اللغة SAML مع بيان النعوت يُنشئه ويُضمِّنه رسالة البروتوكول SOAP وفقاً للمرجع [b-OASIS SAML token].

2) يرسل كيان التصديق إلى المتلقي رسالة البروتوكول SOAP التي تحمل توقيع أمن خدمات شبكة الويب.

3) يتحقق المتلقي من التوقيع الرقمي.

4) يمكن أن تستعمل معلومات بيان اللغة SAML في قرارات مراقبة النفاذ.

2.1.2.6 طرائق أذنات اللغة SAML لتأكيد الموضوع

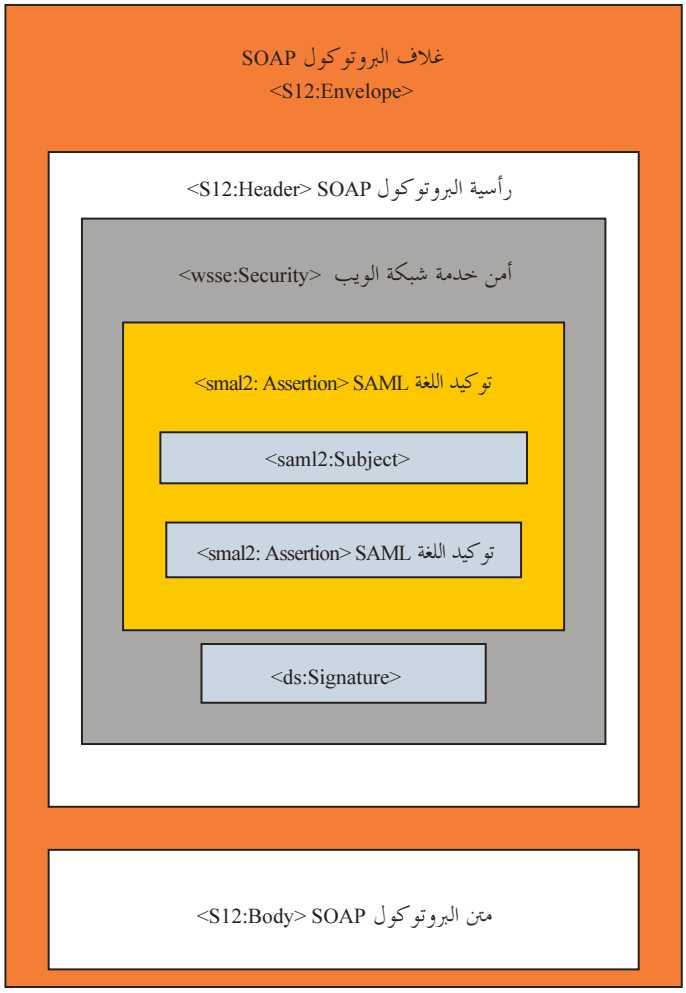
يحدد المعيار OASIS، *أمن خدمات شبكة الويب: أوصاف أذنات اللغة SAML 1.1* [b-OASIS SAML token]، كيفية إرفاق توكيد اللغة SAML برسالة البروتوكول SOAP، ويعرِّف طريقتين إلزاميتين لتأكيد الموضوع هما:

- صاحب المفتاح؛
- ضمانات المرسل.

وتظهر في الشكل 2 العناصر الرئيسية للغة XML لرسالة البروتوكول SOAP المبينة وفقاً للمرجع [b-OASIS WSS SOAP].

ويوضع توكيد اللغة SAML في الرأسية <wsse:Security> التي تضم أيضاً التوقيع الرقمي <ds:Signature>. ويستعمل متلقي رسالة البروتوكول SOAP التوقيع الرقمي للتحقق من أن مرسل الرسالة يعرف المفتاح المستخدَم في حساب التوقيع عبر معالجة متن البروتوكول SOAP وفي التحقق من تكامله. وخوارزمية المعالجة هي SHA 1 وخوارزمية التوقيع RSA_SHA 1 على النحو المحدد في المرجع [b-OASIS WSS SOAP]. وتُعطى قيمة التوقيع في عنصر التوقيع الرقمي <ds:SignatureValue> من النعت <ds:Signature>.

وهنالك طريقتان لتأكيد الموضوع تحددان طرقاً مختلفة لنقل المعلومات من المفتاح إلى جهاز الاستقبال.



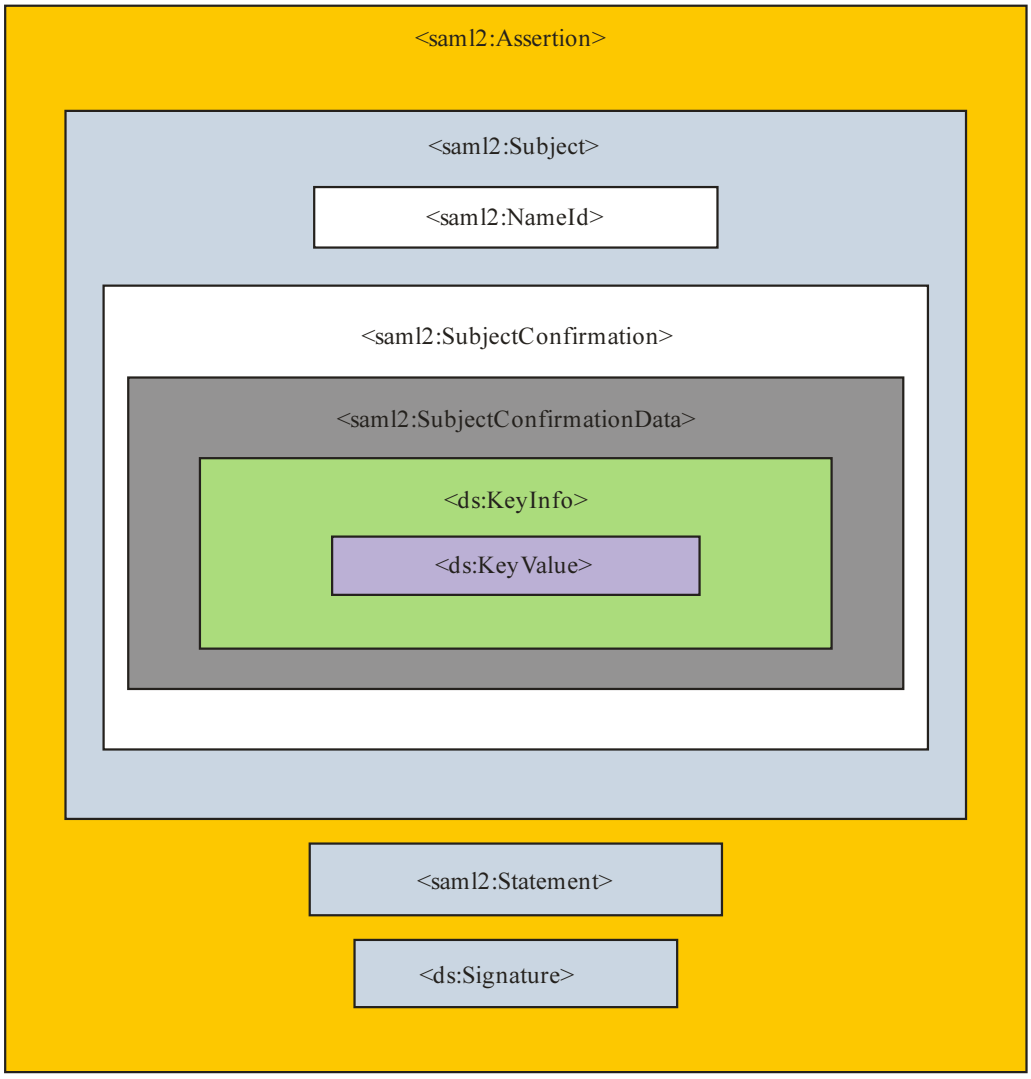
الشكل 2 – بنية رسالة البروتوكول SOAP مع توكيد اللغة SAML

وتصف الفقرات التالية طريقتي تأكيد الموضوع.

1.2.1.2.6 طريقة تأكيد موضوع حامل المفتاح

يبين الشكل 3 بنية توكيد اللغة SAML المستخدمة في طريقة تأكيد موضوع حامل المفتاح. ويدل نعت طريقة العنصر <saml2:SubjectConfirmation> على طريقة تأكيد الموضوع (حامل المفتاح).

وتحدد الطريقة أنه يجب على المرسل (المسمى أيضاً كيان التصديق) إثبات أنه مخوّل لإجراء البيانات عن الموضوع من خلال إثباته معرفة المفتاح المعرف في العنصر <ds:KeyValue> الوارد في العنصر <ds:KeyInfo> لتوكيد اللغة SAML. ويعرف العنصر <ds:KeyInfo> مفتاحاً عمومياً أو سرياً يستخدم لتأكيد هوية الموضوع. كما تحدد الطريقة أنه يجوز للمرسل أن يفعل ذلك بتوقيع ملخص متن البروتوكول SOAP بذلك المفتاح. ويرد التوقيع في العنصر <ds:Signature> من الرأسية، أمن خدمة شبكة الويب، على النحو المبين في الشكل 2.



ITU-T Y.2722(11)_F03

الشكل 3 – بنية توكيد اللغة SAML المستخدمة في طريقة تأكيد موضوع حامل المفتاح

يحصل مستقبل رسالة البروتوكول على المفتاح باستعمال المعلومات التي يتيحها كيان التصديق (في العنصر <ds:KeyInfo>). ثم يقوم المستقبل بحساب التوقيع الرقمي لمتن البروتوكول SOAP ويتحقق من تطابقه مع التوقيع الذي قدمه كيان التصديق. فإذا تطابقا أمكن عندها إحالة موضوع وبيانات توكيد اللغة SAML إلى كيان التصديق وأمكن اعتبار محتويات متن البروتوكول SOAP التي يوفر المفتاح حماية تكاملها واردة من كيان التصديق.

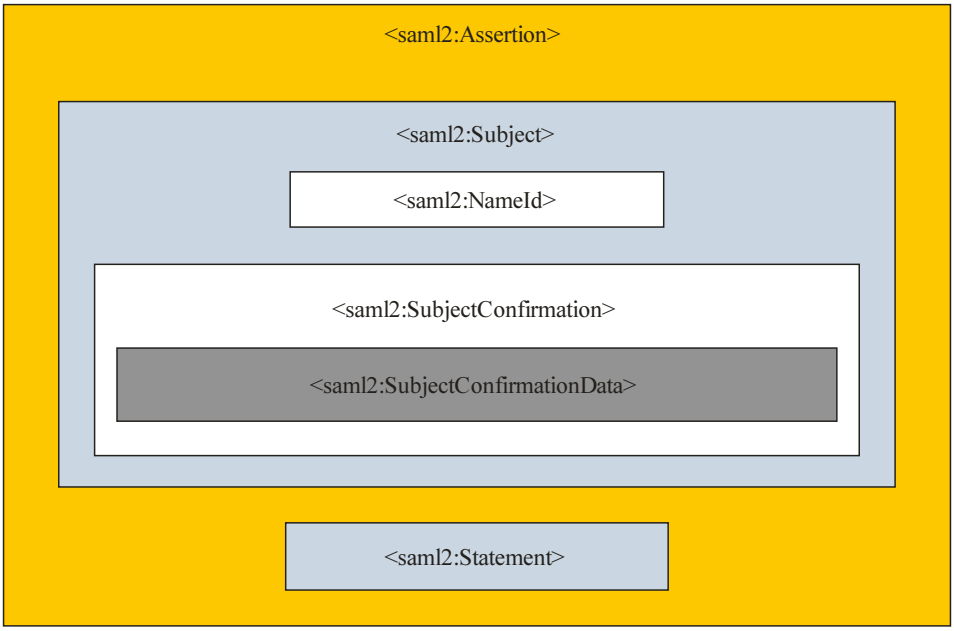
2.2.1.2.6 طريقة تأكيد موضوع ضمانات المرسل

يبين الشكل 4 بنية توكيد اللغة SAML المستخدمة في طريقة تأكيد موضوع ضمانات المرسل. ويدل نعت الطريقة في العنصر <saml2:SubjectConfirmation> على طريقة تأكيد الموضوع (ضمانات المرسل).

ويعلن مستقبل ما الثقة في كيان التصديق كي يجعل توكيدات اللغة SAML المتعلقة بموضوع ما في إطار ظروف تشير فيها قيمة النعت Method للعنصر <SubjectConfirmation> إلى النعت Method لضمانات المرسل.

يحصل كيان التصديق على توكيد واحد أو أكثر أو على إحالات للتوكيدات من سلطة واحدة أو أكثر ويضعها في رسالة بروتوكول SOAP. ثم يقوم بحساب توقيع ملخص توكيدات اللغة SAML ومتن الرسالة SOAP. ويرد التوقيع في العنصر <ds:Signature> في رأسية أمن الخدمة (WS المبينة في الشكل 2). ويتيح كيان التصديق خيارياً معلومات للمستقبل عن المفتاح الذي استعمل لحساب التوقيع. وإن لم تتوفر مثل هذه المعلومات، من المفترض أن يتعرف المستقبل هوية المفتاح بوسائل أخرى.

ويتحقق المستقبل من صحة التوقيع. وإذا كان التوقيع صحيحاً، تأكد المستقبل من أن البيانات بشأن الموضوع أعدها كيان التصديق.



ITU-T Y.2722(11)_F04

الشكل 4 – بنية توكيد اللغة SAML المستخدمة في طريقة تأكيد موضوع ضمانات المرسل

2.2.6 الاستيقان القائم على الشهادات

يمكن استخدام شهادات التوصية [ITU-T X.509] لتطبيق، أو خدمة على وجه التحديد، حسب السياق والمستوى المطلوب للضمان. ويرد وصف استعمال الشهادات [ITU-T X.509] لأغراض الاستيقان في التوصية [ITU-T Y.2704]، آليات الأمن وإجراءاته في شبكات الجيل التالي.

3.2.6 الاستيقان القائم على كلمة المرور

يمكن استعمال الاستيقان القائم على كلمات المرور لتطبيق، أو خدمة على وجه التحديد، حسب السياق والمستوى المطلوب للضمان. ويرجى الرجوع إلى التوصية [ITU-T X.1035] للحصول على وصف لآليات الاستيقان القائم على كلمة المرور.

4.2.6 كلمة مرور لمرة واحدة

يمكن استعمال كلمة مرور لمرة واحدة لتطبيق، أو خدمة على وجه التحديد، حسب السياق والمستوى المطلوب للضمان. وهنالك طريقة واحدة لاستخدام كلمة مرور المرة الواحدة يرد وصفها في المرجع [b-IETF RFC 2289].

5.2.6 استعمال اتفاق الاستيقان والمفتاح (AKA) للاستيقان المتبادل

يستعمل النظام العالمي للاتصالات المتنقلة (UMTS) بروتوكول اتفاق الاستيقان والمفتاح (AKA) من أجل توفير استيقان متبادل للمحطة المتنقلة والشبكة. والبروتوكول UMTS AKA بروتوكول تحدٍّ ورَدٍّ يستعمل مفتاحاً طويل الأمد مشتركاً بين الوحدة العالمية لهوية المشترك (USIM) ومركز الاستيقان (AuC). وتوجد هذه الكيانات في البطاقة العالمية للدارة المتكاملة (UICC) للمحطة المتنقلة وفي الشبكة الأصلية للمحطة المتنقلة على التوالي. وفي ترتيبات تجارية معينة، يمكن لمورد خدمة الهوية أن يوفر وظائف مركز الاستيقان. ويوصَّف البروتوكول AKA في المرجع [ATIS 33102].

6.2.6 إدراج الاستيقان القائم على بنية المفاتيح العمومية (PKI) في النظام الفرعي للوسائط المتعددة العاملة ببروتوكول الإنترنت (IMS)

يستند أمن الأنظمة الفرعية للوسائط المتعددة العاملة ببروتوكول الإنترنت (IMS) على الآلية AKA التي تستعمل كلمة مرور مشتركة وبروتوكول تحدٍّ ورَدٍّ لاستيقان شبكة المستعمل. لكن أمن بعض خدمات شبكات الجيل التالي (مثل التلفزيون IPTV) تقوم على أساس شهادات الاستيقان القائم على بنية المفاتيح العمومية (PKI). ومن أجل إتاحة مواءمة خدمات شبكات الجيل التالي التي تستعين بشهادات PKI مع أمن النظام IMS، لعل من المستحسن أن يدرج الاستيقان PKI في استيقان النظام IMS بحيث تُدعم قوة أمن النظام IMS.

ويتيح إدراج استيقان النظام IMS في الاستيقان PKI لتجهيزات المستعمل وشبكته أن تستيقن كل جهة أخرى تستند إلى شهاداتها وأن توافق على مجموعة من مفاتيح التجفير استناداً إلى نفس خوارزميات توليد المفاتيح المستخدمة في الاتفاق AKA. ولهذه الغاية، تحتاج تجهيزات المستعمل وشبكته إلى أن تكون مزودة بالمفاتيح والشهادات الخاصة اللازمة، وأن تكون قادرة على القيام بعمليات الاستيقان PKI.

وفيما يتعلق بالاتفاق بشأن مفتاح التجفير (*CK*) ومفتاح التكاملية (*IK*) تحدد الآلية الواردة للإدراج خيارين هما:

1) إبرام اتفاق بشأن المفاتيح *CK* و*IK* مع استعمال كلمة مرور مشتركة بين وظيفة المستعمل النهائي وكيان وظيفي لأوصاف مستعمل الخدمة S-5 (SUP-FE) الذي يرد تعريفه في التوصية [ITU-T Y.2012]؛

2) إبرام اتفاق بشأن المفاتيح *CK* و*IK* دون استعمال كلمة مرور مشتركة.

ويبين الشكل 5 التدفق النوعي للنداء في الخيار الأول والشكل 6 في الخيار الثاني.

1.6.2.6 اصطلاحات

تستعمل الاصطلاحات التالية في هذه الفقرة:

- "|" تعني تسلسل السلسة.
- *CK* تعني مفتاح التجفير.
- *IK* تعني مفتاح التكاملية.
- *K()* تعني تجفير مفتاح تناظري.
- N_{pr} *[ ]* تعني تجفير بواسطة مفتاح خاص للشبكة N_{pr}.
- N_{pu} *[ ]* تعني تجفير بواسطة مفتاح عمومي للشبكة N_{pu} يُعطى في شهادة الشبكة.
- U_{pr} *[ ]* تعني تجفير بواسطة مفتاح خاص للمستعمل U_{pr}.

2.6.2.6 كيانات منخرطة في الاستيقان

- S-5 – كيان وظيفي لأوصاف مستعمل الخدمة (SUP-FE).
- وظيفة المستعمل النهائي: والكيان قادر على إدارة زبائن البروتوكول SIP.
- كيان وظيفي لمراقبة جلسة النداء S-n (CSC-FE) حيث تكون S-n أحد الكيانات التالية:
  - كيان وظيفي لمراقبة جلسة النداء لخدمة S-1 (S-CSC-FE)؛
  - كيان وظيفي لمراقبة جلسة النداء للمخدم المساعد S-2 (P-CSC-FE)؛
  - كيان وظيفي لمراقبة جلسة النداء لاستجواب S-3 (I-CSC-FE).

ويستعمل الكيان S-n للدلالة على أحد هذه الكيانات عندما لا يوجد اختلاف بينها طالما تعلق الأمر بإجراء الاستيقان الموصوف. راجع التوصية [ITU-T Y.2012] للاطلاع على أوصاف الكيانات الوظيفية في شبكة الجيل التالي (S-1 وS-2 وS-3 وS-5 ووظيفة المستعمل النهائي).

3.6.2.6 إبرام اتفاق بشأن المفتاحين CK وIK باستعمال كلمة مرور مشتركة بين وظيفة المستعمل النهائي والكيان S-5 (الخيار 1)

يبين الشكل 5 تدفق النداء. وفيما يلي مراحله الأساسية:

1) ترسل وظيفة المرسل النهائي طلب تسجيل بروتوكول بدء الجلسة (SIP) في الوحدة *IMPU* و*IMPI* إلى الكيان S-n.

2) يطلب الكيان S-1 استجواباً عشوائياً *RAND* و*CK* و*IK* من الكيان S-5. وتتحدد القيم *RAND* و*CK* و*IK* في المرجع [ATIS 33102].

3) يستقبل الكيان S-5 *RAND* و*CK* و*IK* من S-5 للمستعمل.

4) يرسل S-n إلى وظيفة المستعمل النهائي رسالة غير مرخَّص 401 وفق بروتوكول SIP مع استجواب *RAND* وقيمته المجفرة $N_{pr}[RAND]$.

وتقوم وظيفة المستعمل النهائي بما يلي:

- استقبال القيم *A* التي يفترض أن تساوي *(RAND)* و*B* التي يفترض أن تساوي $N_{pr}[RAND]$؛
- استعادة مفتاح الشبكة العمومي N_{pu}؛
- تجفير *B* باستعمال المفتاح N_{pu} ومقارنة النتيجة مع *A*. وإذا تساوت القيمتان، تم استيقان الشبكة عندئذ وإلاّ فإن إجراء الاستيقان قد أخفق؛
- توليد المفتاحين *IK* و*CK* باستعمال كلمة المرور المشتركة K_s؛
- توليد قيمة $U_{pr}[N_{pu}[K]|K(RAND)]$.

5) ترسل وظيفة المستعمل النهائي إلى الكيان S-n رسالة تسجيل SIP في المعرفات *IMPU* و*IMPI* والقيمة $U_{pr}[N_{pu}[K]|K(RAND)]$.

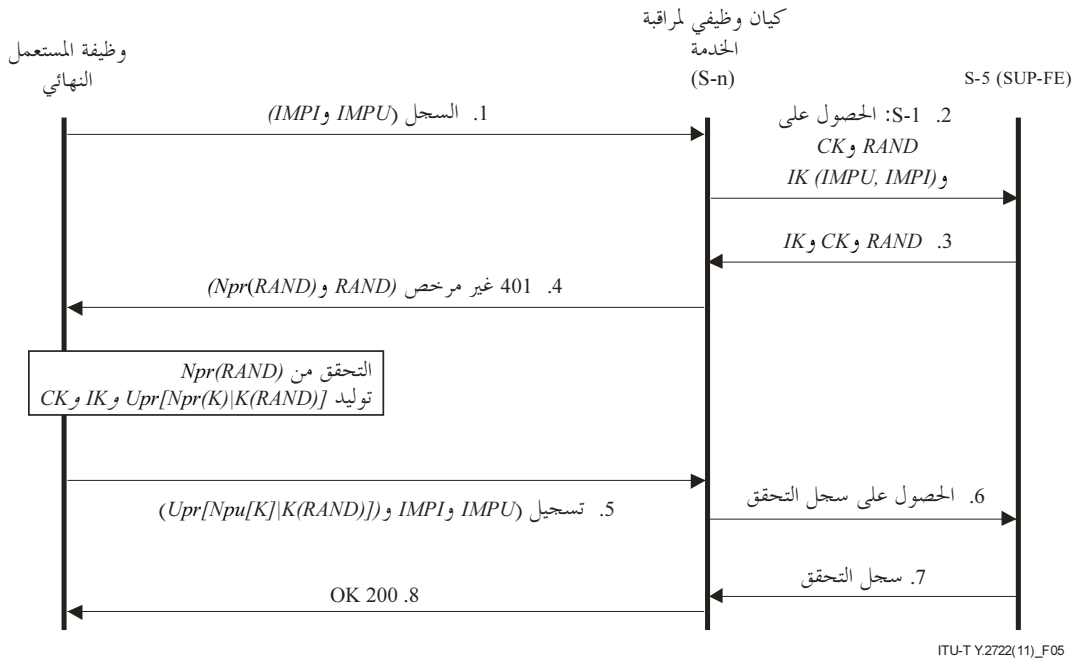
6) يرسل الكيان S-1 إلى الكيان S-5 بيانات وصلت في المرحلة 5 ويطلب التحقق منها وسجل المستعمل.

ويجري الكيان S-5 العمليات التالية:

- يُستعلم عن شهادة المستعمل للحصول على مفتاحه العمومي U_{pu}؛
- يُجفَّر باستعمال المفتاح U_{pu} القيمة الواصلة *C* التي يفترض أن تساوي $U_{pr}[N_{pu}[K]|K(RAND)]$ لاستعادة القيمة *D|E* حيث D يفترض أن تساوي $N_{pu}[K]$ و*E* يفترض أن تساوي *K(RAND)*؛
- يُجفر باستعمال مفتاح الشبكة الخاص N_{pr} القيمة *D* للحصول على *'K*؛
- يُجفر باستعمال *'K* القيمة E للحصول على *'RAND*؛
- يُقارن بين *'RAND* و*RAND*. وإذا تساويا، يكون استيقان المستعمل قد تم.

7) يرسل الكيان S-5 نتيجة الاستيقان وسجل المستعمل إلى الكيان S-1.

8) يستعمل الكيان S-1 السجل للتحقق من أن المستعمل المستيقن مرخص له تسجيل واستقبال الخدمة المطلوبة. وإذا تحقق ذلك، يبلغ الكيان S-n وظيفة المستعمل النهائي بأن النفاذ مضمون باستخدام رسالة OK 200 وفق بروتوكول SIP.



الشكل 5 – إدراج آلية استيقان النظام IMS في الاستيقان PKI (الخيار 1)

4.6.2.6 إبرام اتفاق بشأن المفتاحين CK وIK دون استعمال كلمة مرور مشتركة بين وظيفة المستعمل النهائي والكيان S-5 (الخيار 2)

يبين الشكل 6 تدفق النداء. وفيما يلي مراحله الأساسية:

1) ترسل وظيفة المستعمل النهائي طلب تسجيل البروتوكول SIP في معرفي المستعمل *IMPU* و*IMPI* إلى الكيان S-n.

2) يطلب الكيان S-1 رداً عشوائياً *RAND* من الكيان S-5. وتتحدد قيمة *RAND* في المرجع [ATIS 33102].

3) يستقبل الكيان S-1 القيمة *RAND* من S-5 للمستعمل المحدد.

4) يرسل الكيان S-n إلى وظيفة المستعمل النهائي رسالة غير مرخَّصة 401 وفق بروتوكول SIP مع القيمة *RAND* وقيمتها المجفرة $N_{pr}[RAND]$.

وتقوم وظيفة المستعمل النهائي بما يلي:

- استقبال القيمة *A* التي يفترض أن تساوي *RAND* والقيمة *B* التي يفترض أن تساوي $N_{pr}[RAND]$؛
- استعادة مفتاح الشبكة العمومي N_{pu}؛
- تجفير القيمة *B* باستعمال N_{pu} ومقارنة النتيجة مع *A*. إذا تساوت القيمتان، تم استيقان الشبكة وإلاَّ أخفق إجراء الاستيقان؛
- توليد المفتاحين *IK* و*CK* باستعمال المفتاح *K* المولَّد عشوائياً؛
- توليج القيمة $U_{pr}[N_{pu}[K]|K(RAND)]$.

5 ترسل وظيفة المستعمل النهائي إلى الكيان S-n رسالة تسجيل البروتوكول SIP في المعرّفين *IMPU* و*IMPI* فضلاً عن القيمة $U_{pr}[N_{pu}[K]|K(RAND)]$.

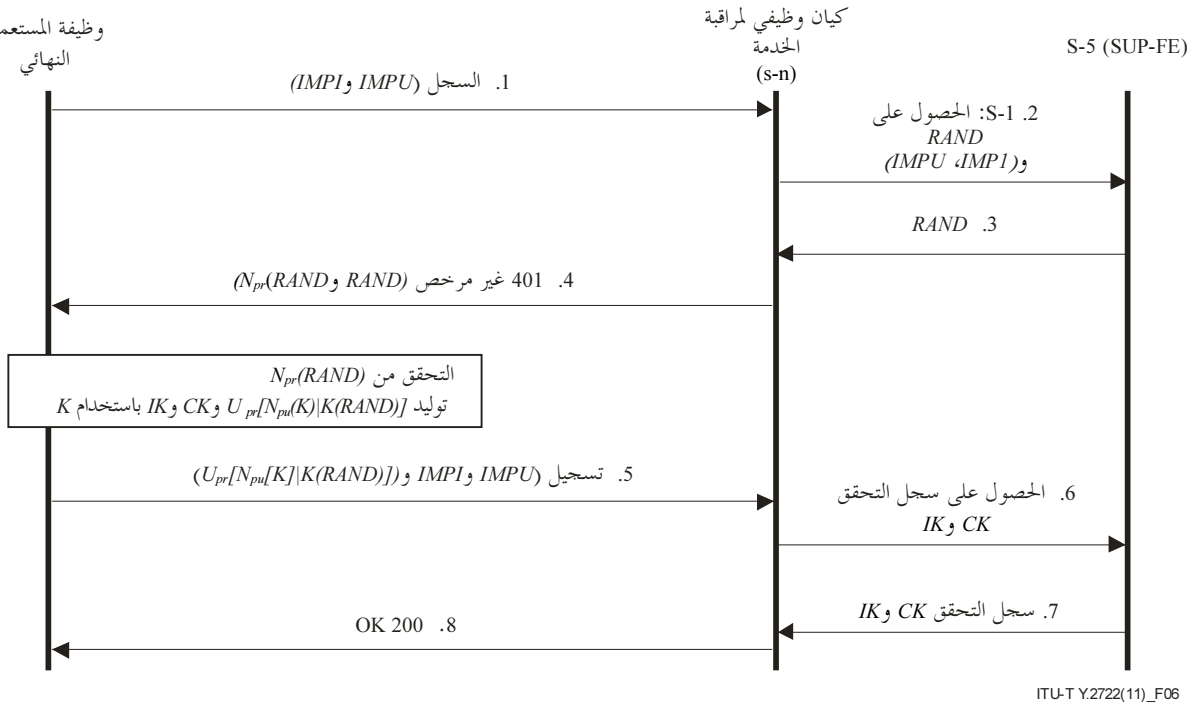
6 يرسل الكيان S-1 إلى الكيان S-5 بيانات وصلت في المرحلة 5 ويطلب التحقق منها وسجل المستعمل والمفتاحين *CK* و*IK*.

ويقوم الكيان S-5 بالعمليات التالية:

- يستعلم عن شهادة المستعمل للحصول على مفتاحه العمومي U_{pu}؛
- يجفر باستعمال U_{pu} القيمة *C* المستقبَلة التي يفترض أنها تساوي $U_{pr}[N_{pu}[K]|K(RAND)]$ من أجل استعادة القيمة *D*|*E*، حيث يفترض أن *D* تساوي $N_{pu}[K]$ و*E* (*K(RAND)*؛
- يجفر باستعمال مفتاح الشبكة الخاص N_{pr} القيمة *D* من أجل الحصول على القيمة *'K*؛
- يجفر باستعمال *'K* القيمة *E* للحصول على *'RAND*؛
- يقارن بين *'RAND* و*RAND*. وإذا تساويا، يتم استيقان المستعمل وتكون *'K = K*. وتتشارك وظيفة المستعمل النهائي مع الكيان S-5 في المفتاح *K*؛
- يولد المفتاحين *CK* و*IK* باستعمال المفتاح *K* المشترك. وعلى سبيل المثال، يمكن استخدام نفس الوظائف لتوليد المفتاحين *CK* و*IK* المحددين في المرجع [ATIS 33102] وذلك باستعمال *K*.

7 يرسل الكيان S-5 نتيجة الاستيقان وسجل المستعمل والمفتاحين *CK* و*IK* إلى الكيان S-1.

8 يستعمل الكيان S-1 السجل للتحقق من أن المستعمل المستيقن مرخص له بالتسجيل واستقبال الخدمة المطلوبة. وإذا تحقق ذلك يبلِّغ الكيان S-n وظيفة المستعمل النهائي بأن النفاذ مضمون باستخدام رسالة OK 200 وفق بروتوكول SIP.



الشكل 6 – إدراج آلية استيقان النظام IMS
في الاستيقان PKI (الخيار 2)

5.6.2.6 مقارنة الخيارين 1 و2

يقدم الجدول 1 المقارنة بين آليات الخيارين 1 و2.

الجدول 1 – مقارنة بين الخيارين 1 و2 للاتفاق الرئيسي بين وظيفة المستعمل النهائي والكيان S-5 بشأن المفتاحين *CK* و*IK*

	الخيار 1 (مع كلمة مرور مشتركة)	**الخيار 2 (دون كلمة مرور مشتركة)**
المنافع	يعيد استعمال آلية AKA بصورة كاملة بهدف إبرام اتفاق بشأن المفتاحين *CK* و*IK*	لا يتطلب كلمة مرور مشتركة بين وظيفة المستعمل النهائي والكيان S-5
المضار	يتطلب الحصول على كلمة مرور مشتركة بين وظيفة المستعمل النهائي والكيان S-5	يتطلب إدخال تعديلات على التطبيقات المستخدمة في وظيفة المستعمل النهائي (على البطاقات الذكية مثلاً) وفي الكيان S-5 من أجل تفعيل الاتفاق بشأن *CK* و*IK*

ينبغي اعتماد الخيار 1 لتبسيط اتفاق المفاتيح بشأن المفتاحين *CK* و*IK* عندما تتشارك وظيفة المستعمل النهائي والكيان S-5 في كلمة المرور. وينبغي أن يكون الخيار 2 هو المستعمل في حال عدم وجود سر مشترك بين وظيفة المستعمل النهائي والكيان S-5.

ويجب أن تدعم تطبيقات آليات الإدراج هذه الخيارين على حد سواء.

متطلبات الكيان الوظيفي S-5

إضافة إلى المقدرات الواردة في المرجع [ATIS 33102]، يجب أن يكون الكيان S-5 قادراً على:

- تخزين شهادات المستعملين والشبكة، واستخراج هذه الشهادات من مخزون الشهادات.
- إجراء عملية فك التجفير استناداً إلى المفتاح PKI على النحو الوارد في المرحلة 6 (بالنسبة إلى كل من الخيارين).
- استخدام بروتوكول القطر المعدل للحصول على المعلومات الواردة في المرحلة 6 (للخيارين) والمعلومات الضرورية للتفاوض مع وظيفة المستعمل النهائي بشأن الاستيقان القائم على المفتاح PKI.
- التفاوض مع وظيفة المستعمل النهائي وإبرام اتفاق بشأن طريقة الاستيقان القائم على المفتاح PKI.

6.6.2.6 متطلبات وظيفة المستعمل النهائي

يجب أن تكون وظيفة المستعمل النهائي قادرة على:

- تخزين مفتاح المستعمل الخاص U_{pr} بصورة أمينة.
- تخزين كلمة المرور المشتركة K_s (بالنسبة إلى الخيار 1 فقط) بصورة آمنة.
- تخزين شهادة شبكة X.509 في مفتاح الشبكة العمومي N_{pu}.
- توليد مفتاح K لجلسة واحدة بصورة عشوائية وإجراء تجفير تناظري للمفتاح K.
- توليد المفتاحين *CK* و*IK* باستعمال كلمة المرور المشتركة K_s على النحو الوارد في المرجع [ATIS 33102] (للخيار 1 فقط).
- توليد المفتاحين *CK* و*IK* على النحو الوارد في المرحلة 6 وذلك للخيار 2.
- إجراء عمليتي التجفير وفك التجفير استناداً إلى المفتاح PKI على النحو الوارد في المرحلتين 4 و5 لكل من الخيارين.
- إدارة عملاء البروتوكول SIP بصيغته المعدلة التي تمكن من إرسال المعلومات الواردة في المرحلتين 4 و5.
- التفاوض مع الكيان S-2 وإبرام اتفاق بشأن استعمال الاستيقان القائم على البنية PKI.

7.6.2.6 متطلبات الكيان S-1

فيما يلي المتطلبات الإضافية للكيان S-1:

- أن يكون قادراً على إنشاء رسائل SIP مع المعلومات الواردة في المرحلة 4 (لكل من الخيارين).
- أن يكون قادراً على استعادة المعلومات الواردة في المرحلة 5 من الرسائل SIP وأن يعيد توضيبها في رسائل بروتوكول القطر على النحو الوارد في المرحلة 6 (للخيارين).
- أن يكون قادراً على إجراء التجفير القائم على PKI الوارد في المرحلة 4 (للخيارين).
- أن يكون قادراً على فهم تبليغ الكيان S-5 بشأن استعمال الاستيقان القائم على البنية PKI.

8.6.2.6 متطلبات السطوح البينية للبروتوكول SIP بين الكيانات المشاركة

تتم الاتصالات بين وظيفة المستعمل النهائي والكيان S-1 عبر الكيانين الوظيفيين S-2 وS-3 ليسا أساسيين في عملية الاستيقان ولا يظهران في الشكل 5 والشكل 6:

وهنالك سطوح بينية SIP بين:

- وظيفة المستعمل النهائي والكيان S-2.
- الكيان S-2 والكيان S-3.
- الكيان S-1 والكيان S-3.

ويجب أن تكون هذه السطوح البينية قادرة على التفاوض بشأن استعمال الاستيقان القائم على البنية PKI (بما في ذلك الخيار الخاص بتوليد المفاتيح) وعلى نقل المعلومات الواردة في المرحلتين 4 و5 (للخيارين).

9.6.2.6 متطلبات السطوح البينية لبروتوكول القطر بين الكيانات المشاركة

هنالك سطوح بينية لبروتوكول القطر بين:

- الكيان S-1 والكيان S-5.
- الكيان S-3 والكيان S-5.

ويجب أن تكون هذه السطوح البينية قادرة على التفاوض بشأن استعمال الاستيقان القائم على البنية PKI (بما فيها الخيار المحدد لتوليد المفاتيح) ونقل المعلومات الواردة في المرحلة 6 (للخيارين).

7.2.6 إدراج الاستيقان القائم على البنية PKI وآليات توكيد اللغة SAML

تسمح اللغة SAML بامتلاك كيان واحد (مثال المورد IdSP) لإجراء الاستيقان وكيان آخر (طرف معوِّل مثل مورد خدمة تطبيقات) لاستعمال نتائج الاستيقان. وفي مثل هذا السيناريو يمكن لمورد خدمة الهوية (IdSP) استخدام عدة طرائق استيقان بينما يعتمد مورّد خدمة التطبيقات (ASP) على توكيدات لغة SAML للمورد IdSP. ويعود هذا السيناريو بالنفع على كل من موردّي خدمات الهوية ومورّدي التطبيقات. وفيما يلي منافع موردي خدمة التطبيقات (ASP):

- لا يلزم مورد التطبيقات باستخدام طرائق استيقان عديدة.
- يمكن لمورّد خدمة التطبيقات (ASP) أن يدعم طائفة واسعة من خدمات التطبيقات على اختلاف متطلبات ضمان الاستيقان فيها.

وفيما يلي منافع مورّدي خدمة الهوية:

- يمكنه عرض خدماته في إدارة الهوية وخصوصاً الاستيقان للعديد من موردي خدمة التطبيقات.
- يستطيع مورد خدمة الهوية (وخاصة عندما يكون مورّد شبكة NGN في نفس الوقت) استعمال بنيته التحتية المُنشرة للاستيقان كي يعرض خدمات إدارة الهوية على الموردين الآخرين.

وتحدد هذه الفقرة آلية لاستيقان الزبون تستعمل توكيدات اللغة SAML والاستيقان القائم على البنية PKI. وتتيح الآلية بموازاة تلك الواردة في الفقرة 6.2.6 *إدراج الاستيقان القائم على البنية PKI في النظام IMS* لموردي الشبكات NGN الاستفادة من البُنى التحتية القائمة على المفاتيح العمومية واستعمالها.

وتستند هذه الآلية إلى *طريقة إعادة توجيه الربط HTTP* SAML المحددة في المرجع [ITU-T X.1141].

1.7.2.6 كيانات مشاركة في الاستيقان وتدفق المعلومات

- وظيفة المستعمل النهائي: هذا الكيان قادر على إدارة عمليات زبون شبكة الويب وتوفير الاستيقان القائم على البنية PKI [ITU-T X.509].
- مخدم التطبيقات (AS): كيان يوفر خدمة الويب، ويؤدي دور الطرف المعوّل. وهو يعمل طرفاً طالباً للغة SAML على النحو المحدد في [ITU-T X.1141].
- والكيان A-2: كيان وظيفي لبوابة التطبيق (APL-GW-FE) يمكن من إجراء الاستيقان القائم على البنية PKI ويعمل كطرف مستجيب للغة SAML على النحو المحدد في [ITU-T X.1141].
- الكيان S-5: كيان وظيفي لأوصاف مستعمل الخدمة (SUP-FE).

ويبين الشكل 7 تدفق معلومات إجراء الاستيقان – وترد أدناه المراحل الأساسية لتبادل بيانات الاستيقان القائم على البنية PKI مع توكيد اللغة SAML. راجع التوصية [ITU-T Y.2012] للاطلاع على أوصاف الكيانات الوظيفية في شبكة الجيل التالي (وظيفة المستعمل النهائي وAS وA-2 وS-5).

2.7.2.6 الاصطلاحات

يستعمل النص الاصطلاحات التالية:

"|" تدل على تسلسل السلسلة.

$K()$ تدل على تجفير مفتاح تناظري.

K_s تدل على كلمة مرور مشتركة بين الكيانين A-2 وAS.

$N_{pr}[]$ تدل على تجفير بمفتاح الشبكة الخاص N_{pr}.

$N_{pu}[]$ تدل على تجفير بمفتاح الشبكة العمومي N_{pu} المتوفر في شهادة الشبكة.

$U_{pr}[]$ تدل على تجفير بمفتاح المستعمل الخاص U_{pr}.

RAND تدل على رد يتولد عشوائياً.

3.7.2.6 معلمات الآلية

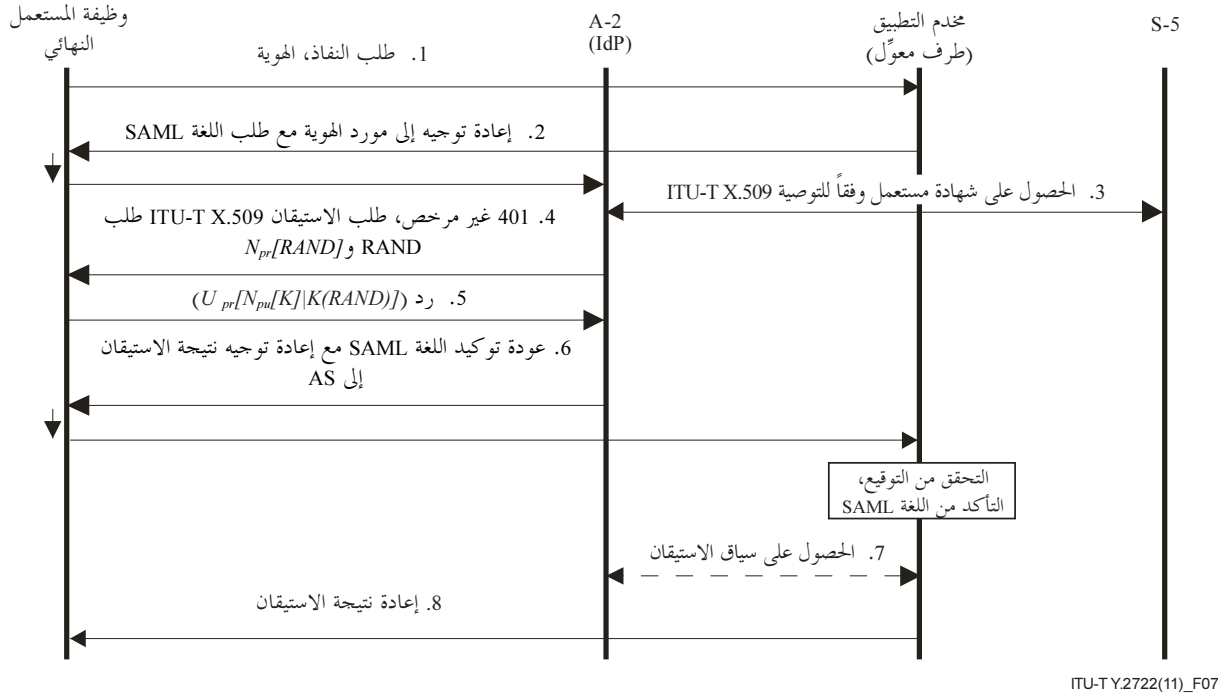
تحدد هذه الفقرة المعلمات الخاصة بالآلية. وفيما يلي قائمة بالمعلمات:

`pki-auth-challenge` – معلمة نقل القيمة *RAND*

`pki-auth-challenge-encrypted` – معلمة نقل القيمة $N_{pr}[RAND]$

`pki-auth-user-signature` – معلمة نقل القيمة $U_{pr}[N_{pu}[K]|K(RAND)]$

`pki-auth-keyinfo` – معلمة نقل القيمة $K_s(K)$



الشكل 7 – المراحل الأساسية لتبادل بيانات الاستيقان القائم على البنية PKI وتوكيد اللغة SAML

والاستيقان المتبادل بين وظيفة المستعمل النهائي والكيان A-2 مماثل للإجراء المستعمل في آلية إدراج الاستيقان القائم على البنية PKI في استيقان النظام IMS الوارد في الفقرة 6.2.6.

وفيما يلي المراحل الأساسية للإجراء الذي يستند إلى الاستيقان القائم على البنية PKI وتوكيدات اللغة SAML:

1) يُصدر زبون الويب لوظيفة المستعمل النهائي طلب بروتوكول HTTP إلى مخدم التطبيق (AS). ويضم الطلب معرّف المستعمل والعنوان URL لكيان A-2.

2) يستجيب مخدم التطبيق الذي يعمل كطرف طالب للغة SAML لطلب البروتوكول HTTP بإرسال طلب اللغة SAML. ويشفر طلب اللغة SAML في رأسية موقع الاستجابة HTTP مع حالة البروتوكول HTTP بالقيمة 302 أو 303. ويرسل عميل وظيفة المستعمل النهائي طلب اللغة SAML من خلال إصدار طلب HTTP GET إلى الكيان A-2 الذي يعمل كمستجيب اللغة SAML. ويتحدد إجراء إعادة توجيه البروتوكول HTTP المعروفة باسم *إعادة توجيه الربط HTTP* في المرجع [ITU-T X.1141]. ومن أجل ضمان الاستيقان والتكاملية للرسالة المشفرة URL ينبغي توقيعها على النحو الوارد في الفقرة 2.5.4.2.10 *"اعتبارات الأمن"* من التوصية [ITU-T X.1141]. ويجب استعمال كلمة المرور المشتركة K_s للتوقيع.

3) بعد التأكد من صلاحية التوقيع يحصل الكيان A-2 من الكيان S-5 على شهادة المستعمل النهائي ويتحقق من صلاحيتها. وتحتوي الشهادة على المفتاح العمومي لوظيفة المستعمل النهائي.

4) يستجيب الكيان A-2 لوظيفة المستعمل النهائي برسالة رد HTTP تشير إلى أن الاستيقان باستعمال شهادة [ITU-T X.509] مطلوب. ويتم ذلك بوضع قيمة رأسية الرد `WWW-Authenticate` [b-IETF RFC 2616] في المعلمة "`pki-auth`". ويتضمن متن الرسالة المعلمتين `pki-auth-challenge` و`pki-auth-challenge-encrypted` اللتين تحملان القيمتين لرد المولد عشوائياً، *RAND* وتشفيره $N_{pr}[RAND]$ على التوالي. ويجب أن تتخذ الرأسية `Content-Type` القيمة `application/x-www-form-urlencoded`.

5) وظيفة المستعمل النهائي:

- استعادة القيمة *A* التي يفترض أن تساوي *RAND* والقيمة *B* التي يفترض أن تساوي $N_{pr}[RAND]$؛
- استعادة مفتاح الشبكة العمومي N_{pu}؛
- فك تشفير القيمة *B* باستعمال N_{pu} ومقارنة النتيجة مع القيمة *A*. وإذا تساوت القيمتان تم الاستيقان وإلاَّ توقف إجراء الاستيقان؛
- توليد مفتاح المرور *K*؛
- توليد القيمة $U_{pr}[N_{pu}[K]|K(RAND)]$ ووضع المعلمة `pki-auth-user-signature` في تلك القيمة وإرسالها في متن رسالة HTTP POST إلى الكيان A-2. ويجب أن تتخذ رأسية الرسالة `Content-Type` القيمة `application/x-www-form-urlencoded`؛

وبعد هذه المرحلة يتحقق الكيان A-2 من صحة الرد. ويُجري لهذا الغرض العمليات التالية:

- الاستعلام عن شهادة المستعمل للحصول على المفتاح العمومي للمستعمل U_{pu}؛
- فك تشفير القيمة *C* الواصلة التي يفترض أن تساوي $U_{pr}[N_{pu}[K]|K(RAND)]$ لاستعادة القيمة *D*|*E* حيث يفترض أن تساوي *D* قيمة $N_{pu}[K]$ و*E* القيمة *K(RAND)*، وذلك باستعمال المفتاح U_{pu}؛
- فك تشفير القيمة *D* باستعمال مفتاح الشبكة الخاص N_{pr} وذلك للحصول على القيمة *K'*؛
- فك تشفير القيمة *E* باستعمال *K'* للحصول على *RAND'*؛
- مقارنة القيمتين *RAND'* و*RAND* . وإذا تساويتا، تم استيقان المستعمل وكانت *K = K'*. وتشارك الكيانان وظيفة المستعمل النهائي وA-2 في المفتاح *K*.

6) إذا تمت جميع المراحل آنفة الذكر بنجاح، يجري الكيان A-2 العمليات التالية:

- توليد توكيد لغة SAML يعطي النعت Method للعنصر <SubjectConfirmation> قيمة مستندات المرسل؛
- حساب القيمة $K_s(K)$؛
- إدراج التوكيد في رد SAML. ثم إرسال الرد SAML وحساب القيمة $K_s(K)$ عبر HTTP بنفس الطريقة الواردة للطلب SAML في المرحلة 2 (أي كجزء من سلسلة الاستفسار). نقل القيمة $K_s(K)$ في المعلمة `pki-auth-keyinfo`؛
- من أجل ضمان الاستيقان الأصلي والتكاملية في الرسالة المشفرة URL، ينبغي توقيع الكيان A-2 عليها على النحو المحدد في الفقرة *2.5.4.2.10 "اعتبارات الأمن"* من المرجع [ITU-T X.1141]. وينبغي استعمال المفتاح K_s المشترك للتوقيع؛

بعد التأكد من صلاحية الموقع URL، الموقع يضمن مخدم التطبيق (AS) أن التوكيد SAML أجراه الكيان A-2. ويتحقق المخدم AS من التوكيد ذاته (كي يضمن استيفاء *الشروط*). وبعد ذلك، يستعيد مخدم التطبيق القيمة $K_s(K)$ ويفك تشفيرها باستعمال المفتاح المشترك K_s للحصول على القيمة *K*. وعند هذه النقطة يستيقن المخدم AS وظيفة المستعمل النهائي ويتشارك الكيانان في المفتاح *K* الذي يمكن استعماله لتوفير أمن الاتصالات بينهما؛

7) يحصل مخدّم التطبيق على معلومات عن سياق الاستيقان إذا نصت الشروط على ذلك فيما يتعلق باتخاذ قرار الاستيقان. وفي هذه الحالة يجيب الكيان A-2 بإرسال المعلومات المحددة في صنف سياق الاستيقان ITU-T – X.509، المفتاح العمومي [ITU-T X.1141].

8) يرسل المخدّم AS نتيجة قرار الاستيقان إلى وظيفة المستعمل النهائي.

4.7.2.6 متطلبات إضافية للكيانات المشاركة في عملية الاستيقان

سعياً لتوفير الآلية المذكورة يجب على الكيانات المشارِكة استيفاء المتطلبات التالية:

1.4.7.2.6 متطلبات وظيفة المستعمل النهائي

يجب أن تكون وظيفة المستعمل النهائي قادرة على:

- إدارة الزبون HTTP.
- تخزين مفتاحه الخاص U_{pr} (في بطاقة ذكية مثلاً) بصورة أمينة.
- الحصول على مفتاح الشبكة العمومي N_{pu}.
- إجراء التشفير وفك التشفير.
- توليد مفتاح K.

2.4.7.2.6 متطلبات مخدم التطبيق (AS)

- يجب أن يوفر المخدم AS اللغة SAML [ITU-T X.1141].
- يجب أن يحصل على المفتاح السري المشترك (K_s) مع الكيان A-2.

3.4.7.2.6 متطلبات الكيان الوظيفي A-2

يجب أن يكون الكيان الوظيفي A-2 قادراً على:

- توفير البروتوكول HTTP.
- تخزين مفتاحه الخاص N_{pr} بصورة أمينة.
- الحصول على المفتاح العمومي للمستعمل U_{pu}.
- إجراء التشفير وفك التشفير.
- توكيد الرد العشوائي *RAND*.
- توفير اللغة SAML [ITU-T X.1141].
- الحصول على المفتاح السري المشترك (K_s) مع الكيان AS.

4.4.7.2.6 متطلبات الكيان الوظيفي S-5

ينبغي أن يكون الكيان الوظيفي S-5 قادراً على تخزين شهادات المستعمل ITU-T X.509 أو استخراجها من المخزون (أو كلا الأمرين معاً).

5.7.2.6 متطلبات إضافية للسطوح البينية القائمة بين الكيانات المشارِكة

فيما يلي متطلبات السطوح البينية:

- يجب على السطح البيني القائم بين وظيفة المستعمل النهائي ومخدم التطبيق أن يوفر البروتوكول HTTP [b-IETF RFC 2616].
- يجب على السطوح البينية القائمة بين وظيفة المستعمل النهائي والكيانات الوظيفية A-2 أن توفر البروتوكول HTTP [b-IETF RFC 2616].
- يجب على السطح البيني القائم بين الكيان A-2 ومخدم التطبيق أن يوفر اللغة SAML [ITU-T X.1141].
- يجب على السطح البيني القائم بين الكيان A-2 والكيانات الوظيفية S-5 أن يوفر آلية السؤال والجواب التي تتيح للكيان A-2 الحصول على شهادات مستعمل X.509 من الكيان S-5.

8.2.6 دمج الاستيقان القائم على الهوية المفتوحة مع استيقان اتفاق AKA

إن دمج استيقان اتفاق AKA مع الاستيقان القائم على الهوية المفتوحة يتيح ضم مقدرات إدارة الهوية التي تركز على الشبكة إلى تلك التي تركز على المستعمل. وتتيح آلية الدمج هذه:

- لموردي الشبكة أن يقدموا خدمات هوية إلى مستعملي النفاذ إلى تطبيقات الويب.
- للمستعملين المزوَّدين بتسجيل الدخول لمرة واحدة (SSO) إمكانية عبور شبكة النظام IMS وبيئة خدمات الويب باستعمال تطبيق ISIM قائم، فضلاً عن تطبيقات SIM الأخرى التي تعول على اتفاق AKA.
- للمستعملين أن يراقبوا معرّفات هوياتهم العمومية على الويب على النحو المحدد في المرجع [b-OpenID v.2] أثناء الاستفادة من خدمات شبكة الجيل التالي.
- تحسين أمن المستعمل من خلال إشراك مشغِّل شبكة المستعمل الموثوق في خيط النفاذ إلى تطبيقات الويب.

ويصف التقرير التقني [b-3GPP TR 33.924] عدة حلول لإدراج الهوية المفتوحة (OpenID) في الاتفاق AKA الذي يعوّل على استعمال وظيفة مخدم الانطلاق (BSF).

وترد في هذه الفقرة آلية إضافية لمزج *الهوية المفتوحة* والاتفاق AKA. ولذا تطالب مواصفة *الهوية المفتوحة* بتنوع آليات الاستيقان.

ويمكن للهوية المفتوحة (OpenID) العمل مع تكنولوجيات أخرى مثل OAuth على النحو المبين في التذييل الثاني.

1.8.2.6 الكيانات المشاركة في الاستيقان وتدفق المعلومات

- وظيفة المستعمل النهائي. هذا الكيان قادر على إدارة عملاء الويب والاتصال بتطبيق SIM المناسب.
- مخدم التطبيق – كيان يقدم خدمات شبكة الويب. ويؤدي دور الطرف المعوّل.
- الكيان A-2: كيان وظيفي لبوابة التطبيق (APL-GW-FE) قادر على العمل لمزود هوية *OpenID* [b-OpenID v.2]. (يشارك الكيان A-2 خيارياً عدم التطبيق مفتاحاً سرياً للأمد القصير على النحو المحدد في [b-OpenID v.2].)
- S-5 – كيان وظيفي لأوصاف مستعمل الخدمة (SUP-FE).

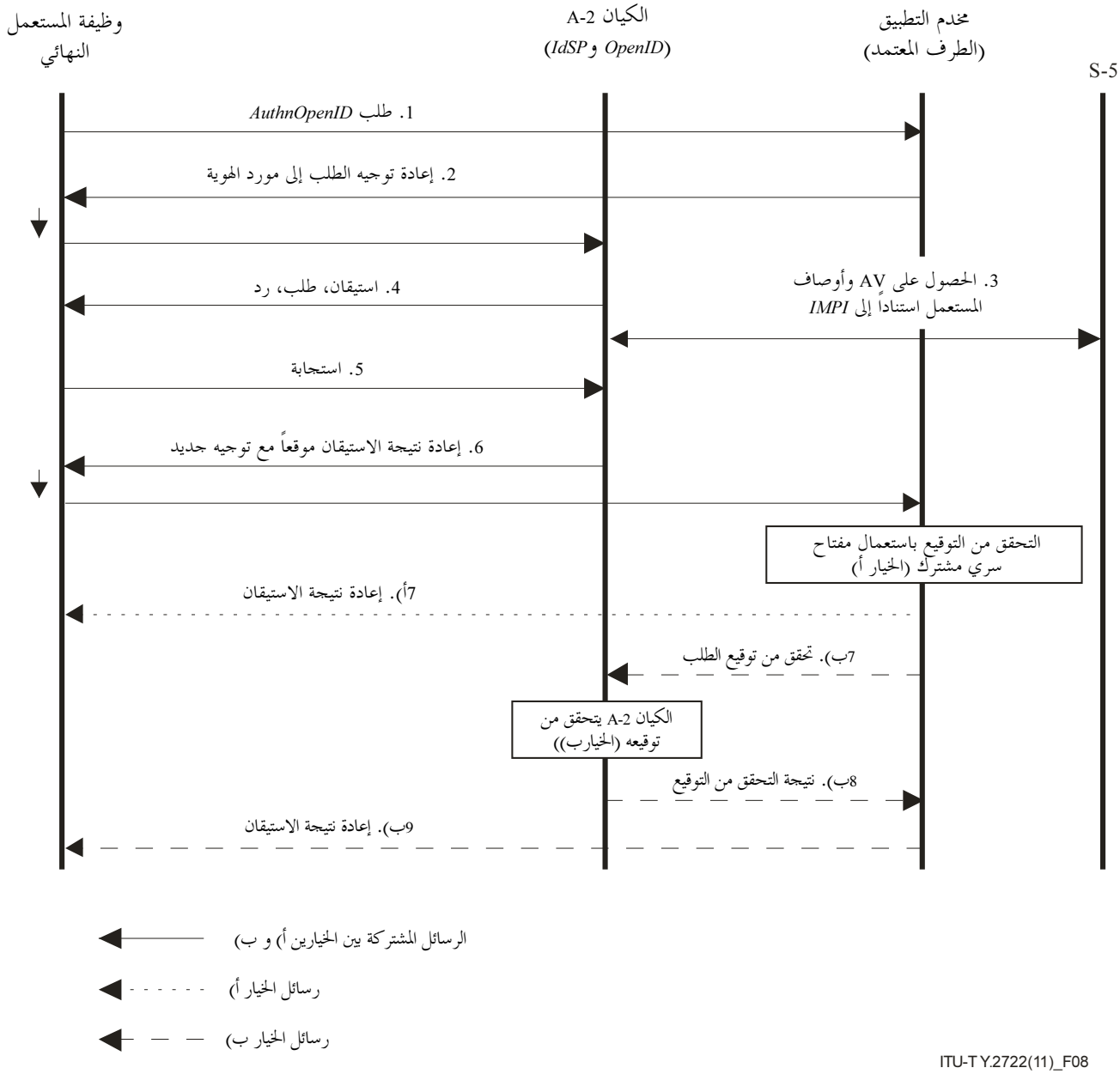
يبين الشكل 8 تدفق معلومات إجراء الاستيقان. ولا يظهر إجراء إقامة مفتاح التوقيع للأمد القصير بين مخدم التطبيق والكيان A-2. ويبين الشكل المراحل الأساسية للإجراء فيما يتعلق بخياري الهوية المفتوحة:

أ) يشارك الكيان A-2 عدم التطبيق مفتاحاً سرياً.

ب) لا يشارك الكيان A-2 مخدم التطبيق مفتاحاً سرياً.

أما المراحل المشتركة بين الخيارين فهي من 1 إلى 6. وتقتصر المرحلة 7أ) على الخيار أ) فقط.

أما المراحل 7ب) و8ب) و9ب) فهي تتعلق بالخيار ب) فقط.



الشكل 8 – دمج آلية استيقان اتفاق AKA مع الهوية المفتوحة

وفيما يلي الخطوات الأساسية للإجراء:

1) يُصدر عميل الويب في وظيفة المستعمل النهائي طلب استيقان *AuthnOpenID* إلى مخدم التطبيق. ويشمل الطلب معرف هوية OpenID.

2) يقوم مخدم التطبيق عن طريق استعمال معرّف الهوية OpenID المقدّم باكتشاف موقع الموارد الموحد للكيان A-2، والذي يعمل كمورد هوية OpenID، ويعيد توجيه طلب استيقان المستعمل إلى موقع الموارد الموحد هذا.

وبعد هذه الخطوة، يربط الكيان A-2 معرف هوية المستعمل بالهوية المناسبة (مثل IMSI أو IMPI).

3) يحصل الكيان A-2 من الكيان S-5 على متجه الاستيقان واتفاق المفاتيح AV، والمظهر الجانبي للمستعمل استناداً إلى الهوية IMPI.

4) يرسل الكيان A-2 إلى وظيفة المستعمل النهائي طلب استيقان باستعمال الطريقة HTTP Digest AKA [المعيار b-IETF RFC 4169] أو [المعيار b-IETF RFC 3310]. ويشمل الطلب سؤالاً وكمية تمكن وظيفة المستعمل النهائي من استيقان الشبكة.

وبعد هذه الخطوة، تستيقن وظيفة المستعمل النهائي من الشبكة بالطريقة المحددة في [المعيار b-IETF RFC 4169] أو [المعيار b-IETF RFC 3310].

5) ترسِل وظيفة المستعمل النهائي إلى الكيان A-2 رداً اختبارياً على النحو الموصف في [المعيار b-IETF RFC 4169] أو [المعيار b-IETF RFC 3310].

وبعد هذه الخطوة يستيقن الكيان A-2 من وظيفة المستعمل النهائي على النحو الموصف في [المعيار b-IETF RFC 4169] أو [المعيار b-IETF RFC 3310].

6) يرسل الكيان A-2 إلى وظيفة المستعمل النهائي رسالة موقعة تؤكد أن معرف الهوية *OpenID* المدَّعى يخص المستعمل. وتُوقع الرسالة باستعمال مفتاح سر متقاسم مع مخدم التطبيق، وذلك في حالة الخيار (أ). وبالنسبة إلى الخيار (ب) تُوقع الرسالة باستعمال مفتاح سر الكيان A-2. وتشمل الرسالة طلباً لإعادة توجيه عميل الويب الخاص بوظيفة المستعمل النهائي إلى مخدم التطبيق. ويرد الوصف التفصيلي لإجراءات التوقيع وإعادة التوجيه في المعيار [b-OpenID v.2]. كما يحدد المعيار تدابير منع للهجمات تستند إلى إعادة استعمال تأكيد الاستيقان الموقع.

خطوات خاصة بالخيار أ) حصراً:

7أ) بعد التحقق من التوقيع الممهور على الرد المتلقَّى في الخطوة 6، يخطِر مخدم التطبيق وظيفة المستعمل النهائي بنتائج الاستيقان. ويستعمِل مخدم التطبيق مفتاح سر متقاسم مع الكيان A-2 من أجل هذا التحقق.

في حال فشل واحدة من الخطوات التالية: الخطوات من 1 إلى 6 أو إلى 7أ) – يتوقف إجراء الاستيقان.

خطوات خاصة بالخيار ب) حصراً:

7ب) يرسل مخدم التطبيق نسخة من الرسالة المتلقاة في الخطوة 6 إلى الكيان A-2 مع طلب للتحقق من التوقيع.

8ب) بعد التحقق من توقيعه، يبلِّغ الكيان A-2 مخدم التطبيق بالنتيجة.

9ب) يقوم مخدم التطبيق بإبلاغ وظيفة المستعمل النهائي بنتائج الاستيقان.

في حال فشل واحدة من الخطوات التالية: الخطوات من 1 إلى 6 أو إلى 7ب) أو إلى 8ب) أو إلى 9ب) – يتوقف إجراء الاستيقان.

2.8.2.6 متطلبات إضافية بخصوص الكيانات المشاركة في الاستيقان

دعماً للآلية المشروحة، يجب على الكيانات المشاركة استيفاء المتطلبات التالية:

1.2.8.2.6 متطلبات لوظيفة المستعمل النهائي

يجب أن تكون وظيفة المستعمل النهائي قادرة على:

- الاستيقان باستعمال طريقة HTTP Digest AKA؛
- الاتصال بالتطبيق ISIM.

2.2.8.2.6 متطلبات لمخدّم التطبيق

يجب أن يكون بمقدور مخدّم التطبيق دعم مواصفة الصيغة 2.0 *OpenID* [المعيار b-OpenID v.2].

3.2.8.2.6 متطلبات للكيان الوظيفي A-2

يجب أن يكون الكيان الوظيفي A-2 قادراً على:

- إجراء الاستيقان بالطريقة HTTP Digest AKA.
- ربط معرف الهوية OpenID الخاص بالمستعمل بمعرف هوية مناسب (مثل IMSI أو IMPI).
- العمل كمورد هوية OpenID.

4.2.8.2.6 متطلبات للكيان الوظيفي S-5

لا توجد متطلبات أخرى بالنسبة للكيان الوظيفي S-5 خلاف الواردة في التوصية [ITU-T Y.2012].

3.8.2.6 متطلبات إضافية للسطوح البينية بين الكيانات المشاركة

فيما يلي المتطلبات الخاصة بالسطوح البينية:

- يجب أن يدعم السطح البيني بين وظيفة المستعمل النهائي ومخدم التطبيق الاستيقان OpenID على النحو المحدد في المواصفة 2.0 [المعيار b-OpenID v.2].
- يجب أن تدعم السطوح البينية بين وظيفة المستعمل النهائي والكيانات الوظيفية A-2 البروتوكول HTTP Digest AKA [المعيار b-IETF RFC 4169] أو [المعيار b-IETF RFC 3310].

لا توجد أي متطلبات محددة الآلية للسطح البيني بين الكيانين الوظيفيين A-2 وS-5.

4.8.2.6 آلية التشغيل *OpenID* وAKA بينياً من أجل سيناريو تجزئة مطراف المستعمل

إن السيناريو الموصوف في هذه الفقرة يدعم أيضاً سيناريو التجزئة الذي يرد وصفه في المعيار [b-3GPP TR 33.924]. ويعود هذا السيناريو إلى الحالة التي يكون فيها وسيط الاستيقان (كيان يملك نفاذاً إلى البطاقة UICC) ووسيط التصفح لا يقعان في مطراف مستعمل واحد.

وبالنظر إلى حل AKA المباشر المشروح في هذه الفقرة، فإن المورد IdSP يناظر الوظيفة NAF/BSF الفاشلة، ويدعم الحل تماماً السيناريوهات الموصوفة في [المعيار b-3GPP TR 33.924]. وتعتمد الآلية على الاستيقان AKA المباشر بدلاً من الاستيقان القائم على المعمارية GBA.

9.2.6 معمارية عامة للدعم (GBA)

توصِّف المعمارية العامة للدعم (GBA) إطاراً لدعم الاستيقان وللتوصل إلى اتفاق المفاتيح الذي ينهض بالاستيقان 3GPP وبالآلية AKA. وتسهل المعمارية GBA استيقان المستعمل النهائي من الوظيفة NAF ويمكن استعمالها في إدارة الهوية في شبكات الجيل التالي لكي تمكن من:

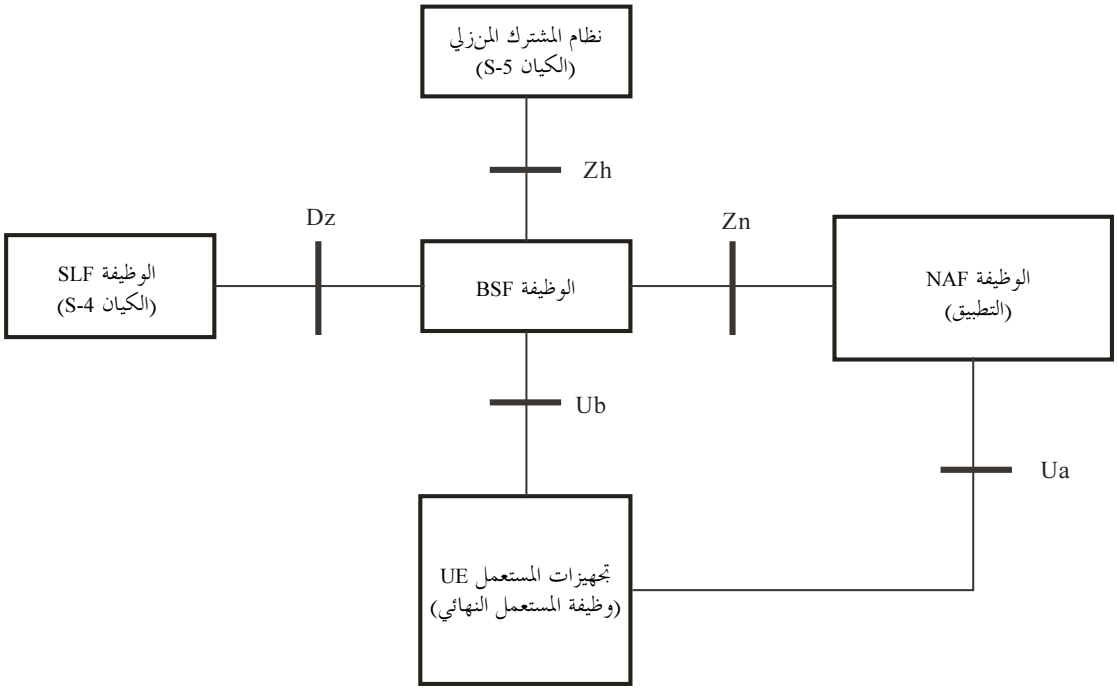
- الاستيقان واتفاق المفاتيح.
- حماية الخصوصية.
- الاستيقان الوحيد.

والمعمارية GBA تُعد بمثابة آلية استيقان تتألف من ثلاثة أجزاء:

- مستعمل نهائي يسعى إلى الحصول على خدمات الشبكة باستعمال مطراف المستعمل (UE).
- مخدم تطبيق (يسمى وظيفة تطبيق الشبكة أو NAF).
- كيان موثوق (يسمى وظيفة مخدم الدعم أو BSF)، حيث يشارك في الاستيقان وعملية تبادل المفاتيح بين كيانين آخرين.

وتمكن المعمارية GBA من استيقان المستعمل النهائي الذي يستعمل المطراف UE من مخدم التطبيق (NAF) دون الكشف عن اثباتات ومفاتيح سر المستعمل النهائي طويلة الأمد للمخدم NAF عن طريق استعمال كيان موثوق (BSF).

ويصور الشكل 9 معمارية GBA [b-ETSI TS 133 220] ويوفر التقابل بين الكيانات المعرّفة في مشروع الشراكة لتكنولوجيات الجيل الثالث اللاسلكية (3GPP) والكيانات الوظيفية الموصّفة في التوصية [ITU-T Y.2012].



ملاحظة – يشير الوسم بين الأقواس إلى الكيانات الموصفة في التوصية [ITU-T Y.2012].

ITU-T Y.2722(11)_F09

الشكل 9 – نموذج شبكي بسيط للدعم

وفيما يلي الخطوات الأساسية لعملية المعمارية GBA:

1) تطلب الوظيفة NAF الاستيقان وتتفاوض من أجل استعمال المعمارية GBA على النقطة المرجعية Ua.

2) يقوم عميل الوظيفة BSF الجارية على تجهيزات المستعمل باستهلال عملية الدعم على النقطة المرجعية Ub. وتجلب الوظيفة BSF معلومات الاستيقان وقيم الضبط الأمنية لمستعمل المعمارية GBA من النظام HSS على النقطة Zh. ويجري استيقان متبادل بين مطراف المستعمل والوظيفة BSF باستعمال http Digest AKA. وينتج عن عملية الاستيقان هذه تلقي تجهيزات المستعمل لمعرف هوية لمعاملة الدعم (B-TID) من الوظيفة BSF وإنشاء مفتاح مشترك (Ks) بين مطراف المستعمل والوظيفة BSF.

3) تقوم تجهيزات المستعمل باشتقاق Ks_NAF من المفتاح Ks وترسل معرّف B-TID (إلى جانب البيانات الخاصة بالتطبيق) إلى الوظيفة NAF.

4) ترسل الوظيفة NAF معرف B-TID إلى الوظيفة BSF عبر النقطة المرجعية Zn.

5) واستناداً إلى المعرف B-TID، تحدد الوظيفة BSF المفتاح Ks الذي ينبغي استعماله وتشتق منه Ks_NAF وترسله إلى الوظيفة NAF.

6) وفي النهاية، يمكن لتجهيزات المستعمل والوظيفة NAF أن يستيقن كل منهما من الآخر باستعمال المفتاح المشترك Ks_NAF. وتعتمد عملية الاستيقان الفعلية على البروتوكول القائم بين تجهيزات المستعمل والوظيفة NAF. فعلى سبيل المثال، من مواصفات المعمارية GBA، أنه يمكن للتطبيقات القائمة على البروتوكول HTTP

استعمال إما الاستيقان HTTP Digest [المعيار b-IETF RFC 2617] أو متواليات تجفير مفتاح مشترك مسبق TLS [المعيار b-IETF RFC 4279].

ملاحظة – تلجأ الوظيفة BSF إلى الوظيفة SLF عبر النقطة المرجعية Dz للحصول على اسم النظام HSS الذي يتضمن البيانات الخاصة بالمشترك. لا توجد حاجة إلى الوظيفة SLF عند تشكيل الوظيفة BSF بصورة تتيح لها استعمال نظام HSS محدد سلفاً.

ويرد توصيف تقابل كيانات المعمارية GBA مع كيانات الشبكات NGN في التوصية ITU-T Y.2012، *المتطلبات الوظيفية ومعمارية شبكات الجيل التالي*، على النحو التالي:

- تقابل الوظيفة NAF كيان *التطبيقات* في الشكل 3. معمارية وظيفية عامة لشبكات الجيل التالي من التوصية [ITU-T Y.2012].
- النظام HSS يقابل الكيان الوظيفي S-5 (المظهر الجانبي لمستعمل الخدمة).
- الوظيفة SLF تقابل الكيان الوظيفي S-4 (موقع الاشتراك).
- تجهيزات المستعمل تقابل وظيفة المستعمل النهائي.

10.2.6 الاستيقان القائم على الهوية IMSI

حسب مستوى الضمان المطلوب، يمكن استعمال هوية المشترك في الخدمة المتنقلة الدولية (IMSI) في شبكة قائمة على بروتوكول النفاذ اللاسلكي (WAP) لأغراض الاستيقان بما يوفر توافقاً عكسياً. وحيث إن الهوية IMSI عبارة عن سلسلة هجائية فريدة، فإنه يمكن استعمالها كهوية لكيان ما لخدمة معينة.

وهذا النهج:

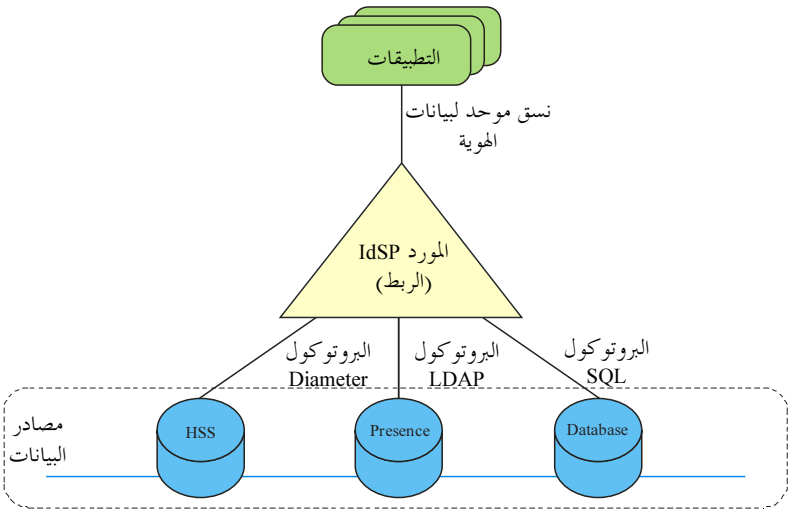
- يستعمل شفرة الهوية IMSI كهوية كيان في التطبيقات اللاسلكية؛
- ويوفر قناة خدمة يعوَّل عليها بشرط أن يكون للنقطة الطرفية هوية IMSI شرعية، وذلك عندما تطلب هذه النقطة الاستيقان؛
- وفيه، تفترض جميع الأنظمة الثقة في نتائج استيقان بوابة البروتوكول WAP وتقدم خدماتها لهذا الكيان؛
- يمكن استخدامه ليوفر استيقاناً وحيداً بفضل فرادة هوية IMSI لنفس النقطة الطرفية بين الخدمة GPRS/CDMA 1x وتطبيقات لا سلكية (مثل صندوق البريد اللاسلكي، وما إلى ذلك)؛
- يوفر الأمن لشفرة هوية IMSI.

3.6 الربط والرباط

تنص التوصية [ITU-T Y.2720]، *إطار إدارة الهوية في شبكات الجيل التالي، على أنه يمكن ربط معلومات الهوية (مثل معرفات الهوية والإثباتات والنعوت) معاً لتكوين رباط لضمان هوية كيان ما.*

ومن أهداف أي حل يمكِّن من الربط تجميع الأنماط المختلفة لمعلومات الهوية من مصادر مختلفة وتقديمها للتطبيقات في نسق موحد يمكنها فهمه.

ويوضح الشكل 10 مفهوم هذا الحل. ويصور الشكل ثلاثة أمثلة مصادر لمعلومات الهوية: النظام HSS ومخدم الحضور وقاعدة بيانات تتعلق ببيانات المستعمل الخاصة بالتطبيق. وقد يحتاج أي تطبيق إلى الأنواع الثلاثة كلها من المعلومات لاتخاذ القرار المتعلق بالاستيقان والتخويل. وفي المثال المصور، تستخدم آلية الربط البروتوكولات Diameter وLDAP وSQL للحصول على البيانات من المصادر المعنية. وتقدم هذه البيانات بعد ذلك إلى التطبيق في نسق يمكن فهمه. وبالتالي، فإن آلية الربط ترفع عن كاهل التطبيقات عبء دعم بروتوكولات عديدة للاتصال بمصادر معلومات الهوية المختلفة.



ملاحظة– تمد آلية الربط التطبيقات بنسق موحد لجميع بيانات الهوية.

الشكل 10 – ربط معلومات الهوية

4.6 الاكتشاف

تفيد التوصية [ITU-T Y.2720]، *متطلبات إدارة الهوية وحالات الاستعمال في شبكات الجيل التالي*، بأن *مورّد خدمة الهوية في شبكات الجيل التالي ضروري لدعم وظائف وقدرات اكتشاف مصادر معلومات الهوية* داخل ميدان NGN/IdSP وبين ميادين NGN/IdSP مختلفة.

وتورد هذه الفقرة أمثلة لآليات قياسية تدعم هذه المتطلبات مع إشارات مرجعية إلى المواصفات ذات الصلة.

1.4.6 الاكتشاف داخل الشبكة الواحدة

تعرِّف التوصية [ITU-T Y.2012]، *المتطلبات الوظيفية ومعمارية شبكات الجيل التالي* كياناً خاصاً – الكيان الوظيفي لموقع الاشتراك (SL-FE) – يقدم عنواناً للكيان الوظيفي للمظهر الجانبي لمستعمل الخدمة (SUP-FE)، الذي يخزّن معلومات الهوية الخاصة بمشترك معين. ويمكّن الكيان SL-FE من اكتشاف الكيان SUP-FE المسؤول عن تخزين المظاهر الجانبية للمستعملين وبيانات الموقع المتعلقة بالمشتركين وبيانات حالة الحضور. ويمكن لكيانات الشبكة اللجوء إلى الكيان SUP-FE للحصول على معلومات الهوية هذه. وكما يرد في التوصية [ITU-T Y.2012]، قد تلجأ كيانات الشبكة التالية إلى الكيان SL-FE للحصول على عنوان الكيان SUP-FE المناسب:

- الكيان الوظيفي لدعم التطبيق (AS-FE)؛
- الكيان الوظيفي للاستفسار عن التحكم في دورة النداء (I-CSC-FE)؛
- الكيان الوظيفي لخدمة التحكم في دورة النداء (S-CSC-FE).

ويرد في المعيار [3GPP TS 23.228] توصيف لآلية تتيح لهذه الكيانات العثور على عنوان للكيان SUP-FE الذي يخزن معلومات هوية مستعمل معين في شبكة أي مشغل. ويلاحظ أن تقابل كيانات التوصية [ITU-T Y.2012] مع كيانات [المعيار 3GPP TS 23.228] يكون كالتالي:

- الكيان AS-FE يقابل دعم التطبيق؛
- الكيان I-CSC-FE يقابل وظيفة الاستفسار عن التحكم في دورة النداء؛
- الكيان S-CSC-FE يقابل وظيفة خدمة التحكم في دورة النداء؛

- الكيان SL-FE يقابل وظيفة تحديد موقع الاشتراك.

2.4.6 الاكتشاف بين الشبكات

تشمل الأمثلة على آليات اكتشاف مورد IdSP بين الشبكات الأمثلة المتضمنة في اللغة SAML [التوصية ITU-T X.1141] والوظيفة ID-WSF [المعيار b-LA WSF]. وتعتمد هذه الآليات على اتفاقات يتم إبرامها مقدماً بين الكيانات المشاركة (مثل مورد خدمة الهوية (IdSP) والطرف المعوِّل) أو أعضاء في اتحاد.

والصيغة OpenID [المعيار b-OpenID v.2] مثال آخر يوصِّف آلية اكتشاف تمكّن طرف معوّل من تحديد موقع مورّد خدمة الهوية على أساس معرّف هوية OpenID مقدَّم من المستعمل.

5.6 الاتصالات وتبادل المعلومات المتعلقة بإدارة الهوية

توصي هذه الفقرة ببروتوكولات وآليات الاتصال وتبادل معلومات الهوية.

1.5.6 أمن اتصالات إدارة الهوية وتبادل معلوماتها

يوصي هذا القسم بآليات توفير السلامة لاتصالات إدارة الهوية وحماية سريتها.

1.1.5.6 حلول تقوم على الإصدار 2.0 من اللغة SAML (SAML 2.0) [ITU-T X.1141]

من أجل السلامة وحماية الخصوصية، يوصي الإصدار SAML 2.0 باستعمال قناة مؤمنة أو بروتوكول شبكي مؤمن مثل TLS أو IPsec بحيث يشكَّل لكي يحمي الرزم المرسلة عبر التوصيل الشبكي.

ولحماية السلامة على مستوى الرسالة، يمكن استعمال التوقيع XML إضافة إلى قناة الاتصال المؤمنة. ويتعين عند استعمال التجفير باللغة XML اتباع تعليمات الفقرة 4.8 من التوصية [ITU-T X.1141]، "قواعد تركيب توقيع اللغتين SAML وXML ومعالجته".

وبالنسبة إلى حماية السرية على مستوى الرسالة، يمكن استعمال التجفير باللغة XML إلى جانب قناة الاتصال المؤمنة. ويتعين عند استعمال التجفير باللغة XML اتباع تعليمات الفقرة 4.8 من التوصية [ITU-T X.1141]، "قواعد تركيب توقيع اللغتين SAML وXML ومعالجته".

2.1.5.6 إطار هوية خدمات الويب (يعرَّف بالإطار ID-WSF)

لاستعمال إطار هوية خدمات الويب من المفترض تأمين سلامة الاتصالات الخاصة به وحماية سرية الرسائل المتداولة بين المرسلين والمستقبلين. وكما هو الحال مع الإصدار SAML 2.0، يوصي هذا الإطار باستعمال قناة مؤمنة أو بروتوكول شبكي مؤمن مثل TLS أو IPsec بحيث يتم تشكيله لكي يحمي الرزم المرسلة عبر التوصيل الشبكي [المعيار "أمن الإطار b-LA ID-WSF"].

1) حماية قناة طبقة النقل

عند استعمال طبقة مقبس مؤمنة (SSL) أو أمن طبقة النقل (TLS) كبروتوكول شبكي مؤمن للإطار ID-WSF، يتعين استعمال الإصدارات SSL 3.0 وTLS 1.0 أو الأحدث. ويتعين على أي كيان يقوم بإرسال توصيل SSL (3.0) أو TLS (1.0) أن يقدم، أو يوافق على متواليات تجفير مناسبة أثناء التعارف. وفيما يلي أمثلة غير حصرية لمتواليات التجفير المناسبة للإصدار TLS (1.0) (أو ما يعادلها للإصدار SSL 3.0).

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_CBC_SHA
- TLS_DHE_DSS_WITH_AES_CBC_SHA

وللتوقيع والتحقق من رسائل البروتوكول، يُوصى بأن تستعمل الكيانات المتصلة شهادات ومفاتيح خاصة تختلف عن الشهادات والمفاتيح الخاصة المستعملة في توفير الحماية للقناة SSL أو TLS.

ويمكن استعمال بروتوكولات أمن أخرى مثل IPsec أو Kerberos طالما تتبع تدابير أمنية معادلة.

2) حماية سرية الرسائل

في وجود الوسطاء، يتعين على الكيانات المتصلة فيما بينها التأكد من عدم الكشف عن معلومات حساسة لكيانات غير مخولة. وفي هذه الحالة، يتعين على هذه الكيانات استعمال آليات السرية التي وضعتها منظمة OASIS من أجل أمن رسائل SOAP لأمن خدمات الويب [المعيار b-OASIS WSS SOAP] وذلك لتجفير غلاف البروتوكول SOAP والمحتوى <S:Body>.

3) قواعد سلامة الرسائل

لا تطبق قواعد سلامة الرسائل الواردة في هذه الفقرة إلا عند استعمال [المعيار b-OASIS WSS SOAP] من أجل رسالة من رسائل البروتوكول ID-WSF ملتزمة بالبروتوكول SOAP طبقاً للإصدار 2.0 الملزِم للبروتوكول Liberty SOAP [b-LA SOAP binding].

وفي هذه الحالة، يتحتم على المرسل وضع توقيع وحيد <ds:Signature> في الرأسية <wsse:Security> وهذا التوقيع يُعد ضرورياً للإشارة إلى جميع مكونات الرسالة التي يتعين توقيعها.

ويُعد هذا التوقيع ضرورياً، على نحو خاص، للإشارة إلى عنصر متن البروتوكول SOAP (العنصر نفسه) وإذنة الأمن المصاحبة للتوقيع، وكل رأسيات الرسالة المحددة في الإصدار 2.0 الملزم للبروتوكول Liberty SOAP [b-LA SOAP binding]، بما في ذلك قدرات الرأسيات المطلوبة والاختيارية.

ومن أمثلة إذنة الأمن العنصر <saml2:Assertion> المرسل في الرأسية <wsse:Security>. والعناصر wsu: رأسية خاتم التوقيت في wsse: قدرة رأسية الأمن، wsa: معرف هوية الرسالة، wsa: تؤدي إلى (RelatesTo) وsb: الإطار (Framework)، sb: المرسل (Sender)، sb: هوية الإنفاذ (InvocationIdentity)، كلها أمثلة لعناصر الرأسيات التي ستتم الإشارة إليها في أي توقيع.

وتجدر الإشارة إلى أنه يتعين توخي الحذر عند بناء العناصر المدرجة في المعلمات المرجعية في مراجع النقاط الطرفية، حيث إنها سترقى فيما بعد إلى فدرات لرأسية البروتوكول SOAP. وينبغي اتخاذ التدابير المناسبة لتفادي التضارب بين نعوت الهوية أو تكرارها، وذلك باستعمال، على سبيل المثال، تقنيات لاستحداث الهويات التي تتسم بالتفرُّد.

وعند توقيع رسالة، يتعين على المرسل إدراج التوقيع XML الناتج في العنصر <ds:Signature> كتابع للرأسية <wsse:Security>.

والعنصر <ds:Signature> ضروري للإشارة إلى مفتاح التأكيد المستهدف بعنصر <ds:KeyInfo>. والعنصر <ds:KeyInfo> ضروري لإدراج العنصر <wsse:SecurityTokenReference> بحيث يمكن وضع مفتاح التأكيد المستهدف ضمن الرأسية <wsse:Security>. ويُوصى بإدراج المرجع للالتزام بالتوجيه المحدد في القسم 2.4.3 من *أمن خدمات الويب*: [المعيار *SAML Token Profile 1.1* لمنظمة OASIS، [b-OASIS SAML token]].

'1' قواعد المعالجة للمرسل:

- يتعين بناء وصقل عنصر الرأسية <wsse:Security> للالتزام بالقواعد المحددة في أمن خدمات الويب: [المعيار SAML Token Profile 1.1 لمنظمة OASIS، [b-OASIS SAML token]].
- عنصر الرأسية <wsse:Security> ضروري لكي يكون هناك النعت mustUnderstand بالقيمة المنطقية true.
- ويتعين على المرسل وضع إذنة أمن لاستيقان الرسالة كتابع مباشر للعنصر <wsse:Security>.

- وعلى المرسل اتباع قواعد سلامة الرسائل المحددة للمرسلين والمستقبلين عند استعمال آليات استيقان الرسائل.

والاعتبارات التالية لا تطبق على إذنات الحمالة:

- بالنسبة إلى قيم الضبط الخاصة بالنشر التي تحتاج إلى استيقان مستقل للرسالة، يتحتم تنفيذ الالتزام بتوقيع متن الرسالة وأجزاء الرأسية ووضع العنصر <ds:Signature> كتابع مباشر للرأسية <wsse:Security>.
- وبالنسبة إلى قيم الضبط الخاصة بالنشر التي لا تحتاج إلى استيقان مستقل للرسالة، يمكن تنفيذ التزام التحقق بربط الشهادة والمفتاح المستعملين لإجراء استيقان الكيانات النظيرة بالشهادة والمفتاح الموصوفين في إذنة استيقان الرسالة. ولتأمين ذلك، يتعين وجود ضمان للسلطة التي تُصدر الإذنة لتحقيق الضمان، بحيث يمكن التحقق من أن مفتاح التأكيد، دون أدنى لبس، يطابق الشهادة والمفتاح المستعملين في إجراء استيقان الكيانات النظيرة. وهذا الأمر ضروري للتخفيف من التهديدات المتعلقة بهجمات استبدال الشهادات. ويُوصى بأن تلتزم الشهادة أو سلسلة الشهادات بمفتاح التأكيد المستهدف.

'2' قواعد المعالجة للمستقبِل:

- يتعين على المستقبل تحديد العنصر <wsse:Security> الذي سيكون المستقبل هدفه. **ويجب** أن يلتزم ذلك بالقواعد المحددة في معيار *أمن رسائل البروتوكول SOAP لأمن خدمات الويب* لمنظمة OASIS [b–OASIS WSS SOAP]، والمظاهر الجانبية المطبقة لإذنات أمن خدمات الويب (*مثل أمن خدمات الويب:* [*المعيار SAML Token Profile 1.1* لمنظمة OASIS، [b-OASIS SAML token]] لإذنات SAML).
- العنصر <wsse:Security> للرأسية ضروري للحصول على النعت mustUnderstand بالقيمة المنطقية true، ويجب أن يكون بمقدور المستقبل معالجة فدرة الرأسية هذه طبقاً لمعيار [b-OASIS WSS SOAP] والمظاهر الجانبية المناسبة لإذنات أمن خدمات الويب (*مثل أمن خدمات الويب:* [*المعيار SAML Token Profile 1.1* لمنظمة OASIS، [b-OASIS SAML token]] لإذنات SAML).
- ويتعين على المستقبل تحديد إذنة الأمن وتحديد ما إذا كان يثق في الجهة التي أصدرت الإذنة.
- ويتعين على المستقبل التحقق من صلاحية توقيع جهة الإصدار على الإذنة. وهذا التحقق ضروري للالتزام بقواعد التحقق الأساسية الموصوفة في *قواعد تركيب ومعالجة التوقيع* XML (الإصدار الثاني) للاتحاد العالمي لخدمات الويب (W3C)، [المعيار b-W3C XML signature]. ويُوصى بأن يتحقق المستقبِل، بقدر الإمكان، من صلاحية دلالات الثقة لمفتاح التوقيع وتفادياً لمخاطر الاستيقان غير السليم.
- وإذا كانت الرسالة موقعة، يتعين على المستقبل تحديد العنصر <ds:Signature> المحمول داخل الرأسية <wsse:Security>.
- ما لم تكن آلية الأمن المستخدمة peerSAMLV2، يتعين على المستقبِل تحليل محتويات العنصر <ds:KeyInfo> المحمول ضمن العنصر <ds:Signature> واستعمال المفتاح الموصوف في هذا العنصر للتحقق من العناصر الموقعة. وفي حال استعمال آلية الأمن peerSAMLV2، فإن المفتاح يكون هو مفتاح العميل المستعمل في استيقان العميل SSL/TLS.
- ويتعين على المستقبِل اتباع قواعد سلامة الرسائل المحددة للمرسلين والمستقبلين عند استعمال آليات استيقان الرسائل.

4) معالجة الرسائل ذات الإذنة WSS ITU-T X.509

ترد في هذه الفقرة دلالات وقواعد المعالجة للآليات التي تستعمل رسائل قيمتها ITU-T X.509. ويمكن الاطلاع على مثال لذلك في التذييل الأول.

وتدعم معرّفات الموارد الموحدة هذه استيقانَ الرسالة أحادي الاتجاه (المرسل) ويكون شكلها كالتالي:

- *urn:liberty:security:2003-08:PEER:X509*، حيث يمكن للعنصر PEER أن يختلف حسب آلة استيقان النظراء المستخدمة (قد يكون فارغاً أو TLS أو ما شابه، مثلاً).

وتستعمل آلية استيقان الرسائل WSS X.509 المظهر الجانبي لإذنة الشهادة ITU-T X.509 في أمن خدمات الويب [b-OASIS WSS X.509 profile] كوسيلة يستيقن بها مرسل الرسالة من مستقبلها. وآلية استيقان الرسائل تلك أحادية الاتجاه. بمعنى، أنه لا يتم الاستيقان إلا من مرسل الرسالة. ولا يقع ضمن نطاق هذه التوصية تناول متى ينبغي استيقان رسائل الرد وإن كانت تجدر الإشارة إلى أنه يمكن الاعتماد على هذه الآلية لاستيقان رسائل الرد أيضاً. ومع ذلك يُوصى بالتنبه إلى أن الاستيقان المستقل لرسائل الرد لا يوفر نفس دلالات حماية قطارات الرسائل، كما هو الحال في آلية الاستيقان المتبادل بين الكيانات النظيرة.

وبالنسبة إلى قيم الضبط الخاصة بالنشر، والتي تحتاج إلى استيقان الرسالة بمنأى عن استيقان الكيانات النظيرة، يتعين على الكيان المرسل إجراء استيقان للرسالة بتقديم ما يثبت أن لديه مفتاح مرتبط بالإذنة ITU-T X.509. ويتعين على المستقبِل تمييز هذا المفتاح بأنه يخص الكيان المرسل.

عندما يقوم المرسل بتطويع مفتاح التأكيد المستهدف لتوقيع عناصر الرسالة، فإن التوقيع يضمن تخويل وسلامة العناصر المشمولة بالتوقيع. ومع ذلك، لا يخفف ذلك وحده من التهديدات المتعلقة بالرد والإدخال وبعض أصناف الهجمات المتعلقة بتعديل الرسائل. ولتأمين الرسائل من هذه التهديدات، يتعين وجود آلية من آليات دعم استيقان الكيانات النظيرة يتسنى استعمالها، أو النموذج الأساسي لمعالجة الطلب الملزم SOAP.

'1' قواعد المعالجة للمرسل:

تضاف القواعد الواردة في هذه الفقرة إلى القواعد العامة لمعالجة استيقان الرسائل الموضحة في هذه التوصية.

- يتعين على المرسل إثبات امتلاكه لمفتاح خصوصي مصاحب للتوقيع الذي يُستحدث بالاقتران مع المظهر الجانبي للإذنة WSS ITU-T X.509.
- وبالنسبة إلى قيم الضبط الخاصة بالنشر والتي تحتاج إلى استيقان مستقل للرسالة، يتعين تنفيذ الالتزام بتوقيع أجزاء الرسالة، حسبما يتناسب، وتسجيل المعلومات في الرأسية <wsse:Security> (كما هو وارد في المعيار [b-OASIS WSS SOAP]).
- وبالنسبة إلى قيم الضبط التي لا تحتاج إلى استيقان مستقل للرسالة، يتعين على المرسل تنفيذ هذا الالتزام بصقل رأسية الأمن بالعنصر <ds:KeyInfo> الذي يحمل الشهادة.

ويتعين التحقق بصورة لا لبس فيها من استعمال نفس الشهادة والمفتاح المستعملين في إجراء استيقان الكيانات النظيرة. وهذا الأمر ضروري للحد من التهديد المتعلق بهجمات استبدال الشهادات. وتجدر الإشارة كذلك إلى أن هذا الاستمثال لا ينطبق إلا على الآليات *ClientTLS:X509*.

'2' قواعد المعالجة للمستقبِل:

- إذا اعتبرت سياسات التحقق من الصلاحية أن استيقان الكيانات النظيرة يكفي لأغراض الاستيقان، فإنه يتعين على المستقبل وضع شهادة ومفتاح مقابلين للمستعملين في إجراء استيقان النظراء باستعمال معلومات المفاتيح المقابلة المرسلة في الرسالة. ويسمح ذلك لمستقبل الرسالة بتحديد ما إذا كان مرسل الرسالة راغباً في استعمال هوية معينة مستيقن منها للنقل. ويمكن حمل المعلومات المتعلقة بالمفتاح SSL/TLS للرسالة في متن الرسالة باستعمال إذنة الأمن ITU-T X.509 لأمن رسائل البروتوكول SOAP للمنظمة OASIS.

6.6 حماية المعلومات التي يمكن التعرف على أصحابها شخصياً (PII)

طبقاً للتوصية ITU-T Y.2720، إطار *إدارة الهوية في شبكات الجيل التالي*، تخضع حماية المعلومات PII للوائح وطنية وإقليمية. فعلى الرغم من أن الآليات والإجراءات المستخدمة في دعم حماية المعلومات PII قد تختلف باختلاف هذه اللوائح، فإنها تقوم على مبادئ أساسية واحدة.

وتقدم هذه الفقرة إطلالة مختصرة على إجراءات حماية المعلومات PII الموصفة في التقرير الخاص للمعهد الوطني الأمريكي للمعايير والتكنولوجيا المعنون "*دليل لحماية المعلومات التي يمكن التعرف على أصحابها شخصياً (PII)*" [التقرير b-NIST-SP 800-122]. ويمكن استعمال مواصفات التقرير الخاصة *بحماية سرية المعلومات PII* كإرشادات لمصممي أنظمة إدارة الهوية. وفيما يلي الفئات المحددة لوسائل الحماية:

- وسائل حماية تشغيلية:
  - استحداث سياسات وإجراءات.
  - الوعي والتدريب والتعليم.
- وسائل حماية تتعلق حصراً بالخصوصية:
  - التقليل إلى أدنى حد من استعمال المعلومات PII وجمعها والاحتفاظ بها.
  - إجراء تقييمات لآثار الخصوصية.
  - معلومات ضد التعرف.
  - معلومات مبهمة.
- وسائل التحكم الأمنية:

يوفر قسم *وسائل التحكم الأمنية* توجيهات بشأن آليات وإجراءات الأمن التي لا تخص المعلومات PII، وإن كان يمكن استخدامها لحماية المعلومات PII. وبالمثل، يمكن استعمال آليات أمن المعلومات التي لا تخص المعلومات PII الموصفة في التوصية [ITU-T Y.2704] لحماية المعلومات PII.

7.6 وظائف الهوية الاتحادية

توضح التوصية [ITU-T Y.2721]، *متطلبات إدارة الهوية وحالات الاستعمال في شبكات الجيل التالي، أن المفهوم العام للاتحاد هو أن يتاح لكل عضو في الاتحاد الاحتفاظ باستقلاله مع تسهيل تبادل معلومات الهوية المحددة للسماح بتقديم خدمات اتحادية*.

وتوصي هذه الفقرة باستعمال آليتين قياسيتين مطبقتين على نطاق واسع تتيحان للمستعمل النفاذ إلى خدمات متعددة دون الاشتراك في كل خدمة من هذه الخدمات على حدة.

وتوفر توصية اللغة SAML [التوصية ITU-T X.1141] حلاً قياسياً للاتحاد. وهي تستعمل عادة من جانب الشركات التجارية والمنظمات الحكومية وموردي الخدمات التابعين لها.

ويوصِّف الإصدار OpenID [b-OpenID v.2] حلاً متمحوراً حول المستعمل، وهذا الحل شائع استعماله للنفاذ إلى خدمات الويب على الإنترنت.

1.7.6 التجسير والتشغيل البيني

تشرح هذه التوصية عدداً من الآليات التي تدعم التجسير والتشغيل البيني بين الحلول والاتحادات المختلفة لإدارة الهوية. ويرد في الفقرات التالية وصف الآليات الرئيسية:

- دمج الاستيقان القائم على بنية المفاتيح العمومية مع النظام IMS (الفقرة 6.2.6).
- دمج الاستيقان القائم على بنية المفاتيح العمومية وآليات التحقق SAML (الفقرة 7.2.6).
- دمج الاستيقان القائم على المعرف *OpenID* مع استيقان AKA (الفقرة 8.2.6).
- المعمارية العامة للدعم (الفقرة 9.2.6).
- الربط والرباط (الفقرة 3.6).
- وظائف الهوية الاتحادية (الفقرة 7.6).

2.7.6 اكتشاف الموردين IdSP في بيئة اتحادية

تعرِّف التوصية SAML [التوصية ITU-T X.1141] في الفقرة 3.4.11 *المظهر الجانبي لاكتشاف مورد الهوية*، وهو الذي يمكِّن مورد الخدمة من اكتشاف مورد هوية المستعمل. والمظهر الجانبي موصَّف دعماً للمظهر الجانبي SAML Web Browser SSO (المعرَّف في الفقرة 1.4.11 من التوصية [ITU-T X.1141]).

ويوصِّف الإصدار OpenID [b-OpenID v.2] آلية اكتشاف تمكن أي طرف معول من تحديد موقع المورد IdSP لأي مستعمل استناداً إلى المعرف OpenID المورد للمستعمل.

8.6 التحكم في النفاذ إلى معلومات الهوية

تتطلب التوصية [ITU-T Y.2721] حصر النفاذ إلى معلومات الهوية بالجهات المخولة رهناً باللوائح والسياسات السارية. وتصف هذه الفقرة الآليات التي يمكن استخدامها للتحقق من امتيازات التخويل.

1.8.6 آلية قائمة على اللغة SAML لتبادل النعوت

يمكن استعمال عمليات التحقق SAML التي تتضمن بيانات النعوت كآلية لإدارة الامتيازات. ويمكن استعمال الآلية الموصوفة في الفقرة 1.2.6 لتوزيع إذنات SAML.

2.8.6 البنية التحتية لإدارة الامتيازات على أساس التوصية ITU-T X.509

يمكن استخدام إطار شهادة النعت المعرّف في التوصية [ITU-T X.509] كآلية في بنية تحتية لإدارة الامتيازات.

9.6 تسجيل الدخول لمرة واحدة

تسجيل الدخول لمرة واحدة (SSO) عبارة عن إمكانية شبكية تتيح للمستعمل التسجيل مرة واحدة والنفاذ إلى خدمات تطبيقات متعددة للشبكة دون الحاجة إلى تكرار طلب تقديمه إثباتات الاستيقان لكل خدمة تطبيق على حدة. وتحسِّن هذه الإمكانية، إلى حد كبير، من خبرة المستعمل بتمكينه من استقبال خدمات متنوعة دون الحاجة إلى الاحتفاظ بإثباتات متعددة للاستيقان (مثل أزواج اسم المستعمل/كلمة المرور). وحيث إن التسجيل SSO يتيح للمستعمل امتلاك مجموعة واحدة من إثباتات الاستيقان للنفاذ إلى خدمات تطبيقات متعددة، فإنه يسهل على موردي الخدمات إنفاذ قواعد أكثر صرامة في وضع الإثباتات. ومن شأن ذلك أن يساعد في تحسين أمن الشبكة.

ومن جهة أخرى، إذا طال إثباتات المستعملين الخلل، فإن الأثر على الشبكات القائمة على التسجيل SSO قد يكون أكبر من الأثر الواقع على الأنظمة التي لا تدعم التسجيل SSO. ولذلك، من الضروري للتسجيل SSO استخدام آليات آمنة. وتقدم هذه الفقرة استعراضاً شاملاً للعديد من الآليات التي يمكن استعمالها من أجل دعم التسجيل SSO.

1.9.6 آلية قائمة على المعمارية GBA

تشرح الفقرة 9.2.6 استعمال المعمارية للاستيقان عن مستعمل أي وظيفة NAF. ولذا، فإن المعمارية GBA توفر بفعالية آلية وحيدة لتسجيل مستعمل في جميع الوظائف NAF الممكنة بالمعمارية GBA على الشبكة. وفي الواقع، إذا قام مستعمل بالتسجيل للدخول إلى وظيفة NAF، فهذا يعني أن BSF وUE قد استيقن كل منهما من الآخر وأقاما مفتاحاً مشتركاً (Ks). وبالتالي، فإن عملية تسجيل دخول المستعمل للوظيفة NAF التالية تتألف من الخطوات 1 و3 و4 و5 و6 (سيتم تجاوز الخطوة 2) وهو ما يرد شرحه في الفقرة 9.2.6. وثانية، ينتج عن العملية مفتاح (Ks_NAF) سري يجري تقاسمه بين UE ووظيفة NAF جديدة. ويمكن استعمال هذا المفتاح السري في الاستيقان بين UE وNAF.

ويُوصى باستعمال التسجيل SSO القائم على المعمارية GBA في البيئات التي تُستخدم فيها المعمارية GBA.

2.9.6 آلية قائمة على اللغة SAML

يرد توصيف آليات التسجيل SSO القائمة على اللغة SAML في الفقرة 4.11، *المظاهر الجانبية للتسجيل SSO في SAML* بالتوصية [ITU-T X.1141]، التي تعرّف مجموعة من المظاهر الجانبية للغة SAML الداعمة للتسجيل SSO، تشمل أيضاً مظهراً جانبياً للتسجيل *خروج لمرة واحدة* (القسم 4.4.11). وموصف المظهر الجانبي عملية تتيح للمستعمل الخروج من كل التطبيقات التي قام بالتسجيل فيها باستعمال التسجيل SSO.

ويفترض الإصدار SAML v.2 علاقات الثقة بين المورد IdSP والأطراف المعولة (RPs) القائمة سلفاً. ويدعم هذا الإصدار كذلك معرفات الهوية المستعارة المتاحة بين موردين IdSP وRP. وهذا الإصدار يناسب التطبيقات، حيث توجد اتفاقات تعاقدية مثل اتفاقية مستوى الخدمة (SLA) أو معلومات ومعاملات عالية القيمة.

3.9.6 آلية قائمة على المعرف OpenID

يدعم الاستيقان OpenID Authentication 2.0 إمكانية التسجيل للدخول لمرة واحدة للسماح للمستعملين النهائيين بالنفاذ إلى أكثر من طرف معول واحد بمجرد استيقان المستعمل بنجاح. وهو لا يحتاج إلى علاقة ثقة بين المورد IdSP والأطراف المعولة (RPs). ونظراً لأنه لا يدعم إلا النسق القائم على URL/URI في تعريف المستعملين، فإن نظام أسماء الميادين (DNS) ضروري لاستعماله. ولذا، فهو يناسب تطبيقات خدمات الويب التي تتضمن معلومات ومعاملات أقل قيمة نسبياً.

10.6 تسجيل خروج لمرة واحدة

الفقرة 7.2.8 من *بروتوكول تسجيل الخروج لمرة واحدة SAML* [التوصية ITU-T X.1141] تمكن المستعمل النهائي من تسجيل الخروج من العديد من الدورات المشارك فيها في وقت واحد تقريباً. ودورات المشاركة هي تلك الدورات المقامة خلال مورد IdSP (بمعنى أن يكون المورد IdSP قد تحقق من هوية المستعمل بالنسبة للدورات المقامة بين المستعمل والتطبيقات). ويكون المورد IdSP على علم بكل الدورات المستيقن عنها مع الأطراف المعولة المختلفة التي يكون المستعمل قد أقامها من خلال المورد IdSP. ويشمل ذلك عدم سريان إثباتات الاستيقان (مثل ملفات cookies والتأكيدات) للدورات المنتهية. ويمكن استعمال البروتوكول في الحالات التالية:

1) عند تسجيل خروج المستعمل من واحدة من الدورات مع بيان أنه يرغب في الخروج من جميع الدورات المستهلة من خلال المورد IdSP.
2) عندما يبين المستعمل للمورد IdSP بصورة مباشرة أنه يرغب في الخروج من جميع الدورات.
3) عندما يقوم المورد IdSP بإخراج المستعمل بدون طلب منه (نتيجة لفترات الشغور مثلاً).

ويعرِّف البروتوكول الكيانات المشاركة وسلوكها وتدفق الرسائل ونسق الرسائل المتبادلة. وتشرح الفقرات الفرعية التالية استعمال البروتوكول في الحالات المدرجة أعلاه.

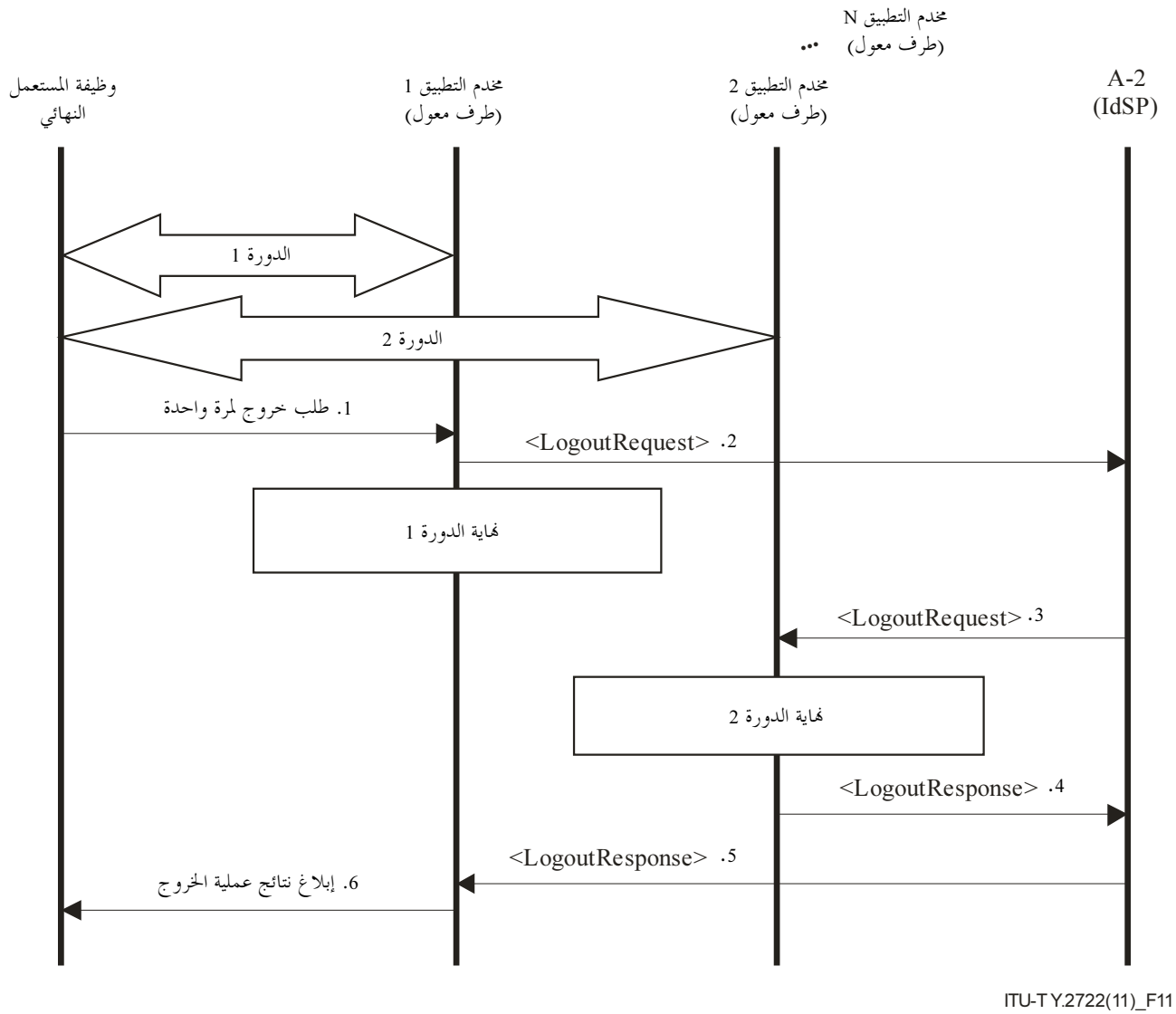
1.10.6 عمليات تسجيل خروج المستعملين من واحدة من الدورات مع بيان أنه يرغب في الخروج من جميع الدورات المستهلة من خلال المورد IdSP

يوضح الشكل 11 الخطوات الأساسية لتدفق الرسائل، والتي يرد شرحها أدناه.

1.1.10.6 الكيانات المشاركة في العملية وتدفق المعلومات

فيما يلي الكيانات المشاركة:

- وظيفة المستعمل النهائي.
- مخدم التطبيق 1 (AS1) – كيان يقدم خدمة. وهو يقوم بدور أحد الأطراف المعولة. وهو يعمل كطالب ومستجيب SAML على النحو المحدد في التوصية [ITU-T X.1141].
- مخدم التطبيق 2 (AS2) – كيان يقدم خدمة. وهو يقوم بدور أحد الأطراف المعولة. ويعمل كطالب ومستجيب SAML على النحو المحدد في التوصية [ITU-T X.1141].
- A-2: كيان وظيفي لبوابة التطبيق (APL-GW-FE)، يعمل كمورد IdSP وكطالب ومستجيب SAML على النحو المحدد في التوصية [ITU-T X.1141].



ITU-T Y.2722(11)_F11

الشكل 11 – تسجيل خروج لمرة واحدة قائم على اللغة SAML
طلبه مستعمل في دورة مشاركة

وفيما يلي الخطوات الأساسية لعملية تسجيل خروج لمرة واحدة (تُعرَّف كذلك بالخروج لمرة واحدة):

1) تقدم وظيفة المستعمل النهائي طلب تسجيل خروج عند مخدم التطبيق 1 (AS1) مع بيان أنه يرغب في الخروج من جميع الدورات المشارك فيها.

2) يطلب مخدم التطبيق 1 الخروج من جميع الدورات المشاركة بإرسال طلب <LogoutRequest> إلى الكيان A-2. ينبغي توقيع الطلب لأغراض الاستيقان وحماية السلامة على النحو المحدد في الفقرة 7.2.8 من التوصية [ITU-T X.1141].

يحاول مخدم التطبيق بعد هذه الخطوة إنهاء الدورة 1. ولهذا الغرض يحدد مخدم التطبيق (AS1) عدم سريان إثباتات استيقان الدورة (مثل التأكيدات والملفات cookies) وهو ما يُجبر وظيفة المستعمل النهائي على المضي في عملية الاستيقان إذا أصدر طلباً آخر للمخدم AS1.

3) يقوم الكيان A-2، بعد التحقق من صلاحية الطلب من المخدم AS1، بإرسال رسائل <LogoutRequest> إلى كل الأطراف المعولة (لا يبين الشكل 1 إلا المخدم AS2). وينبغي توقيع الطلبات على النحو المحدد في الفقرة 7.2.8 من التوصية [ITU-T X.1141].

وبعد التحقق من صلاحية طلب الخروج، يحاول المخدم AS2 إنهاء الدورة 2.

4) يقوم المخدم AS2 بإبلاغ مرسل طلب الخروج (الكيان A-2) بنتائج محاولة الخروج بإرسال رد <LogoutResponse>، وينبغي توقيع هذا الرد.

5) يقوم الكيان A-2 بإرسال رد <LogoutResponse> للمرسل الأول لطلب الخروج (المخدّم AS1) يبلّغه فيه بنتائج تسجيل الخروج لمرة واحدة (مثل النجاح الكامل أو الخروج الجزئي). وينبغي توقيع الرد.

وبعد هذه الخطوة، يحدِّث الكيان A-2 قائمته الخاصة بالدورات النشطة ويُبطل سريان إثباتات الاستيقان (مثل الملفات cookies والتأكيدات) للدورات التي يتعين إنهاؤها.

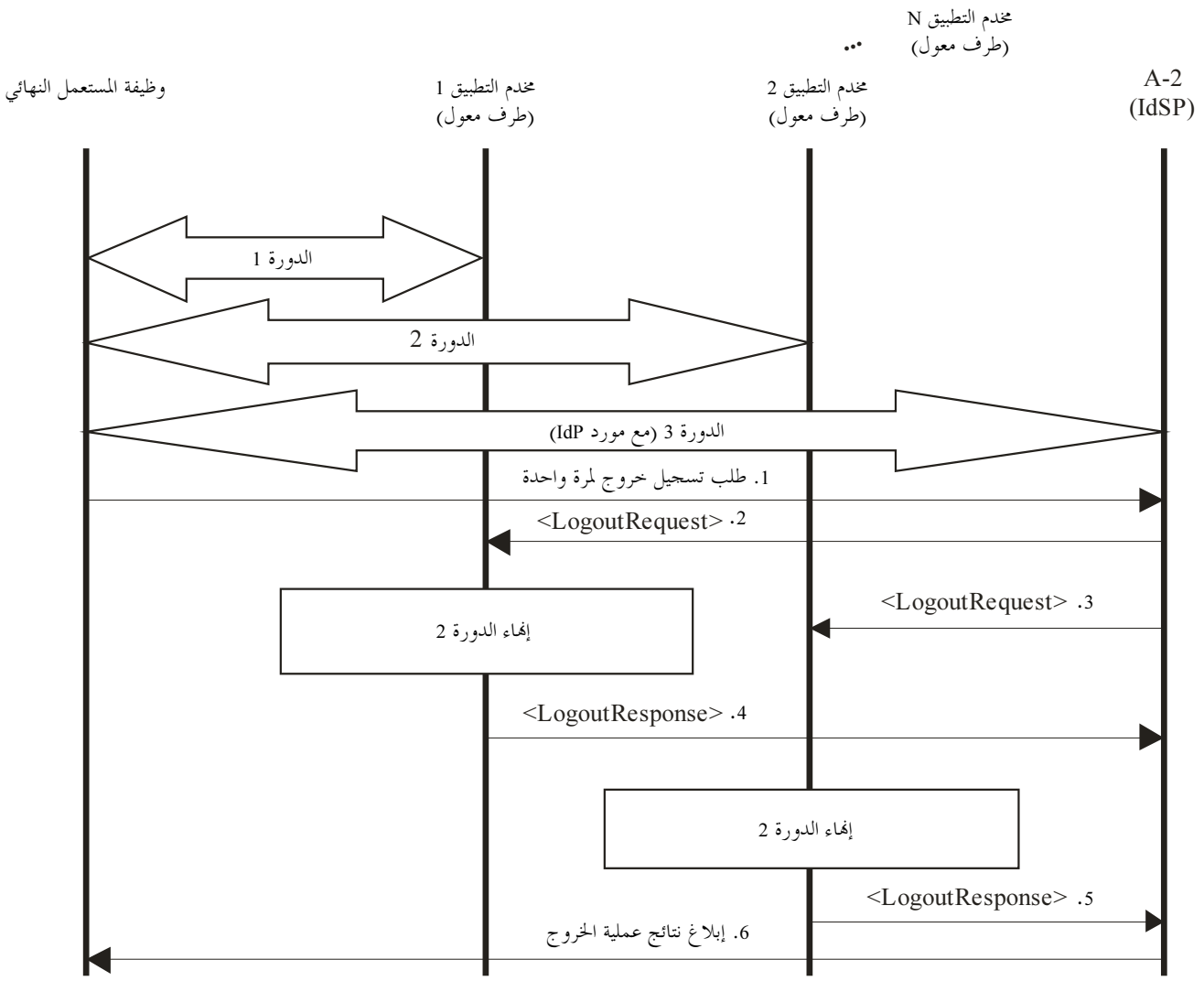
6) يردُّ المخدم AS1، بنتائج الخروج، على طلب وظيفة المستعمل النهائي المقدم في الخطوة 1.

2.10.6 يبين المستعمل بطريقة مباشرة للمورد IdSP رغبته في الخروج من جميع الدورات

يوضح الشكل 12 الخطوات الأساسية لتدفق الرسائل، والتي يرد شرحها أدناه.

1.2.10.6 الكيانات المشاركة في العملية وتدفق المعلومات

الكيانات المشاركة في عملية الخروج هي نفسها الموضحة في القسم 1.1.10.6. وفي حالة الاستعمال هذه، تكون لوظيفة المستعمل النهائي دورة مستقلة (الدورة 3) مع الكيان A-2 (المورد IdSP). وتستعمل هذه الوظيفة الدورة لإرسال طلب تسجيل خروج لمرة واحدة في الخطوة 1. والخطوات الأخرى للعملية تماثل الخطوات الموضحة في الفقرة 1.1.10.6.



ITU-T Y.2722(11)_F12

الشكل 12 – تسجيل خروج لمرة واحدة مطلوب من مستعمل عند مورد IdSP

فيما يلي الخطوات الأساسية لعملية تسجيل الخروج لمرة واحدة:

1) تطلب وظيفة المستعمل النهائي الخروج لمرة واحدة مباشرةً عند الكيان A-2.

2) يرسل الكيان A-2 الطلب <LogoutRequest> إلى المخدم AS1. ينبغي توقيع الطلب لأغراض الاستيقان وحماية السلامة على النحو المحدد في الفقرة 7.2.8 من التوصية [ITU-T X.1141].

وبعد التحقق من صلاحية الطلب، يقوم المخدم AS1 بمحاولة إنهاء الدورة 1. ولهذا الغرض يبطل المخدم AS1 سريان إثباتات استيقان الدورة (مثل التأكيدات والملفات cookies)، وهو ما يُجبر وظيفة المستعمل النهائي على المضي في عملية اسيتقان جديدة إذا ما أصدرت طلباً آخر للمخدم AS1.

3) يرسل الكيان A-2 الطلب <LogoutRequest> إلى المخدم AS2 (كما يرسل الطلب لجميع المخدمات الأخرى في الدورات المشاركة). وهذه الخطوة مماثلة للخطوة 2.

وبعد التحقق من صلاحية طلب الخروج، يحاول المخدم AS2 إنهاء الدورة 2.

4) يقوم المخدم AS1 بإبلاغ مرسل طلب الخروج (الكيان A-2) بنتائج محاولة الخروج بإرسال رد <LogoutResponse>، ينبغي توقيعه أيضاً.

5) وعلى نحو ما تم في الخطوة السابقة، يبلغ المخدم AS2 مرسل طلب الخروج (الكيان A-2) بنتائج محاولة الخروج بإرسال رد <LogoutResponse> موقّع.

ويقوم الكيان A-2 بعد هذه الخطوة بتحديث قائمته الخاصة بالدورات النشطة ويُبطل سريان إثباتات الاستيقان (مثل الملفات cookies والتأكيدات) للدورات المقرر إلغاؤها.

وبعد التحقق من صلاحية ردود الخروج جميعها، يبلغ الكيان A-2 وظيفة المستعمل النهائي بنتائج الخروج لمرة واحدة. ويُعَدُّ هذا رداً على طلب وظيفة المستعمل النهائي في الخطوة 1.

7 الأمن

تتناول الآليات الواردة في هذه التوصية، هي والآليات الموصفة في التوصية [ITU-T Y.2704]، متطلّبات أمن إدارة الهوية الخاصة بالتوصية [ITU-T Y.2721].

التذييـــل الأول

استيقان الرسائل WSS ITU-T X.509 v3

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يوضح المثال التالي طريقة لمعالجة الرسائل ذات الإذنات WSS X.509، كما هو وارد في الفقرة 2.1.5.6

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org /soap/envelope/"
      xmlns:sb="urn:liberty:sb:2006-08"
      xmlns:pp="urn:liberty:id-sis-pp:2003-08"
      xmlns:sec="urn:liberty:security:20 06-08"
      xmlns:wsse="http://docs.oasis-open.org/wss/2004 /01/oasis-200401-wss-wssecurity-
      secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
      utility-1.0.xsd"
      xmlns:wsa="http://www.w3.org/2005/08/addressing">

<s:Header>
<!-- see Liberty SOAP Binding Specification for which headers are required and optional -
->

<wsa:MessageID wsu:Id="mid">...</wsa:MessageID>

<wsa:To wsu:Id="to">...</wsa:To>

<wsa:Action wsu:Id="action">...</wsa:Action>

<wsse:Security mustUnderstand="1">

       <wsu:Timestamp wsu:Id="ts">
       <wsu:Created>2005-06-17T04:49:17Z</ wsu:Created >
       </wsu:Timestamp>

       <wsse:BinarySecurityToken
              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-
token-profile-1.0#X509v3 "
              wsu:Id="X509Token"
              EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binar y">
              MIIB9zCCAWSgAwIBAgIQ...
       </wsse:BinarySecurityToken>

       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>

                     <!-- in general include a ds:Reference for each wsa: header added
according to SOAP binding -->

                     <!-- include the MessageID in the signature -->
                     <ds:Reference URI="#mid">...</ds:Reference>

                     <!-- include the To in the signature -->
                     <ds:Reference URI="#to">...</ds:Reference>

                     <!-- include the Action in the signature -->
                     <ds:Reference URI="#action">...</ds:Reference>

                     <!-- include the Timestamp in the signature -->
                     <ds:Reference URI="#ts">...</ds:Reference>

                     <!-- bind the security token (thwart cert substitution attacks) -->
                     <ds:Reference URI="#X509Token">
```

```
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/x
mldsig#sha1"/>
                        <ds:DigestValue>Ru4cAfeBABE...</ ds:DigestValue>
                    </ds:Reference>

                    <!-- bind the body of the message -->
                    <ds:Reference URI="#MsgBody">
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
                        xmldsig# sha1"/>
                        <ds:DigestValue>YgGfS0pi56pu...</ds:DigestValue>
                    </ds:Reference>
            </ds:SignedInfo>
            <ds:KeyInfo>
                    <wsse:SecurityTokenReference>
                        <wsse:Reference URI="#X509Token" />
                    </wsse:SecurityTokenReference>
            </ds:KeyInfo>
            <ds:SignatureValue>
                    HJJWbvqW9E84vJVQkjjLLA6nNvBX7mY00TZhwBdFNDElgscS XZ5Ekw==
            </ds:SignatureValue>
        </ds:Signature>
</wsse:Security>
</s:Header>

<s:Body wsu:Id="MsgBody">
        <pp:Modify>
            <!-- this is an ID-SIS-PP Modify message -->
        </pp:Modify>
</s:Body>


</s:Envelope>
```

التذييـــل الثاني

آلية قائمة على التخويل المفتوح والمعيار OpenID "OpenID+OAuth" للتحكّم في النفاذ

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

تشرح الفقرة 8.2.6 استعمال المعيار OpenID لاستيقان مستعمل لأي وظيفة NAF. وبالتالي، تعرض طرح تخويل مفتوح (OAuth) قائم على المعيار OpenID لحماية المعلومات PII والتحكم في النفاذ.

1.II التخويل المفتوح (RFC 5849)

التخويل المفتوح (OAuth) عبارة عن بروتوكول مفتوح لتمكين التطبيق من النفاذ إلى معلومات المستعمل النهائي من خدمة الويب في حال حصول التطبيق على تخويل من المستعمل النهائي. وتُنقل معلومات المستعمل النهائي بصورة آمنة دون الكشف عن هوية المستعمل.

والهدف من البروتوكول OAuth هو الحصول على إذنة نفاذ من مخدم الويب يمكن استعمالها فيما بعد لتبادل البيانات الخاصة بالمستعمل مع خدمة الويب (مثل معلومات التقويم أو دليل العناوين). وتتألف العملية الاعتيادية للتخويل المفتوح (OAuth) من أربع خطوات متتالية:

1) التماس إذنة "طلب".

2) التماس تخويل الإذنة وهو ما يعني موافقة المستعمل.

3) تبادل إذنة الطلب المخولة من أجل إذنة "نفاذ".

4) استعمال إذنة النفاذ للتعامل مع بيانات خدمة الويب للمستعمل.

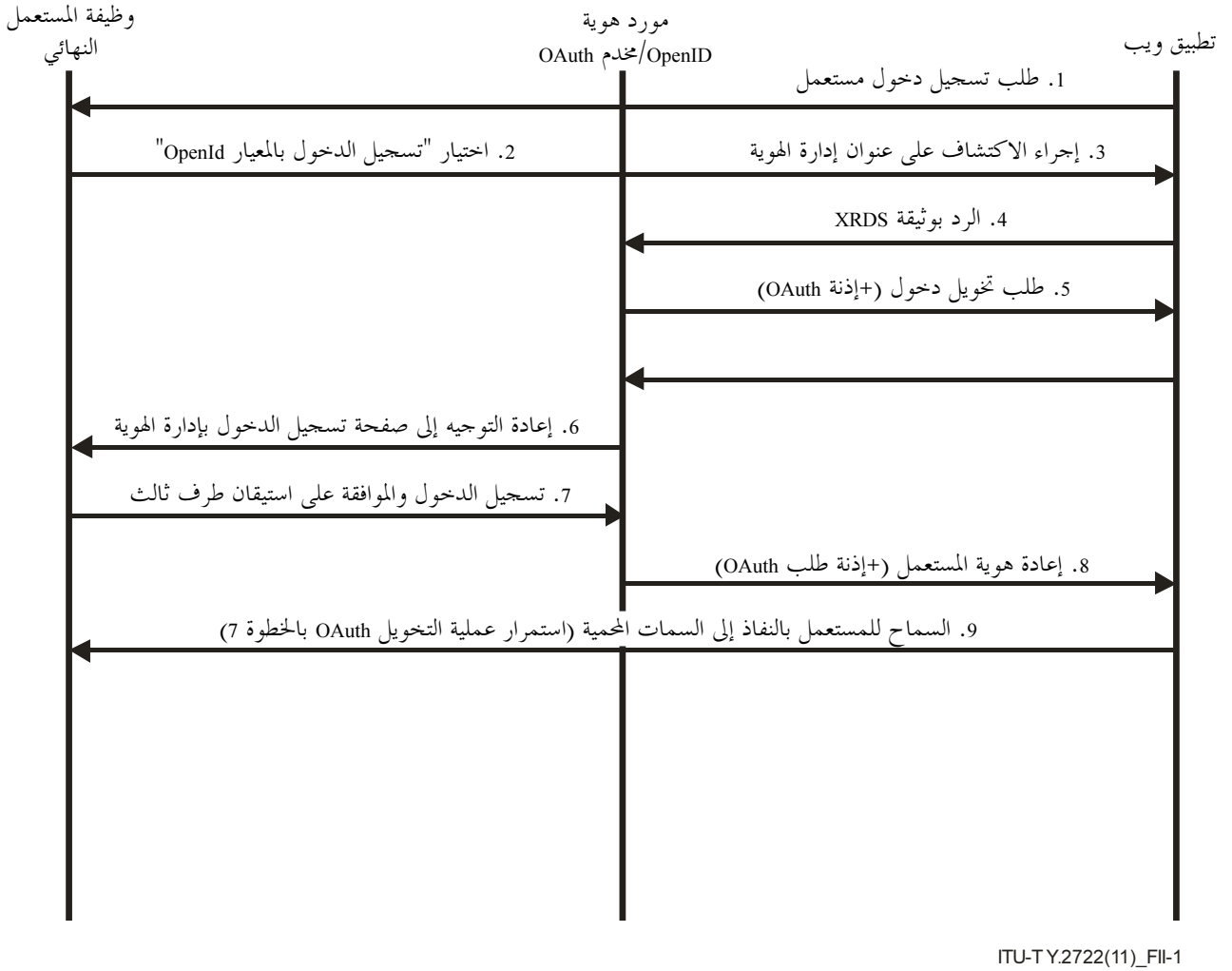
ولمزيد من المعلومات عن البروتوكول OAuth، راجع المعيار [b-IETF RFC 5849].

2.II استعمال المعيار OpenID بالاقتران مع البروتوكول OAuth

على الرغم من إمكانية استخدام المعيار OpenID كآلية إدارة هوية للاستيقان من المستعملين، يمكن أيضاً استخدام البروتوكول OAuth في منح التخويل لبيانات المستعملين الحساسة. وفي مثل هذا السيناريو، يوفر مورّد خدمة الهوية وظائف مدمجة فيعمل كمورد هوية OpenID (OP) ومورد خدمة تخويل مفتوح على السواء.

3.II تدفق التخويل OpenID + OAuth

مع التخويل المشترك OpenID+OAuth تظل سلسلة الخطوات كما هي على نحو كبير. ويتمثل الاختلاف في أن الحصول على إذنة طلب OAuth مخولة (الخطوتان 1 و2) ينتهي بطلب الاستيقان OpenID. وبهذه الطريقة، يمكن للمستعمل الموافقة على تسجيل الدخول والنفاذ إلى الخدمة في وقت واحد.



الشكل II.1– استيقان قائم على OpenID+OAuth

فيما يلي الخطوات الأساسية:

1) يطلب تطبيق الويب من المستعمل النهائي الدخول بتقديم مجموعة من خيارات الدخول بما فيها استعمال حساب المعيار OpenID.

2) يختار المستعمل "تسجيل الدخول بالمعيار OpenID".

3) يرسل تطبيق الويب طلب "اكتشاف" للمورد IdSP للحصول على معلومات عن النقطة الطرفية لاستيقان الدخول للمورد IdSP.

4) يعيد المورد IdSP وثيقة XRDS تتضمن عنوان النقطة الطرفية.

5) يرسل تطبيق الويب طلب استيقان دخول إلى عنوان النقطة الطرفية للمورد IdSP.

6) يعيد هذا الإجراء المستعمل إلى صفحة دخول اتحادية للمورد IdSP إما في نفس نافذة المتصفح أو في نافذة لحظية، ويُطلب من المستعمِل تسجيل الدخول.

7) وبمجرد أن يسجل المستعمل دخوله، يعرض المورد IdSP صفحة تأكيد ويُخطر المستعمل بأن هناك تطبيقاً لطرف ثالث يطلب الاستيقان. وتطلب الصفحة من المستعمل التأكيد، أو رفض، ربط حساب دخوله لدى المورد IdSP بدخول تطبيق الويب، ويُطلب من المستعمل بعد ذلك الموافقة على النفاذ إلى مجموعة محددة من خدمات المورد IdSP. ويجب أن يوافق المستعمل على تبادل معلومات الدخول ومعلوماته لمواصلة الاستيقان.

8) إذا وافق المستعمل على الاستيقان، يعيد المورد IdSP المستعمل إلى الموقع URL المحدد في المعلمة *openid.return_to* للطلب الأصلي. ويُلحق معرف هوية مقدم من المورد IdSP ليس له علاقة بالحساب الفعلي للمستعمل في إدارة الهوية سواء اسم المستعمل أو كلمة المرور باعتباره معلمة السؤال *openid.claimed_id*. وإذا ما تضمن الطلب أيضاً تبادل نعوت، يمكن إلحاق المزيد من معلومات المستعمل. وبالنسبة للتخويل OpenID+OAuth، تُعاد كذلك إذنة طلب OAuth مخولة.

9) يستعمل تطبيق الويب معرِّف الهوية المقدم من المورد IdSP للتعرّف على المستعمل وإتاحة النفاذ إلى سمات التطبيق وبياناته. وبالنسبة للتخويل OpenID+OAuth، يستعمل تطبيق الويب إذنة الطلب لمواصلة تتابع التخويل OAuth والحصول على نفاذ إلى خدمات المورد IdSP للمستعمل.

ثبت المراجع

[b-ETSI TS 133 220] ETSI TS 133 220 V6.3.0 (2004), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*.
<http://datatracker.ietf.org/doc/rfc2616/>

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.
<http://datatracker.ietf.org/doc/rfc2617/>

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*. <http://www.rfc-editor.org/rfc/rfc3310.txt>

[b-IETF RFC 4169] IETF RFC 4169 (2005), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2*.
<http://www.ietf.org/rfc/rfc4169.txt?number=4169>

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.
<http://datatracker.ietf.org/doc/rfc4279/>

[b-IETF RFC 5849] IETF RFC 5849 (2010), *The OAuth 1.0 Protocol*.
<http://tools.ietf.org/html/rfc5849>

[b-LA WSF] Liberty Alliance (2008), *Web Services Framework: A Technical Overview*.
<http://www.projectliberty.org/liberty/content/download/4120/27687/file/idwsf-intro-v1.0.pdf>

[b-LA ID-WSF security] Liberty Alliance Project (2007), *Liberty ID-WSF Security Mechanisms Core version 2.0-errata version 1.0*.

[b-LA SOAP binding] Liberty Alliance Project Web Services Security (WSS) (2006), *Liberty SOAP Binding Version 2.0*.

[b-NIST-SP 800-122] NIST Special Publication SP 800-122 (2010), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.
<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

[b-OASIS SAML token] OASIS (2006), *Web Services security: SAML Token Profile 1.1, and its Approved Errata 1*.

[b-OASIS WSS SOAP] OASIS (2004), *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*.

[b-OASIS WSS X.509 profile] OASIS (2006), *Web Services Security X.509 Certificate Token Profile 1.1*.

[b-OpenID v.2] *OpenID Authentication 2.0*.
<http://openid.net/specs/openid-authentication-2_0.html>

[b-W3C XML signature] World Wide Web Consortium (W3C) (2008), *XML Signature Syntax and Processing (second edition)*.

[b-3GPP TR 33.924] 3GPP TR 33.924 Release 9 (2009), 3rd Generation Partnership Project, *Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking (Release 9)*.

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 تلفزيونية وبرامج صوتية 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 البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	**البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2012