الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1251

(2009/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

إطار عام لتحكم المستعمل في الهوية الرقمية

التوصيـــة ITU-T X.1251

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.1251

إطار عام لتحكم المستعمل في الهوية الرقمية

ملخص

تعرف التوصية ITU-T X.1251 إطاراً عاماً لتعزيز تحكّم المستعملين في معلومات هوياتهم الرقمية وتبادلها. كما تعرّف هذه التوصية قدرات للمستعملين وقدرات وظيفية لتبادل معلومات الهوية الرقمية. ويشمل العمل تزويد المستعمل بالقدرة على التحكم في الكشف عن المعلومات التي تقود إلى تعرّف هوية أصحابها.

المصدر

وافقت لجنة الدراسات 17 (2009-2012) لقطاع تقييس الاتصالات على التوصية ITU-T X.1251 بتاريخ 25 سبتمبر 2009 بموجب إجراء القرار 1 للجمعية العالمية لتقييس الاتصالات.

كلمات مفتاحية

عقد رقمي – هوية رقمية – عميل هوية رقمية – هوية – تبادل الهوية – إدارة الهوية – مخدّم الهوية.

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/.

© ITU 2010

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

المحتـــويات

الصفحة

1 مجال التطبيق 1

2 المراجع..... 1

3 المصطلحات والتعاريف 1

1.3 مصطلحات معرَّفة في وثائق أخرى:..... 1

2.3 مصطلحات معرَّفة في هذه التوصية..... 2

4 المختصرات..... 3

5 الاصطلاحات 3

6 قُدُرات عامة..... 3

1.6 قدرات المستعمل 3

2.6 القُدُرات الوظيفية 4

3.6 خطوط توجيهية خاصة بالأمن 5

7 التبادل المعزز القائم على تحكم المستعمل للهوية الرقمية..... 5

1.7 مقدمة..... 5

2.7 التهديدات الأمنية 6

3.7 النموذج المفاهيمي لتبادل الهوية الرقمية..... 6

4.7 العقد الرقمي..... 7

5.7 ثلاث طبقات لتبادل الهوية 9

8 الإطار العام لتبادل الهوية الرقم 10

1.8 مبادئ التصميم 10

2.8 مكونات الإطار العام 11

التذييـــل I – المبدأ التوجيهي للتنفيذ المرجعي لإطار عام لتحكم المستعمل في الهوية الرقمية باستعمال الثقة في خدمة الويب وتكنولوجيا بطاقة المعلومات 13

1.I مقدمة..... 13

2.I الخلفية..... 13

3.I قدرات الإطار العام لتبادل الهوية الرقمية..... 15

ثبت المراجع..... 17

التوصيـــة ITU-T X.1251[1]

إطار عام لتحكم المستعمل في الهوية الرقمية

1 مجال التطبيق

تحدد هذه التوصية إطاراً عاماً لتعزيز تحكم المستعملين في معلومات الهوية الرقمية الخاصة بهم وتبادل هذه المعلومات.

كما تحدد التوصية قدرات تبادل معلومات الهوية الرقمية. ويشمل ذلك تزويد المستعمل بالقدرة على التحكم في الكشف عن معلومات قابلة للتعرف الشخصي.

ملاحظة – لا يشير استعمال مصطلح "هوية" في هذه التوصية فيما يتصل بإدارة الهوية (IdM) إلى معناه المطلق. وعلى وجه التحديد، لا يرقى المصطلح إلى أي إثبات قطعي للهوية.

2 المراجع

تحتوي التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع بعض الأحكام التي تشكل أحكاماً في هذه التوصية، بموجب الإحالة إليها في النص. ففي تاريخ نشر هذه التوصية، كانت الطبعات المذكورة لا تزال صالحة. وبما أن جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يتعيَّن على مستعملي هذه التوصية السعي إلى تطبيق أحدث صيغ التوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات السارية حالياً. والإحالة داخل هذه التوصية إلى وثيقة ما لا يُضفي على هذه الوثيقة صفة توصية.

[ITU-T X.1205] التوصية ITU-T X.1205 (2008)، *لمحة عامة عن الأمن السيبراني*.

[ITU-T X.1205] التوصية ITU-T X.1205 (2009)، *مقدرات أساسية للإدارة العالمية المعززة للهوية وإمكانية التشغيل البيني*.

3 المصطلحات والتعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى:

تستعمل هذه التوصية المصطلحات التالية المُعرَّفة في وثائق أخرى:

1.1.3 **الإثباتات** [b-ITU-T X.1252]: مجموعة بيانات تُقدم كدليل على هوية و/أو استحقاقات مزعومة.

2.1.3 **الكيان** [b-ITU-T X.1252]: أي شيء له وجود قائم بذاته ومميز يمكن تعريفه في السياق.

ملاحظة – يمكن أن يكون الكيان شخصاً طبيعياً أو حيواناً أو شخصاً اعتبارياً أو منظمة أو شيئاً فاعلاً أو منفعلاً أو تطبيقاً برمجياً أو خدمة وما إلى ذلك أو مجموعة مما تقدم. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط النفاذ والمشتركين والمستعملين وعناصر الشبكة والشبكات والتطبيقات والخدمات والأجهزة والسطوح البينية وما إلى ذلك.

3.1.3 **الاتحاد** [b-ITU-T X.1252]: للمستعملين ومورّدي الخدمات ومورّدي خدمات الهوية.

4.1.3 **معرّف الهوية** [b-ITU-T X.1252]: هو نعت واحد أو أكثر يستعمل لتحديد هوية كيان ضمن سياق.

5.1.3 **الهوية** [b-ITU-T X.1252]: تمثيل كيان في شكل واحد أو أكثر من عناصر المعلومات التي تتيح تمييز الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية، يُفهم مصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تُحَدّ المجموعة المتنوعة من النعوت بإطار ذي حدود محددة (سياق) يوجد فيه الكيان ويتفاعل.

---

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

ملاحظة – يُمثّل كل كيان بهوية واحدة شاملة تضم جميع عناصر المعلومات المحتملة التي تميّز ذلك الكيان (النعوت). بيد أن هذه الهوية الشاملة هي قضية نظرية عصية على أي وصف واستعمال عملي لأن العدد الكلي لجميع النعوت المحتملة لا حصر لها.

6.1.3 إدارة الهوية [b-ITU-T Y.2720]: 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)؛
- تمكين تطبيقات الأعمال التجارية والأمن.

7.1.3 مورد خدمة الهوية (IdSP) [b-ITU-T X.1252]: كيان يقوم بالتحقق من معلومات هويات الكيانات الأخرى مع الحفاظ عليها وإدارتها ويمكن أن يستحدثها ويخصصها.

8.1.3 معلومات قابلة للتعرف الشخصي (PII) [b-ITU-T Y.2720]: المعلومات الخاصة بأي شخص [حي] والتي تجعل من الممكن التعرف على هذا الفرد (بما في ذلك المعلومات التي تسمح بالتعرف على الشخص عندما تدمج مع معلومات أخرى حتى وإن كانت هذه المعلومات لا تعرِّف الشخص بوضوح).

9.1.3 الطرف المعوِّل [ITU-T Y.2720]: كيان يعوّل على تمثيل أو ادعاء هوية من جانب كيان طالب/مؤكِّد ضمن بعض السياقات المطلوبة.

10.1.3 المستعمل [b-ITU-T X.1252]: أي كيان يستفيد من مورد، مثل نظام أو معدات أو مطراف أو عملية أو تطبيق أو شبكة مشاع.

11.1.3 نظام متمحور حول المستعمل [b-ITU-T X.1252]: نظام إدارة هوية يمكّن المستعمل من التحكم في، وإنفاذ، مختلف سياسات الخصوصية والأمن الناظمة لتبادل معلومات الهوية بين الكيانات، بما فيها معلومات قابلة للتعرّف الشخصي.

2.3 مصطلحات معرَّفة في هذه التوصية

تُعرِّف هذه التوصية المصطلحات التالية:

1.2.3 دائرة الثقة: مجموعة من المعايير الموضوعة لربط المنظمات ضمن اتحاد لأغراض النفاذ الموثوق إلى موارد بعضها البعض. يلاحظ أن دائرة الثقة هي النتيجة النهائية لانضمام منظمات إلى اتحاد ما.

2.2.3 العَقْد الرقمي: عَقْد يُبرم بصيغة رقمية ويوقّع عليه كيانان تم التوصل إلى اتفاق بينهما.

3.2.3 الهوية الرقمية: تمثيل رقمي لمعلومات معروفة عن فرد محدد أو مجموعة أو منظمة.

4.2.3 عميل الهوية الرقمية: برنامج وسيط يوفر للمستعمل إدارة الاستيقان والإثبات، وخدمة تبادل معلومات الهوية وحماية الخصوصية.

5.2.3 انتحال الهوية: جريمة يتمكن الجاني فيها من الحصول على معلومات قابلة للتعرف الشخصي (PII)، نحو أرقام بطاقات الضمان الاجتماعي وأرقام رخص قيادة السيارات ويستعملها لفائدته الشخصية.

6.2.3 بيانات الهوية: المعلومات التي تعرف هوية مستعمل بما فيها عناوين موثوقة (صادرة عن شبكة) و/أو غير موثوقة (صادرة عن مستعمل).

7.2.3 تبادل الهوية: عملية إرسال بيانات هوية مستعمل بين مورد هوية وطرف معني من خلال عميل هوية رقمية.

8.2.3 مثبّت الهوية: مكوّن برمجي من عميل هوية رقمية يُتاح للمستعمل ويستطيع المستعمل من خلاله التحكم في هوياته الرقمية وإرسالها.

9.2.3 مخدّم الهوية: مخدم يدير الإثباتات وبيانات الهوية ويقدمها إلى عميل الهوية الرقمية.

9.2.3 مثبّت الهوية: مكون برمجي من عميل هوية رقمية يتاح للمستعمل ويستطيع المستعمل من خلاله التحكم في هوياته الرقمية وإرسالها.

10.2.3 مزامنة الهوية: عملية تحديث بيانات هوية المستعمل المنشورة لطرف معني عندما يتغير مصدر البيانات عند مورد هوية.

11.2.3 نهاية الهوية: عملية إلغاء بيانات هوية مستعمل من التخزين عند انقضاء فترة صلاحيتها.

12.2.3 إذنة الهوية: نموذج بيانات هوية رقمية يتضمن معلومات قابلة للتعرف الشخصي للمستعمل والإثباتات.

13.2.3 التحايل: عملية احتيال جنائي تنطوي على محاولة الحصول على معلومات حساسة من قبيل اسم المستعمل وكلمة المرور وتفاصيل بطاقة الائتمان بادعاء صفة كيان موثوق في اتصال إلكتروني.

14.2.3 سياسة السرية: بيان السياسة التي تحدد قواعد حماية النفاذ إلى المعلومات الشخصية السرية ونشرها.

4 المختصرات

تستعمل هذه التوصية المختصرات التالية:

CoT دائرة الثقة *(Circle of Trust)*

DIC عميل الهوية الرقمية *(Digital Identity Client)*

DIIF إطار عام لتبادل معلومات الهوية الرقمية *(Digital Identity Interchange Framework)*

IdM إدارة الهوية *(Identity Management)*

IdS مخدم الهوية *(Identity Server)*

IdSP مورّد خدمة الهوية *(Identity Service Provider)*

PII معلومات قابلة للتعرف الشخصي *(Personally Identifiable Information)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

RP الطرف المعول *(Relying Party)*

SP مورد الخدمة *(Service Provider)*

XML لغة وسم قابلة للتوسيع *(eXtensible Markup Language)*

5 الاصطلاحات

لا توجد.

6 قُدُرات عامة

تعرف هذه التوصية المجموعة التالية من القدرات. والقدرات الوظيفية وتلك المحددة للمستعمل الواردة أدناه إلزامية إذا لم يرد خلاف ذلك.

1.6 قدرات المستعمل

يلزم توفير ما يلي للوفاء بقدرات المستعمل:

1) آليات الاستيقان المتبادل.

2) توفير سطح بيني للاستيقان يتيح آليات مختلفة للاستيقان من عميل الهوية الرقمية (DIC).

3) توفير منتقى بمنتقي الهوية الذي يتيح له اختيار الإثباتات التي يتوجب استعمالها للاستيقان. وقد يكون اختيار الإثباتات المستعملة للاستيقان مقيداً بشروط أخرى في بعض المواقع الإلكترونية. وللتسهيل على المستعمل قد يفوض مورد خدمة الهوية باختيار طريقة الاستيقان والإثباتات المصاحبة لها (إمكانية أن يختار المستعمل مورد خدمة الهوية وليس إثباتاً خاصاً من أجل الاستيقان عند ذلك المورد).

4) توفير سطح بيني حساس ومتسق من أجل إدارة معلومات أوراقه الثبوتية بأقصى حد من الأمن.

5) توفير الملء الأوتوماتي بعملية التسجيل أو الاشتراك في موقع إلكتروني وذلك من أجل التقليل إلى أبعد حد من تعامل المستعمل مع الموقع، بما في ذلك التحكم الكامل للمستعمل في تشغيل وتوقيف هذه الآليات. وهذا الأمر خياري.

6) توفير معلومات الهوية في أي وقت يرغب فيه المستعمل والسماح له بالتحكم الكامل في تبادل الهوية مع استعمال آلية مناسبة لحماية الخصوصية.

7) توفير التحديثات الأوتوماتية لمعلومات الهوية المتقاسمة عند تغيير المصدر الأصلي وفق التحكم الكامل للمستعمل.

8) توفير التحكّم الكامل للمستعمل في كيفية وضع سياسات الأمن والخصوصية وكيفية إنفاذها للتحكم في عمليات تبادل الهوية قبل تقاسم معلومات الهوية بحيث يمكن للمستعمل أن يؤثر تأثيراً مباشراً على وضع سياسة ما وإنفاذها.

9) السماح للمستعملين بالاطلاع على تفاصيل معلومات الهوية التي يتقاسمونها مع كل كيان.

10) دعم مقدرات إدارة دورة الاستيقان من أجل تجنيب المستعمل إعادة عملية الاستيقان عند مورد خدمة الهوية كل مرة يريد فيها الاطلاع على مواقع إلكترونية.

2.6 القُدُرات الوظيفية

يرد فيما يلي تعريف القدرات الوظيفية لإطار تبادل الهوية الرقمية. وهذه القدرات ضرورية لتوفير الحد الأدنى من الوظائف اللازمة لإطار تبادل الهوية الرقمية.

1) توفير إدارة الإثباتات الكاملة القادرة على إدارة معلومات أوراق إثبات المستعمل لأغراض الاستيقان.

2) دعم إدارة وصلة تبادل الهوية من أجل تزويد المستعمل برؤية كاملة للكيانات التي يتصل بها المستعمل بهدف تبادل الهوية.

3) دعم آليات استيقان متعددة يمكن أن تشمل الاستيقان القائم على كلمات السر وعلى البنية التحتية للمفاتيح العمومية وعلى العوامل البيومترية.

4) دعم آلية تبادل الهوية القادرة على توفير وصلة ثنائية الاتجاه لتقاسم معلومات هوية المستعمل بين الكيانات التي تستخدم عميل DIC.

5) دعم آلية تعاقد رقمي من أجل إبرام عقد لتبادل الهوية واستعماله لإنفاذ سياسات الأمن والخصوصية بهدف تحرير معلومات قابلة للتعرف الشخصي (PII).

6) توفير مزامنة معلومات الهوية لتحديث معلومات الهوية الموزعة والمتقاسمة بصورة مستمرة عندما يتغير مصدر معلومات هوية منتشرة. وتقتصر معلومات الهوية التي تحتاج إلى المزامنة على المعلومات PII التي يغيرها المستعمل مباشرة.

7) توفير تحويل الإذنة عالمياً من أجل جعل الإطار قابلاً للتشغيل مع الأنظمة القائمة لإدارة الهوية.

8) جعل الإطار بعيداً كل البعد عن عملية الاستيقان ذاتها تجنباً للربط بين العميل DIC وآليات الاستيقان المتوفرة عند موردي خدمات الهوية (أو على الأقل تمكين الإطار من توفير جميع آليات الاستيقان بيسر خصوصاً تلك الخاصة بمشغلي الاتصالات).

9) توفير آلية لتمكين مورد خدمة الهوية من التفاعل مع المستعمل أثناء عملية الاستيقان والاطلاع على سطحه البيني الخاص بالاستيقان (GUI) إن اقتضى الأمر.

10) إتاحة إمكانية تخزين إذنات الهوية في وسائط مختلفة (مفتاح USB، بطاقة SIM، خدمة تخزين في الشبكة، وغير ذلك) مع تحديد طبقة التخزين بوضوح لاستعمالها من جانب العميل DIC.

3.6 خطوط توجيهية خاصة بالأمن

حرصاً على وضع إطار أمين لتبادل الهوية الرقم DIIF، يوصى باتباع الخطوط التوجيهية التالية الخاصة بالأمن:

- يعتمد أمن اتصالات الإطار DIIF على نموذج الثقة المستخدم الذي يستند عادة إلى البنية التحتية الرئيسية للإدارة (من قبيل البنية PKI أو المفتاح السري).
- استعمال بعض أشكال بروتوكول أمن طبقة النقل من أجل توفير تكاملية البيانات وسريتها (من قبيل التجفير مثلاً) عند نقل الرسالة في الشبكة.
- توقيع العقد الرقمي توقيعاً رقمياً من جانب الأطراف التي تبرم اتفاقاً؛ وقد يكون التوقيع المجفر خياراً عند الحاجة.
- توقيع البيانات التي تضم معلومات الهوية والمخزنة في الكيان DIC توقيعاً رقمياً ومجفراً وهو في التخزين.
- نظراً لأنه يتاح للمستعمل أن ينقل إذنة هويته من جهاز إلى آخر، يجب أن توضع سياسة للحفاظ على أمن البيانات خلال نقلها.

7 التبادل المعزز القائم على تحكم المستعمل للهوية الرقمية

1.7 مقدمة

أنشئ اتحاد الهويات [b-LA-FF] لتوصيل معلومات الهوية الموزعة بين مورّد خدمة الهوية (IdSP) ومورد الخدمة (SP). فإذا أراد مورد الخدمة ضمان معلومات الاستيقان من مورّد خدمة الهوية، فلا بد من علاقة ثقة بين الطرفين. ويسمَّى ميدان الثقة هذا دائرة الثقة (CoT) التي قد تضم مورداً واحداً أو أكثر لخدمة الهوية والخدمة. والمستعمل المستيقن منه في دائرة الثقة يمكنه النفاذ إلى موردي الخدمة داخل دائرة الثقة دون إجراء استيقان إضافي. أي أن المستعمل يحتاج إلى إجراء استيقان مرة واحدة ضمن دائرة ثقة واحدة.

بَيد أن عدد عمليات الاستيقان التي على المستعمل القيام بها تزيد مع تزايد عدد دوائر الثقة. ففي هذه الحالة، يتعين على مستعمل ما أن يقدم استيقاناً في كل مرة يقوم فيها بزيارة لدائرة ثقة. وذلك يعني أن على المستعمل أن يدير معلومات الإثباتات الواردة من مورد خدمة الهوية داخل دائرة ثقة. وغالباً ما ينسى المستعمل كلمة المرور أو تسجيلها بحيث يزداد احتمال الإفشاء غير المسموح. ويقدم الاتحاد داخل دائرة الثقة سبلاً ملائمة لتبادل معلومات هوية المستعملين. غير أن تقاسم معلومات الهوية بين دوائر ثقة مختلفة يقتضي اتفاق عمل مسبق وهو ما يستغرق وقتاً طويلاً نتيجة للإجراءات القانونية المتضمنة. فإذا لم يخرج ميدان إدارة الهوية عن حدود بيئة المؤسسة، فإن تكنولوجيا الاتحاد تقدم حلاً ممكناً بطريقة ناجعة وفعالة. ولكن إذا توسع ميدان نظام إدارة الهوية إلى الإنترنت، يصعب التوصل إلى اتفاقات عمل بين المؤسسات الخاصة بجميع الاتحادات.

وفي أنظمة إدارة الهوية القائمة على التطبيق على النطاق الواسع، فإن خدمات وسياسات الهوية يمكن تصميمها للوفاء بمتطلبات مورّدي خدمات الهوية وموردي الخدمة ومستمثلة لمتطلبات التطبيقات (مثل تزويد المستعمل بمعلومات حسابه). وعند تقديم خدمة هوية للمستعمل يتم تبادل الهوية عادة بين مورد خدمة الهوية ومورد الخدمة مباشرة. وفي هذه الحالة، للمستعملين سلطة محدودة على نشر معلومات هوياتهم.

ونظراً لتبادل معلومات الهوية بين كيانات المؤسسة دون تدخل المستعمل، فإن مراقبة الأمن وحماية الخصوصية يمكن أن يُهملا. وتظهر المشكلة عندما يحاول كيانان تقاسم معلومات هوية المستعمل التي تعود إلى المستعمل. إذ يتعين عليهما التوصل إلى اتفاق مسبق بشأن العمل وسياسة الخصوصية نظراً لأنهما يتعاملان بهوية المستعمل. فإن لم يحتج كيان سوى إلى تقاسم هوية المستعمل مع صاحبها الأصلي، فما على كل كيان إلا أن يبرم اتفاقاً ويضع سياسة أمن وخصوصية مع صاحب الهوية على استعمال معلومات هويته. (أو مع الكيان المكلف بإدارة هويته).

وفي مسعىً لحل هذه المشكلة، تضع هذه التوصية إطاراً عاماً لتعزيز تحكم المستعملين عند تبادل معلومات الهوية الرقمية الخاصة بهم.

2.7 التهديدات الأمنية

من المرجّح جداً وجود العديد من التهديدات الأمنية التي تظهر في أنظمة إدارة الهوية ما لم يتم التصدي لها بشكل ملائم. ويرد وصف للتهديدات الأمنية العامة في الفضاء السيبراني في التوصية [ITU-T X.1205].

وفي أنظمة إدارة الهوية، هناك تهديدات أمنية شتى تنال من حصانة النظام أو تودي إلى خرق أمني يعرّض أي منظمة للمخاطر. ويُعد تزوير الهوية واحداً من أكثر أنماط هذه التهديدات الأمنية استشراءً في بيئة إدارة الهوية.

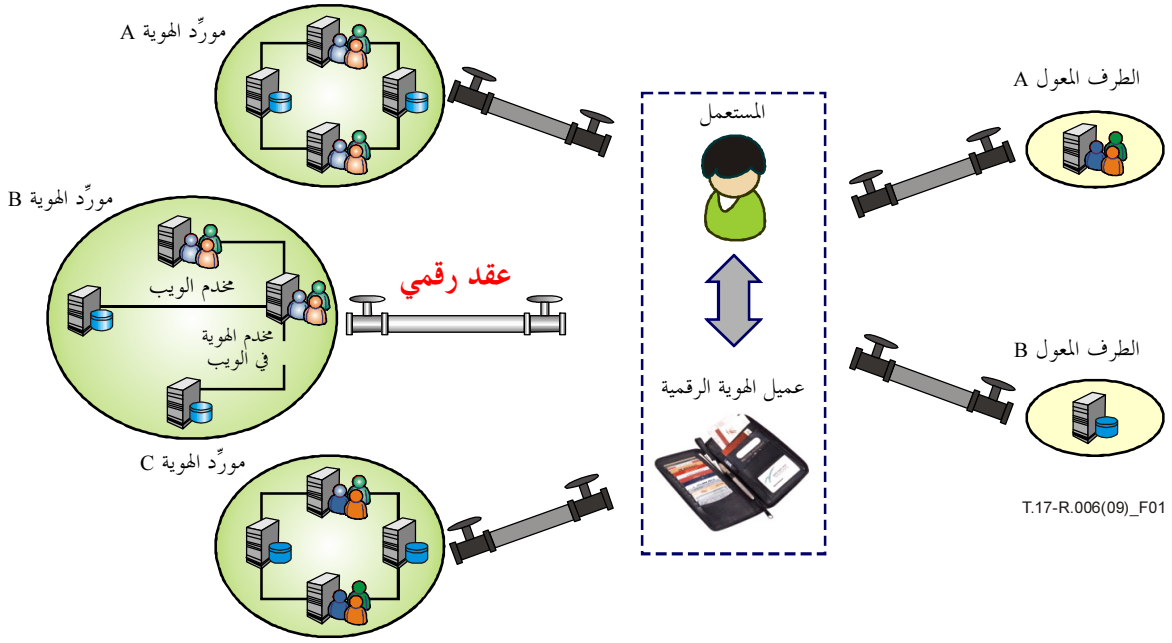
وتزوير الهوية قضية أمنية فائقة الأهمية، خاصة لدى الهيئات التي تخزن وتدير كميات كبيرة من معلومات الهوية الشخصية. فالخروقات التي ينجم عنها فقدان لبيانات شخصية لا تقف وحسب عند زعزعة ثقة العملاء والمؤسسات مما يؤدي على خسائر كبيرة تلحق بسمعة المنظمة، بل إن هذه الخروقات الخاصة بالبيانات يمكن أن تسبب تكاليفاً باهظةً من الناحية المادية للمنظمات.

فالتحايل هو محاولة يقدم عليها طرف ثالث تلمساً لمعلومات سرِّية لدى فرد أو جماعة أو منظمة، غالباً بتقليد علامة تجارية محددة ذائعة الصيت أو بالظهور بمظهرها، وذلك بغرض الربح المادي عادةً. فيصمَّم موقع التحايل على شبكة الويب ليقلد الموقع المشروع على الويب للمنظمة التي يجري انتحال علامتها التجارية. ويسعى المهاجم لخداع المستعملين بحيث يفصحوا عن بيانات شخصية مثل أرقام بطاقات الائتمان والإثباتات المصرفية على الخط، وغير ذلك من معلومات حساسة يمكن أن يستعملها/تستعملها بعد ذلك في أعمال احتيال. ويُعد التحايل في أنظمة إدارة الهوية تهديداً خطيراً، لأن معلومات استيقان الضحية أو أية معلومات أخرى قابلة للتعرف الشخصي – إذا وقعت في يد مهاجم – يمكن أن تُستعمل في سرقة الهوية أو في أي نشاط احتيالي آخر.

3.7 النموذج المفاهيمي لتبادل الهوية الرقمية

في هذا النموذج المفاهيمي، يستخدم الإطار العام لتبادل الهوية الرقمية مفهوم عميل الهوية الرقمية الذي يمكن أن يتحكم في تبادل معلومات الهوية الرقمية. ويمكن لعملية التحكم التي تتيح للمستعمل التحكم في تحرير معلومات الهوية أن تخفف كثيراً من الهجمات التي تهدد أمن النظام والتي يرد وصفها في الفقرة الخاصة بالتهديدات الأمنية (انظر الفقرة 2.7).

ويوضح الشكل 1 النموذج المفاهيمي لتبادل الهوية الرقمية.



الشكل 1 – النموذج المفاهيمي لتبادل معلومات الهوية الرقمية

1.3.7 مخدم الهوية

مخدّم الهوية هو المخدم الرئيسي الذي يورد معلومات عن هوية المستعمل إلى كيان يطلبها. أو يطلب معلومات الهوية لعميل DIC من أجل خدمات الويب. ويمكن لمخدم الهوية أن يكون مورد خدمة هوية، إذا كان يورد معلومات عن الهوية؛ وإلا فيمكن أن يكون طرفاً معولاً (RP) إذا كان يستخدم معلومات الهوية التي يقدمها المستعمل. ويمكن لمخدّم الهوية أن يؤدي دوري مورد خدمة الهوية والطرف المعول. وفي هذه الحالة، ينشر مخدم الهوية معلومات هوية من أجل بعض خدمات الويب بينما يحتاج إلى معلومات هوية المستعمل لبعض خدمات الويب الأخرى. ويمكن لمخدم ما في شبكة الويب أن يطلب من مخدّم الهوية أن يزوّده بمعلومات هوية المستعمل لكي يقوم بتقديم خدمة ويب.

2.3.7 عميل الهوية الرقمية

عميل الهوية الرقمية هو برنامج يوفر للمستعمل إدارة الاستيقان والإثبات والجلسة، فضلاً عن خدمات تبادل معلومات الهوية وحماية الخصوصية. وإذا احتاج لتقاسم معلومات الهوية مع مورد خدمة الهوية أو الطرف المعوّل، يقيم عميل الهوية الرقمية وصلة مع مخدم الهوية في شبكة الويب ضمن ميدان ما. ويمكن لعميل الهوية الرقمية أن يبرم عقداً مع مخدم الهوية في شبكة الويب لوضع أحكام وشروط خدمة تبادل الهوية بحيث تعزز حماية الخصوصية وجوانب الأمن عند تبادل معلومات الهوية. وتنساب معلومات كل هوية مستعمل عبر عميل الهوية الرقمية بحيث يمكن للمستعمل المعني أن يتحكم في تقاسم معلومات الهوية الخاصة به/بها. وعلى نحو خاص وطبقاً للسياسة المتفق عليها بين المستعمل والكيان، يحظى المستعمل بتحكم كامل في بيانات الهوية التي يتم تبادلها والغرض منها والجهة المرسلة إليها والمدة التي ستستعمل خلالها. ولا توجد حاجة لاكتشاف معلومات هوية المستعمل على اعتبار أن لدى العميل كل معلومات الوصلة اللازمة لتلقي معلومات الهوية وإرسالها.

3.3.7 مورد خدمة الهوية

مورد خدمة الهوية هو الكيان الذي يدير معلومات هوية المستعمل ويوفر خدمات الاستيقان والتخويل وخدمات تبادل الهوية لمخدّمات الويب. ومورّد خدمة الهوية هو نموذج الدور المفاهيمي الذي يمكن أن يسند إلى الكيان الذي يقوم بإدارة الهوية ويقدم هذه المعلومات عندما يطلبها عميل الهوية الرقمية. ويقوم مورّد خدمة الهوية بإدارة معلومات الهوية التي يقدمها المستعمل أو المعلومات التي يولدها بنفسه.

4.3.7 الطرف المعوّل

الطرف المعول هو نموذج لدور مفاهيمي آخر للكيان الذي يطلب هوية المستعمل من عميل الهوية الرقمية ويقدم خدمة باستعمال المعلومات التي يحصل عليها عن الهوية. ولا يعول هذا الطرف على مورد خدمة هوية للاستيقان. ويلجأ المستعمل إلى عميل الهوية الرقمية من أجل استيقانه لدى الطرف المعول.

5.3.7 المستعمل

يرد تعريف المستعمل في الفقرة 3. وفي النموذج النظري يدل المستعمل عادة على شخص أو مشترك في سياق إدارة الهوية المتمركزة على المستعمل. والمستعمل هو المستعمل النهائي الذي يمتلك عميل هوية رقمية ويشغله.

4.7 العقد الرقمي

يتحتم على معلومات الهوية الشخصية المنسابة بين مورد خدمة الهوية والطرف المعول أن تمر عبر عميل من عملاء الهوية الرقمية في بيئة لإدارة الهوية متمحورة حول المستعمل. وهذا يتيح فرصة للمستعمل كي يتحكم باستعمال المعلومات الخاصة بهويته/هويتها. ولا يبرم العقد الرقمي إلا بين مستعمل ومورد خدمة هوية أو بين مستعمل وطرف معوّل. ولا يسمح بالعقد متعدد الأطراف لاحتمال أن يتسبّب في تعقيد المسائل الإدارية التي يتعيّن على المستعمل التعامل معها. والعقد الرقمي هو المكون الأساسي الذي يمكن أن يوفر تحكماً دقيقاً للمستعمل في حركة المعلومات الخاصة بهويته/هويتها. ويوضح الشكل 2 هيكل العقد الرقمي.

T.17-R.006(09)_F02

الشكل 2 – هيكل لعقد رقمي

تشمل أنماط الضوابط التي يمكن تعريفها في العقود الرقمية أية سياسات لازمة للتوسط في علاقة تبادل معلومات هوية. واستناداً إلى ما تنص عليه اللوائح أو المتطلبات الأخرى الخاصة بالسياسات، قد لا يلزم وجود عقد رقمي عند كل عملية تبادل للهوية. فهو لا يلزم إلا عند الحاجة للتحكم بانسياب أو إخفاء معلومات الهوية الشخصية المتقاسمة. وشأن هذا المكون في المرونة وقابلية التوسع شأن العقود الحقيقية (مثل اتفاقات عدم الإفصاح). وبعد، نظراً لإمكانية كون العقود الرقمية بحد ذاتها وثائق مكتوبة بلغة وسم قابلة للتوسيع (XML)، فبوسعها إدارة ما يخصها من مراجعة وتعديل وحذف (على غرار العقود الحقيقية). ومن بين عناصر هذه العقود:

1) الشروط العامة: تصف الإصدار وتاريخ الاتفاق وتاريخ السريان علاوة على أي إشعار لمستعمل. وتعد الشروط العامة عنصراً إلزامياً في العقد الرقمي.

2) الغرض: الغاية التي ستُستخدم من أجلها معلومات الهوية الشخصية للمستعمل. وهذا عنصر إلزامي.

3) مراجع النعوت: تبين نعوت الكيان الذي يشير إليه العقد. وهذا عنصر إلزامي.

4) السياسة الأمنية: يلزم وجود هذا العنصر لاحتواء الاستيقان وسياسة أمن المعلومات، إذ يبين هذا العنصر كيف يمكن استيقان كيانين وكيف تؤمَّن المعلومات. وهذا عنصر إلزامي.

5) سياسة الخصوصية: يمكن لهذا العنصر أن يشمل أي نوع من أنواع بيان سياسة الخصوصية. ويمكن توصيف تزامن وإنهاء المعلومات للهوية الشخصية هنا. ويجب توفير حماية الخصوصية بما يتمشى مع قوانين الخصوصية المطبقة إقليمياً/وطنياً ويعد هذا عنصراً اختيارياً.

6) سياسة التحكم بالنفاذ: يمكن في هذا العنصر وصف أية سياسة تحكم بالنفاذ أو سياسة تخويل. ويعد هذا عنصراً اختيارياً.

7) مراجع السياسات: يمكن هنا توصيف مراجع تحيل إلى سياسات معرّفة في الخارج. ويعد هذا عنصراً اختيارياً.

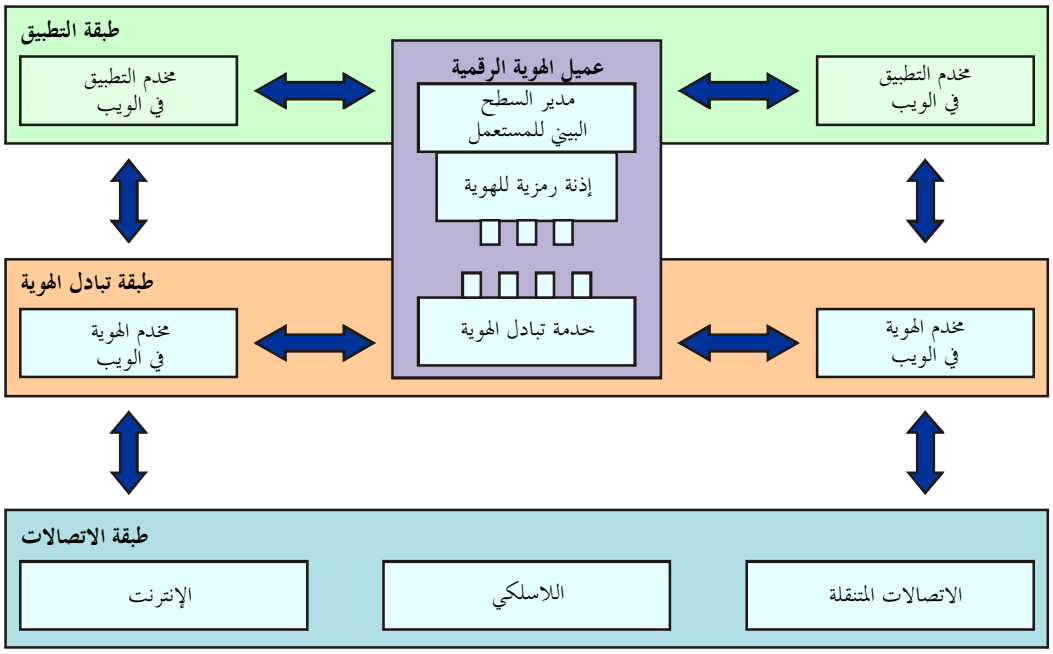
8) التوقيع: يمكن للعقد أن يُبرم بين كيانين توصّلا إلى اتفاق بشأن مضمون العقد الرقمي. وبالتالي، يمكن للعقد أن يحمل توقيعين رقميين كحد أقصى يمثلان الكيانين المتفقين على العقد. ومن ثم، ونتيجة للأسباب الواردة في الفقرة الأولى في هذا البند، لا يجوز أن يتضمن العقد أكثر من توقيعين. ويتحتم على الكيانين توقيع العقد كي يكون سارياً وسليماً. ويُعتبر توقيع المستعمل على العقد بمثابة موافقة على مضمونه. ويغطي تأثير التوقيع الوارد في العقد من الأحكام العامة إلى مراجع السياسات العامة (كما هو مبيّن في الشكل 2). وهذا عنصر إلزامي.

5.7 ثلاث طبقات لتبادل الهوية

تُعرّف هذه الفقرة ثلاث طبقات: طبقة التطبيق وطبقة تبادل الهوية وطبقة الاتصال.

1.5.7 طبقة التطبيق

يمكن لطبقة التطبيق أن تكون تطبيقاً عادياً في شبكة الويب يعمل في بيئة الإنترنت أو بيئة اتصالات متنقلة. فعلى سبيل المثال، يستعمل مستعمل متصفح الويب لطلب خدمة في شبكة الويب من مخدم في شبكة الويب. وعندما يحتاج كيان في التطبيق لطلب خدمة هوية أو استيقان، فهو يطالب بتقديم الخدمة في طبقة تبادل الهوية. ويتم وضع عميل الهوية الرقمية منطقياً في طبقتي التطبيق وتبادل الهوية معاً ليوصل بينهما بحيث يقدما خدمات سلسة إلى المستعمل فيما يتعلق بالهوية. وفي كل مرة يحاول فيها مستعمل تسجيل دخول إلى موقع الويب، يطلب/تطلب من منتقي الهوية، وهو أحد مكونات إدارة السطح البيني للمستعمل باختيار إذنة تمثل هوية لاستيقان موقع الويب. وعندما يحتاج تطبيق في الويب لتقاسم معلومات هوية المستعمل استجابةً لطلب خدمة من المستعمل، فلا يتطلب الأمر سوى استدعاء واحدة من خدمات تبادل الهوية المقدَّمة في طبقة تبادل الهوية. ويتوفر تحديد موقع وصف خدمة في طبقة تبادل الهوية من أجل إدارة تطبيق في شبكة الويب.



الشكل 3 – طبقة تبادل الهوية

2.5.7 طبقة تبادل الهوية

توفر طبقة تبادل الهوية طبقة وصلة شفافة لتبادل الهوية لكي تسهل تبادل الهوية بين الكيانات وتمكِّن المستعمل من التحكم الكامل في إنفاذ سياسات الأمن والخصوصية الخاصة به/بها.

وبفضل إدخال هذه الطبقة، يمكن تطوير تقاسم معلومات الهوية بين مختلف الكيانات ونشره بمعزل عن حيثيات أي تطبيق نظراً لأن التطبيق لا يلزمه معرفة تفاصيل عملية تبادل الهوية. وبالإضافة إلى ذلك، يمكن لطبقة تبادل الهوية أن توفر شتى الوظائف المتعلقة بتبادل الهوية لحلول إدارة الهوية القائمة التي ليس لديها مقدرات لتبادل الهوية. ويرد الوصف التفصيلي لكيفية امتثال سياسة أمن وخصوصية مرافق طبقة تبادل الهوية في الفقرة الخاصة بالعقد الرقمي (انظر الفقرة 4.7).

3.5.7 طبقة الاتصال

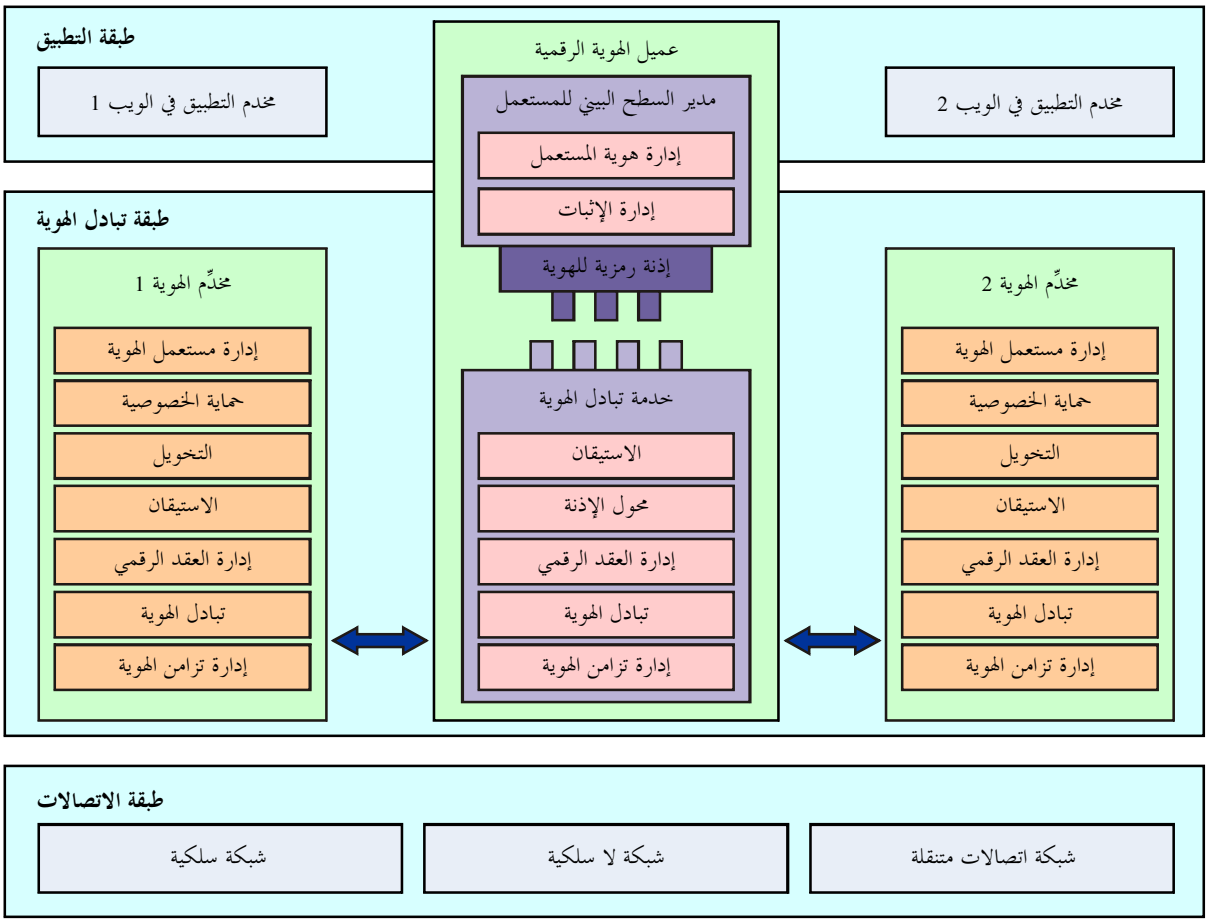
طبقة الاتصال هي طبقة مستقلة تتولى مسؤولية نقل البيانات من جهاز إلى آخر.

8 الإطار العام لتبادل الهوية الرقمية

1.8 مبادئ التصميم

يعتمد الإطار العام مبادئ التصميم التالية ليوفر تبادلاً سلساً للهوية بين الكيانات في بيئة حاسوبية تضم الخدمة المتنقلة والحوسبة في كل مكان.

- **الاستقلالية** – لا يرتبط الإطار العام بأي تطبيق محدد أو بيئة شبكة محددة. وبعبارة أخرى، ينبغي أن يكون الإطار العام متكيفاً في حد ذاته مع أية بيئة عند الضرورة.
- **قابلية التوصيل** – في بيئة حوسبة متنقلة أو منتشرة في كل مكان، يمكن لمستعمل أن يعمل بعدة أجهزة لأغراض العمل أو التسلية. وفي هذه الحالة، يحتاج المستعمل إلى معلومات الهوية الأساسية التي يمكن أن تثبت هويته/هويتها. وينبغي أن تُصمم هذه المعلومات بحيث تتلاءم مع أي جهاز وتمكّن المستعمل من إدخال معلومات هويته/هويتها فحسب في الجهاز لاستعماله.
- **المرونة** – ينبغي أن يُصمم الإطار العام ليكون مرناً بما فيه الكفاية ليتلاءم مع أي جهاز ابتداءً بمحطة العمل وانتهاءً بجهاز الحوسبة الصغير المنتشر في كل مكان. وينبغي أن يكون الإطار العام طيّعاً بما فيه الكفاية ليكون قابلاً للتشكيل كي يتكيف مع مختلف بيئات الحوسبة.
- **قابلية التدرّج** – لا بد من أن يكون الإطار العام بحد ذاته قابلاً للتشغيل من ميدان واحد إلى ما بين الميادين دون أن يستلزم مزيداً من الاتصالات والحوسبة من أجل إدراجه في نظام قائم.



T.17R.006(09)_F04

الشكل 4 – الإطار العام لتبادل الهوية الرقمية

2.8 مكونات الإطار العام

ويعد عميل الهوية الرقمية المكون الأساسي في هذا الإطار العام، إذ يسهل إقامة وصلة الهوية التي توصل بين جميع مورّدي خدمات هوية المستعمل وأطرافها المعنية. وللمستعمل أن يسترجع/تسترجع هويته/هويتها ويحدِّثها/تحدِّثها كلما دعت الحاجة إليها باستعمال الوصلة المقامة مسبقاً.

ويتألف عميل الهوية الرقمية من ثلاثة أجزاء: مدير السطح البيني للمستعمل وخدمة تبادل الهوية وإذنة الهوية.

ويمثل الشكل 4 المكونات الوظيفية للإطار العام.

1.2.8 إدارة هوية المستعمل

يدير هذا المكون معلومات هوية المستعمل المزمع تقاسمها بين الكيانات. فلدى خدمة الهوية، تركز إدارة الهوية على التخزين بصورة رئيسية. ومن جهة أخرى، تسعى إدارة الهوية لدى عميل الهوية الرقمية لأن تركز على السطح البيني للمستعمل الذي يقدم معلومات الهوية للمستعمل.

2.2.8 حماية الخصوصية

يدير هذا المكون الوظيفة المتصلة بالخصوصية التي تحمي معلومات هوية المستعمل. ويتتبع معلومات التدقيق المتصلة باستخدام هوية المستعمل والغرض منه. وتطبق هذه الوظيفة أيضاً قيود الخصوصية الموصوفة في عقد رقمي كلما استُعملت هوية المستعمل عن قصد أو بغير قصد. ويجب توفير حماية الخصوصية وفقاً لقوانين الخصوصية النافذة على الصعيد الإقليمي/الوطني.

3.2.8 التخويل

الغرض من خدمة التخويل هو اتخاذ القرارات فيما يتعلق بحقوق نفاذ المستعمل، وإنفاذ قرارات التخويل طبقاً لامتيازات المستعمل. ويُعد التخويل خدمة اختيارية لا تُقدم إلا عند الحاجة للتحكم بالنفاذ إلى الموارد على أساس حقوق المستعمل.

4.2.8 الاستيقان

يوفر هذا المكون إطاراً عاماً تنوعياً للاستيقان يدعم شتى أنواع آليات الاستيقان. وتشمل خدمة الاستيقان الاستيقان المتبادل للعميل والمخدمات على السواء.

5.2.8 مدير العقد الرقمي

يدير هذا المكون قائمة العقود الرقمية المبرمة بين المستعمل ومورد خدمة الهوية من أجل الاستيقان والتحكم بالنفاذ وحماية الخصوصية. ويدير المدير دورة حياة أي عقد رقمي يحمل توقيعاً رقمياً.

6.2.8 تبادل الهوية

هذا هو المكوّن الأساسي الذي يوفر خدمة تبادل الهوية. وينقسم تبادل الهوية إلى خدمتين: الاسترجاع والتحديث، ففي حال تخزين معلومات الهوية لدى كيان ما، يمكن للعميل DIC استرجاع هويته من الكيان والعكس. وفي حال تغير معلومات الهوية المخزنة لدى الكيان، يمكن للكيان تحديث أو الدفع بمعلومات الهوية المحدثة لديه إلى العميل DIC والعكس. وتناول هذا المكون بمزيد من التفصيل يقع خارج نطاق هذه التوصية.

7.2.8 مدير تزامن الهوية

يدير هذا المكون عملية تزامن الهوية لدى عميل الهوية الرقمية. وعندما تغير معلومات الهوية المخزنة لدى مورّد خدمة هوية، يقوم مورد خدمة الهوية بتحديث الهوية المتغيّرة لدى العميل DIC. ولدى العميل DIC. ولدى العميل DIC، يقوم هذا المكون بعملية تحديث في وظيفة تبادل معلومات الهوية من أجل كل طرف معول تقاسم هوية المستعمل مع عميل الهوية الرقمية. ويجدر بالذكر أن الطرف المعول الذي قام العميل DIC بتسلّم هوية لمرة واحدة مؤهل دون غيره لتلقي الهوية المحدّثة.

8.2.8 مدير السطح البيني للمستعمل

يمثل هذا المكوّن السطح البيني البياني للمستعمل من أجل معلومات هوية المستعمل ومعلومات الإثباتات. ويكون لهذا المكوّن صلة وثيقة بمخدّم التطبيق في شبكة الويب عموماً عندما يحتاج مستعمل لتسجيل دخوله بواسطة الاستيقان أو عندما يتقاسم/تتقاسم معلومات هويته/هويتها من أجل خدمة ما.

9.2.8 إدارة الإثبات

يدير هذا المكوّن معلومات إثبات الاستيقان الخاصة بالكيان أو المولدة في الموقع. ويجوز أن يكون لمستعمل واحد إثباتات متنوّعة من قبيل كلمة المرور وشهادة X.509 والخواص البيومترية. ويُحدد تمثيل بياني مشترك لمعلومات الإثبات كي تكون متّسقة أمام ممارسات المستعمِل.

10.2.8 إذنة الهوية

إذنة الهوية هي نموذج بيانات للهوية الرقمية. ويمكن إدخالها إلى عميل الهوية الرقمية لتوصيل مدير السطح البيني للمستعمل مع خدمة تبادل الهوية لتمكين عميل الهوية الرقمية من القيام بوظيفته. ويمكن تحقيق التمثيل المنطقي للإذنات الرمزية عندما يكون مدير السطح البيني للمستعمل مرفقاً. فمثلاً عندما يبدل مستعمل بيئة عمله من حاسوب شخصي إلى هاتف متنقل، فإنه لا يحتاج إلا لحمل الإذنات وإدخالها في الهاتف المتنقل. ويمكن أن تكون المعدّات التي تحوي هذه الإذنة بطاقة ذكية أو الإذنة يتم إدخالها عن طريق مقبس USB، وما إلى ذلك.

11.2.8 خدمة تبادل الهوية

يتولى هذا الجزء من الخدمة مسؤولية تبادل الهوية والتزامن. ووفقاً لنوع الشبكة أو منصّة الاتصالات المستعملة، يتعيّن تعديل هذا الجزء كي لتلاءم مع البيئة. فعلى سبيل المثال، تختلف تماماً وحدة خدمة تبادل الهوية في حاسوب شخصي عنها في هاتف متنقل.

12.2.8 محوّل الإذنة

يحول هذا المكون الإذنة الصادرة عن نظام آخر لإدارة الهوية إلى إذنة يتسنى فهمها ومعالجتها في الإطار العام لتبادل الهوية الرقمية. ويُعدّ هذا مكوّن البوابة للعمل البيني مع أنظمة إدارة الهوية الأخرى القائمة من أجل تبادل مختلف الإذنات (مثل تلك الخاصة بالهوية والأمن). وهذا مكوّن اختياري.

التذييل I

المبدأ التوجيهي للتنفيذ المرجعي لإطار عام لتحكم المستعمل في الهوية الرقمية باستعمال الثقة في خدمة الويب وتكنولوجيا بطاقة المعلومات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

ملاحظة – يقدم هذا التذييل مثالاً عن تقابل الثقة في خدمة الويب [b-WS-TRUST] وبطاقة المعلومات [b-IS-INTEROP] مع قدرات هذه التوصية.

1.I مقدمة

يصف هذا التذييل كيفية تلبية المتطلبات الواردة في هذه التوصية بواسطة الثقة في خدمة الويب وتكنولوجيا بطاقة المعلومات كما هو وارد في المعيار [b-CARDSPACE].

2.I الخلفية

2.1.I عميل الهوية الرقمية

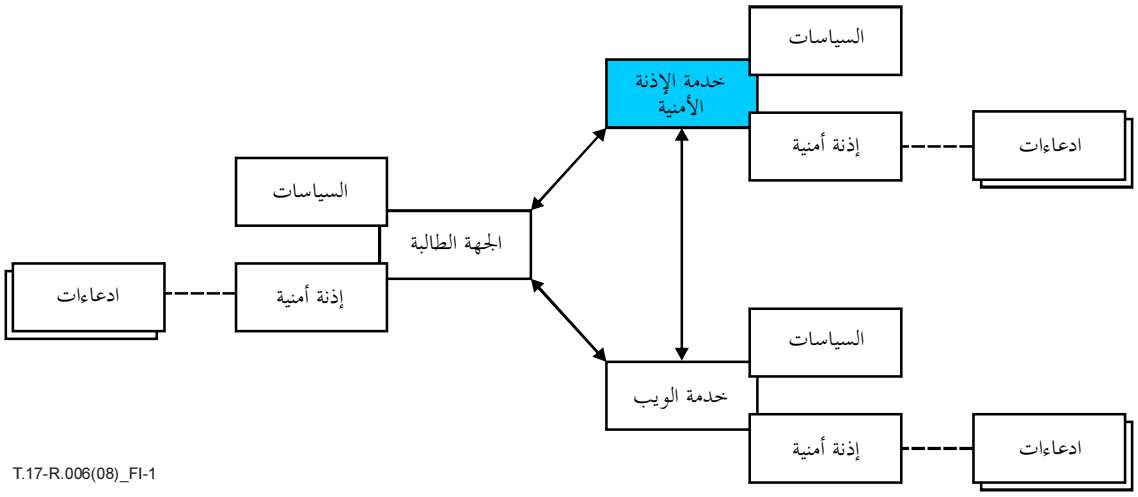
تصف الفقرة 2.3.7 "مفهوم عميل الهوية الرقمية الذي يمكن أن يتحكم في تبادل الهوية الرقمية".

2.2.I طبقة تبادل الهوية

تصف الفقرة 2.5.7 "طبقة لتبادل الهوية لكي تسهل تبادل الهوية بين الكيانات وتتيح للكيان التحكم الكامل في إنفاذ سياسات الأمن والخصوصية الخاصة به".

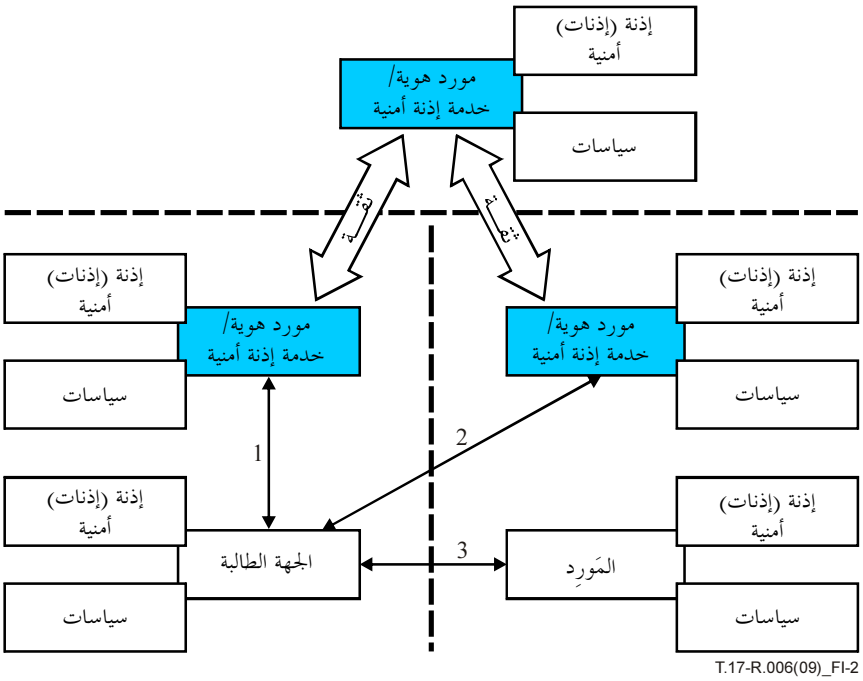
2.3.I الثقة في خدمة الويب

تعرّف مواصفة الثقة في خدمة الويب التمديدات القائمة على أمن خدمة الويب لتوفر إطاراً عاماً لطلب الإذنات الرمزية الأمنية وإصدارها، وللتوسط في علاقات ثقة. وعادةً تقوم جهة طالبة بإرسال رسالة طلب إذنة أمنية (RST) إلى خدمة إذنة أمنية (STS) نيابة عن كيان ما وتتلقى رداً على طلب الإذنة الأمنية (RSTR) يحوي عادة هذه الإذنة الأمنية. ثم يمكن بعد ذلك إرسال الإذنة الأمنية الحاوية مجموعة من الادعاءات إلى خدمة الويب كبرهان على هوية الجهة الطالبة. ويمكن اختيارياً إرسال طلب إذنة أمنية إلى خدمة الإذنة الأمنية مشفوعاً بطلب التحقق من صلاحية الإذنة الأمنية الصادرة من قبل أو إلغائها. ويبين الشكل 1.I هذه المعاملات.



الشكل 1.I – الثقة المباشرة في خدمة الويب

ويمكن استعمال الثقة في خدمة الويب لتنفيذ نماذج متنوعة خلاف نموذج الثقة المباشرة البسيط. إذ يُستعمل في بعض الحالات نموذج غير مباشر حيث يرسل مورّد خدمة هوية (IP)/خدمة إذنة أمنية (STS) طلب إذنة أمنية إلى خدمة إذنة أمنية أخرى بغية تلبية طلب الإذنة الأمنية الأصلي، كما يظهر في الشكل 2.I.



الشكل 2.I – الثقة غير المباشرة في خدمة الويب

4.2.I بطاقة المعلومات

يرد وصف تكنولوجيا بطاقة المعلومات في الملامح العامة لقابلية التشغيل البيني لمنتقي الهوية [b-IS-INTEROP]. وتتيح تكنولوجيا بطاقة المعلومات لمنتقي هوية ولمكونات نظام الهوية المصاحبة له أن يديروا هوياتهم الرقمية من مختلف موردي الهوية، وأن يستخدموها في شتى السياقات للنفاذ إلى الخدمات على الخط.

وتستلم الكيانات بطاقات معلومات عند إقامتها علاقة مع مورّدي خدمات الهوية. وتحتوي بطاقات المعلومات هذه على بيانات شرحية تصف الإذنة الأمنية المحتمل طلبها عبر الثقة في خدمة الويب، علاوة على الآليات الأمنية المستعملة لحماية تبادل الرسائل واستيقانها. ويركّب كيان ما، نمطياً، بطاقات المعلومات لديه في مخزن بطاقات يمكن النفاذ إليه من منتقي الهوية التابعين له. وتوصَّف السياسة الأمنية للطرف المعول عبر السياسة الأمنية لخدمة الويب [b-WS-SECURITY] ويمكن استرجاعها بطرق شتى بما فيها الطرق المدمجة في صفحات الويب. وتوصّف السياسة الأمنية نمطياً الآليات المعرّفة في أمن خدمة الويب من أجل الاستيقان وحماية الرسالة. ويقيّم منتقي الهوية سياسة الطرف المعول ومجموعة بطاقات المعلومات المركبة في مخزن بطاقات المستعمل، ويتيح للكيان الانتقاء من مجموعة بطاقات المعلومات ما يطابقه (أي القادرة على الحصول على إذنة أمنية تطابق السياسة الأمنية). ثم يستعجل منتقي الهوية الكيان في تقديم معلومات الاستيقان، عند الضرورة، ويرسل طلب إذنة أمنية إلى خدمة الإذنة الأمنية الموصّفة في بطاقة المعلومات المنتقاة. عندئذ يمكن إرفاق الإذنة الأمنية من الرد الناتج عن على طلب إذنة أمنية برسالة تُرسَل إلى الطرف المعول. وفي الحالة التي يكون فيها موقع الويب عبارة عن الطرف المعول، يمكن وضع الإذنة الأمنية كرد على الاستمارة التي تحتوي على السياسة الأمنية [b-IS-GUIDE].

3.I قدرات الإطار العام لتبادل الهوية الرقمية

تورد هذه الفقرة ثانية قدرات الإطار العام لتبادل الهوية الرقمية وتصف كيفية استعمال الثقة في خدمة الويب و/أو تكنولوجيا بطاقة المعلومات لتلبية هذه المتطلبات.

1.3.I قدرات عامة

1.1.3.I قدرات المستعمل

ينبغي للإطار العام لتبادل الهوية الرقمية تحقيق الأهداف التالية:

1) *توفير منتقي هوية يتيح له اختيار الإثبات الذي يستعمله في الاستيقان.*

يتيح منتقي الهوية، حسب وصفه الوارد في بطاقة المعلومات، ممارسة آمنة وبديهية ومتسقة للكيان ويسمح له بانتقاء بطاقات معلومات تمثل هويات متنوعة يقدمها موردو خدمة هوية مختلفون بآليات استيقان متنوعة.

2) *توفير سطح بيني حساس ومتسق لإدارة معلومات الإثبات الخاصة به/بها بالحد الأقصى من الأمن.*

يتيح منتقي الهوية، حسب وصفه الوارد في بطاقة المعلومات، ممارسة آمنة وبديهية ومتسقة للكيان.

3) *دعم الملء الآلي لاستمارات التسجيل أو الاشتراك في موقع للويب اختصاراً إلى أدنى حد لمعاملات المستعمل مع الموقع، بما في ذلك التحكم الكامل للمستعمل في تفعيل وتعطيل مثل هذه الآليات، وهذه القدرة اختيارية.*

يمكن لقيم الادعاء الواردة في الإذنة الأمنية المستعملة بالاقتران مع منتقي الهوية، حسب وصفه الوارد في بطاقة المعلومات، أن تقدم معلومات يدخلها الكيان نمطياً عند التسجيل.

4) *إتاحة معلومات الهوية في أي وقت يرغب فيه المستعمل، وتمكين المستعمل من التحكم الكامل في تبادل الهوية بواسطة آلية مناسبة لحماية الخصوصية.*

تقوم فرضية تكنولوجيا بطاقة المعلومات على أن مورد خدمة الهوية لا يقدم معلومات هوية إلا نزولاً على طلب الكيان. وتتوفر سياسة الخصوصية للطرف المعول ومورد خدمة الهوية ضمن السطح البيني الآمن لمستعمل منتقي الهوية أثناء انتقاء بطاقة المعلومات.

5) *توفير تحديثات آلية لمعلومات الهوية المتقاسمة عندما يتغير المصدر الأصلي وذلك تحت سيطرته/ سيطرتها الكاملة.*

يمكن لقيم الادعاء الواردة في الإذنة الأمنية المستعملة بالاقتران مع منتقي الهوية، حسب الوصف الوارد في بطاقة المعلومات، أن تقدم معلومات يدخلها الكيان نمطياً عند التسجيل. ونظراً لإمكانية أن يطلب الطرف المعول نفس قيم الادعاء الواردة في الإذنة الأمنية عند كل زيارة، فإنه يسهّل نشر التغيرات في هذه القيم.

6) *تزويد المستعمل بالتحكم الكامل في كيفية وضع سياسات الأمن والخصوصية وكيفية إنفاذها بغية التحكم في تبادل الهوية قبل تقاسم معلوماتها بحيث يكون للمستعمل تأثير مباشر على وضع السياسات وإنفاذها.*

تتوفر السياسة الأمنية للطرف المعول ومورد خدمة الهوية ضمن السطح البيني الآمن لمستعمل منتقي الهوية، حسب الوصف الوارد في بطاقة المعلومات، وذلك أثناء انتقاء بطاقة المعلومات.

2.1.3.I قدرات وظيفية

1) *دعم الإدارة المتكاملة للإثباتات التي يمكن أن تدير معلومات إثباتات المستعمل من أجل الاستيقان.*

تضم تكنولوجيا بطاقة المعلومات منتقي هوية وسطح بيني لمستعمل إدارة البطاقة.

2) *دعم إدارة وصلة لتبادل الهوية لتزويد المستعمل برؤية شاملة للكيانات التي لها توصيلات معها من أجل تبادل الهوية*

في حالة إعادة إذنة أمنية تمثل دورة من مورد خدمة هوية، يمكن لمورد خدمة الهوية أن يوفر سطحاً بينياً ليتيح للكيان رؤية مجموعة الدورات المقامة.

3) *دعم آليات متعددة للاستيقان يمكن أن تشمل الاستيقان القائم على كلمات السر وعلى البنية التحتية للمفاتيح العمومية وعلى العوامل البيومترية.*

الثقة في خدمة الويب وأمن خدمة الويب يوفران بروتوكولاً متسقاً وبديهياً يدعم مختلف آليات الاستيقان. وتوفر تطبيقات تكنولوجيا بطاقة المعلومات سطوحاً بينية بديهية لبرمجة التطبيق لاستهلال عملية الاستيقان.

4) *دعم آليات تبادل الهوية التي يمكن أن توفر وصلة ثنائية الاتجاه لتقاسم معلومات هوية المستعمل بين كيانات تستعمل عميل الهوية الرقمية*

يؤدي منتقي الهوية ومخزن البطاقات، باستخدام تكنولوجيا بطاقة المعلومات، الوظائف المرتبطة بعميل الهوية الرقمية.

5) *دعم آلية العقد الرقمي لإبرام عقد لتبادل الهوية ولكي يستعمل في إنفاذ سياسات الأمن الخصوصية المتعلقة بالكشف عن معلومات PII.*

تتوفر السياسة الأمنية للطرف المعول ومورد خدمة الهوية ضمن السطح البيني الآمن لمستعمل منتقي الهوية، حسب الوصف الوارد في بطاقة المعلومات، أثناء انتقاء بطاقة المعلومات.

6) *دعم تزامن معلومات الهوية بغية تحديث معلومات الهوية الموزعة والمتقاسمة على نحو متسق عند تغيّر مصدر معلومات الهوية الموزعة. وتقتصر معلومات الهوية التي يتعيّن مزامنتها على المعلومات PII التي يغيّرها المستعمل مباشرة.*

يمكن لقيم الادعاء الواردة في الإذنة الأمنية المستعملة بالاقتران مع منتقي الهوية، حسب الوصف الوارد في بطاقة المعلومات، أن تقدم معلومات يدخلها الكيان نمطياً عند التسجيل. ونظراً لإمكانية أن يطلب الطرف المعول نفس قيم الادعاء الواردة في الإذنة الأمنية عند كل زيارة، فإنه يسهل نشر التغيرات في هذه القيم.

7) *دعم التحويل إلى الإذنة الشاملة لجعل الإطار العام قابلاً للتشغيل البيني مع الأنظمة القائمة لإدارة الهوية*

توفر الثقة في خدمة الويب آلية لتبادل الإذنات. ويمكن لرسالة طلب إذنة أمنية أن تتضمن إذنة أمنية واحدة أو أكثر، فضلاً عن بيان لهوية الطرف المعول. ويمكن للرد على طلب إذنة أمنية أن يتضمن إذنة أمنية مناسبة للطرف المعول.

2.3.I قدرات إضافية

ينبغي للإطار العام لتبادل الهوية الرقمية أن يوفر آلية توسيع لمنتقي الهوية والبروتوكولات المصاحبة له لإتاحة الدعم لدخول وإرسال شتى آليات الاستيقان وضمان المعلومات المتصلة به.

ويشمل ذلك (على سبيل المثال لا الحصر) الدعم لأجهزة قراءة البطاقات الذكية وأجهزة إدخال الخواص البيومترية، علاوة على أنساق البيانات المصاحبة لها من قبيل تلك الموصوفة في [b-NIST].

ثُبت المراجع

[b-CARDSPACE] Microsoft (2006, April). *Introducing Windows CardSpace*

[b- ETSI 133 980] ETSI , *ETSI TR 133 980 V7.5.0 Technical Report*

[b-IS-INTEROP] Microsoft (2007, April). *Identity Selector Interoperability Profile V1.0*

[b-IS-GUIDE] Microsoft (2007, April). *A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers*

[b-ITU-T Y.2091] ITU-T Recommendation Y.2091 (2008), *Terms and definitions for Next Generation Networks*

[b-ITU-T Y.2701] ITU-T Recommendation Y.2701 (2007), *Security requirements for NGN release 1*

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

[b-LA-FF] Liberty Alliance. *Liberty ID-FF Protocols and Schema Specification (ver 1.2)*

[b-NIST] National Institute of Standards and Technology (2006, March). *FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employess and Contractors*

[b-WS-SECURITY] OASIS (2007, July 1). *WS-SecurityPolicy 1.2*

[b-WS-TRUST] OASIS (2007, March 19). *WS-Trust 1.3*

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