الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T X.1250

(2009/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

مقدرات أساسية للإدارة العالمية المعززة للهوية وإمكانية التشغيل البيني

التوصيـــة ITU-T X.1250

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.119–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

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

التوصيـــة ITU-T X.1250

مقدرات أساسية للإدارة العالمية المعززة للهوية وإمكانية التشغيل البيني

ملخص

تصف التوصية ITU-T X.1250 المقدرات الأساسية لقابلية التشغيل البيني (أي، لتحسين التبادل والثقة في معرفات الهوية للإدارة العالمية للهوية التي تستعملها الكيانات في شبكات الاتصالات/تكنولوجيا المعلومات) والخدمات. وترتبط تعاريف إدارة الهوية واحتياجاتها بالسياق إلى حدٍ بعيد، وغالباً ما تخضع لسياسات وممارسات شديدة الاختلاف في البلدان المختلفة وتشمل المقدرات حماية المعلومات المحددة القابلة للتعريف الشخصي (PII) ومراقبتها.

المصدر

وافقت لجنة الدراسات 17 (2009-2012) لقطاع تقييس الاتصالات على التوصية ITU-T X.1250 بتاريخ 25 سبتمبر 2009 بموجب إجراء القرار 1 للجمعية العالمية لتقييس الاتصالات.

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/.

المحتـــويات

الصفحة

التوصيـــة ITU-T X.1250[1]

مقدرات أساسية للإدارة العالمية المعززة للهوية وإمكانية التشغيل البيني

1 مجال التطبيق

تصف هذه التوصية المقدرات الأساسية المعززة للإدارة العالمية للهوية وإمكانية التشغيل البيني والتي تستعمل شبكات الاتصالات والخدمات العامة. وتُجمع هذه المقدرات ضمن المجالات الوظيفية التالية:

- نماذج مشتركة مهيكلة لإدارة الهوية.
- توفير النعوت (بما فيها معرف الهوية) والتفويض والمقدرات.
- اكتشاف موارد ومقدرات واتحادات مورّد خدمة الهوية.
- إمكانية التشغيل البيني فيما بين منصات الإدارة، وموردي خدمة الهوية واتحادات الموردين بما فيهم موردي جسر خدمة الهوية.
- الأمن والإجراءات الأخرى المتخذة للحد من التهديدات والمخاطر، بما في ذلك حماية ومراقبة موارد الهوية والمعلومات التي يمكن بها تعرّف هوية صاحبها شخصياً والخصوصية.
- التدقيق والمطابقة، بما في ذلك إنفاذ السياسة الأمنية وحماية المعلومات المعرّفة بهوية صاحبها شخصياً.
- الأداء والموثوقية والتيسر في مقدرات إدارة الهوية.

تتميز شبكات وخدمات الاتصالات/تكنولوجيا المعلومات اليوم بتنوعها الشديد وتوزعها الواسع وتوصيلها البيني العالي، وتتميز رغم ذلك بقدر كبير من الاستقلال الذاتي في إدارة الهوية. وبينما تتطور هذه الشبكات والمقدرات، يمكن أن يعيق حجمها وتعقيدها إمكانية تشغيلها البيني ضمن مقدرات إدارة الهوية. ولهذا السبب، تعتمد مقدرات إدارة الهوية في هذه التوصية إلى حد كبير على ما هو موجود من مقدرات شبكة ونماذج عامة، بما في ذلك أفضل الممارسات المتبعة فعلاً. ومن أجل الاضطلاع بإدارة الهوية العالمية وإمكانية التشغيل البيني، تصف هذه التوصية مسيراً للتطور وسبلاً لتوسيع المقدرات القائمة حيثما أمكن ذلك. كما تعرّف التوصية وظيفة جسر الهوية التي يمكن استخدامها في العديد من أنظمة إدارة الهوية وأشكال الدعم لإدراج المقدرات القائمة لإدارة الهوية.

ويتوقف تنفيذ مقدرات إدارة الهوية في كل بلد على المتطلبات الخاصة بالولاية القضائية الوطنية.

ملاحظة – لا يشير استعمال تعبير "هوية" في هذه التوصية فيما يتصل بإدارة الهوية (IdM) إلى معنى الهوية المطلق. وعلى وجه الخصوص، لا يشكّل المصطلح أي إثبات صلاحية إيجابي لشخص ما.

2 المراجع

لا توجد.

---

[1] قد يتعذر تطبيق هذه التوصية في بعض البلدان نظراً لتعارضها مع التشريعات المحلية.

3 التعاريف

1.3 المصطلحات المعرّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في أماكن أخرى:

1.1.3 المدعي [b-ITU-T Y.2720] و[b-ITU-T X.811]: كيان أو ممثل كيان رئيسي لأغراض الاستيقان. ويحتوي كيان مدعي على الوظائف اللازمة للدخول في تبادلات استيقان نيابة عن الكيان الرئيسي.

2.1.3 المعلومات القابلة للتعريف الشخصي (PII) [b-ITU-T Y.2720]: المعلومات المتعلقة بأي شخص حي والتي من شأنها أن تعرف هوية هذا الفرد (بما في ذلك المعلومات الكفيلة بتعرف هوية شخص عند اختلاطها بمعلومات أخرى حتى ولو لم تحدد المعلومات بوضوح هوية الشخص).

3.1.3 الطرف المعني [b-ITU-T Y.2720]: كيان معني على تمثيل أو ادعاء هوية من جانب الطرف الطالب.

2.3 المصطلحات المعرّفة في هذه التوصية

تُعرِّف هذه التوصية المصطلحات التالية:

1.2.3 الوكيل: كيان يعمل نيابةً عن كيان آخر.

2.2.3 الهوية الغفلية: خاصية تعذر تعرف الهوية ضمن مجموعة كيانات.

ملاحظة – تمنع الهوية الغفلية تتبع الكيانات أو سلوكها مثل تحديد مكان المستعمل وتواتر استعمال الخدمة وإلى ما غير ذلك.

3.2.3 النعت: معلومات تخص كياناً ما وتحدد أحد خصائص الكيان.

4.2.3 الاستيقان: انظر استيقان الكيان.

5.2.3 ضمان الاستيقان: الثقة الناتجة في عملية الاستيقان الذي يكون فيها طرف الاتصال الكيان المدعي أو المتوقع.

6.2.3 الإسناد: تصاحب أو جمع أو ربط صريح.

7.2.3 الادعاء: تصريح يتقدم به المدعي لقيمة أو قيم لنعت هوية واحد أو أكثر لموضوع رقمي تكون عادة محل نزاع أو جدل.

8.2.3 كيان: أي شيء له وجود منفصل قائم بذاته ويمكن تحديده في سياق ما.

ملاحظة – يجوز للكيان أن يكون شخصاً مادياً أو حيواناً أو شخصاً قانونياً أو منظمة أو شيئاً فاعلاً أو منفصلاً أو جهازاً أو تطبيق برمجية أو خدمة أو غير ذلك، أو مجموعة من هذه العناصر. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط النفاذ والمشتركين والمستعملين وعناصر الشبكة والشبكات وتطبيقات البرمجيات والخدمات والأجهزة والسطوح البينية وغيرها.

9.2.3 استيقان الكيان: عملية تهدف إلى تحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدمة.

10.2.3 الاتحاد: رابطة تجمع مستعملين وموردي خدمات وموردي هويات.

11.2.3 معرف الهوية: نعت واحد أو أكثر يستعمل لتعرف هوية كيان في سياق ما.

12.2.3 الهوية: تمثيل لكيان على شكل عنصر معلومات واحد أو أكثر يتيح للكيان (الكيانات) أن يكون متميزاً في سياق ما. ويعني مصطلح الهوية لأغراض إدارة الهوية هوية سياقية (مجموعة من النعوت) مثل: يتحدد تنوع النعوت بإطار له شروط حدود معرّفة (السياق) يتواجد فيها الكيان ويتفاعل.

ملاحظة – يتمثل كل كيان في هوية متكاملة واحدة تضم جميع عناصر المعلومات الممكنة التي تميز هذا الكيان (النعوت). بيد أن الهوية المتكاملة مسألة نظرية عصية على كل وصف واستعمال محلي لأن عدد النعوت الممكنة كلها لا نهائي.

13.2.3 مورد جسر خدمة الهوية: مورد خدمة هوية يعمل كوسيط بين موردي خدمة هوية آخرين.

14.2.3 إدارة الهوية: مجموعة من الوظائف والمقدرات (مثل عمليات الإدارة والصيانة والكشف وتبادل الاتصالات والربط وإنفاذ السياسة والاستيقان والتأكيد) التي تستعمل للأغراض التالية:

- ضمان معلومات الهوية (من قبيل المعرفات والإثباتات والنعوت)؛
- ضمان هوية كيان ما (من قبيل المستعملين/المشتركين والمجموعات وأجهزة المستعمل والمنظمات وموردي الشبكات والخدمات وعناصر الشبكة وأغراضها والأغراض الافتراضية)؛
- توفير تطبيقات الأعمال التجارية والأمن.

15.2.3 مورد خدمة الهوية: كيان يتحقق من ويحفظ ويدير وقد يستحدث ويخصص معلومات هوية لكيانات أخرى.

16.2.3 نموذج الهوية: تعبير هيكلي لنعوت كيان (مثال، سلوك كيان ما) قد يستعمل في بعض عمليات التعرف.

17.2.3 بيان: تمثيل لكيان من خلال رصده أو اكتشافه (مثال، دون تصريح ذاتي). (للمقارنة مع تصريح.)

18.2.3 الهوية المستعارة: معرِّف هوية يبقى ربطه مع كيان ما غير معروف أو معروف بصورة محدودة فقط في السياق الذي يستعمل فيه.

19.2.3 الكيان الطالب: كيان يقوم بتمثيل هوية أو ادعائها أمام طرف معتمَد في إطار الطلب.

20.2.3 غرض مطرافي: هو غرض (مثل بطاقة وحدة هوية المشترك (SIM)) يمكن أن يكون على علاقة مع جهاز مطراف شبكي (مثل هاتف متنقل).

21.2.3 الثقة: الاعتقاد الجازم في موثوقية وصحة المعلومات؛ أو في قدرة كيان ما على التصرف المناسب في سياق محدد.

22.2.3 المستعمل: كيان يستعمل مورداً، مثل نظام أو جهاز أو مطراف أو عملية أو تطبيق أو شبكة شركة.

23.2.3 المستعمل المركزي: نظام إدارة الهوية الذي يتيح للمستعمل القدرة على التحكم وتنفيذ مختلف سياسات الخصوصية والأمن التي تتحكم بتبادل المعلومات عن الهوية بما فيها المعلومات الشخصية بين الكيانات.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

DHCP بروتوكول دينامي لتحكم المخدم (*Dynamic Host Control Protocol*)

ID معرِّف (*Identifier*)

IdM إدارة الهوية (*Identity Management*)

IdSP مورّد خدمة الهوية (*Identity Service Provider*)

IT تكنولوجيا المعلومات (*Information Technology*)

NGN شبكة (شبكات) الجيل التالي (*Next Generation Network(s)*)

PII معلومات تعرف الهوية شخصياً (*Personally Identifiable Information*)

RFID التعرف بواسطة الترددات الراديوية (*Radio Frequency IDentification*)

SIM وحدة هوية المشترك (*Subscriber Identity Module*)

URL موقع الموارد الموحد (*Uniform Resource Locator*)

5 الاصطلاحات

لا توجد.

6 اعتبارات عامة

أفضى نمو مقدرات الاتصالات وتطورها إلى انتشار مجموعة من الخدمات الإلكترونية للمستهلكين وقطاع الأعمال والحكومة. إذ لم تعد تكنولوجيات الاتصالات القائمة على بروتوكول الإنترنت مقتصرة على كونها مجرّد مورد لتصفح المعلومات، بل أصبحت فعالية لا غنى عنها في إجراء المعاملات الإلكترونية اليومية.

تهدف المقدرات الواردة في هذه التوصية إلى دعم تطوير ونشر مقدرات إدارة هوية مهيكلة وقابلة للتشغيل البيني في إطار عام مشترك لأنظمة شبكات وخدمات الاتصالات/تكنولوجيا المعلومات كافة، بيد أن ذلك يبقى خاضعاً للسياسات الإقليمية والوطنية فيما يتعلق بالمعلومات التي تعرّف هوية صاحبها شخصياً وبالخصوصية.

وتشمل المقدرات الواردة في هذه التوصية:

أ) أمثلة لنماذج هيكلية ومشتركة لإدارة الهوية

تنطوي إدارة الهوية عادة على تبادل هوية واحدة أو أكثر بين كيانات تستخدم شبكة أو خدمة اتصالات/تكنولوجيات معلومات واتصالات. وحرصاً على الوفاء بالمستوى المرغوب لضمان الاستيقان، يقرر الأطراف أو يطلبون إرسال معلومات إضافية لبعضهم البعض أو لطرف ثالث موثوق. وقد تضم الاتصالات الأولية تعبيراً عن تفضيل عملية استيقان أو تفويض. وقد يختار أحد الطرفين أو كلاهما أن يبقى غفلاً أو أن يستعمل هوية مستعارة. ويحوز تمثيل هذه الأنواع من التبادل على شكل نماذج مشتركة يرد وصف مقدراتها في هذه التوصية. وتتيح هذه النماذج تزويد أطراف متعددة بمقدرات الهوية حسب الاقتضاء. كما أن النماذج مهمة في تطبيق مقدرات إدارة هوية قابلة للتشغيل بينياً ترد وتتوفر في شبكات من قبيل شبكات الجيل التالي.

ب) توفير وحماية مقدرات الإثباتات والمعرفات والنعوت والنماذج مع الحفاظ على مستويات ضمان معروفة

وتشترك جميع أنشطة إدارة الهوية بفئات معلومات للهوية هذه وتوفيرها وصيانتها واستعمالها وإلغائها و/أو حمايتها.

ج) كشف عن موارد ومقدرات واتحادات مورد خدمة الهوية

من أهم التحديات التي تواجه إدارة الهوية في عالم دينامي ومتنوع لمقدرات الشبكات وتطبيقاتها هو الكشف عن مصادر الهوية والخدمات التي تقدمها غالباً ما تكون مقدرات الكشف ضرورية لاستيفاء مستويات الضمان المطلوبة.

د) قابلية التشغيل بين منصات الهوية ومورديها واتحاداتها بما فيها مورد خدمة الهوية الوسيط

في ظل بنية تحتية واسعة الانتشار للشبكات العامة والمقدرات ومع العدد الكبير لمستعملي وموردي الاتصالات الجوالة، قد تنطوي إدارة الهوية على أعداد فائقة من الاستفسارات والردود بين الأطراف والاتحادات المختلفة التي تعمل فيها. وقابلية التشغيل البيني عالمياً بين الأطراف التي تزود بمقدرات إدارة الهوية أمر أساسي ويضم بروتوكولات مشتركة لوضع الاستفسارات لمقدرات الهوية.

هـ) الأمن وتدابير أخرى للتخفيف من تهديدات ومخاطر الهوية بما فيها مراقبة موارد الهوية ومعلومات تعرف الهوية شخصياً

نظراً لأن معلومات تعرف الهوية ومواردها مكونات هامة وحساسة وحاسمة في الشبكات، وخاصة تلك التي تشكل جزءاً من البنية الأساسية الوطنية الهامة وتؤثر على الخصوصية الشخصية، فإن معلومات وموارد تعرف الهوية تتطلب حماية الأمن القائمة على تحليل مخاطر بيئة إدارة الهوية.

و) التدقيق والامتثال ومنها إنفاذ السياسات وحماية معلومات تعرف الهوية شخصياً

يخضع توفير إدارة الهوية عموماً لعدة متطلبات قانونية وتنظيمية وحكومية وتجارية تستدعي مستوى من مقدرات التدقيق والامتثال. وهذه المقدرات واسعة التنوع وتضم التدقيق في الامتثال للأحكام التنظيمية، وتدابير لحماية المعلومات الشخصية وتنبيهات المستهلك والحفاظ على دقة إشارات التوقيت المناسبة وإمكانية التتبع.

ز) قابلية الاستعمال والتعميم: الأداء والاعتمادية والتيسر والطابع الدولي والاستعادة بعد الكوارث

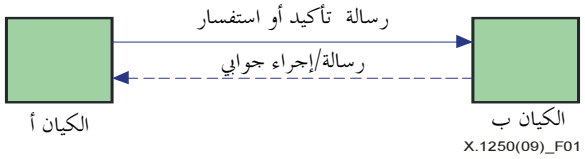
مقدرات إدارة الهوية قابلة للاستعمال والتعميم من أجل استعمالها في سياق التطور الدائم والشامل لأنظمة الهوية. ونظراً لأن معلومات وموارد تعرف الهوية الذي تبني على أساسه تستيقن الكيانات من بعضها البعض، كأن تقبل بعضها البعض الآخر بوصفها شركاء في الاتصال، فغالباً ما تكون عناصر من البنية التحتية الهامة وتتطلب التقيد بمستوى معين من مقدرات الأداء والاعتمادية والتيسر والمقدرات.

7 مقدرات الإدارة العالمية للهوية وإمكانية التشغيل البيني

تقدم هذه الفقرة أمثلة لنماذج ممكنة لإدارة الهوية، وتضع مجموعة من مقدرات قابلة للتشغيل بينياً لإدارة الهوية ومن المكونات الأساسية للهوية. كما تناقش هذه الفقرة اكتشاف مقدرات الهوية وقابلية التشغيل البيني ومد الجسور وضمان أمن إدارة الهوية والحماية ومراقبة واستعمال المعلومات المحددة شخصياً (PII) والتدقيق والامتثال. ويستعرض العمل أيضاً الطابع الدولي والأداء والموثوقية والتيسر.

1.7 أمثلة لنماذج ممكنة لإدارة الهوية

من المعاملات الأولية في إدارة الهوية، عملية الاستفسار والرد البسيطة التي تشترك فيها معظم عمليات تبادل المعلومات كما يبين الشكل 1. ويتمثل أبسط شكل من تبادل الرسائل في طرفين يستعملان بروتوكولاً ونموذج معلومات متفق عليهما.

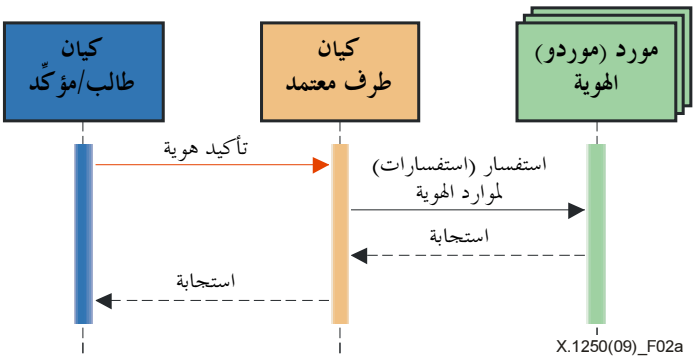


الشكل 1 – عملية الاستفسار والرد لتبادل المعلومات

يمكن للأطراف المشاركة في هذه العملية أن تكون أي نوع كيان. والكيان يمكن أن يكون شخصاً أو حيواناً أو شخصاً اعتبارياً أو منظمة أو غرضاً فاعلاً أو منفصلاً أو جهازاً أو تطبيق برمجية أو خدمة وغيرها أو مجموعة من هذه العناصر. وفي سياق أمثلة الاتصالات للكيانات تدرج نقاط النفاذ والمشتركون والمستعملون وعناصر الشبكة والشبكات وتطبيقات البرمجيات والخدمات والأجهزة والسطوح البينية وغيرها. ويمكن أن يكون الكيان أي غرض مادي أو افتراضي مثل تجهيزات الشبكة أو البرمجيات أو أجهزة المطراف أو أجهزة الاستشعار أو الأغراض المادية الموسومة وسماً فاعلاً (مثلاً باستعمال تقنيات RFID أو الشفرات البصرية) أو الأغراض الموسومة وسماً منفعلاً. فعلى سبيل المثال، يمكن التعامل مع أجهزة الشبكة ككيانات خاضعة لمقدرات خاصة من إدارة الهوية نيابة عن مستعملين نهائيين وسلطات حكومية. وفي سياق إدارة الحقوق الرقمية، يمكن أن يكون الكيان ملكية فكرية أو مادة محمية بأحكام حقوق النشر، من قبيل محتوى متعدد الوسائط أو محتوى تلفزيوني قائم على بروتوكول الإنترنت (IPTV). والنوع الخاص من الهوية هو المجموعة. وهوية المجموعة هي تقاطع النعوت المشتركة لهويات أعضاء مجموعة ما.

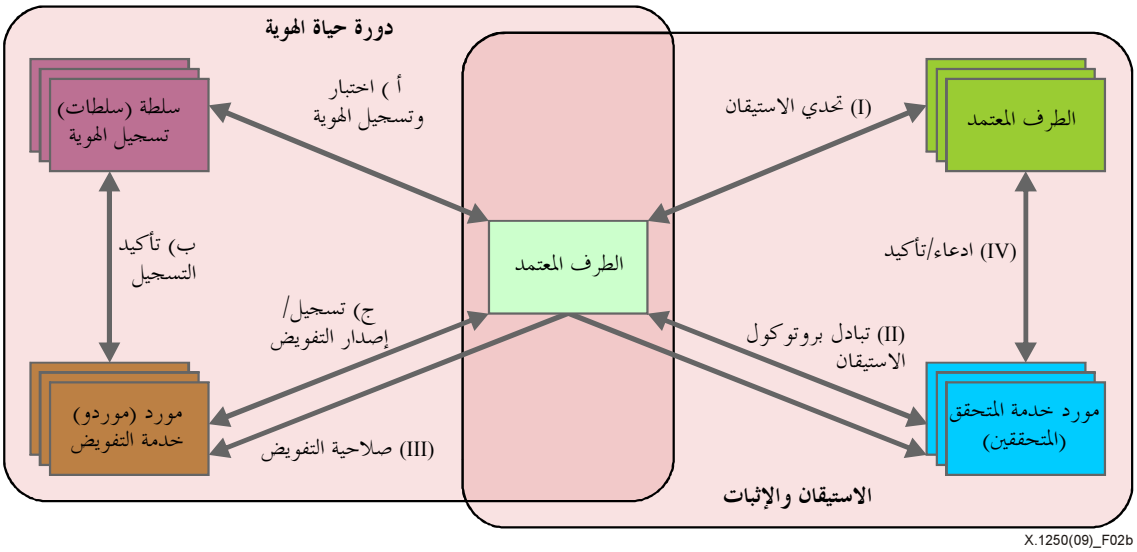
وينطوي استعمال إدارة الهوية في معظمه على نماذج معقدة. فمثلاً، حيثما لا يكون الطرف المعتمد، الذي يتلقى الادعاء في الأصل مورد خدمة هوية، تنفصل وظيفة مورّد خدمة الهوية عن الطرف المعتمد وتتمايز عنه، كما يبيّن الشكل 2 أ أو 2 ب. ويقيِّم الطرف المعتمد الإجابات الواردة من مورد (موردي) خدمة الهوية والحكم على كفاية مستوى التأكد من استيقان الكيان. والوظيفة الأولى لمورد خدمة الهوية هو إدارة وضع معلومات الهوية وتحديثها والتحقق منها وتعليقها وإلغائها.

وهنالك العديد من نماذج تبادل معلومات الهوية. أحد النماذج شائعة الاستعمال هو نموذج الاستفسار الرد ثلاثي الأطراف المبين في الشكل 2 أ. وتستند بعض البروتوكولات الجديدة المفتوحة لإدارة الهوية إلى هذا النموذج.



الشكل 2 أ – مثال عن نموذج إدارة الهوية ثلاثي الأطراف

ويصور الشكل 2 ب نموذجاً آخر لإدارة الهوية يتيح للطرف الطالب مزيداً من التحكم في علاقات الهوية.



الشكل 2 ب – مثال لنموذج خماسي الأطراف ويتمركز على المستعمل لإدارة الهوية

وتحظى النماذج "المتمركزة حول المستعمل" (أي التي تتطلب تفعيل مراقبة كامل الطرف الطالب عند استعمال الهويات) باهتمام كبير وقد يصبح إلزامياً أيضاً في الولايات القضائية الوطنية والإقليمية. ويقدم الشكل 2 ب مثالاً يعرض فيه موردو خدمة مختلفون أدواراً ومقدرات متخصصة لإدارة الهوية. وتمر جميع الاستفسارات/الردود عبر الطرف الطالب. ولأغراض هذه الأنواع من النماذج، تتحدد الكيانات على النحو التالي:

- **مورد الهوية:** وهو كيان يصون ويدير وقد يستحدث معلومات هويات موثوقة لكيانات أخرى (مثل: مستعمل نهائي ومنظمات وأجهزة) وتقدم خدمات قائمة على الهوية. وهذا الكيان المسؤول عن تخصيص نعوت الهوية

وإصدارها (أي هوية لمشترك إلى مورّد تفويض في سياق محدد) مثلاً وإدراجها أيضاً). مسؤول عن إدارة دورة حياة الهوية التي تشمل التحقق من الهوية وتسجيلها وحفظها وكذلك إلغاءها.

- **مورّد خدمة التفويض**: الكيان الذي يقدم المقدرات المتصلة بإصدار الإثباتات والأذون (مثل الإثباتات التي تسند الأذون إلى معرفات ونعوت أخرى يمكن التحقق منها).
- **مورّد خدمة التحقق**: الكيان الذي يقدم مقدرات تقدير معلومات هوية (مثل الادعاءات والأوراق الثبوتية) و يصنفها حسب صلاحيتها.
- **الطرف المعتمد** [b-ITU-T Y.2720]: كيان يعتمد على تمثيل هوية أو ادعائها من خلال طلب/تأكيد كيان في سياق طلب ما.

ويمكن تجميع تدفق المعلومات عموماً ضمن فئتين رئيسيتين:

أ) دورة حياة الهوية

- **تسجيل الهوية وإثباتها (أي إدراجها)**: يمثل تدفق المعلومات افتتاح هوية في سياق محدد مثل عمليات التسجيل والتثبت المصاحبة لتخصيص نعوت تنطوي على هوية كيان من هذا القبيل وهذا السياق. فقد ينطوي ذلك مثلاً على التحقق من الإثباتات وتوثيقها بأن شخصاً حقيقياً مصاحبٌ لاسم مشترك أو اسم مستعار له.
- **تأكيد التسجيل**: يمثل تدفق المعلومات هذا التفاعلات الجارية بين مورد خدمة هوية ومورد خدمة إثبات لتأكيد الهويات المسجلة.
- **تسجيل/إصدار الإثبات**: يمثل تدفق المعلومات هذا تبادل المعلومات بين مورد خدمة إثبات الطرف الطالب لتسجيل هوية والحصول على إذن إسناد إثبات (أو إثباتات) إلى اسم أو اسم مستعار ونعوت أخرى مصاحبة للكيان.

ب) الاستيقان والتأكيد

- **التأكيد**: يمثل تدفق المعلومات هذا تبادل المعلومات بين الطرف المعتمد ومورد خدمة التحقق للحصول على تصنيف الادعاء.
- **تحدي الاستيقان**: يمثل تدفق المعلومات هذا طرفاً معتمداً يعترض سبيل طرف طالب ويطالبه بالاستيقان. فيمكن مثلاً للطرف المعتمِد أن يوجّه طرفاً طالباً صوب مورد محدد لخدمة تحقق، أو يمكن لكيان الطرف الطالب أن يختار مورداً محدداً لخدمة التحقق.
- **تبادل رسائل بروتوكول الاستيقان**: يمثل تدفق المعلومات هذا تبادل رسائل بروتوكول استيقان مورد خدمة التحقق من كيان الطرف الطالب.
- **صلاحية صحة الإثبات**: يمثل تدفق المعلومات هذا تبادل المعلومات بين مورد خدمة التحقق ومورد خدمة التفويض للتحقق من صحة التفويضات عند الضرورة.

النماذج الواردة في هذه التوصية ليست حصرية، إلا أنها تتوخى المرونة، وقد تشمل سياقات يوجد فيها العديد من موردي خدمة الهوية، فضلاً عن حالات تكون فيها الأطراف الطالبة أو المعتمدة مورّداً لخدمة الهوية أيضاً.

ج) تغيرات التأكيد

- **الإنابة**: يمكن لتأكيد أن يحوي أيضاً تعبيراً عن التحقق أو "الإنابة" المفضلين. إذ إن تعبير التحقق المفضل يوجه الطرف المعتمد إلى خدمة مورد خدمة هوية محددة ليستجوبها، شريطة أن يتمكن الطرف المعتمَد من إقامة سلسلة ثقة مع مورد خدمة الهوية المفضل. وتوفر الإنابات وسيلة للاستجابة للحالات التي ينوب فيها كيان

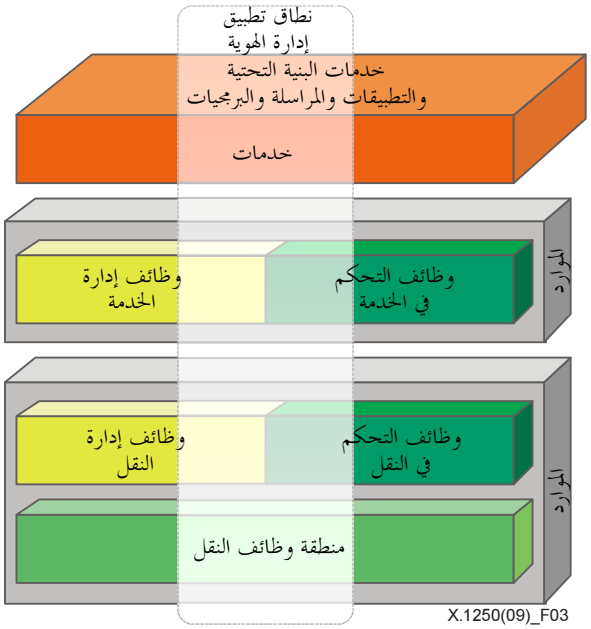
عن كيان آخر. ومثل هذه الإنابات شائعة مثلاً عندما ينوب أحد الأبوين عن طفل أو ينوب راشد عن راشد آخر معوق أو ينوب موظف عن شركة أو ينوب وكيل عن عميل أو تنوب دولة عن مواطن أو العكس.

- ويمكن استعمال الإنابات لتزويد الكيان المناب بقسم ما من المقدرات والحقوق المخولة المخصصة للكيان الذي ترتبط به الهوية. وفي مثل هذه الظروف، قد يتضمن استجواب الطرف المعتمَد لمورد خدمة الهوية طلبات إضافية للتحقق من أن المنيب قد سجل النائب كوكيل مأذون له. ويأتي هذا الطلب زيادة على استيقان الوكيل. ويمكن للنموذج ثلاثي الأطراف أن يضم علاقات هوية متقاسمة أو منابة بين العديد من الكيانات. أما مدى تسلسل الإنابة (أي إنابة الإنابة) فهو خاضع للتكنولوجيا المتوفرة والقوانين والتشريعات أو الأعمال التجارية وللسياسة الاتحادية والقانونية.
- **الغفلية واستعارة الهوية**. يمكن لأي كيان أيضاً أن يثبت تأكيد هوية غفل أو مستعارة. وفي مثل هذه الحالات، يتوقف مستوى ضمان الهوية على عوامل خارجية يتعين على الطرف المعتمد مراعاتها وبالإمكان التوصل إلى انعدام مستوى التأكد من الكيان. وتستعمل الهويات الغفل أو المستعارة حيث لا يتطلب النشاط المعني تحققاً فعلياً (مثلاً عندما يكون النشاط من الابتذال بحيث تنتفي الحاجة لأي نوع من تكاليف إدارة الهوية). وإضافة إلى ذلك، قد تتطلب بعض سياسات أو قوانين أو تشريعات حماية البيانات استعمال الغفلية أو استعارة الهوية.

2.7 مجموعة قابلة للتشغيل البيني من مقدرات إدارة الهوية

أظهرت إدارة الهوية مقدرةً مشتركة لجميع طبقات نماذج شبكة أساسية من قبيل ما يوجد في شبكات الجيل التالي. [b-ITU-T Y.2012]، [b-ITU-T Y.2720]. وتستعمل مقدرات إدارة الهوية المتنوعة في قسم التطبيقات للتحكم بخدمة الشبكة وكجزء من وظيفة النقل التي تقوم عليها، وفي مقدرات الإدارة المستعملة لإدارة هذه الطبقات.

وتفتقر هذه الطبقات للتنسيق فيما بينها حالياً في إدارة الهوية. وتماشياً مع السياسات الإقليمية والوطنية، ينبغي دعم مقدرات إدارة الهوية القابلة للتشغيل البيني في كل طبقة من طبقات الشبكة.



الشكل 3 – نطاق تطبيق قابلية التشغيل بين طبقات شبكة إدارة الهوية

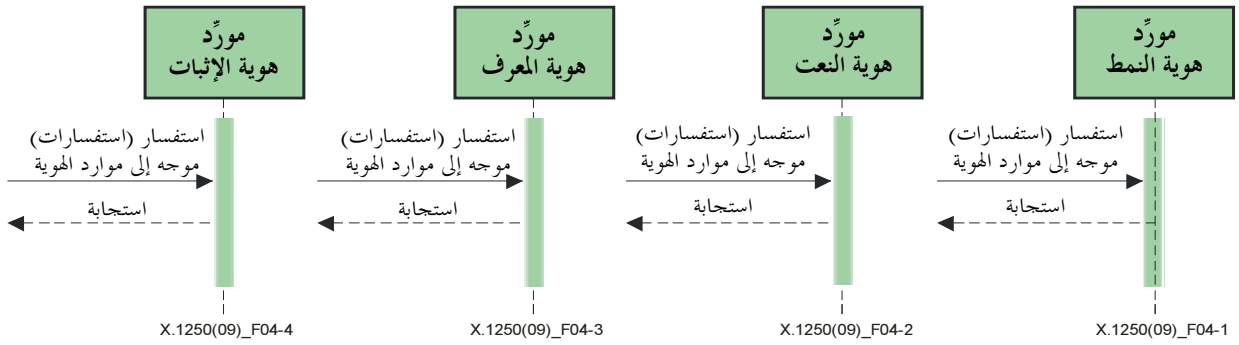
ويظهر الشكل 3 أن مقدرات إدارة الهوية قد توجد في جميع الطبقات العمودية لمعمارية الشبكة وأن هنالك حاجة لعمليتي المزامنة والاتساق على حد سواء.

3.7 المكونات الأساسية الأربعة للهوية

حرصاً على تسهيل استعمال مقدرات إدارة الهوية القابلة للتشغيل البيني، تقسم هذه التوصية معلومات الهوية إلى الفئات الأربع الأساسية التالية:

- مقدرات معرف الهوية،
- مقدرات صحة الإثبات،
- مقدرات النعوت،
- مقدرات النمط.

ويمكن استعمال تجميع كل من الفئات الأربع من معلومات الهوية دعماً لمزيد من سويات الدقة لضمان الهوية يمكن تقديمها بوصفها مقدرات هوية إما بشكل منفرد أو ضمن تركيبة ما من مختلف الكيانات، كما يتبين ذلك من الشكل 4. ويمكن اعتبار الرسم امتداداً لذلك المبين في الشكل 2 إذ يستعمل عادة نموذج الاستفسار–الاستجابة. وليس من الضروري استعمال كل مقدرات الهوية هذه في تنفيذ إدارة هوية. إذ إن استعمالها – ووجودها كمقدرات – يتوقف على السياق، لا سيما المستوى المنشود أو اللازم لضمان استيقان الكيان.



الشكل 4 – مثال عن أربع مقدرات أساسية للاستفسار عن الهوية

وقد تكون الفوارق بين مقدرات الهوية هذه غير واضحة. فللتفويضات مثلاً معرفاتها الخاصة بها ويحتفظ الموردون ببعض معلومات النعت بشأن هوية مصاحبة يتعلق بها الإثبات، وبوسع المورد أن يحتفظ بملف تسجيل يتصل باستعمال الإثبات حيث يُستعمل هذا الملف في تحليل النمط للإقلال إلى أدنى حد من سرقة الهوية والاحتيال.

ويمكن أيضاً تقديم كل هذه المقدرات كرزمة موحدة من قبل موردي إدارة الهوية في العديد من التطبيقات من قبيل الاتصالات/تكنولوجيا المعلومات والاتصالات، أو موردي الخدمات المالية، أو مؤسسة أو منظمة على علاقة خاصة بمستعمل نهائي أو عميل. أما مدى "انفتاح إدارة الهوية" وإمكانية التشغيل البيني فهو قرار قائم على الثقة والاحتياجات المتشابهة وعلاقات الأعمال والمتطلبات التنظيمية أو القانونية.

1.3.7 مقدرات المعرّف

المعرّفات هي نعوت (مثل الأسماء) تُسند عموماً لكيان ما من أجل إدارة أنظمة المعلومات أو لأغراض عنونة الاتصالات. فهي عادة لها استعمالات متخصصة. وعلى سبيل المثال، تستعمل أرقام الهواتف والمواقع URL والعناوين الإلكترونية للنفاذ إلى خدمة أو جهاز، أو لتسيِّر شبكات اتصالات على حدٍ سواء.

2.3.7 مقدرات الإثبات

تُستعمل الإثباتات لإتاحة استيقان كيانات طرف واحد أو طرفي عملية تبادل معلومات أو معاملة. ويعتمد أحد أقدم أشكال إثبات الشهادة والذي لا يزال الأوسع انتشاراً على معيار الشهادة الرقمية استناداً إلى التوصية ITU-T X.509 [b-ITU-T X.509]. وتشمل أشكال الإثباتات الأخرى إثباتات صادرة عن الحكومة مثل البطاقات المتعلقة بالوظائف وبطاقات SIM المتنقلة اللاسلكية وبطاقات ائتمان المؤسسات المالية أو بطاقات الصرف الآلي (ATM).

كما تشمل الإثباتات تمثيلات القياس الحيوي أحياناً. وتتطلب بعض التطبيقات القدرة على توفير التحقق السريع من صحة الإثباتات التي لم تلغ. غير أنه يجب توقع احتمال أن تفضي عمليات التحقق إلى معلومات تتبع ومورد خدمة الهوية مما قد يشكل خطراً على الخصوصية. لذا فإن الإثباتات القوية التي لا تتطلب عمليات تحقق هامة.

إن التعقيد في استعمال عامة الناس للإثباتات الرقمية على نطاق واسع قد تتضاءل من خلال اعتماد طرائق إدارة هوية متمحورة حول المستعمل مع مقدرات إدارة الإثباتات مثل المحفظة الرقمية [b-ITU-T X.1251]. وتبعاً للسياق، قد يتضمن توفير الإثبات القدرة على استعمال مجموعة متنوعة من الإثباتات لتلبية مختلف مستويات الضمان المطلوبة لاستيقان الكيان.

3.3.7 مقدرات نعت

غالباً ما تكون النعوت كخصائص الكيانات ساكنة نسبياً تُلتقط كجزء من عملية الإثبات أو تخصيص المعرّف (مثل الأسماء والعنوان الفعلي ومعلومات الاتصال، وما إلى ذلك). وفي حالات أخرى، من قبيل الموقع المرجعي الحالي للكيان بالنسبة للأرض، يمكن للنعوت أن تكون عالية الدينامية.

وقد تتطلب مقدرات كشف النعوت والاستفسار عنها مقدرات بروتوكولات متخصصة قابلة للتشغيل البيني. وتقدم هذه البروتوكولات عادة نوعاً من التحقق خاصة عن استخدام البروتوكول PII في حماية ومراقبة الكيان ذي الصلة للمعلومات المعرّفة بهوية صاحبها شخصياً. وقد توفر أيضاً بعض البروتوكولات والمنصات الجديدة المتمحورة حول المستعمل والقابلة للتشغيل البيني وسيلة للمستعمل النهائي ليحدد أسلوب معالجة معلومات النعت.

4.3.7 مقدرات النمط

أنماط الهوية تعبيرات منظمة من نعوت كيان ما يمكن استعمالها في بعض عمليات تعرف الهوية.

وقد تتكون من هوية ترصد أو تكتشف (أي دون ادعاء أو تأكيد) مثل معلومات السمعة أو معلومات تتعلق بمعاملات مصاحبة لكيان. وغالباً ما يكون كشف سرقة الهوية بالغ الأهمية. وتُستعمل أيضاً مقدرات تخصصية لهوية النمط دعماً لمقدرات الأمن السيبراني، من قبيل التوقيع النمطي لفيروس أو هجوم على البنية التحتية.

وعلى غرار مقدرات هوية النعت، عندما تتناول الأنماط أشخاصاً فعليين فإنها تحتكم أيضاً إلى مصفوفة محتملة من الاتحادات والمتطلبات القانونية والتنظيمية المتوسعة والهامة والمتضاربة أحياناً، لا سيما لحماية المعلومات المعرّفة بهوية صاحبها شخصياً. وفي بعض الولايات القضائية، وفي حال استعمال البروتوكول PII تخضع مثل هذه المقدرات استبقاء بيانات النمط والتحاليل لسياسات لها دلالتها من حيث حماية البيانات والخصوصية، وهي تشمل منع جمع البيانات وآليات حذف البيانات.

5.3.7 مقدرات عامة لإدارة بيانات إدارة الهوية

ينطبق عدد من مقدرات إدارة الهوية على إدارة نظام إدارة الهوية وعلى إدارة بيانات إدارة الهوية من أجل كل مقدرات الهوية. وتشمل المقدرات توفير الدعم لما يلي:

- قدرة الطرف الطالب على النفاذ إلى معلومات الهوية الخاصة به وحذفها وتعديلها ومراقبتها والتحكم فيها، رهناً بالقوانين والتشريعات و/أو السياسات المطبقة؛
- قدرة الكيانات المخولة (مثل مدراء النظام والأبوين وسلطات السلامة العامة وإنفاذ القانون والأطراف الثالثة الأخرى المخولة) على النفاذ إلى معلومات الهوية الخاصة بها وتعديلها ومراقبتها، رهناً بالقوانين والتشريعات و/أو السياسات المطبقة؛
- استيراد وتصدير معلومات الهوية، رهناً بالقوانين والتشريعات و/أو السياسات المطبقة؛
- آلية إيضاح نوع من المعلومات حول مستوى نوعية المعلومات التي يقدمونها للأطراف المعنية. ويتطلب ذلك اتفاقاً بين هذه الأطراف بشأن القيمة الإعلامية؛
- قدرة الطرف الطالب على تفويض إدارة معلومات الهوية الخاصة به إلى كيان آخر؛
- إدارة دورة حياة جميع الهويات، مع وسيلة للتحقق السريع من الوضع الراهن للمعلومات، رهناً بالقوانين والتشريعات و/أو السياسات المطبقة؛
- آلية مشتركة لتعرّف جميع الهويات والتحكم في نشرها، رهناً بالقوانين والتشريعات و/أو السياسات المطبقة.

6.3.7 مستويات ضمان الكيان

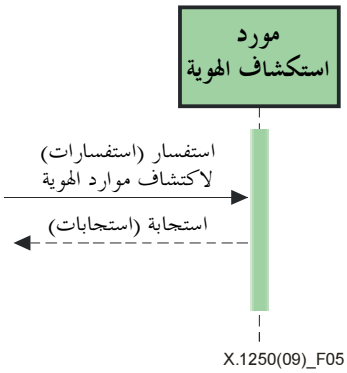
للموارد وأساليب توفيرها مستويات ضمان تصاحبها وتتفاوت كثيراً تبعاً لعدد كبير من العوامل التقنية والإدارية التي تتمشى مع السياسات والمعايير ذات الصلة بالسياق.

وتشمل المقدرات توفير ما يلي:

- بيان مستويات ضمان معلومات المعرّف العام، خاصةً لسلطات التسجيل في الاتصالات العامة، بما في ذلك معرفات التوزيع الفرعي للمخصصين في أنظمة التسمية والترقيم؛
- بروتوكول مشترك يبين مستويات الضمان المصاحبة للمعلومات المقدمة. ويوصى باعتماد آليات مشتركة عالمية ومفتوحة؛
- آلية تمكّن طرف طالب أو طرف معتمَد أو على سبيل المثال مورد خدمة هوية من تحديد شروط الضمان والصلاحية لخدمة هوية ما، ومن تحديد الإجراء الواجب إذا لم تستوف الشروط.

4.7 مقدرات اكتشاف الهوية

يشكل اكتشاف مصادر كل من المقدرات الأساسية الأربع لإدارة الهوية تحدياً حرجاً لإدارة الهوية في عالم مقدرات وتطبيقات الشبكة الذي يتسم بدينامية عالية وتنوع شديد. فثمة مصادر ضخمة موزعة ومستقلة بذاتها. وليس مجرد وجود مقدرات إدارة الهوية كاف. إذ تحتاج الأطراف المعنية لوسائل معيارية لتعلم بوجودها وبكيفية الوصول إليها كما يبين الشكل 7 أدناه. ولعل عملية الاكتشاف تستدعي دعم بروتوكول جديد للاكتشاف يماثل في طبيعته البروتوكول الدينامي لتحكم المخدم (DHCP) حيث يمكن لعميل أن يكتشف مخدم DHCP ويحصل على عنوان IP ومعلومات البوابة. وإلى ذلك، قد تكون عملية الاكتشاف ببساطة أن يقدم حامل الهوية موقع موارد موحداً (URL) أو OID إلى الطرف المعتمَد.



الشكل 5 – مثال عن مقدرات الاستفسار–الاستجابة لاكتشاف الهوية من أي كيان

بالإضافة إلى ذلك، فإن اكتشاف مقدرات الهوية ينبغي أن يشمل اكتشاف المقدرات المتيسرة من الاتحادات. فبعض الاتحادات والجماعات المستعملة لبروتوكولات محددة وضعت حلولاً جزئية لتلبية احتياجات الاكتشاف ضمن حدود جماعات المستعملين لديها. ولكن لا توجد حالياً وسيلة للاكتشاف العالمي بين الاتحادات. وحبذا وجود نظام يدعم الاكتشاف. وتشمل المقدرات المرغوبة للاكتشاف توفير ما يلي:

- سياسات اتفاق الأعمال التجارية لموردي خدمة الهوية عبر الاتحادات أو الميادين؛
- طريقة موحدة لتسجيل الدخول وتسجيل الخروج، ونشر هذه المقدرة بطريقة معيارية بحيث يتسنى اكتشافها.

5.7 إمكانية التشغيل البيني ومد الجسور

تعد إمكانية التشغيل البيني العالمي بين الأطراف الموردة لموارد إدارة الهوية متطلباً أساسياً للتوريد. وتصف هذه الفقرة مقدرات وضع استفسارات في اتحاد أو من خلال المورِّد الوسيط.

وتقوم الاتحادات على أساس مبدأ القبول المتبادل لنتائج الاستيقان بين الميادين المشاركة وليس على تقاسم معلومات الهوية بين هذه الميادين.

1.5.7 المقدرات المتصلة بالاتحاد

تشمل المقدرات المتصلة بالاتحاد ما يلي:

- إمكانية أن يقيم الطرف المعتمَد ميدان استيقان (مثل الأمن) عبر التحالفات والمشاركة في الاتحادات؛
- الحصول على تخويل من الطرف الطالب لتوحيد هويات الأطراف الطالبة، رهناً بالقوانين والتشريعات والسياسات المطبقة؛
- قدرة طرف طالب على تفويض السلطة لتوحيد هويته، رهناً بالقوانين والتشريعات والسياسات المطبقة.

2.5.7 المقدرات المتصلة بجسر الهوية

تشمل المقدرات المتصلة بجسر الهوية ما يلي:

- قدرة طرف طالب على تحديد الأذون والممنوعات فيما يتصل بمقدرات مد جسور الهوية؛
- آلية لاكتشاف مورد خدمة هوية الطرف الطالب ذي الصلة؛
- آلية مد جسور الهوية:

أ) للسماح باتحاد حسابات طرف طالب لدى مورد خدمة هوية وطرف معتمد في مختلف ميادين الاستيقان شريطة أن يكون لكل منها أذون من الطرف الطالب ومن مورِّد جسر خدمة الهوية؛

ب) لنقل عنوان مورد خدمة هوية في رسالة جوابية إلى طرف معتمد؛

- آلية لتحقيق التشغيل البيني لمعلومات طرف طالب واردة من أحد موردي خدمة الهوية والسماح باستجلائها واستعمالها من قبل مورد خدمة هوية وأطراف ترحيل ذوي صلة في ميادين مختلفة (كحال شبكتين)؛
- وسيلة لتبليغ الطرف المعتمَد أو مورد خدمة هوية عند حدوث تغيير في سياسات مورد خدمة جسر الهوية، وذلك حيثما يستحدث اتحاد عبر مورد خدمة جسر الهوية. إذ تتيح هذه الآلية للطرف المعتمد أو مورد خدمة الهوية خيار إنهاء مشاركته في الاتحاد.
- وسيلة لتبليغ الطرف الطالب عند حدوث تغيير في سياسات مورد خدمة جسر الهوية، وذلك حيثما يستحدث اتحاد ما عبر مورد خدمة جسر هوية. إذ تتيح هذه الآلية للطرف الطالب استكمال عملية القبول والمشاركة في الاتحاد.

6.7 أمن إدارة الهوية

لا بد من توفير الحماية الأمنية لمعلومات الهوية ولموارد الشبكة التي تقدم مقدرات الهوية لما تتسم به من قيمة وحساسية ولكونها مكونات حيوية في الشبكات، لا سيما تلك التي تعد جزءاً من البنية التحتية الوطنية الحرجة. ويشمل تأمين البنية التحتية لإدارة الهوية السياسات الإدارية والممارسات التشغيلية والتكنولوجيات والتقنيات المستخدمة للحيلولة دون اختراق أنظمة وبيانات إدارة الهوية المستقرة منها والعابرة.

وتكمل هذه الفقرة أفضل الممارسات الأمنية الواردة في التوصية [b-ITU-T X.1205] ببضع مقدرات لتساعد في تأمين البنى التحتية لإدارة الهوية، ومن بين هذه المقدرات:

- معاملات آمنة (تمتاز مثلاً بالسرية والسلامة والحماية من التكرار) بين جميع الأطراف (الطالبة والمعتمدة والموردة لخدمة الهوية)؛
- توفير آليات لعدم رفض تعاملات إدارة الهوية؛
- تأمين اكتشاف مقدرات الهوية، ضد انتحال صفة مورِّد هوية مثلاً؛
- تسجيل المعلومات الأمنية لمعاملات إدارة الهوية؛
- تنفيذ مقدرات كشف نشاط الاقتحام والتصدي له استناداً إلى تحليل تعامل إدارة الهوية، وربما إنذار أصحاب الهوية بالهجمات المشتبهة على معلومات الهوية الخاصة بهم؛
- توفير الوسائل اللازمة للسماح لأطراف الترحيل بإعلام موردي خدمة الهوية باختراق هويتهم. وتأمين مقدرة التبليغ هذه من الاستغلال.

وتعد سياسات وتوجيهات الاستعمال – المشار إليها أحياناً "بإدارة الهوية" – إجراءات هامة أيضاً في بيئة مورِّد خدمة الهويات المتعددة للإقلال من التهديدات والمخاطر، وكذلك لحماية المعلومات المعرّفة بهوية صاحبها شخصياً. وفيما يتعلق الأمر بالاتحادات والتحالفات ومورِّدي الجسر، يمكن لجميع أطراف الترحيل وموردي خدمة الهوية المشاركين أن ينشروا هذه الإجراءات. كما أن الاستعمال المتزايد لتطبيقات إدارة الهوية المتمحورة حول المستعمل قد يمكّن المستعملين النهائيين الطالبين من توصيف سياسات لها إسناد إلى نعوت الهوية الخاصة بهم، وفق الوصف والتوصية الواردين في الفقرة 7.7. ويعود تنفيذ مقدرات الأمن المشتركة بين الأطراف المشاركة في اتحاد بفوائد هامة، ينبغي أن تزود الاتحادات بمواصفات أمنية متطورة بشكل جيد.

وتضم المقدرات المرغوبة لأمن إدارة الهوية والسياسة ما يلي:

- مقدرات ضمان استيقان الهوية وفق المبادئ التوجيهية المطبقة؛
- آلية عدم رفض معاملات إدارة الهوية؛
- إرساء دينامي لآليات محدودة زمنياً من أجل العلاقات العابرة والمتغيرة. وقد يتطلب ذلك مورد جسر يحظى بثقة الطرفين والانتماء إلى اتحاد واحد أو أكثر ؛

- الأمن بين الاتحادات، بما في ذلك آليات التفاوض من أجل الاتصالات الآمنة بين الاتحادات وتبادل المعلومات فيما بينها للتصدي للتهديدات على الأمن السيبراني؛
- تزويد تطبيقات التخويل في أغراض المطراف بوسيلة للتفويض بالنفاذ إلى معلومات هوية المستعمل النهائي لغرض المطراف، رهناً بالقوانين والتشريعات والسياسات المطبقة؛
- آلية إرسال تبليغ إلى مورد خدمة الهوية وجميع الأطراف المتأثرة ذات الصلة عند الإفادة باختراق هوية أو إلغائها؛
- طريقة آمنة لتعلم مقدرات الهوية؛
- تسجيل المعلومات الأمنية لمعاملات إدارة الهوية بتفصيل واف لتثبيت المسؤولية وتمكين التحليل القانوني؛
- مقدرات كشف الاقتحام والتصدي له من أجل معاملات إدارة الهوية؛
- آليات تسمح لأطراف الترحيل بالإبلاغ عن اختراق الهوية.

7.7 حماية المعلومات المحددة شخصياً (PII) والتحكم فيها واستعمالها

تحمل المحافظة على المعلومات المحددة شخصياً أوجهاً عدة. ويشتمل وجهان فيها على استعمال المقدرات الأمنية في البنية التحتية لإدارة الهوية، واستعمال المقدرات التي توفر للكيانات الشفافية والإشعار بشأن استعمال معلومات الهوية الخاصة بهم بالاقتران مع القدرة على إسناد أفضلياتهم إلى تلك المعلومات. وفي هذا السياق، يتألف "الإسناد" من آلية ما ثابتة تمكن طرفاً ثالثاً بحوزته معلومات الهوية من اكتشاف المقدرات المصاحبة لسياسة المعلومات المحددة شخصياً الخاصة بالكيان. وعلى نحو متزايد، يتاح تنفيذ هذه الأنواع من الأفضليات ضمن منصات المنتج المتمحور حول المستعمل وضمن مقدرات مورِّد جسر خدمة الهوية على السواء.

ويجب في بعض الولايات القضائية الوطنية والإقليمية، جمع المعلومات المحددة شخصياً بطريقة منصفة وطبقاً لغاية صريحة ومشروعة. وينبغي أن تقتصر المعلومات ذات الصلة المتبادلة في الأطراف المتواصلة مع بعضها البعض على البيانات اللازمة للسماح لطرف الترحيل بتقديم خدمة أو مورد إلى طرف طالب.

ومن منظور الخصوصية في بعض الولايات القضائية الوطنية، هناك عدد من المبادئ يجب مراعاتها:

- يجب أن يكون إسناد المعلومات PII لغايات محددة وواضحة وقانونية وأن يتم بطريقة تتمشى مع هذه الغايات؛
- يجب أن تكون المعلومات PII ملائمة وذات صلة وثيقة غير زائدة فيما يتعلق بالغايات التي وضعت و/أو تستعمل من أجلها؛
- يجب أن تكون المعلومات PII دقيقة ويجب تحديثها؛ ويجب اتخاذ كل خطوة معقولة من أجل ضمان محو أو تصحيح البيانات غير الصحيحة أو غير الكاملة التي تتعلق بالغايات التي جمعت من أجلها والتي تستعمل من أجلها؛
- يجب الإبقاء على المعلومات PII في شكل يتيح تحديد مواضيع البيانات خلال فترة لا تتجاوز المدة اللازمة لتحقيق الغاية التي جُمِعت البيانات من أجلها أو التي تستعمل من أجلها؛
- ينبغي عدم تقاسم المعلومات PII بين تطبيقات ذات أغراض مختلفة؛
- يجب ألا تقتصر المعلومات PII على الحد الأدنى الضروري لغاية محددة؛
- يجب أن تكون المعلومات PII أمينة. ويجب اتخاذ التدابير التقنية والتنظيمية الملائمة من أجل حماية هذه المعلومات من الإتلاف المتعمد أو غير المتعمد أو من إضاعتها عرضاً أو كشفها أو النفاذ إليها لتغييرها دون ترخيص، وخصوصاً عندما تنطوي العمليات على إرسال بيانات عبر شبكة ما، وكذلك من جميع الأشكال غير القانونية من العمليات؛
- يحق للأشخاص النفاذ إلى المعلومات PII الخاصة بهم وتصحيحها أو محوها؛
- يجب عدم الاحتفاظ بالمعلومات PII لمدة أطول من الغاية المحددة.

وتتطلب تشريعات أخرى آليات حماية تشمل استعمال التبليغات كلما يتم النفاذ إلى حساب أو تتغير المعلومات. وينبغي استعمال المعلومات المعرِّفة التي يمكن تحديدها شخصياً في شبكات وخدمات الاتصالات/تكنولوجيا المعلومات والاتصالات طبقاً لغاية نهائية صريحة. وفي ضوء هذه الغاية النهائية، بوسع المرء أن يقدّر الطبيعة الوافية غير المغالية للبيانات المسجلة، وفئات الأشخاص أو المنظمات التي يمكن أن تتلقى هذه البيانات، والمدة الممكنة لحفظ البيانات المجمعة.

وتشمل المقدرات ما يلي:

- جمع وتأمين وحماية المعلومات PII بما يتمشى مع مبدأ حماية البيانات والخصوصية والقانون. وينبغي أن تشمل أوجه الحماية، كحد أدنى، تلك التي نصت عليها منظمة التعاون والتنمية في الميدان الاقتصادي كمبادئ توجيهية للخصوصية على الصعيد العالمي. ويمكن للوائح الإقليمية/الوطنية أن تفرض الالتزام بمتطلبات إضافية (مثل التوجيهات الأوروبية لحماية البيانات 95/46/EC)؛
- تأمين وحماية إدراك حدود تقليص جمع المعلومات المعرِّفة بهوية صاحبها شخصياً إلى أقصى حد. وينبغي الحصول عليها لغايات محددة وصريحة ومشروعة فقط بموافقة صاحب البيانات؛
- الخصائص من قبيل عندما يقيم مورد خدمة هوية اتحاداً منفصلاً بين هوية طرف طالب وطرفين معتمَدين أو أكثر، ينبغي ألا تتمكن الأطراف المعتمَدة من استعمال المعلومات التي يزودهم بها مورد الهوية لتحديد أن الهويات تشير إلى الطرف الطالب؛
- خدمة تبليغ عند تغيّر نعوت هوية الطرف الطالب؛
- خدمة تبليغ عند تغيّر إعلانات الموافقة للطرف الطالب؛
- توفير إنذار أصحاب الهويات بنشاط من معاملات إدارة هوية يفسره مورد خدمة الهوية على أنه محاولة لاختراق هوياتهم؛
- توفير إمكانية إبلاغ أصحاب الهويات باختراق أنظمة ومقدرات مورد الهوية؛
- القدرة على إنفاذ حدود المدة على تخزين المعلومات PII بحيث لا تبقى لمدة تتجاوز مدة الغاية المحددة لها؛
- قدرة الكيانات ذات الصلة على التحقق من المعلومات PII الخاصة بها وتصحيحها وحذفها وفقاً للقوانين والقواعد الناظمة والسياسات.

8.7 التدقيق والمطابقة

تخضع إدارة الهوية لمختلف المتطلبات القانونية والتنظيمية والصناعية التي يمكن أن تتطلب مستوى معين من التدقيق والمطابقة. ومن أمثلة إجراءات التدقيق والمطابقة، الحفاظ على سجلات أمنية وحماية المعلومات الشخصية واستعمالها على النحو المناسب، وإشعار الكيانات التي تنطبق عليها المعلومات. وعلى التدقيق الالتزام بمقدرات حماية المعلومات المحددة شخصياً التي ورد وصفها في الفقرة 7.7 أعلاه وخاصة بسبب احتمال انخراط طرف جديد قد ينجم عنه خرق لقوانين الخصوصية وتشريعاتها وسياساتها.

وتشمل المقدرات ما يلي:

- آليات تمكين التحليل القانوني؛
- آليات مشتركة وآمنة لتبادل معلومات تدقيق إدارة الهوية؛
- دمغة التوقيت؛
- دمغ السجلات بطبعة زمنية ترتبط بالسياق، حسب أهمية المعلومات المدققة وقيمة الوقت؛
- إيلاء الاهتمام الكافي لضمان أن تفي عمليات تدقيق إدارة الهوية بمتطلبات الخصوصية المنطبقة.

1.8.7 مقدرات دقة الطبعة الزمنية

لدقة الطبعة الزمنية أهمية بالغة في إدارة دورات حياة الهوية وفي الحفاظ على الأمن في أنظمة إدارة الهوية، لأن جميع معلومات الهوية تقع في أطر زمنية محددة. ويصف التدقيق وقوع الأحداث ضمن تلك الأطر الزمنية. وتعد الطبعة الزمنية أساسية لأغراض التدقيق، إذ تحدد دقة الطبعة الزمنية نوعية بيانات التدقيق أو حتى قابلية استعمالها في مواقع الحدث المناسبة بغية القيام بالتدقيق الكافي لمقدرات الشبكة والتطبيق على درجة عالية من اللاتزامن والتوزيع. وتشمل المقدرات المنشودة مقدرات دقة الطبعة الزمنية الكافية للتدقيق في مواقع مرجعية مشتركة متفق عليها تناسب مستوى من الضمان يُتفق عليه بشكل متبادل.

9.7 الأداء والموثوقية والتيسر

لئن كانت إدارة الهوية مقدرة شبكية هامة، ينبغي أن تصمَم وتنفَذ لتحقق أهداف الأداء والموثوقية والتيسر. ويوصى بأن يكون شأن أهداف موثوقية وتيسر إدارة الهوية قابلة للمقارنة بوظائف الشبكة الحرجة الأخرى في إدارة الهوية تشكل جوهر الاستيقان وتخويل النفاذ وجميع المعاملات في الشبكة. ويعني ذلك، على سبيل المثال، ضمان أن أهداف قدرة إدارة الهوية، والدعم البيئي، والتوصيلية وافية. وينبغي أن يلبي أداء إدارة الهوية (من ناحية زمن الإجابة على استفسار مثلاً) الحمولات المتوقعة لاستفسارات إدارة الهوية.

ولا يتجانس تيسر نظام إدارة الهوية عبر جميع المكونات (عناصر الإصدار وعناصر البحث وعناصر الإلغاء) ويجب ربطه في نهاية المطاف بمستوى الضمان في الإثبات. ويحبذ توفر متطلبات التيسر التالية، بيد أنها ستختلف بين مكونات فِدَر البناء (التخزينية ونظام التسجيل ومقدرة الإلغاء):

- الموثوقية والتيسر بمستويات تقارن بمثيلاتها في عناصر وأنظمة ومقدرات الشبكة الحرجة الأخرى؛
- تضمين مقدرات إدارة الهوية في خطط الانتعاش بعد مرور الكوارث؛
- تطبيقات إدارة هوية توفر أوقات استجابة معقولة في معاملات إدارة الهوية.

10.7 التدويل

تقتضي إمكانية التشغيل البيني على الصعيد العالمي لتوفير الدعم لاستعمال منظومات حروف متنوعة ولغات متنوعة. وهناك إقرار بأهداف التدويل كشرط هام في التصميم والدعم لجميع التطبيقات العامة القائمة على الشبكة، بما فيها مقدرات إدارة الهوية.

بيبليوغرافيا

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

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

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity*.

[b-ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

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

[b-IETF RFC 2560] IETF RFC 2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

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، 2010