الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1255
(2013/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

إطار لاكتشاف معلومات إدارة الهوية

التوصيـــة ITU-T X.1255

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	**X.1279–X.1250**
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

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

التوصيـــة ITU-T X.1255

إطار لاكتشاف معلومات إدارة الهوية

ملخص

الغرض من التوصية ITU-T X.1255 هو توفير إطار معمارية مفتوحة يمكن من خلاله اكتشاف معلومات إدارة الهوية. ولا بد أن تُمثَّل معلومات إدارة الهوية هذه بسبل مختلفة وبدعم من أطر ثقة مختلفة أو من أنظمة أخرى لإدارة الهوية باستخدام مخططات بيانات شرحية مختلفة. وسيمكّن هذا الإطار، على سبيل المثال، الكيانات العاملة في سياق أحد أنظمة إدارة الهوية من استخراج معرفات هوية من أنظمة أخرى لإدارة الهوية على الوجه الصحيح. ودون القدرة على اكتشاف مثل هذه المعلومات، يُترك المستخدمون والمنظمات (أو البرامج التي تعمل نيابة عنهم) لتحديد أفضل السبل لإثبات مصداقية وأصالة هوية مناسبة، سواء لمستخدم أو لمورد في نظام أو لمعلومات أو لغير ذلك من كيانات. واستناداً إلى هذه المعلومات، يعود للمستخدم أو للمنظمة قرار التعويل من عدمه على إطار ثقة معين أو نظام آخر لإدارة الهوية لمثل هذه الأغراض. وتشمل المكونات الأساسية للإطار المطروح في هذه التوصية ما يلي: 1) نموذج بيانات كيان رقمي، 2) بروتوكول السطح البيني لكيان رقمي، 3) واحداً أو أكثر من أنظمة معرفات الهوية/أنظمة الاستخراج، 4) واحداً أو أكثر من سجلات البيانات الشرحية. وتشكل هذه المكونات أساس إطار المعمارية المفتوحة.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1255	2013/09/04	17

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، 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

التوصيـــة ITU-T X.1255

إطار لاكتشاف معلومات إدارة الهوية

1 مجال التطبيق

تتناول عملية اكتشاف معلومات إدارة الهوية حقيقة ضرورية أن يكون بمقدور المرء الحصول على المعلومات ذات الصلة بمعرَّفات الهوية، بما في ذلك تلك التي تستخدم قواعد تركيب عناوين البريد الإلكتروني وتلك التي تمثل مواقع الموارد الموحدة إلى جانب معرَّفات الهوية الثابتة. وعملية الاكتشاف هذه عنصر أساسي لتمكين قابلية التشغيل البيني عبر أنظمة معلومات غير متجانسة.

يتمثل مجال تطبيق هذه التوصية في إطار يقوم بما يلي:

- يمكِّن من اكتشاف معلومات ذات صلة بالهوية ومَنشأها، بما في ذلك المعلومات الجاري تحديدها مثل الخدمات والعمليات والكيانات؛
- يمكِّن من اكتشاف نعوت المعلومات ذات الصلة بالهوية بما في ذلك، على سبيل المثال لا الحصر، الشعارات البصرية وأسماء المواقع التي يمكن أن يقرأها الإنسان؛
- يمكِّن من اكتشاف نعوت التطبيقات وخواصها الوظيفية؛
- يصف نموذج بيانات وبروتوكولاً لتمكين قابلية التشغيل البيني على المستوى الشرحي لتمثيل المعلومات المشار إليها أعلاه في البيئات غير المتجانسة لإدارة الهوية والنفاذ إليها واكتشافها.

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.

[ISO 8601] ISO 8601 (2004), *Data elements and interchange formats - Information interchange - Representation of dates and times*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في توصية أخرى:

1.1.3 الكيان [b-ITU-T Y.2720]: أي شيء يكون له وجود قائم بذاته ومميز يمكن تعريفه بصورة متفردة. ومن أمثلة الكيان، في سياق إدارة الهوية، المشتركون والمستعملون وعناصر الشبكة والشبكات وتطبيقات البرمجيات والخدمات والأجهزة. ويجوز أن يكون للكيان الواحد عدة معرفات هوية.

2.1.3 مقدم الهوية [b-ITU-T Y.2720]: كيان يقوم باستحداث معلومات هوية موثوقة للكيانات الأخرى مع الحفاظ عليها وإدارتها (وتضم هذه الكيانات الأخرى المستعملين/المشتركين والمنظمات والأجهزة) ويقدم خدمات خاصة بالهوية تقوم على الثقة والأعمال التجارية والأشكال الأخرى من العلاقات.

3.1.3 الطرف المعوِّل [b-ITU-T Y.2720]: كيان يعوّل على تمثيل أو ادعاء هوية من جانب كيان طالب/مؤكِّد.

4.1.3 الثقة [b-ITU-T Y.2720]: مقياس الاعتماد على سمة أو قدرة أو قوة أو الوثوق بشخص أو شيء ما.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 ارتباط: علاقة، إن وجدت، بين كيانين عُرفت هويتيهما.

2.2.3 الكيان الرقمي: هيكل بيانات مستقل عن الآلة يتكون من واحد أو أكثر من العناصر التي يمكن لأنظمة المعلومات المختلفة أن تحللها لغوياً؛ ويساعد هذا الهيكل على تمكين قابلية التشغيل البيني بين أنظمة المعلومات المتنوعة في شبكة الإنترنت.

3.2.3 اكتشاف: فعل أو عملية البحث عن المعلومات المستهدَفة أو تحديد موقعها، أي اكتساب المعرفة المتعلقة بالهدف.

4.2.3 العنصر: جزء من كيان رقمي يتكون من زوج النمط–القيمة، حيث يمثِّل النمط بمعرّف هوية ثابت قابل للاستخراج، وتمثل القيمة المعلومات الرقمية ذات الصلة بذلك النمط.

5.2.3 السجلات المتحدة: مجموعة من السجلات القابلة للتشغيل البيني تسجل البيانات الشرحية وتشارك في مجموعة مشتركة من أساليب تبادل المعلومات بشكل موثوق وفي نسق مفهوم عموماً.

6.2.3 معرِّف الهوية: تسلسل من البتات المستخدمة للحصول على معلومات عن حالة الكيان الجاري التعرف على هويته، ويتم ذلك عن طريق نظام استخراج مناسب.

7.2.3 إدارة الهوية: الوسائل التي يمكن بها التحقق من صحة معلومات إدارة الهوية، سواء لمستخدم أو لمورد في نظام أو لمعلومات أو لغير ذلك من كيانات.

8.2.3 معلومات إدارة الهوية: المعلومات ذات الصلة بالهوية بما فيها جميع أنماط البيانات الشرحية المرتبطة بالهوية والمنشأ والارتباط والثقة.

9.2.3 البيانات الشرحية: المعلومات المهيكلة التي تتعلق بهوية مستخدمين أو أنظمة أو خدمات أو عمليات أو موارد أو معلومات أو غير ذلك من كيانات.

10.2.3 معرف الهوية الثابت: معرف هوية فريد يستخرج معلومات عن حالة كيان رقمي، وهي معلومات قابلة للاستخراج طيلة وجود الكيان الرقمي على الأقل.

11.2.3 المنشأ: المعلومات المتعلقة بأي مصدر للمعلومات بما في ذلك الطرف أو الأطراف المشاركة في توليدها و/أو عرضها و/أو الشهادة بصحتها.

12.2.3 السجل: آلية لتسجيل البيانات الشرحية بشأن الكيانات الرقمية ومخططات حفظ البيانات الشرحية، وهي توفر القدرة على البحث في السجل عن معرفات الهوية الثابتة على أساس استخدام مخططات البيانات الشرحية.

13.2.3 المستودع: سطح بيني يتيح إيداع الكيانات الرقمية كودائع، ويمكِّن الاحتفاظ بها، ويوفر نفاذاً آمناً إلى الكيانات الرقمية عبر معرفات هوياتها.

14.2.3 نظام الاستخراج: نظام يقبل معرفات الهوية المعروفة للنظام كمدخلات ويوفر معلومات ذات صلة بحالة الكيان الذي يجري التعرف على هويته.

15.2.3 نقطة التماس: سجل ضمن نظام السجلات المتحدة يُختار ليُربط بينياً مع سجل معين في اتحاد آخر وعادةً ما يكون ذلك لأغراض التبادل بين النظراء.

16.2.3 إطار الثقة: نظام إدارة هوية يُلتزم فيه بمجموعة من الالتزامات التي يمكن لكل من الأطراف المختلفة إثباتها لنظرائه من الأطراف الأخرى. وتشمل هذه الالتزامات بالضرورة: أ) ضوابط للمساعدة في ضمان الوفاء بالالتزامات، وب) تعويضات عن عدم الوفاء بهذه الالتزامات.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

API سطح بيني لبرمجة التطبيقات *(Application Program Interface)*

Bits أرقام اثنينية *(Binary Digits)*

BNF شكل باكوس – ناور *(Backus Normal Form)*

DE كيان رقمي *(Digital Entity)*

DEIP بروتوكول السطح البيني للكيان الرقمي *(Digital Entity Interface Protocol)*

DNA الحمض النووي الصبغي *(Deoxyribonucleic acid)*

HTTP بروتوكول نقل النصوص المترابطة *(Hypertext Transfer Protocol)*

ID معرف الهوية *(Identifier)*

IdM إدارة الهوية *(Identity Management)*

IdP مقدم الهوية *(Identity Provider)*

MAC التحكم في النفاذ إلى الوسائط *(Media Access Control)*

P2P التبادل بين النظراء *(Peer-to-Peer)*

PKI بنية تحتية للمفاتيح العمومية *(Public Key Infrastructure)*

RP الطرف المعوِّل *(Relying Party)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

TF إطار الثقة *(Trust Framework)*

URL المحدد الموحد لموقع المورد *(Uniform Resource Locator)*

XML لغة تشفير قابلة للتوسيع *(Extensible Markup Language)*

5 الاصطلاحات

لا توجد.

6 التوصية

تعنى هذه التوصية بإطار معمارية مفتوحة لدعم اكتشاف معلومات إدارة الهوية. وهي تتناول المواضيع التالية:

أ) مفهوم الثقة، وهو جانب هام من جوانب إدارة الهوية؛

ب) معلومات الثقة، التي يمكن استخدامها لتحديد المقدار الذي يمكن فيه التعويل على أي معلومة من معلومات إدارة الهوية؛

ج) السجلات المتحدة للاكتشاف؛

د) معمارية قابلية التشغيل البيني للاتحاد؛

هـ) مناقشة الاتحادات ذات التراتبية وبين النظراء على حد سواء.

يستند اكتشاف معلومات إدارة الهوية إلى استخدام البيانات الشرحية التي تم الحصول عليها من سجل أو نظام سجلات متحدة. ويتضمن الإطار وجود وسيلة لاستخراج معرفات ثابتة للهوية. وبصفة عامة، ستتعدد الأطراف التي تشغِّل السجلات المتحدة التي يتعين عليها أن تدعم نموذج بيانات الكيان الرقمي لتمثيل قيود البيانات الشرحية وبروتوكول السطح البيني للكيان الرقمي لتحقيق قابلية التشغيل البيني لهذه السجلات. ويفترض استخدام مخططات متعددة، ويتعين على كل سجل أن يوفر

تفاصيلَ عن مخططاته للبيانات الشرحية التي تدعمها معرفات الهوية الثابتة لكل سجل علناً أو بشكل مكتوم. ويمكن الإفصاح علناً عن مخططات تدعمها معرفات الهوية الثابتة دعماً مكتوماً، في حال الرغبة بذلك، أو يمكن إبقاؤها طي الكتمان مع ما يرتبط بها من مخططات بيانات شرحية للاستخدام المحدود ضمن مجتمعات مقيدة.

ويقدم التذييلان I وII على التوالي لمحة عامة عن سيناريوهات الاستخدام ومثالاً عن وصف BNF لقيد نمط (BNF هو ترميز مقيّس لتمثيل قواعد النحو الخالية من السياق).

1.6 مفاهيم الثقة

كلمة "الثقة" هي مصطلح فني وتحمل عدداً من الدلالات. فالثقة في شخص أو عملية تعني عموماً الشعور بمستوى معين من الاطمئنان بشأن تمخض الأحداث عن نتيجة معينة، حتى لو لم تحدَد تلك الأحداث على وجه الدقة. بيد أن بناء أنظمة اكتشاف سيتطلب توصيفاً إضافياً. فمجرد القول أن زيداً يمكن أن يثق بعمر لا يعني أنه يمكن أن يثق بعمر في جميع مآلات الحدث الممكنة. فالثقة بأن عَمراً سيقدم خدمة مقابل دفعة مالية ليس كالثقة في إبقائه لتلك الدفعة سراً أو عدم إفشائه أسماء كل من سدد مثل هذه المدفوعات.

وأهم قضية في أطر الثقة هي إدارة الهوية، أي أن الأطراف في أي تعامل معين هم حقاً من يدّعون. ولكن الثقة في نتائج تعامل معين مع طرف معين لا تتوقف على هوية ذلك الطرف فحسب وإنما أيضاً على نعوت أخرى للادعاءات والتأكيدات التي أدلى بها ذلك الطرف. ويتطلب تقييم تلك النعوت بطريقة متسقة مفردات أو مجموعة من المقاييس التي يمكن تطبيقها على تلك النعوت. ويمكن لأطراف ثالثة تقوم بدور وكالات تصنيف إطار الثقة أن تطبق هذه القياسات والأوصاف أو يمكن حساب القيمة المتوسطة عبر مجموعات التصنيفات من المستخدمين، كما هو الحال في أنظمة التوصية وغيرها من تطبيقات التماس المساهمات من مجموعة كبيرة من المصادر. ويرد أدناه وصف الفئات الموصى بها لتلك القياسات والأوصاف.

القوة: مستوى الجدارة بالثقة. ما مدى احتمال أن يُقرن هذا الطرف قوله بالفعل؟ وما مدى احتمال صحة تأكيد الهوية (على سبيل المثال، أنا مالك هذه البرمجيات ويعود ريعها لي)؟ ويرجح أن يعبَّر عن ذلك بعلامة رقمية أو حرفية.

التصنيف: ما هو نمط الجدارة بالثقة الجاري تأكيدها؟ هل يمكن إنشاء فئات للمعيار؟ فالهوية هي فئة في حد ذاتها. وتشمل الفئات الأخرى الجدارة بالثقة المالية (على سبيل المثال، مدى احتمال أن يبرّ طرف معين بوعده في المعاملات المالية)، والخصوصية (مدى احتمال أن يكتم طرف معين معلومات يدعي أنه لن ينشرها)، والموثوقية (على سبيل المثال، مدى احتمال صحة المعلومات الواردة من طرف معين). وهناك أصناف أخرى ممكنة رفيعة المستوى ومستويات أدق في تفاصيلها ممكنة لكل صنف.

طول سلسلة الثقة: تعتمد بعض معاملات الثقة على سلسلة من الثقة، وكثيراً ما تُرى هذه السلسلة في ضوء التسلسل التراتبي للشهادة أو طبقات البرمجيات الموقَّعة رقمياً. ويسري هذا المفهوم بصورة عامة على جميع مجالات الثقة: وكلما طالت سلسلة التأكيدات الموثوق بها وصولاً إلى مرتكز ثقة ما، ضعف المستوى النهائي للثقة. ومن شأن قياس طول هذه السلسلة أن يكون القياس الرئيسي للجدارة بالثقة بأي هوية أو تأكيد آخر.

ومن شأن كل هذه النعوت (وغيرها كثير) أن تكون مرشحة للإدراج في سجلات البيانات الشرحية التي تصف مقدمي الهوية، والأطراف المعولة، وأي مكونات أخرى تشارك في معاملات موثوق بها.

2.6 معلومات الثقة

تناقَش أدناه ثلاثة جوانب متميزة من معلومات الثقة فيما يتعلق بالوظائف والإجراءات التي ينطوي عليها الاكتشاف المتحد وتلك الخاصة بالكيانات المكونة المشاركة.

1.2.6 معلومات الثقة في رد اكتشاف

إن تمكين اكتشاف معلومات إدارة الهوية هو الهدف الرئيسي للمعمارية المفتوحة المطروحة في هذه التوصية، ولكن يعود قرار الثقة للمستخدم. ويمكن دعم خواص وظيفية أو خدمات إضافية ضمن المعمارية في شكل مكونات/وحدات اختيارية (برمجيات و/أو عتاد). وبهذا المعنى، يمكن أن تشمل المعمارية إطار ثقة وقدرة اختيارية، فضلاً عن تعزيزها/إغنائها لرد الاكتشاف بمعلومات الثقة أو حتى دعمها في قرار الثقة. وتتمكن الكيانات الخارجية من تحديد ما إذا كانت ترغب في الحصول على معلومات الثقة هذه مباشرة. فيمكنها أن تختار إبطال هذه الميزة وتسعى إلى جمع معلومات الثقة بمفردها أو حتى من مصادرها الخاصة لاتخاذ قرار الثقة.

2.2.6 الثقة في نظام الاكتشاف

يجب الوثوق في نظام الاكتشاف، بحيث تشعر الأطراف الخارجية بالثقة في استخدام قدراته لتسجيل معلومات إدارة الهوية أو النفاذ إليها. ويمكن تحقيق هذا النمط من الثقة بواسطة وسائل مختلفة، بما في ذلك إنشاء أساليب محددة إلى جانب السياسات والإجراءات المرتبطة بها لأغراض الموثوقية. وهي قد تشمل تقييم المكونات المنفَّذة كجزء من الإطار، والإجراءات (التدابير) المتخذة بشأن المكونات أو الأطراف الخارجية سيئة السلوك، والتكيف مع الأطر الأمنية القوية وأطر الخصوصية. غير أن تحديد منهجية دقيقة لتحقيق هذا النوع من الثقة يقع خارج نطاق هذه الوثيقة.

3.2.6 الثقة في الأطراف الخارجية

يجب أن تدعم المعمارية السياسات والإجراءات التي تشجع الأطراف الخارجية الموثوقة على استخدام المعمارية لغرض تسجيل المعلومات. ولأسباب أمنية، يجب أن تتمكن كيانات المكون التي تشارك مباشرة في تسجيل معلومات إدارة الهوية من التحكم في البيانات المدرجة في النظام وكشف و/أو تجنب الحالات التي تحاول فيها أطراف خبيثة تسجيل معلومات كاذبة.

وينبغي دعم الطلبات مجهولة المصدر، ولكن الكثير منها قد لا يؤدي إلى ردود مفيدة إلا إذا كانت هوية فرادى الطالبين معروفة مسبقاً بوسيلة ما أخرى. وفي مثل هذه الحالات، ينبغي لقدرة إدارة الهوية، السارية على المكونات كافة بما فيها المستخدمون/الطالبون، أن توفر القدرة على التحقق من صحة الهوية. وضمن هذا الإطار، يعيّن مقدم هوية مخوَّل ومعترف به لكل مكون معرفَ هوية ثابت وفريد يمكن أن تُستخرج بواسطته المعلومات ذات الصلة بالمكون. وكما سبق الذكر، لا يُفترض أي افتراض بشأن كيف يمكن لأي مكون من مكونات حالة محددة أن يتخذ قرار الثقة بهذه المعلومات.

ويجب، بالنسبة للعديد من طلبات الهوية، التحقق من صحة هوية السائل (طرف خارجي أصدر طلب اكتشاف) قبل إصدار رد. وفي الحالة العامة، يقيَّم جميع السائلين قبل اتخاذ أي إجراء آخر. ولا تتخذ المعمارية أي قدرة لصنع القرار ضمنها، ولكن قبل صياغة الرد النهائي على طلب اكتشاف، يمكن الاستعانة بآلية خارجية لدعم القرار للحصول على إذن مسبقاً من منتجي الهوية.

3.6 السجلات المتحدة للاكتشاف

يرد وصف نظام السجلات المتحدة للاكتشاف في هذه التوصية بهدف تمكين العثور على البيانات الشرحية وغيرها من المعلومات بشأن معرفات الهوية، فضلاً عن أطر الثقة وأنظمة إدارة الهوية الأخرى، وتقييمها. ويمكن للسجلات المتحدة أن تعمل معاً لتبادل كيانات البيانات الشرحية الخاصة بها رهناً بأي مقيدات مرعية. ويمكن حفظ المعلومات الفعلية المقابلة لهذه البيانات الشرحية في السجلات الخاصة بكل منها (إذا ما سُمح بمثل هذا الحفظ) في واحد أو أكثر المستودعات الموزعة؛ وفي بعض الحالات قد يتعذر تماماً النفاذ إلى المعلومات المقابلة لهذه البيانات الشرحية في شبكة الإنترنت. وفي الحالة الأخيرة، يُحدد عادة هذا القيد باستخراج المعرف من المعلومات ذات الصلة بحالة الكيان، سوى أن السجل يمكن أن يختار تقديم تلك المعلومات أيضاً.

وضمن نظام السجلات المتحدة، يمكن أن يقدم سجل معين قيد بيانات شرحية لكيان معين إلى سجل ثان إما كنسخة كاملة من القيد الأصلي للبيانات الشرحية أو كملخص لذلك القيد الأصلي. ومن شأن هذه التقدمة أن تضم القيد الأصلي أو بديلاً عنه وتوصَف على نحو يحدد مصدره ونمط المجتمع أو الميدان الممثَّل في ذلك السجل. وبالتالي يمكن للسجل الأولي نفسه

أن يكون بمثابة نقطة تجميع عبر الميادين للعديد من السجلات الأخرى، وأن يوفر خدمة بحث يمكن أن تحيل الباحثين إلى سجلات أخرى لجمع معلومات إضافية. ويشار إلى نقاط التجميع هذه في بعض الأحيان كنقاط تماس.

وقد صُمم مكون السجل في المعمارية حول عدة مفاهيم أساسية. وبالإضافة إلى تطلُّب تعيين معرف هوية لكل كيان مسجَّل، فإن قيود البيانات الشرحية في السجل هي نفسها مهيكلة ككيانات رقمية، ولكل منها معرف هوية مرتبط بها؛ ويسمح ذلك بالإشارة إلى قيود البيانات الشرحية بشكل منفصل، وستستخرج معرفاتها معلومات الحالة الراهنة لكيانات البيانات الشرحية حتى لو انتقلت القيود من سجل إلى آخر أو توفرت من سجلات متعددة.

ولا شيء في المعمارية يحد من عدد كيانات البيانات الشرحية التي يمكن تسجيلها لكيان رقمي واحد. وقد يُرغب بتوليد كيانات متعددة للبيانات الشرحية لنفس المعلومات عندما ينظر إليها من وجهات نظر مختلفة، ولفئات مختلفة من الجمهور، وهلم جرا. وتتبسط إلى حد كبير إدارة كيانات البيانات الشرحية هذه عن طريق استخدام معرفات الهوية الفريدة والثابتة: على سبيل المثال، يسهل تحديد ما إذا كانت مدونتان من البيانات الشرحية تحيلان أو لا تحيلان إلى نفس المعلومات الأساسية. كما يمكن إنشاء كيانات إضافية لإقامة صلة الوصل فيما بين فرادى الكيانات الشرحية بسبل يتعذر التوصل إليها بخلاف ذلك من خلال البحث عبر فرادى الكيانات.

وتتيح المعمارية إقامة العلاقات بين العديد من المستودعات والسجلات والعديد الآخر منها، في كلا الاتجاهين. ويمكن لمستودع معين أن يقدم البيانات الشرحية لنفس الكيانات إلى سجلات متعددة، ويمكن لسجل معين قبول البيانات الشرحية من مستودعات متعددة. وجمع البيانات الشرحية من مستودعات متعددة في سجل واحد يمكِّن اتحاد تلك المستودعات. والسماح لتلك المستودعات بتقديم البيانات الشرحية لنفس الكيانات إلى سجلات متعددة يمكِّن المستودع الواحد من أن يكون جزءاً من اتحادات متعددة قد تتمايز فيما بينها بخدمة مجتمعات مختلفة وباستخدام مخططات مختلفة للبيانات الشرحية وبنُهُج مختلفة للفهرسة والبحث وبغير ذلك من القدرات.

وأخيراً، يمكن لحالة قيد في السجل أن تتحد مع سجلات أخرى. ويمكن لسجلات متعددة أن تدفع فيما بينها كيانات البيانات الشرحية، أو الكيانات التي تمثل دالة قيود البيانات الشرحية الأصلية. ويمكن لسجل معين، يدعى Reg1، أن يقدم إلى سجل ثان يدعى Reg2 قيد بيانات شرحية لكيان معين، إما كنسخة كاملة من قيد البيانات الشرحية الأصلي أو كملخص للقيد الأصلي. ومن شأن هذه التقدمة أن تضم القيد الأصلي أو بديلاً عنه في كيان رقمي (DO) وتوصَف على نحو يحدد ورودها من السجل Reg1 ونمط المجتمع أو الميدان الممثَّل في ذلك السجل. فإذا كان السجل Reg1 متحداً دائماً مع السجل Reg2، يمكن للسجل Reg2 أن يكون بمثابة نقطة تجميع عبر الميادين للعديد من السجلات الأخرى، وأن يوفر خدمة بحث يمكن أن تحيل الباحثين إلى سجلات أخرى أو مباشرة إلى الكيانات الرقمية نفسها حسب نهج تجميع وفهرسة قيود البيانات الشرحية التي يُحتمل عدم تجانسها.

وفي حين أن تركيز هذه التوصية ينصبّ على إدارة الهوية، تمكن الاستفادة من مثل هذا النظام أيضاً لاكتشاف أنواع أخرى من المعلومات في الأنظمة الموزعة المعقدة في الإنترنت مثل تلك التي تنطوي على "الحوسبة السحابية" أو "إنترنت الأشياء". ويتم الحصول على معلومات الاستخراج في نظام السجلات المتحدة من فرادى أنظمة إدارة الهوية. واستخدام آلية الاكتشاف في الاتحاد سيمكِّن التشغيل البيني لأنظمة إدارة الهوية، بصفة أعم؛ وسيوفر معلومات مناسبة لكيان ليستخبر عن أنظمة إدارة الهوية الأخرى، وللمساعدة في تنمية الثقة في استخدام معرفات الهوية من تلك الأنظمة.

ويستخدم عدد كبير من الجماعات تكنولوجيا السجل الأساسية، وقد استفاد بعضها من الإصدارات مفتوحة المصدر، وطور بعضها الآخر نماذج مسجلة الملكية على مقاس متطلباتها على أساس مواصفات مفهومة في إطار مشترك. ويتحقق الاتحاد عبر بروتوكولات لتبادل المعلومات. وسينصرف جزء هام من العمل المستقبلي القائم على هذه التوصية إلى إيضاح هذه المواصفات ثم إضفاء الطابع الرسمي عليها لتعريف البروتوكولات والإجراءات المناسبة إلى جانب مخططات البيانات الشرحية الملائمة، وتحديد نهج مقبول عموماً للحفاظ على الخصوصية، حسب الاقتضاء. أما كيفية القيام باختيار نظام معين لإدارة الهوية أو التعويل عليه فهي خارج نطاق هذه التوصية.

7 معمارية قابلية التشغيل البيني للسجلات المتحدة

يستند نظام السجلات المتحدة في هذه التوصية إلى معمارية مفتوحة تتيح قابلية التشغيل البيني عبر أنظمة معلومات غير معيّنة (للاطلاع على وصف لمعمارية تمثيلية، انظر التذييل I). وهي توفر وسيلة للاستيقان من المعلومات والنفاذ إلى المعلومات المهيكلة ككيانات رقمية والمحفوظة في معظم أنماط أنظمة الحفظ العادية. والكيان الرقمي هو معمارية البيانات الشائعة التي تمكّن التشغيل البيني لأنظمة في شبكة الإنترنت؛ وعناصر الكيان الرقمي هي مادة رقمية، أي بيانات مطبوعة، بما فيها معرف الهوية الثابت الفريد لهذه المادة.

وتستخدم ثلاثة عناصر معمارية في إدارة الكيانات الرقمية. ويمكن استخدام كل من هذه المكونات بمفردها، لكنها تكمل بعضها البعض، وتوفر معاً قدرة موزعة واستيعابية لإدارة المعلومات في شبكة الإنترنت. والمكونات هي:

أ) نظام معرف هوية استيعابي وموزَّع لتحديد هوية الكيانات الرقمية واستخراج معرّف الهوية؛

ب) مستودعات للنفاذ إلى الكيانات الرقمية وإدارتها؛

ج) سجلات للبحث والاكتشاف المتحد. فباستخدام هذه المكونات، تُمكن إدارة النظام الموزَّع الناتج من خلال مواصفات وبروتوكولات السطح البيني بدلاً من الصيانة المستمرة لمكونات محددة.

والكيانات الرقمية هي العنصر الأساسي الذي تُبنى وتدار من حوله جميع المكونات والخدمات الأخرى. ولا تحل الكيانات الرقمية محل الأنساق وهياكل البيانات القائمة، وإنما توفر وسيلة مشتركة لتمثيل تلك الأنساق والهياكل، مما يتيح توحيد تفسيرها، وبالتالي تناقلها داخل وخارج مختلف أنظمة المعلومات غير المتجانسة وعبر التغييرات في الأنظمة على مر الزمن. ورغم بساطة هذا النموذج في جوهره، لا يستهان بتنفيذه المفصل. وهو يتضمن بروتوكولاً للتفاعل مع الكيانات الرقمية من خلال المستودعات. وفي هذه التوصية، تطابق جميع البيانات الشرحية نموذج بيانات الكيان الرقمي لأغراض التشغيل البيني وسهولة الرجوع إليها.

ويرد أدناه وصف نموذج بيانات الكيان الرقمي وبروتوكول السطح البيني للكيان الرقمي من أجل النفاذ إلى الكيانات الرقمية، إلى جانب معرف هوية و/أو نظام استخراج ونهج السجل/المستودع من أجل النفاذ إلى الكيانات الرقمية. ويوفر هذا النموذج أساس المعمارية المفتوحة. وتمكِّن هذه المكونات معاً إدارة المعلومات المهيكلة ككيانات رقمية على المدى الطويل بتحديد الهوية التي تنفرد بها هذه الكيانات على نحو ثابت، وبتوفير وسيلة للحصول على معلومات عن الحالة الراهنة للكيانات، وتقديم خدمة الحصول على الكيانات أو استخدامها، ووسيلة لتحديد معرفات هوية الكيانات الرقمية على أساس المعلومات الواردة في سجلات البيانات الشرحية.

1.7 نموذج بيانات الكيان الرقمي

يوفر نموذج بيانات الكيان الرقمي الموصوف في هذه الوثيقة وسيلة موحدة لتمثيل قيود البيانات الشرحية ككيانات رقمية، ويمكن أيضاً أن تستخدم لتمثيل أنماط أخرى من المعلومات مثل الكيانات الرقمية. وهو نموذج منطقي يسمح بأشكال متعددة من التشفير والحفظ، ويمكِّن نقطة مرجعية واحدة (أي معرف هوية) لأنماط كثيرة من المعلومات التي قد تكون متاحة في شبكة الإنترنت. ولكل كيان رقمي مجموعة ضمنية من النعوت ومجموعة من النعوت التي يعرّفها المستخدم تتجسد في واحد أو أكثر من العناصر وصفر أو أكثر من العناصر الإضافية التي تحتوي على معلومات مثل النصوص أو ملفات الفيديو أو الصور الممثلة في شكل رقمي. ويمكن أن تتاح جميع هذه العناصر من خلال مواصفات بروتوكول السطح البيني لكيان رقمي المحددة بدقة (انظر الفقرة 2.7)، والتي تتضمن قدرة الاستيقان باستخدام أمن المفتاح العمومي، وربما يمكن أن تنفَّذ وسائل استيقان أخرى باستخدام سطوح بينية لبرمجة التطبيقات على مستوى أعلى، على النحو الذي يمكن أن تقوم مستودعات الكيانات الرقمية بتنفيذه. وهذا يوفر النفاذ مع الخصوصية والأمن للكيانات الرقمية.

ويرتبط النعت الثابت الأساسي لكيان رقمي بمعرف هوية ثابت وفريد، يمكن أن تُستخرج منه المعلومات الراهنة عن حال الكيان الرقمي، بما في ذلك موقعه (مواقعه)، وضوابط النفاذ، والتحقق، عن طريق تقديم طلب استخراج إلى نظام الاستخراج.

ومن الأمثلة على النعوت الضمنية الأخرى لعنصر الكيان الرقمي: تاريخ التعديل الأخير، وتاريخ الإنشاء، والمقاس. ويمكن للمستخدمين ضبط النعوت القابلة للتوسعة من جانب المستخدم بواسطة الأذونات المناسبة.

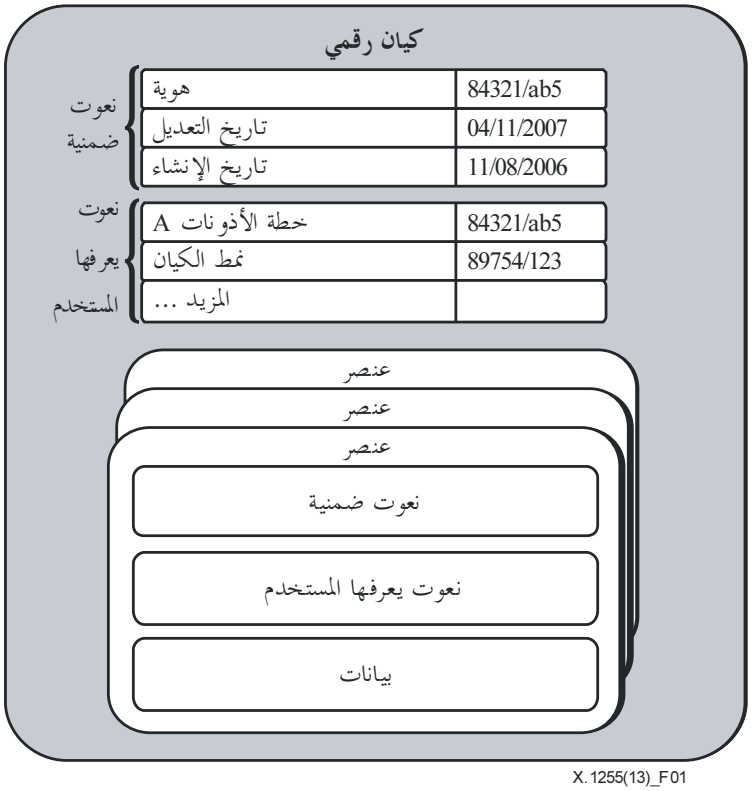
وتشمل النعوت التي لا يتناولها نموذج البيانات الأساسي للكيان الرقمي، الملكية والاستيقان وشروط وأحكام النفاذ. وتشكل هذه النعوت جزءاً هاماً من معظم تطبيقات الكيان الرقمي، ولكن وجود حل واحد يبدو مستبعداً. ويرجح أن ترد معلومات الملكية والتحكم في النفاذ ضمن النعوت القابلة للتوسعة من جانب المستخدم أو في عناصر بيانات منفصلة. ويوفر ذلك سبيلاً مشتركاً للتعامل مع مختلف مخططات الملكية وإدارة المعلومات، فضلاً عن مخططات الاستيقان والتخويل المتعددة، دون الافتراض بأن نهجاً واحداً سيُستخدم في جميع المجالات وجميع مجتمعات المستخدمين.

والجمع بين نموذج بيانات معياري، وبروتوكول معرَّف للتفاعل مع نموذج البيانات، ونظام معرف الهوية/الاستخراج، يوفر عنصراً رئيسياً للإدارة المتماسكة على المدى الطويل للمعلومات في شبكة الإنترنت. وينبغي أن يكون نظام الاستخراج موزعاً وآمناً وعالي الأداء ومصمماً لتمكين الإحالة المرجعية الثابتة إلى كيانات رقمية على مدى فترات طويلة من الزمن وعبر التغيرات في الموقع وأساليب النفاذ، وفي الملكية، وغير ذلك من النعوت القابلة للتغيير.

وتتأتى القدرة الأساسية لاكتشاف معلومات إدارة الهوية من استخدام مكون السجل، الذي يتضمن المستودع. وتتمثل وظيفة السجل الفردي في الاتحاد مع مجموعات من الكيانات الرقمية، وتمكين المستخدمين النهائيين والتطبيقات من البحث والتنقل في عالم الكيانات المسجلة. ويمكن للمستودعات التي تحتوي على مجموعات من الكيانات الرقمية أن تقدم إلى واحد أو أكثر السجلات بيانات شرحية عن الكيانات الرقمية التي تتولى المسؤولية عنها. ويمكن لسجل واحد أن يجمع البيانات الشرحية من مستودعات متعددة، ويمكن لمستودع واحد أن يرسل البيانات الشرحية إلى سجلات متعددة. ويمكن للسجلات أن توفر وظائف البحث والإبلاغ عن الكيانات الممثَّلة، وأن توفر نقطة دخول إلى العالم المهيكل للكيانات الرقمية والمستودعات.

وقد تكون هناك حالات لا تلزم فيها السجلات، بالمعنى الدقيق للكلمة، كحالة الإحالة المباشرة إلى كيان رقمي، مثلاً، في شكل معرف هويته المدمج في كيان رقمي آخر أو في رسالة أو وثيقة أخرى. ولكن في كثير من الحالات، سيكون معرف الهوية مجهولاً أصلاً لدى المستخدم النهائي أو العملية المؤتمتة العاملة نيابة عن المستخدم، مما يقتضي استخدام بعض العمليات المتنوعة من البحث أو الفرز لاكتشاف المرجع اللازم. وحتى لو كان المستخدم على علم بالمعرف فقد يجهل كيفية استخراجه، أو كيفية تفسير نتائج الاستخراج. ويمكن لتدوين وجود كيانات رقمية في السجلات أن يساعد على حل هذه المشكلة بطريقة عامة جداً.

وبتعريف العمليات التي تتفاعل مع نموذج البيانات المحدد، يمكن إنشاء كيانات رقمية واستخدامها لتمثيل معظم أنماط المعلومات المهيكلة. ويرد نقاش ذلك في الفقرة التالية. ويتضح نموذج بيانات الكيان الرقمي المعياري في الشكل 1. ويعد تمثيل الكيانات في شكل مستقل عن تفاصيل التنفيذ لنظام الحفظ ذي الصلة ميزةً أساسية لقابلية التشغيل البيني ، كما أنه يتيح تقييس أنساق ونُهُج حفظ متعددة في نموذج منطقي واحد.



الشكل 1 – مثال توضيحي لكيان رقمي

فيما عدا معرف الهوية الثابت في الجزء العلوي، فإن جميع البيانات التي تظهر في الشكل رقم 1 هي بيانات مفاهيمية فقط. ويمكن لكل عنصر من كيان رقمي أن يتخذ أشكالاً مختلفة، أي مراجع كيانات رقمية من خلال معرف هوية، وكيان رقمي فعلي، وبيانات محلية عادية مكتوبة بشكل مناسب.

ويمكن للسجلات أن تستخدم أو أن تدمج مستودعات لحفظ قيود البيانات الشرحية، والمستودعات هي أنظمة إدارة معلومات توفر النفاذ إلى مجموعات من الكيانات الرقمية عبر بروتوكول السطح البيني للكيان الرقمي. ويمكن تصور المستودعات عموماً على أنها تتضمن كيانات رقمية تقدِّم لها النفاذ. وإذ يُنظر في تفاصيلها، فهي تبدو كبوابات مختلف أنظمة الحفظ والمعلومات وتقيم التقابل بين البيانات الخام والكيانات الرقمية التي يمكن حفظها محلياً أو عن بُعد. ويمكن أن يكون ذلك ببساطة نظام الملفات الحافظ لبيانات كيان رقمي معين في واحد أو أكثر من الملفات المجهولة أو غير المرئية للمستخدم. وبدلاً من ذلك، وخاصة بالنسبة للكيانات المعقدة، يمكن نشر البيانات عبر مواقع وأنظمة متعددة وجمعها معاً في شكل كيان رقمي عند الطلب فقط، حيث يحفظ مكون حفظ واحد "خريطة تقابل" الكيان، فيما يُحفظ الجزء الأكبر من البيانات في الأنظمة الأخرى. وتقنية التفاعل هذه مع الأنظمة القائمة هي مفتاح الاتحاد، لأن المعلومات في نظام معلومات معقد غير معين يمكن أن تقسَّم منطقياً إلى كيانات رقمية، وتمكن إتاحة تلك الكيانات الرقمية بطريقة مقيَّسة باستخدام بروتوكول السطح البيني لكيان رقمي ضمن التطبيقات التي تركز على المستخدم.

ويمكن لعميل الكيان الرقمي أن يحدد موقع واحد أو أكثر من المستودعات لكيان رقمي معين باستخراج معرف هويته. وسيُرد على طلب الاستخراج بموقع واحد أو أكثر من المستودعات ذات الصلة التي يمكن للعميل بواسطتها بدء التعامل مع كيان رقمي.

وعادةً ما توفر برمجيات مستودع الكيانات الرقمية سطوحاً بينية متعددة للشبكة لتنفيذ عمليات على الكيانات الرقمية، وهي بروتوكول السطح البيني لكيان رقمي للتفاعل مع الكيان الرقمي نفسه، وكذلك سطوح بينية مرغوبة محلياً على النحو الذي تحدده خيارات التكنولوجيا الحالية. ولكل من السطوح البينية المختلفة فوائده الخاصة من حيث الأمن، والتوافق مع المخدمات الوكيلة، واستخدام برمجيات العميل في كل مكان. ويُدمج الإطناب الرديف في بروتوكول السطح البيني لكيان رقمي إلى جانب استيقان قوي على مستوى الفرد والمجموعة. ويُدعم الإطناب الرديف بنظام نسخ متطابق يتواصل فيه كل مستودع

للكيانات الرقمية مع المستودعات الأخرى لضمان إدامة تزامن الكيانات المستنسخة. ويستند الاستيقان إما إلى المفاتيح السرية أو العامة/الخاصة أو إلى آليات استيقان أخرى.

وتشمل الميزات البارزة الأخرى الاستنساخ، الذي يسمح بالنسخ المتطابق السهل عبر المستودعات، وقابلية التوسعة من خلال آلية التوصيل بالقبس. ويمكن بناء وحدات التوصيل بالقبس لإدارة أنشطة الكيان ذات النمط المحدد مثل تحليل نسق فيديوي والاستغناء عن فقرة مطلوبة، أو الأنشطة الموجهة لخدمات الشبكة، مثل تقديم البيانات الشرحية إلى سجل كيانات رقمية.

2.7 بروتوكول السطح البيني لكيان رقمي

يتكون كل تفاعل مع الكيان الرقمي من كيان معرَّف هوية يستدعي أو يطبق عملية على الكيان الرقمي. ويجرى التعريف الثابت والفريد لمعلومات إدارة الهوية كافة بشأن الكيان، وكل عملية، والهدف من العملية. وبالإضافة إلى ذلك، فإن الموارد على اختلاف أنواعها هي كيانات معرَّفة الهوية، ويمكن أن تتضمن معلومات حالة المورد ذات الصلة مفتاحه الخاص من بين إدخالات القيود الأخرى.

وتطبّق المستودعات العمليات على الكيانات، علماً بأن المستودعات هي في حد ذاتها كيانات رقمية توفر النفاذ إلى الكيانات التي تحتويها. ويعرّف بروتوكول السطح البيني لكيان رقمي أسلوب اتصال الكيان مع مستودع لطلب تنفيذ عمليات على الكيانات الرقمية التي يتيح المستودع النفاذ إليها. ويمكن استخدام هذه العمليات، على وجه الخصوص، للنفاذ إلى قيود بيانات شرحية تحددها معرفاتها، ولكن يمكن أيضاً النفاذ إلى مثل هذه القيود لغوياً من خلال وسائل أخرى مثل "تطبيقات" السجل المكرسة ومتصفحات شبكة الإنترنت.

والعملية التي تجرى على الكيان الرقمي تنطوي على العناصر التالية:

- EntityID: معرف هوية الكيان الذي يطلب تنفيذ العملية؛
- TargetObjectID: معرف هوية الكيان الذي سيخضع للعملية؛
- OperationID: معرف الهوية الذي يحدد العملية التي ستنفَّذ؛
- Input: تسلسل البتات التي تحتوي على مدخلات العملية، بما في ذلك أي معلمات أو محتويات أو معلومات أخرى؛
- Output: تسلسل البتات التي تحتوي على مخرجات العملية، بما في ذلك أي محتويات أو معلومات أخرى.

ويمكن أن تُرفق معلومات إدارة الهوية أو ترسل كجزء من شهادة تقدم تأكيد ثقة صريحاً أو ضمنياً بشأن المعلومات. بيد أن المتلقي يمكن أن يقبل أو لا يقبل الشهادة إن لم تكن صادرة عن سلطة ثقة مقبولة. ويمكن أيضاً أن تُستخدم التأشيرات بدلاً من الشهادات للإتيان بنتيجة ثقة مماثلة. وتزيد هذه الشهادات أو التأشيرات من احتمال دقة نقل معلومات الهوية، ومع ذلك، فإن التنفيذ الممكن لآليات أمن ضمنية كجزء من هذه المعمارية المفتوحة يمكن أن يتحقق بشكل مستقل من كون الكيان المستفيد من معلومات إدارة الهوية يمتلك المفتاح الخاص المناسب الذي يمكن استخدامه لإقرار صلاحية الكيان ذي الهوية المعرَّفة. ويمكن لأي من طرفي طلب معاملة يتضمن كيانات معرَّفة الهوية أن يطلب من الطرف الآخر تشفير سلسلة بمفتاحه الخاص وإعادتها إلى الطرف الطالب للتحقق من صحتها. ويمكن للأطراف في أي معاملة ضمن نظام تنفيذ وسائل استيقان أخرى، ولكن ليست هناك حاجة *مسبقة* للتفاوض بشأن وسائل أخرى. والآلية المبدئية القابلة للتغير المبينة أدناه تتمثل في استخدام أزواج المفاتيح العامة/الخاصة، وهي قدرة أساسية في بروتوكول السطح البيني لكيان رقمي (DOIP). ولكن يمكن استخدام آليات استيقان أخرى، إذا رُغب في ذلك، حسب اتفاق الطرفين. ويتعين أن يستتبع تنفيذ بروتوكول السطح البيني لكيان رقمي كحد أدنى، الخطوات التالية غير الاختيارية:

أ) إنشاء ارتباط بين الطرف A والطرف B، وهما طرفا التعامل، إلا إذا كان أحدهما موجوداً مسبقاً ويمكن استخدامه لهذا الغرض؛

ب) يمكن للطرف A اختيارياً أن يطلب إلى الطرف B أن يثبت نفسه للطرف A باستخدام أسلوب PKI مثلاً؛

ج) ثم يقدم الطرف A طلباً محدداً إلى الطرف B، حسب الاقتضاء؛

د) يمكن للطرف B اختيارياً أن يطلب إلى الطرف A أن يثبت نفسه للطرف B باستخدام أسلوب PKI مثلاً؛

هـ) يلبي الطرف B هذا الطلب أو يرفضه، حسب الاقتضاء؛

و) ينهى التعامل وإما أن يولّد طلب جديد أو ينهى الارتباط، إذا كان ذلك مناسباً.

ويرد في مرجع البيبليوغرافيا [b-DOIP] مثال على توصيف مفصّل لبروتوكول السطح البيني لكيان رقمي، ولكنها ليست جزءاً رسمياً من هذه التوصية (انظر أيضاً المرجع [b-DO Repo]).

3.7 التفاعلات مع سجل

ينطوي كل تفاعل مع السجل على كيان معرَّف الهوية قد يكون فرداً أو مورد نظام، ولكل تفاعل معرف هوية ثابت يمكن استخدامه للاستيقان من الكيان. وأثناء الإعداد، يمكن تشكيل السجل مسبقاً ليثق بأي عميل أو عملاء من ذوي الهوية المعرَّفة بطريقة ما محددة عبر معرفات الهوية لديه. ويمكن للعملاء أيضاً اختيار الاستيقان من السجلات باستخدام نفس الإجراء. وعلاوة على ذلك، يمكن تشكيل عملاء محددين ليعملوا على النحو المطلوب تحديداً في عملية اتحاد. ومن شأن ذلك أن يسمح بعملية محددة على السجل بالإضافة إلى العمليات التي يشيع توفرها لجميع العملاء الموثوقين. وعندما يتفاعل العملاء مع السجل، يصدر السجل تحدياً–رداً للتحقق من امتلاك العميل المفتاح الخاص المطابق. وحالما يُتحقق من ذلك، يتحقق السجل من أن معرف الهوية عائد للكيان.

ويدعم السطح البيني للسجل العمليات التالية:

- **سجل كيان رقمي:** قد تتكون معلومات التسجيل من البيانات الشرحية فقط، ولكن يمكن أن تتكون أيضاً من بيانات شرحية إلى جانب كيان رقمي تُطبق عليه البيانات الشرحية. ويدير السجل الكيان الرقمي المسجَّل باستخدام مستودع داخلي. وعلاوة على ذلك، يفهرس السجل المعلومات المهيكلة ككيان رقمي باستخدام القواعد المشكَّلة مسبقاً والتي تحدد كيفية التحليل وإصدار التأشيرات وفهرسة المعلومات المحفوظة. وعند الاقتضاء، ينشئ السجل معرف هوية للكيان الرقمي ويتسبب في إدراجه في نظام الاستخراج.
- **إلغاء تسجيل كيان رقمي مسجل سابقاً:** يحذف السجل كياناً رقمياً من مستودعه الداخلي، ويزيل فهرسته، ويحدِّث نظام الاستخراج ليدون حالة حذف الكيان.
- **استرداد كيان رقمي مسجل سابقاً عن طريق معرف الهوية الخاص به:** يسند السجل رقماً تسلسلياً إلى الكيان الرقمي المدار في مستودعه الداخلي ويحيله إلى العميل.
- **البحث:** يحلل السجل الكلمات الرئيسية في عبارة البحث، أو ما يطابقها مطابقة تامة، أو استعلامات نطاق البحث المقابلة للكيانات الرقمية المفهرسة، ويعيد معرفات هوية الكيانات الرقمية المطابقة. ويمكن بسهولة دمج تقنيات بحث أكثر تقدماً، مثل استعلامات باللغة الطبيعية، إذا سمحت نتائج البحوث بذلك.
- **الحصول على رقم آخر معاملة:** إن السجل، الذي يخصص أرقاماً بطريقة تسلسلية إلى كل سجل وعملية إلغاء تسجيل تجرى عليه، يعيد آخر هذه الأرقام إلى عميل مشكَّل للمشاركة في عملية الاتحاد مع السجل. ومن شأن ذلك السماح للعملاء المحتملين (السجلات الأخرى المشاركة في عملية الاتحاد) بتحديد حالة السجل من أجل دفع الكيانات المسجلة حسب طوبولوجيا الاتحاد المشكَّلة ومستوى التجميع المختار.

ورغم إمكانية إيقاف الاستيقان، من المستحسن أن يستيقن السجل من العميل وبالعكس. ويمكن أن يختلف تشفير الرسائل المتبادلة، وهذا الأمر من تفاصيل التنفيذ. ويمكن تشفير الرسائل كعمليات مستودع الكيانات الرقمية، وعند هذه النقطة ستكون معاملة السجل سلسلة من عمليات مستودع، مثل إنشاء كيان وإضافة عنصر. وبدلاً من ذلك، يمكن تشفير الرسائل باستخدام مكتبات تشفير البيانات العائدة لطرف ثالث، شريطة اتفاق كل من المصدر والمتلقي (مقدماً على الأرجح) على استخدام نفس المكتبة.

4.7 أنظمة الاستخراج

تضم مكونات الإطار نظام الاستخراج (ويمكن أن يكون هناك أكثر من نظام واحد) الذي يمكنه إقامة التقابل بين معرفات الهوية والمعلومات المفيدة عن حالة الكيان الرقمي الذي يُتعرف على هويته، مثل موقعه في شبكة الإنترنت، أو معلومات الاستيقان لذلك الكيان، أو مفتاح عمومي مرتبط بمعرف الهوية. وتتيح طبيعة المعمارية المفتوحة للإطار قابلية التشغيل البيني لأنظمة الاستخراج، وهي هدف مرغوب لهذه التوصية. ويمكن تغيير معلومات الحالة حسب الحاجة لتعبر عن الوضع الحالي للكيان المعرَّف هويته دون تغيير معرف الهوية الخاص به، بما يسمح بثبات معرف هوية البند عبر التغييرات في الموقع وغيرها من تغييرات الحالة ذات الصلة.

وإذا كان معرف هوية المورد اللازم معروفاً، يوفر نظام الاستخراج ومجموعة من المستودعات ما يلزم المستخدم النهائي أو العملية المخولان للاطلاع على الكيان أو النفاذ إليه. أما عندما تكون هوية المورد اللازم مجهولة، فسيتعين اكتشافها. وبمصطلحات المكتبات وعلم المعلومات، تدعى الحالة الأولى البحث عن "بند معروف" (أي أنك تعرف ما تريد، وتحتاج إلى معرفة كيفية الحصول عليها). أما الحالة الثانية فعادة ما تتطلب البحث عن الموضوع؛ والهدف من الأدوات المستخدمة في البحث عن الموضوع هو تحويله إلى بحث عن بند معروف. ويتيح سجل الكيان الرقمي القيام بهذا الدور.

وبينما يمكن لحالة في سجل أن تعمل قائمةً بذاتها، لا يمكنها تلبية إلا طلبات الاكتشاف التي تعلم بها. وبتوحيد سجلات متعددة، يمكنها أن تعلم بشأن الكيانات الرقمية المسجلة في مكان آخر، وبالتالي يمكن توسيع البحث عبر كامل مجموعة الكيانات الرقمية. والقدرة على تحديد السجلات التي قد تحتوي على المعلومات المتعلقة بالهوية ذات الصلة هي جانب هام من اكتشاف معلومات إدارة الهوية. ويمكن أن تحتاج المعلومات المتوفرة في نظام واحد لأن يكتشفها نظام آخر قد يكون ذا تصميم مختلف. على افتراض أن كياناً ما قد حدد وسيلة لارتباط هذه الأنظمة المختلفة بالمعلومات التي تحتويها، ينبغي لإطار الاكتشاف أن يتيح اكتشاف هذه الارتباطات. سوى أن هذه التوصية لا تبحث في من يتولى مسؤولية إقامة هذه الارتباطات وأي نوع من المعلومات تمكن إقامة الارتباط معها أو كيفية إقامة الارتباط والنفاذ إليه. وستختلف هذه القضايا، بشكل عام، من سياق إلى آخر، وبالتالي هذه التوصية لا تقترح أي نمط من ممارسات الارتباط. ولتوضيح هذه المسألة، يضاف مصطلح "الارتباط" إلى التعريفات وقد أدرج هذا المفهوم في تعريف معلومات إدارة الهوية.

وفي كثير من الحالات، تتسم الخصوصية بأهمية بالغة، وتدار من خلال استخدام تقنيات إدارة الهوية استناداً إلى معرفات الهوية للأفراد والجماعات، والأدوار، والموارد، وكذلك للشروط والأحكام التي يتم الحصول عليها من البيانات الشرحية المحفوظة.

5.7 الاستعلامات الموزعة والبيانات الشرحية المجمعة في سجلات متحدة

ينبغي لنظام السجلات المتحدة المعروض في هذه التوصية أن يكون متاحاً على نطاق واسع وأن يشكل أساس نظام اكتشاف المعمارية المفتوحة. ويوفر النظام وسيلة موحدة لاكتشاف معلومات إدارة الهوية. ويسمح نظام سجلات متحدة لمقدمي إدارة الهوية متعددين بالمشاركة في توفير سجلات قابلة للتشغيل البيني وتحديد ماهية المعلومات التي يسمحون بالتشارك فيها مع السجلات الأخرى.

وتوفر تكنولوجيا السجل الوسائل التي يمكن بها للأطراف المسؤولة عن إنشاء الكيانات الرقمية في شبكة الإنترنت، بما في ذلك الخدمات والكيانات الأخرى، أن تسجل وجود مجموعة معينة من تلك الكيانات، وأن ترفق ذلك التسجيل بالبيانات الشرحية الوصفية والهيكلية بشأن الكيانات، بما في ذلك معلومات عن المنشأ، فتعزز بذلك اكتشاف الكيانات إما لعامة الجمهور أو لمجتمع محدد. وأحد البيانات الشرحية الرئيسية التي يجب أن تسجَّل لدى الكيان هو معرف الهوية الثابت الخاص به؛ ويجب أن يتسنى استخراج هذا المعرف في شبكة الإنترنت. وبالنسبة إلى الكيانات التي لم يسبق تحديدها، يمكن تشكيل السجل لإنشاء معرفات هوية كجزء من عملية السجل وتوفير الأدوات اللازمة لإداريي الكيان للحفاظ على معلومات الاستخراج.

وسيحقق نظام السجلات المتحدة أربعة أهداف رئيسية للاكتشاف. فأولاً سيمكِّن تطبيق سياسات اختيار موحدة على جميع أطر الثقة وأنظمة إدارة الهوية الأخرى المشاركة. وثانياً سيمكِّن المستخدم من النفاذ إلى معلومات السجل التي يُسمح للمستخدم النفاذ إليها دون الاضطرار إلى التعامل مباشرة مع سجلات متعددة. وثالثاً، فإنه يوفر دعم البنية التحتية

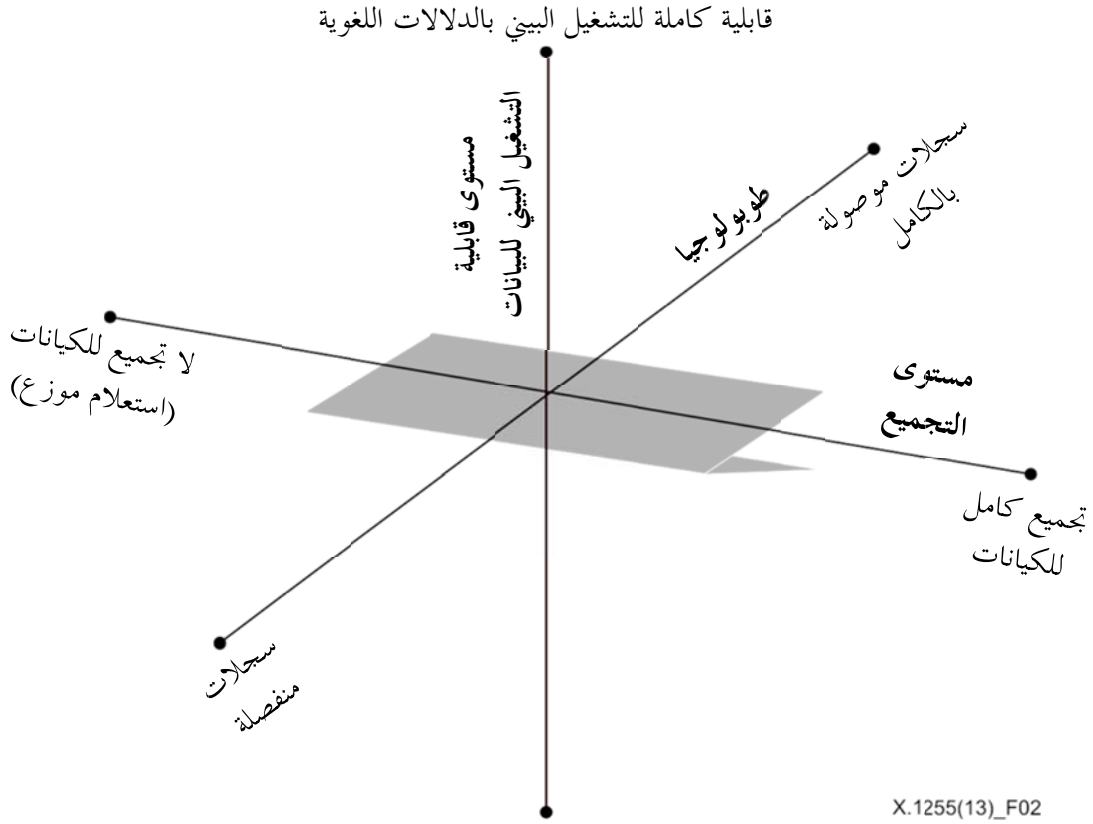
للخصوصية والقيود الأخرى المفروضة على النفاذ التي وضعتها فرادى أنظمة إدارة الهوية. ورابعاً، سيمكّن النفاذ بالدلالات اللغوية إلى السجلات لدعم تعدد اللغات.

ويقدم مفهوم السجلات المتحدة القائم على المعمارية المفتوحة المعروضة في هذه التوصية الفوائد التالية:

- سياسات اختيار موحدة: يمكن اختيار السجلات وأطر الثقة المرتبطة بها أو أنظمة إدارة الهوية الأخرى بشكل أعم، للاستعلام على أساس خصائص المعلومات التي تدعي احتواءها. وعادة ما يجري اختيار نظام إدارة الهوية الذي يقوم بمستوى معين من التحقيق في الخلفية لإثبات معلوماته. وبدلاً من ذلك، يمكن اختيار الحد الأدنى من إطار الثقة أو نظام آخر لإدارة الهوية يكتفي بالتحقق من معلومات بطاقة الائتمان أو رخص قيادة السيارات. وفي الحالة القصوى الأخرى، يمكن اختيار نظام إدارة هوية يجري اختبار الحمض النووي للأفراد. ويمكن اختيار منظمة تتبع سياسات لضمان سلامة الأنظمة. وبهذه الوسائل، يمكن تطبيق أسلوب موحد للاختيار عبر عالم السجلات وأنظمة إدارة الهوية المرتبطة بها.
- البيانات الشرحية المشتركة: يشار إلى ويرتبط مع البيانات الشرحية المشتركة نموذج معياري عام يحدد كيفية تمثيل البيانات الشرحية، وبالتالي كيفية النفاذ إليها لمعالجتها لاحقاً. ولا يحتوي النموذج المعياري على إدخالات قيود محددة.
- النفاذ المتحد: إذا لم يمتلك سجل المعلومات المطلوبة يمكن النفاذ إلى هذه المعلومات من واحد أو أكثر من السجلات الأخرى. والحال في التشغيل العادي أن النظام يعمل بحيث يجعل هذه المعلومات متاحة بسهولة للمستخدم بمعزل عن السجل الذي قد يحتويها. ويمكن تمكين هذا النفاذ بمجموعة متنوعة من الوسائل، بما فيها الاتحاد التراتبي وأنظمة التبادل بين النظراء.
- النفاذ الخاص: ستكون بعض السجلات حكراً على مجموعات معينة من المستخدمين، أو أنماط التطبيقات، أو الأدوار المرتبطة بالاستفادة من النظام؛ وقد تكون بعض السجلات مفتوحة للجميع. وتقوم إحدى وسائل تقييد النفاذ إلى معلومات الاكتشاف على أساس معايير مثل كون هذا التقييد جزءاً أساسياً من النظام. وستُستخدم آلية واحدة أو أكثر توافق عليها السجلات المشاركة، للحفاظ على الخصوصية ضمن النظام.
- النفاذ بالدلالات اللغوية: يستخدم نظام طباعة لتفسير "المطبوعات" المدرجة. ويمكن أن يعين مقدمو الهوية مطبوعات يختارونها وفقاً للمبادئ التوجيهية للتوصيف. وسيمكّن ذلك النفاذ بالدلالات اللغوية إلى المعلومات ذات الصلة بغض النظر عن موضع حفظها في النظام، ويمكنه أن يساعد في تلبية متطلبات تعدد اللغات.

تتوفر البيانات الشرحية في مثل هذا النظام كبيانات مهيكلة، مع معرف هوية ثابت وفريد يرتبط بها وهو موجود طالما وُجد الكيان الرقمي. وقد تختلف البيانات الشرحية الواردة من مختلف السجلات في مجال الموضوع و/أو مخطط البيانات الشرحية، مما يصعِّب القيام ببحث بسيط ومتماسك عبر مجمع السجلات كافة. وإذا اختُصرت البيانات الشرحية من مخططات أو مجالات مواضيع مختلفة إلى مخطط القاسم المشترك الأصغر، وهذا أحد الحلول لتجميع هذا النمط من البيانات، فإن استراتيجية البحث المثلى قد تتمثل في تحديد هوية السجلات التي من شأنها أن تكون أفضل المرشحات لبحث أكثر تفصيلاً. ويمكن لسجلات المصدر أو السجل المجمع أن يقوموا بالتحويل إلى مخطط القاسم المشترك الأصغر. وبدلاً من ذلك، يمكن إقامة التقابل بطريقة ما للبحث نفسه ليستعلم من مختلف مخططات البيانات الشرحية بشكل مناسب، مما يؤدي إلى مجموعة من الاستعلامات التي تتفرع من الأصل.

وفي حين أن تجميع كيانات البيانات الشرحية لاكتشاف المعلومات من ميادين متعددة هو أحد الاحتمالات، فإن إصدار استعلامات موزعة عبر سجلات متعددة يدير كل منها كيانات البيانات الشرحية في ميدانه، هو احتمال آخر. ويتضمن مشهد الاتحاد عبر السجلات مختلف الاحتمالات الأخرى، على النحو الموضح في فضاء ثلاثي الأبعاد في الشكل 2.



الشكل 2 – الاستعلامات الموزعة عبر سجلات متعددة

تظهر في الشكل 2 ثلاثة محاور. ويبين أحد المحاور مستوى تجميع البيانات الشرحية للسجل من انعدام التجميع إلى التجميع الكامل. ويبين المحور الثاني درجة التوصيلية الطوبوغرافية بين السجلات. أما المحور الثالث فيتعلق بقابلية التشغيل البيني للمعلومات من سجلات مختلفة. ويرد وصف كل من هذه المحاور بمزيد من التفصيل أدناه.

ويبين محور مستوى التجميع الدرجة التي أجريت فيها ترتيبات مسبقة عبر السجلات للانخراط في تجميع كيانات البيانات الشرحية. وتبين نقطة أقصى اليسار على المحور الكيانات التي لم تجمَّع عبر السجلات قبل أي استعلام، في حين تبين النقطة على أقصى اليمين على المحور أن جميع الكيانات جرى تجميعها قبل أي استعلام. وتمثل النقاط على طول المحور احتمالات أخرى بما في ذلك تجميع معلومات البيانات الشرحية للقاسم المشترك الأصغر وتجميع مؤشرات البحث، وغير ذلك. وبالتحرك من اليسار إلى اليمين، تنخفض أيضاً مواكبة المعلومات المجمعة لآخر المستجدات؛ وينتج الاستعلام الموزع نتائج أكثر حداثة، في حين أن مواكبة كيانات البيانات الشرحية المجمعة لآخر المستجدات تعتمد على متى كان آخر تجميع لها.

ويبين محور الطوبولوجيا درجة توصيل السجلات. ففي أقصى أحد طرفي المحور، لا تمتلك السجلات توصيلية شبكية فيما بينها، مما يؤدي إلى عدم التشارك في المعلومات؛ ويبين الطرف الأقصى الآخر توصيلية كاملة للسجلات فيما بينها. علماً بأن "كيفية" توصيلها يظل مقرراً بمستوى التجميع، ولا تحدد الطوبولوجيا إلا الوصلات الممكنة.

ويبين مستوى محور قابلية التشغيل البيني للبيانات درجة قابلية التشغيل البيني لكيانات البيانات الشرحية من سجل يقدم خدماته لميدان معلومات معين مع كيانات بيانات شرحية من سجل آخر يقدم خدماته لميدان معلومات مختلف. وبعبارة أخرى، فإن مخططات البيانات الشرحية التي يعتمدها سجل واحد قد تكون أو لا تكون قابلة للتشغيل البيني مع المخططات التي اعتمدها سجل آخر. وفي بعض الأحيان، يكون تحويل كيانات البيانات الشرحية ضرورياً لتحقيق مستوى معين، إن لم يكن بالقدر الكامل، من قابلية التشغيل البيني. وفي حالات أخرى، عند تباعد المخططات كثيراً بالدلالات اللغوية، لا يمكن لأي قدر من التحويل أن يحقق مستوى مفيداً من قابلية التشغيل البيني.

وتلاحَظ عدم صلاحية جميع نقاط الفضاء ثلاثي الأبعاد المبين في الشكل 2. فعلى سبيل المثال، الاستعلام الموزع على العقد المنفصلة يعني ضمناً عدم توزيع الاستعلامات على الإطلاق. وبالمثل، فإن التجميع الكامل للكيانات غير القابلة للتشغيل البيني يعني ضمناً نظاماً لكيانات غير متماسكة. وبحدود صلاحية النقاط الواردة في مصور الفضاء ثلاثي الأبعاد، ينبغي أن يسمح التصميم الأساسي للسجل بمثل هذه الاحتمالات من التشكيل. وكذلك، سواء أُقيم التقابل في تحويل قيود البيانات الشرحية أو في البحث، وسواء قامت السجلات المساهمة أو سجل الجمع بتحويل قيود البيانات الشرحية، فكلها من تفاصيل التنفيذ. وقد تظهر عواقب كبيرة في الأداء، ولكن التصميم الأساسي ينبغي أن يسمح بالاختلافات في التنفيذ.

والنهج المتبع في هذه التوصية لا يحل في حد ذاته مشكلة البحث والاسترجاع عبر أنظمة المعلومات غير المتجانسة، ولكنه يوفر إطاراً مشتركاً يمكن استخدام مختلف النهج فيه. ويرجح في الواقع عدم وجود حل واحد للمشكلة وأن النُهج المثلى يمكن أن تختلف حسب مجتمع الممارسة ومجال الموضوع.

6.7 مخططات البيانات الشرحية

من الأهداف الرئيسية لهذه التوصية توفير أساس لتعريف مجموعة من مخططات البيانات الشرحية "رفيعة المستوى" لدعم اكتشاف المعلومات بشأن: أ) معرفات الهوية المستخدمة في أنظمة إدارة الهوية المختلفة؛ ب) مقدمي الهوية؛ ج) الأطراف المعولة؛ د) أطر الثقة وأنظمة إدارة الهوية الأخرى على جميع المستويات، بما في ذلك السياسات والإجراءات والبنية التحتية التقنية الأساسية. وستكون سيناريوهات الاستخدام المعينة قاطرة العناصر الضرورية في مخططات البيانات الشرحية هذه، ويجب أن تكون سيناريوهات الاستخدام قابلة للتوسعة على مستوى العنصر والمخطط معاً لدعم النمو والتغيير في مجال دينامي.

ويمكن لكل من الكيانات المختلفة المشاركة في إدارة الهوية أن تعرّف المخططات الخاصة بها وأن تقيم التقابل لها، حسب الحاجة، مع مخططات البيانات الشرحية المقيّسة هذه رفيعة المستوى لوصف خدماتها وسياساتها وإجراءاتها، وتسجيل تلك الأوصاف في واحد أو أكثر من مجموعة السجلات المتحدة. ومن شأن هذه السجلات أن تدعم خدمات الاكتشاف عبر الكيانات المسجلة.

في حين أن من الممكن إنشاء مخطط بيانات شرحية واحد لاستيعاب جميع جوانب تكنولوجيات إدارة الهوية والمنظمات ذات الصلة، والسياسات والإجراءات المرتبطة بها، يُقترح البدء بمخطط واحد لكل نمط من أنماط الكيان المعني. وستصبح عملية التوصل إلى مجموعة من مخططات البيانات الشرحية المتفق عليها عملية تعاونية تساهم فيها الأطراف المهتمة بمعرفتها للنعوت التي يجب أن تشملها المخططات؛ ويمكن بعد ذلك اختبار المخططات المتطورة قياساً بمختلف سيناريوهات الاستخدام للوقوف على ما إذا كانت توفر في الواقع المعلومات اللازمة لدعم عمليات الاكتشاف، ويمكن تعزيزها بعدئذ، إذا كان ذلك مناسباً.

7.7 قابلية التشغيل البيني للبيانات الشرحية

تشكل معرفات الهوية مكوناً هاماً في تحقيق قابلية التشغيل البيني للبيانات الشرحية. بيد أن بعض الجوانب الأخرى لقابلية التشغيل البيني هذه بما في ذلك تلك التي تنطوي على التعريف البشري وسياق الوصف، فهي تقع خارج نطاق هذه التوصية. أما النعوت الأخرى الموصفة في البيانات الشرحية، كتلك التي تصف أو تمكّن تشكيلة معينة، مثل أسلوب توصيل معين ونهج التجميع، فهي تقع ضمن نطاق تشغيل السجل. ولأغراض إدارة كيانات البيانات الشرحية في مختلف السجلات، ستسهَّل قابلية التشغيل البيني للبيانات الشرحية إذا اتفقت الأطراف المتعاونة على مخططات مشتركة للبيانات الشرحية. وستدار البيانات الشرحية حينئذ ككيانات متجانسة، فتفسرها السجلات وتعالجها بطريقة متسقة. وتوضح الفقرة 9 أدناه حالتي اتحاد محددتين في سياق مستوى التجميع والطوبولوجيا، وهما بُعدان مطبقان عادة على هذا الإطار.

8 الأنماط ونعوت النمط

توفر السجلات قيود البيانات الشرحية في شكل كيانات رقمية بهدف تبادلها مع غيرها من السجلات المتحدة. ويتكون كل من هذه القيود من مجموعة من العناصر يحوي كل منها حقل "النمط" وحقل "القيمة". وفهم معنى كل نمط أمر بالغ الأهمية لإظهار القيم المرتبطة به في شكل غير تسلسل البتات المبهم أو مجموعة تسلسلات البتات.

ولفهم ما يعنيه النمط، تمثّل الأنماط بمعرفات هوية ثابتة يمكن استخراج معلومات مفيدة منها عن النمط. وبينما يراد للأفراد أن يضعوا وصف الأنماط، هناك حاجة لوسيلة معيارية لوصف وتمثيل الأنماط.

ويُتوقع للجوانب والنعوت المحددة لما سيشكل تعريف نمط في نهاية المطاف أن تتطور مع مرور الوقت، ولكن الجوانب الأربعة التالية تعتبر ضرورية:

- الفئة الأولى من النعوت هي الأبسط وتتكون من أوصاف قابلة للقراءة بشرياً للغرض من النمط. وتهدف هذه الأوصاف لوصف الغرض من النمط، والموارد والمفاهيم التي يصفها، واستخدامه. وهذه النعوت ستدعم الأوصاف بلغات متعددة؛
- أما الفئة الثانية من نعوت وصف النمط فهي تتكون من معلومات منشأه. وينبغي أن يشمل كل تعريف نمط: تاريخه إنشائه، وتاريخ آخر تحديث له، ومقدميه، وحالته، وأي اسم مستعار قد يمتلكه؛
- وتتعلق الفئة الثالثة من النعوت بوصف تصنيف الأنماط وكذلك بقدرة الأنماط على الاستفادة من أنماط أخرى؛
- والفئة الرابعة من النعوت تزود الأنظمة المختلفة بالقدرة على التصرف الدينامي بمورد من نمط معين.

ويرد وصف الفئات الثلاث الأخيرة بمزيد من التفاصيل أدناه.

وعادة ما يستخدم النمط لوصف فئة معينة من الموارد و/أو المفاهيم وفقاً لمجموعة محددة من الخصائص. وتمثل هذه الفئة ميدان قابلية تطبيق نمط ما ويدعى هذا الميدان نوع النمط. فعلى سبيل المثال، من شأن نمط تشفير الأحرف المستخدم لتحديد كيفية تمثيل حرف في نسق اثنيني أن يمتلك نوع تشفير. ومن شأن نمط إنساق البيانات المستخدَم لتحديد كيفية تمثيل هيكل كمجموعة من البتات أن يمتلك نوع إنساق.

وسيشمل كل وصف لنمط نعتاً يحدد نوعه. ويوفر نعت وصف نوع النمط خطة تصنيف بسيطة من شأنها أن تقيِّس وضع أنماط جديدة وتساعد مستخدمي الأنماط على اكتشاف الأنماط القائمة. ونوع النمط هو في نمط حد ذاته ويمكن إضافة أنواع نمط جديدة حسب الحاجة لتوسعة تصنيف النمط.

ولإعادة استخدام الأنماط إلى أقصى حد والتقليل من إنشاء النسخ المزدوجة إلى أدنى حد، سيتمكن كل نمط من وصف نفسه بدلالة الأنماط القائمة. فعلى سبيل المثال، إذا ما احتاج نمط جديد لتوضيح أن مورده مسلسل بلغة XML، ينبغي أن يفعل ذلك بإدراج إشارة إلى نمط تسلسل XML القائم. ويمكن للأنماط أن تستفيد من أنماط أخرى بالتوسعة أو بالحالات الملموسة.

وينبغي أن يشمل كل نمط أي وكل نمط من الأنماط التي يستفيد منها وكيفية الاستفادة. وقدرة الأنماط على تعريف نفسها بدلالة أنماط أخرى لن تحد من ازدواجية الأنماط فحسب، بل ستسمح للمستخدمين أيضاً بتحديد فهمهم لنمط معين بمدى أوسع من الجزئيات.

وأخيراً، ينبغي لوصف النمط أن يمكّن الأنظمة المختلفة من اكتساب القدرة دينامياً على التصرف بأي مورد مكتوب. وينبغي أن يتضمن وصف النمط نعوتاً تحدد موقع ارتباطات و/أو تطبيقات وحدات محددة لخدمة الشبكة، ومنصاتها، والسطوح البينية المرتبطة بها. وسيسمح ذلك لمكتبة معالجة الأنماط العامة بالارتباط الدينامي والآمن بهذه الخدمة، أو بالحصول على وحدة التطبيق ذات الصلة بالنمط وتحميلها وتشغيلها، ومعالجة المورد.

وينفرد كل نمط من الأنماط، وفق البحث أعلاه، بهوية تعرفّه. ولدى استخراج معرفات هوية تلك الأنماط في نظام استخراج محدد مسبقاً، سيُستخلص قيد نمط. ويرد مثال على ترميز BNF لقيد نمط في التذييل II الذي يعرّف من ناحية المفاهيم مجموعة من الكيانات التي تشكل قيد النمط هذا.

وتلزم في الحد الأدنى أربعة أقسام لتعريف النمط تعريفاً متماسكاً لا لبس فيه، وهي: الوصف والمنشأ والنوع والمعالجة.

وقسم الوصف هو تسلسل من واحد أو أكثر من أوصاف قابلة للقراءة بشرياً تحدد غرض واستخدام النمط من بين أمور أخرى. واللغة، التي قد تتوافق مع طلب التعليقات [b-IETF RFC 1766]، والتي تصاغ منها تلك الأوصاف، يتعين أن تمثّل تمثيلاً فريداً بنمطها وأن تسبق الأوصاف.

ويصف المنشأ بيانات الإنشاء، وتاريخ التعديل الأخير، والمساهمين، والأسماء المستعارة (أو معرفات الهوية البديلة)، والحالة. وينبغي أن تتوافق التواريخ مع معيار [ISO 8601]. والمساهمون هم أسماء أفراد أو منظمات ساهمت في إنشاء أو تسجيل نمط في سجل أنماط معين. وتوصَف الأسماء المستعارة للإشارة إلى تسجيلها المسبق في غيرها من سجلات النمط المحلية المعلنة هنا لأغراض إنشاء سياق النمط المعرَّف. وتحدد الحالة ما إذا كان النمط مستخدَم أو ملغى أو تجاوزه الزمن.

ويصف النوع جوهر النمط. وتعريف أنماط جديدة تقوم على تلك القائمة هو تفكير سديد وهو المفتاح لتعريف الأنماط المعقدة. وتتمثل الفكرة الأخيرة بشأن الأنواع في تحديد ما إذا كانت معلومات النوع تعتبر لبنة لتعريف أنماط أخرى أو إنها تعرِّف مظهراً خاصاً من نمط. فعلى سبيل المثال، يُعتبر نمط التشفير الاثنيني في حد ذاته لبنة تسمح بتعريف أنماط أخرى.

ويمكن تمرير المعلومات إلى خدمة تعرف كيف تحلل معلومات النمط وتعالجها. ويستدعي العملاء الخدمة لتركيب المعلومات المعطاة. وينبغي لتعريف الخدمة أن يحدد مكان الوصول إلى الخدمة وكيفية استدعائها والنتائج المتوقعة من تلك الخدمة. ولا يوصى بترميز خاص لتعريف هذه الخدمة.

9 الاتحاد التراتبي والاتحاد بين النظراء

في النهج التراتبي، يُستخدم السجل الرئيسي في تتبع المعلومات المحفوظة في سجلات متعددة من باب الاستقراب، فلا يلزم إلا الرجوع لسجل واحد. ويمكن أن تتعدد السجلات الرئيسية، ولكن يجب أن تكون جميعها معروفة ومستشارة لإجراء بحث كامل.

وفي نهج التبادل بين النظراء، تختار بعض السجلات إقامة علاقة نظراء مع سجلات أخرى منتقاة. وتختلف أسباب ترتيبات التبادل بين النظراء المختارة. وسياسات المنظمة المحيطة بإدارة السجلات، وسياسات الثقة التي تحظر أو تدعم اتحاد نقاط التماس بين السجلات، وتيسر/موثوقية السجلات المشاركة في شبكة التبادل بين النظراء، هي بعض الأسباب التي يمكن أن تحدد السجلات التي يختارها سجل ما لإقامة علاقة نظراء معها.

غير أن التشكيلين التراتبي وبين النظراء كليهما ينطويان على طوبولوجيا الاتحاد ليس إلا، ولا يحددان مستوى التجميع المختار لأحد السيناريوهات. وفيما تتوفر مجموعة متنوعة من مستويات التجميع القابلة للتطبيق، يُستشهد بمثالين محددين أدناه لأغراض التوضيح. ويسلط الجدول 1 الضوء على إيجابيات (يشار إليها بعلامة زائد) وسلبيات (يشار إليها بعلامة ناقص) نظامي الاتحاد إما عند تجميع كيانات البيانات الشرحية تماماً ومسبقاً أو عند نشر الاستعلامات في الوقت الفعلي عبر السجلات في استجابة لاستعلام من نظام إدارة الهوية.

الجدول 1

	الاتحاد التراتبي	الاتحاد بين النظراء
تجميع كامل لكيانات البيانات الشرحية في السجل الجامع	+ تحقق اكتشاف كامل عبر الميدان من خلال عملية التجميع التام + صلة مضمونة للمعلومات المتحققة عبر الميدان من خلال تقييس كيانات البيانات الشرحية أثناء التجميع + كفاءة الأداء بفضل البحث والاستخلاص محلياً – تشكيلة يتعذر تغييرها. وتتطلب عمليات إعداد دقيق قد تتعارض مع سياسات المنظمة – نقاط تعطل واحدة، إما في المجمع الرئيسي، أو في المجمعات الوسيطة – إمكانيات إدراج معلومات ولّى عهدها جراء بطء معدلات تجديد التجميع – إشكالات محتملة في السعة الاستيعابية على أعلى مستوى من التسلسل التراتبي	+ يسمح بالتجمعات المرنة غير الجامدة، التي تلبي احتياجات مجالات اهتمام محددة + غياب نقاط التعطل الواحدة بفضل إمكانية تمكين مسيرات متعددة للاتحاد + صلة مضمونة للمعلومات المتحققة عبر الميدان من خلال تقييس كيانات البيانات الشرحية أثناء التجميع + كفاءة الأداء بفضل البحث والاستخلاص محلياً – لا ضمان لاكتمال الاكتشاف عبر الميدان، ما لم يكن التشكيل موصولاً بالكامل – لزوم جهود عالية التكلفة للتخلص من الازدواجية عند تمكن السجلات من الاتحاد عبر مسيرات متعددة – مخاوف أمنية ما لم تكن جميع نقاط التماس موثوقة.
انتشار الاستعلام عبر السجلات	+ مواكبة الكيانات والمعلومات في هذه الكيانات لآخر المستجدات + نظام ذو سعة استيعابية – لا ضمان لاكتمال الاكتشاف عبر الميدان، بفعل عدم التوفر المرجح لعقد السجل في وقت انتشار الاستعلام – الإخلال بترتيب النتائج بسبب دمج فترة التنفيذ للنتائج – تشكيلة يتعذر تغييرها. وتتطلب عمليات إعداد دقيق قد تتعارض مع سياسات المنظمة – نقاط تعطل واحدة، إما في عقدة السجل الرئيسي، أو في عقد السجل الوسيطة التي تنشر الاستعلامات هبوطاً وتدفع النتائج صعوداً – إشكالات في الأداء جراء عدم متانة العتاد المستخدم لنشر السجل	+ مواكبة الكيانات والمعلومات في هذه الكيانات لآخر المستجدات + نظام ذو سعة استيعابية – لا ضمان لاكتمال الاكتشاف عبر الميدان، بفعل عدم التوفر المرجح لعقد السجل في وقت انتشار الاستعلام حتى بوجود مسيرات الاتحاد الرديفة – الإخلال بترتيب النتائج بسبب دمج فترة التنفيذ للنتائج – لزوم جهود عالية التكلفة للتخلص من الازدواجية عند تمكن السجلات من الاتحاد عبر مسيرات متعددة – إشكالات في الأداء جراء عدم متانة العتاد المستخدم لنشر السجل

تدعم برمجيات السجل وتتيح توليفات مختلفة من المصفوفة المبينة في الجدول 1. وتشكل بعض التوليفات تحديات في التنفيذ أكثر من غيرها. وتعالَج قضايا السعة الاستيعابية باستخدام تكنولوجيا المستودع التي تضفي طابعاً تجريدياً على أنظمة الحفظ الفعلية، وتسمح بالاستخدام المتزامن لأنظمة حفظ متعددة. ويوفّر أيضاً استنساخ السجلات وموازنة حمولتها، مما يخفف من مشكلة السعة الاستيعابية. وكشف النُسخ المكررة الذي من شأنه أن يشكل مشكلة في العلاقات بين العديد من السجلات والعديد الآخر منها، يمكن التخفيف منه إلى حد كبير من خلال استخدام معرفات الهوية الثابتة.

ويفترض تجميع البيانات، على العكس من الاستعلام الموزع، أن السجل الذي يبادر بحركة قيود البيانات الشرحية يقوم بدفعها، بدلاً من الاستجابة لطلبات وردت. ويشار كذلك إلى السجل المورِّد للقيود بالمصدر ويشار إلى المتلقي بالمتلقي. وفي الاتحاد، يكون المتلقي نقطة التماس لنظام السجلات المتحدة. ويعيد سجل المصدر تسيير التغييرات المنفذة بنجاح في بيانات شرحية إلى المتلقي، ومن أمثلة هذه التغييرات إنشاءات أو تنقيحات قيود البيانات الشرحية. وتشمل تلك المعاملات تغييرات حالة كيان، أي إنشاء علاقات وتعديلها وإسناد اسم مستعار إليها وحذفها، وكذلك إضافتها/ إزالتها / الاستعاضة عنها. وكل قيد تسجيل يقدَّم إلى السجل يترجَم إلى إجرائي تسجيل وإزالة تسجيل داخلٍ مركز السجل. وكل إجراء من هذا القبيل هو معاملة تمتلك معرف هوية المعاملة – وهو رقم يتصاعد عادة بدءاً من الصفر. ويسري هذا النهج بالتساوي على السيناريوهات التي ترتَب فيها السجلات بطريقة التبادل بين النظراء، وكذلك بالطريقة التراتبية.

وإذ تشكَّل فرادى السجلات لاستهداف الاستعلامات ونشرها إلى سجلات مختارة، سواء كان التشكيل تراتبياً أو بين النظراء، تُفعَّل انتشارات الاستعلام. وفضلاً عن دعمها لسطوح بينية خاصة بمجتمعات معينة، تدعم سجلات كيان رقمي أيضاً بروتوكول السطح البيني لكيان رقمي كسطح بيني مسبق يمكن تغييره. ويمكن نشر الاستعلامات إلى السجلات الأخرى على أساس استخدام هذا البروتوكول.

التذييل I

سيناريوهات الاستخدام

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

لتوضيح استخدام نظام السجلات المتحدة، يُستشهد ببضعة سيناريوهات مفيدة. ويرد وصف بضعة سيناريوهات أدناه مع نعوت ممكنة تحتاج لأن تسجَّل لتمكين السير المقبول لعملية (عمليات) الاكتشاف.

- يود عميل، إما إنسان أو آلة، أن يحصل على الخدمة من مقدم خدمة في شبكة الإنترنت. فيتطلب مقدم الخدمة إثبات هوية ويقبل بيانات اعتماد الهوية من أي مجموعة من مقدمي الهوية. ويجب على العميل (البرمجيات عموماً) أن يكون قادراً على تحديد مقدمي الهوية المقبولين، وما إذا كان العميل يملك بالفعل أو لا يملك بيانات الاعتماد ذات الصلة من واحد أو أكثر من مقدمي الهوية المقبولين، وكيفية الحصول عليها إن لم تكن في حوزته.

  ويجب على مقدم الخدمة أن يعلن عن مقدمي الهوية المقبولين في الخدمة (الخدمات) ذات الصلة. ويمكن القيام بذلك إما مباشرة من جانب مقدم الخدمة بطريقة مقيَّسة، أو بالرجوع إلى السجل بطريقة مقيَّسة أيضاً. وفي كلتا الحالتين، يجب التعرف على مقدمي الهوية وفق هوياتهم الدقيقة التي ينفردون بها. ويمكن للعميل حينئذ أن يفي بالمتطلبات الحالية للمشاركة في منظمة مقدم الهوية أو أن يكون على علم خلاف ذلك بكيفية تلبية متطلبات مقدمي الهوية، وتقديم بيانات الاعتماد ذات الصلة إلى مقدم الخدمة. وفي حالة الإعلان المباشر من جانب مقدم الخدمة، مشفوعاً بهوية فريدة ودقيقة لمقدم (مقدمي) الهوية ذي الصلة، وقدرة العميل على تقديم بيانات اعتماد خاصة بمقدم الهوية، لن تكون هناك حاجة للسجل. ولكن في جميع الحالات الأخرى، لا بد من أن يكون مستوى معين من المعلومات عن مقدمي الهوية المقبولين قابلاً للاكتشاف. ويمكن السعي مباشرةً للعثور على معرف هوية فريد وثابت في سجل تفاصيل مقدمي الهوية. ولتلبية متطلبات سيناريو الاستخدام هذا، يتعين على البيانات الشرحية التي تصف مقدم هوية معيناً أن تزود العملاء بالمعلومات اللازمة لتحديد ما إذا كان مقدم الهوية هذا خياراً معقولاً في استخدامهم لخدمة معينة. وتشمل النعوت ذات الصلة المعرف الفريد الثابت لمقدم الهوية نفسه، لإمكانية الإحالة المرجعية من أجل استعراض المواقع وأطر الثقة التي يشارك فيها مقدم الهوية مثلاً، وتشمل كذلك السياسات والإجراءات والمتطلبات القانونية، والبرمجيات المطلوبة، وأي جداول رسوم، وما إلى ذلك. وتأتي بعض هذه المعلومات في شكل المستوى الثاني للمصدر غير المباشر، فمثلاً تحدد مشاركة مقدم هوية معين في واحد أو أكثر من أطر الثقة المعرَّفة العديد من التفاصيل التقنية والسياساتية عنه.

- والتفاصيل نفسها التي تسمح للعميل باكتشاف مدى ملاءمة مقدم الهوية من شأنها أن تسمح أيضاً لمقدم الخدمة باكتشاف واحد أو أكثر من مقدمي الهوية ممن تُقبل بيانات اعتمادهم، فيضافون بالتالي إلى قائمة مقدمي الهوية المقبولين لديه. ومن شأن البيانات الشرحية لمقدم الهوية أن تشمل كلتا حالتي الاستخدام هاتين.

- وعلى النقيض من السيناريو الأول، يقوم عميل بالنفاذ إلى خدمة ويقدم بيانات اعتماد هوية لم تعهدها الخدمة قبلئذ. وعلى افتراض أن هذا التقديم لبيانات الاعتماد إلى مقدم الهوية يتكون من معرف هوية أو يُستهل بمعرف هوية يجب أن تقرر الخدمة ما إذا كانت ستقبل أو لا تقبل بيانات الاعتماد، أو تواصل استقصاء إمكانية قبول مثل هذا الاعتماد، أو مجرد أن ترفضه دون مزيد من التحقيق. وسيتعين على السجل، في هذا السيناريو، اكتشاف معلومات عامة عن نمط معرف الهوية ومقدم الهوية الذي يمثله. ويمكن لذلك بدوره أن يؤدي إلى مزيد من عمليات البحث في السجل عن التكنولوجيات المحددة التي يستخدمها مقدم الهوية، بما في ذلك أطر الثقة ذات الصلة.

- وتكون عادة مختلف الكيانات المشاركة في إدارة الهوية، إما صراحة أو ضمناً، أعضاء في واحد أو أكثر من أطر الثقة أو نظام آخر لإدارة الهوية. وسيلزم توصيف نعوت كل نظام لإدارة الهوية من أجل إنشاء مخطط البيانات الشرحية التي تصف إطار الثقة هذا. وتبرز عدة أسئلة هامة هنا. هل نظام إدارة الهوية الموصوف من المنظمة التي توفره، هو مجموعة من المعايير التي تنفذه، ووسيلة لقياس الالتزام بالمعايير، وما إلى ذلك؟ وبغض النظر عن الإجابة عن هذه

الأسئلة، يتضح أن من شأن بعض مقدمي الهوية، وحتى بعض الأطراف المعولة، أن توصَل بشكل مفيد بأوصاف على مستوى أعلى، مثل منظمات InCommon وKantara وSafe-BioPharma وOIX التي يمكن اكتشافها ضمن السجل أو اتحاد السجلات.

وفي الشكل I.1، نوضح سبيلاً يمكن فيه استعمال نظام سجلات متحدة ("النظام") وفق سيناريو استخدام محدد.

الخطوة 1: في هذا المثال يطلب المستخدم النهائي خدمة من طرف معول.

الخطوة 2: يستجيب الطرف المعول بهوية واحد أو أكثر من أطر الثقة التي يثق بها الطرف المعول، وفي هذه الحالة – إطار ثقة واحد (TF1).

الخطوة 3: يذهب المستخدم النهائي إلى النظام بمعرف هوية الإطار TF1.

الخطوة 4: يستجيب النظام بالقيد ذي الصلة بالإطار TF1. وتتضمن المعلومات لإطار TF1 الحد الأدنى من النعوت التي ستلزم للثقة ضمن ذلك الإطار.

الخطوة 5: يقيّم المستخدم النهائي الحد الأدنى من تلك المتطلبات للوقوف على إمكانية كسب ثقة الطرف المعول. ونفترض هنا أن تقييم المستخدم النهائي إيجابي ويدل على قدرته على تلبية الحد الأدنى من النعوت، كرخصة قيادة السيارات على سبيل المثال.

الخطوة 6: يمكن للمستخدم النهائي الآن أن يعود إلى النظام طالباً مقدمي الهوية الواقعين ضمن إطار TF1 الذي يمكن أن يستوعب البروتوكول (البروتوكولات) الذي يدعمه المستخدم النهائي، مثل HTTP والبريد الإلكتروني، ونعرضه هنا كمجرد بروتوكول X.

الخطوة 7: يجد النظام مقدمي الهوية المطابقين لبروتوكول X ضمن إطار TF1.

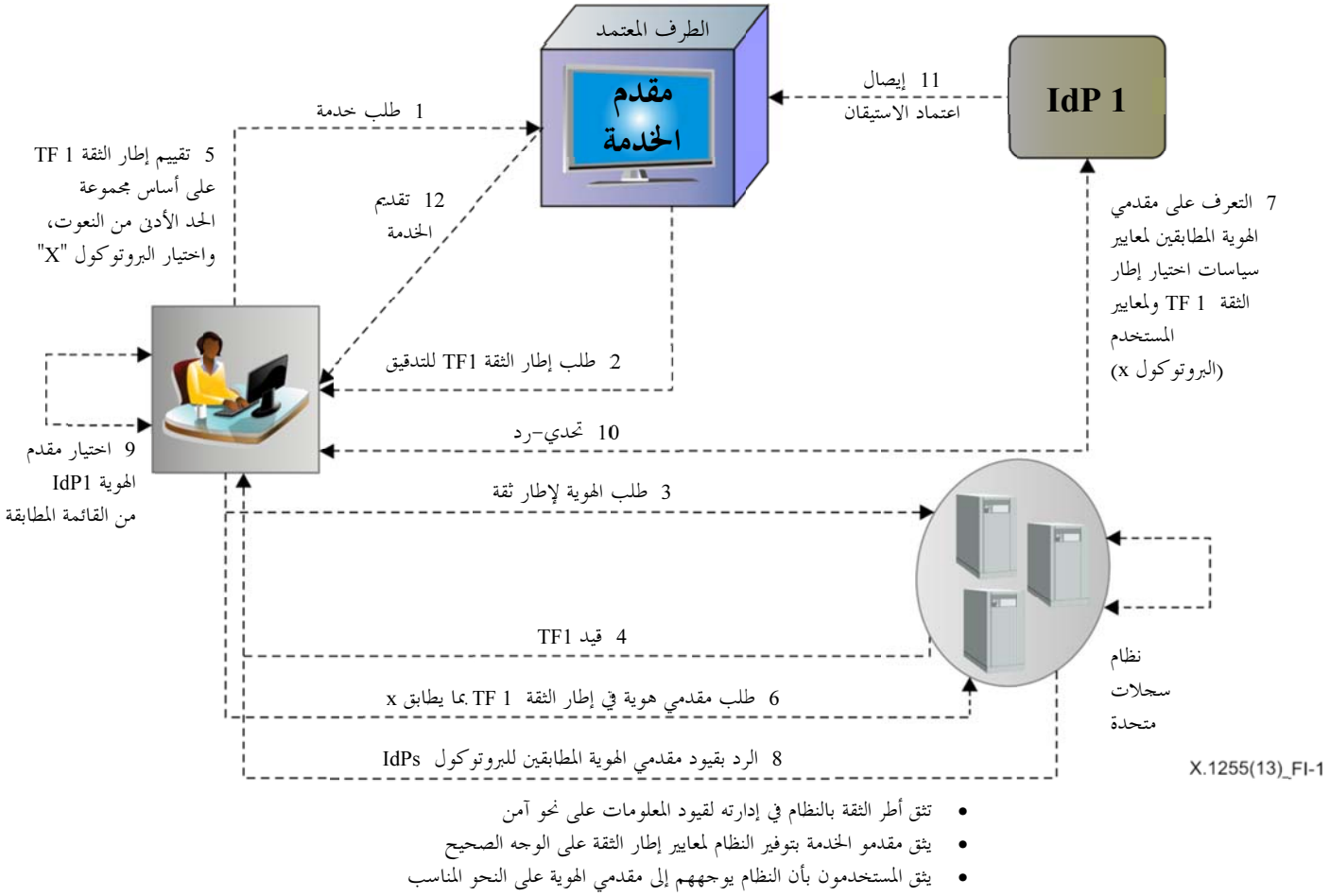
الخطوة 8: ويستجيب هذا النظام للمستخدم النهائي بمجموعة من مقدمي الهوية تتطابق مع متطلبات الطرف المعول والمستخدم النهائي كليهما.

الخطوة 9: يقوم المستخدم النهائي بتقييم مجموعة من مقدمي الهوية مرسَلة من النظام في رده ويقع اختياره على أحدهم (IdP1).

الخطوة 10: وإذ يحصل المستخدم النهائي على النعوت المطلوبة من مقدم الهوية IdP1 ويخاطب ببروتوكول يفهمه مقدم الهوية IdP1، يتفاعل مع مقدم الهوية IdP1 بإرسال تحدٍ وانتظار الرد.

الخطوة 11: يؤدي نجاح تفاعل التحدي/الرد إلى قيام مقدم الهوية IdP1 بإيصال اعتماد الاستيقان إلى الطرف المعول.

الخطوة 12: الطرف المعول، الذي يثق الآن بالمستخدمين النهائيين، يقدم الخدمة المطلوبة.



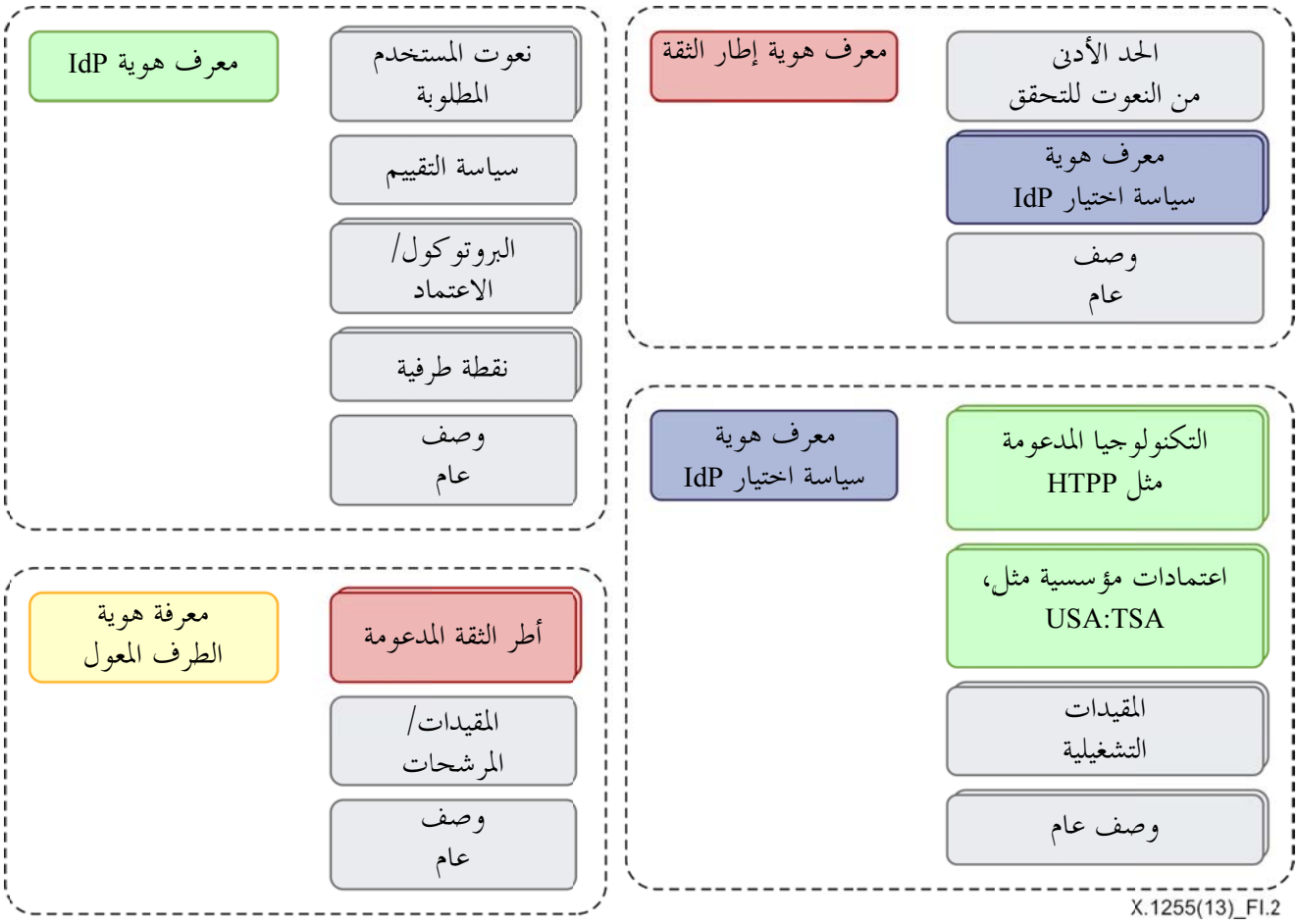
- تثق أطر الثقة بالنظام في إدارته لقيود المعلومات على نحو آمن
- يثق مقدمو الخدمة بتوفير النظام لمعايير إطار الثقة على الوجه الصحيح
- يثق المستخدمون بأن النظام يوجههم إلى مقدمي الهوية على النحو المناسب

الشكل 1.I – استيقان ينطوي على أطر الثقة

في الشكل 2.I نبين المخططات رفيعة المستوى للقيود التي يحتفظ بها نظام السجلات المتحدة والتي من شأنها أن تمكّن التفاعل الموضح في الشكل 1.I وكذلك سيناريوهات الاستخدام الأخرى المذكورة أعلاه. وسيحفظ النظام هذه القيود ككيانات الرقمية يزوَّد كل منها بمعرف هوية ثابت. وسيتواصل إدخال التحسينات على كل منها ضمن مخططات محددة لتأهيلها لتنفيذ أي من النماذج الأولية.

ولكل إطار ثقة معرف هوية، ووصف عام للإطار، ومجموعة من النعوت المستخدمة للاستيقان، ومؤشرات إلى واحدة أو أكثر من سياسات انتقاء مقدم الهوية، وهذه هي نفسها كيانات رقمية منفصلة محفوظة في النظام. وهي بمثابة مستوى إضافي للمصدر غير المباشر بحيث يمكن تصنيف كل مقدمي الهوية الذين يتسعون ضمن إطار ثقة واحد وفقاً لمعايير بدلاً من التعداد. ويمتلك كل كيان من كيانات سياسة اختيار مقدم الهوية معرف هوية، ووصفاً عاماً، وقائمة بالتكنولوجيات مقبولة (مثل البروتوكولات المدعومة)، وقائمة هيئات الاعتماد المؤسسية، (منظمة حكومية مثلاً)، وأي مقيدات تشغيلية خاصة. وتكون العلاقة بين أطر الثقة وسياسات اختيار مقدم الهوية من جهات عديدة إلى جهات عديدة في كلا الاتجاهين، أي يمكن لإطار ثقة معين أن يستوعب سياسات متعددة لاختيار مقدم الهوية، ويمكن لأطر ثقة متعددة أن تتبع سياسة معينة لاختيار مقدم الهوية.

والنمطان المقترحان الباقيان للكيان الذي يحفظه النظام هما مقدمو الهوية والأطراف المعولة. ويمتلك كل مقدم الهوية معرف هوية ثابت، ووصفاً عاماً، ونعوت المستخدم المطلوبة، وسياسة تقييم لتلك النعوت، وبروتوكولات محددة واعتمادات مقبولة، ونقاط طرفية محددة، مثل موقع مقدم الهوية في شكل البروتوكولات المقبولة. ويمتلك كل طرف معول معرف هوية ثابت، ووصفاً عاماً، ومجموعة من أطر الثقة التي يعتمد عليها، وأي مقيدات تشغيلية محددة.



الشكل 2.I – مخططات رفيعة المستوى

التذييل II

ترميز BNF لقيد نمط

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يتمثل ترميز BNF لقيد نمط كما يلي:

```
<type identifier> := <unicode string>
<type> := <description section> <section delimiter>
    <provenance section> <section delimiter>
    <genre section> <section delimiter>
    <processing section>
```

```
<description section> := <language> '=' <human readable description>
[<repetition delimiter> <description section>]
<language> := Any item from RFC 1766
<human readable description> := <unicode string>
```

```
<provenance section> := <creation date> <list delimiter>
<last modified date> <list delimiter>
<contributors> <list delimiter>
<aliases> <list delimiter>
<status>
<creation date> := Conforms to ISO 8601
<last modified date> := Conforms to ISO 8601
<contributors> := <unicode string>
[<repetition delimiter> <contributors>]
<aliases> := <unicode string>
[<repetition delimiter> <aliases>]
<status> := 'in use' | 'deprecated' | 'obsolete'
```

```
<genre section> := <genre> '=' <genre details>
 [<repetition delimiter> <genre section>]
<genre> := 'data structure' | 'encoding' | 'format'
<genre details> := <human readable description>
 [<list delimiter> <genre subsection>]
<genre subsection> := 'form='<form> <list delimiter>
     'relationship=' <relationship> <list delimiter>
     'related to=' <type identifier>
     [<repetition delimiter> <genre subsection>]
<form> := 'expression' | 'manifestation'
<relationship> := 'is equivalent to' | 'is derived from' |
'is informed from'
```

```
<processing section> := <processor type> '=' <processor>
[<repetition delimiter> <processing section>]
<processor type> := 'network service' | 'downloadable program' | 'parsing
function'
<processor> := <network service type> '=' <network service binding> |
   <compatible platform> <list delimiter>
   <program network location> <list delimiter>
   <program arguments> |
   <pseudo code>
<compatible platform> := 'Linux' | 'Windows' | 'Mac OS'
<program arguments> := <type>
     {<list delimiter> <unicode string>}
<pseudo code> := <unicode string>
```

```
<unicode string> := <visible character> [<unicode string>] |
  <whitespace character> <[unicode string>]
<visible character> = Any visible character in Unicode presumably encoded in
UTF-8
<whitespace character> := Any whitespace character in Unicode presumably encoded
in UTF-8
```

ملاحظات:

1) يستخرج معرف <type identifier> الصادر لنظام استخراج عالمي قيدَ <type>.

2) إن جميع المحددات، وهي <section delimiter> و<repetition delimiter> و<list delimiter>، هي من تفاصيل التنفيذ المحددة و لم تعرَّف عن قصد هنا.

3) لم يعرَّف أيضاً نمط <network service type> هنا، ولكن ينبغي أن يشمل الخدمات الشائعة للشبكة حسبما تراه الوكالة المنفذة مناسباً.

4) لم يعرَّف أيضاً إسناد <network service binding> هنا، ولكن ينبغي أن يستند إلى نمط خدمة الشبكة. وينبغي ذكر التعاريف الفعلية التي تتوافق مع كل نمط من أنماط الخدمة هنا.

5) لم يعرَّف أيضاً موقع <program network location> هنا، ولكن ينبغي أن يحدد بروتوكول الشبكة الذي يتعين على العميل استخدامه لتحميل البرنامج من الشبكة.

6) يجوز توسيع منصة <compatible platform> أو توصيفها بتفاصيل أوفى من التعريف الوارد هنا.

بيبليوغرافيا

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[b-IETF RFC 1766] IETF RFC 1766 (1995), *Tags for the Identification of Languages*. <http://www.ietf.org/rfc/rfc1766.txt>

[b-DO Repo] Reilly, S. and Tupelo-Schneck, R. (2010), *Digital Object Repository Server: A Component of the Digital Object Architecture,* D-Lib Magazine, Vol. 16, No. 1/2. <http://dx.doi.org/10.1045/january2010-reilly>

[b-DOIP] Reilly, S. (2009), *Digital Object Protocol Specification*, *Version 1.0,* Corporation for National Research Initiatives. <http://hdl.handle.net/4263537/5045>

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	المطاريف وطرائق التقييم الذاتية والموضوعية
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، 2013