الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1254
(2012/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

إطار ضمان استيقان الكيان

التوصيـــة ITU-T X.1254

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	
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.1254

إطار ضمان استيقان الكيان

الملخص

تعرّف هذه التوصية أربعة مستويات لضمان استيقان الكيان (أي من مستوى الضمان الأول (LoA1) إلى مستوى الضمان الرابع (LoA4)) والمعايير والتهديدات الخاصة بكل مستوى من المستويات الأربعة لضمان استيقان الكيان. وبالإضافة إلى ذلك فهي تعمل على:

- تحديد إطار لإدارة مستويات الضمان؛
- وتوفير التوجيهات فيما يتعلق بتكنولوجيات التحكم التي يتعين استخدامها للتخفيف من حدّة التهديدات للاستيقان، استناداً إلى تقييم المخاطر؛
- وتوفير التوجيهات بشأن تنفيذ التقابل بين ومستويات الضمان الأربعة وخطط ضمان الاستيقان الأخرى؛
- وتوفير التوجيهات لتبادل نتائج الاستيقان التي تستند إلى مستويات الضمان الأربعة.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1254	2012/09/07	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).

نُشر نص مشابه برسم المعيار ISO/IEC 29115. وهو يختلف عن هذا النص في أربعة مواضع: 1) الفقرة 6.1.3: تعريف أوراق الاعتماد مختلف وهو في هذه التوصية يحيل إلى التعريف الوارد في التوصية ITU-T X.1251؛ 2) الجدول 10-1: المعيار ISO/IEC 29115 يتضمن مثالاً للشخصنة يشمل استعمال هوية كيان غير موجود؛ 3) الفقرة 1.2.2.10: المعيار ISO/IEC 29115 يشرح SSL كمثال لقناة محمية؛ 4) الملحق ألف في هذه التوصية، *خصائص أوراق الاعتماد*، معياري.

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 2013

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

جدول المحتويات

الصفحة

1 مجال التطبيق 1

2 المراجع المعيارية 1

3 التعاريف 1

1.3 مصطلحات معرّفة في وثائق أخرى 1

2.3 مصطلحات معرّفة في هذه التوصية 2

4 المختصرات 3

5 الاصطلاحات 4

6 مستويات الضمان 4

1.6 مستوى الضمان الأول (LoA1) 5

2.6 مستوى الضمان الثاني (LoA2) 6

3.6 مستوى الضمان الثالث (LoA3) 6

4.6 مستوى الضمان الرابع (LoA4) 6

5.6 اختيار مستوى الضمان المناسب 7

6.6 تقابل مستويات الضمان وإمكانية التشغيل البيني 8

7.6 تبادل نتائج الاستيقان استناداً إلى مستويات الضمان الأربعة 8

7 الجهات الفاعلة 9

1.7 الكيانات 9

2.7 مورد خدمة أوراق الاعتماد/الإثباتات 9

3.7 هيئة التسجيل 10

4.7 الطرف المعوّل 10

5.7 جهة التحقّق 10

6.7 الطرف الثالث الموثوق 10

8 مراحل إطار ضمان استيقان الكيان 10

1.8 مرحلة الانتساب 10

2.8 مرحلة إدارة أوراق الاعتماد/الإثباتات 13

3.8 مرحلة استيقان الكيان 15

9 الاعتبارات الإدارية والتنظيمية 16

1.9 إرساء الخدمة 16

2.9 الامتثال القانوني والتعاقدي 16

3.9 أحكام مالية 17

4.9 إدارة وتدقيق أمن المعلومات 17

الصفحة

5.9 مكونات الخدمة الخارجية 17

6.9 البنية التحتية التشغيلية 17

7.9 قياس القدرات التشغيلية 17

10 التهديدات وعمليات التحكم 18

1.10 التهديدات لمرحلة الانتساب وعمليات التحكم بها 18

2.10 التهديدات لمرحلة إدارة أوراق الاعتماد/الإثباتات وعمليات التحكم بها 20

3.10 التهديدات لمرحلة الاستيقان وعمليات التحكم بها 25

11 معايير ضمان الخدمة 29

الملحـــق ألف – مواصفات أوراق الاعتماد/الإثباتات 30

التذييل I – الخصوصية وحماية المعلومات التي تعرّف بصاحبها شخصياً 31

ببليوغرافيا ..... **ark not defined.**

مقدمة

يوجد لدى الكثير من المعاملات الإلكترونية داخل أنظمة تكنولوجيا المعلومات والاتصالات أو فيما بينها شروط تتعلق بالأمن تعتمد على مستوى مفهوم أو محدّد من الثقة بهويات الكيانات المعنية. وقد تتضمّن هذه الشروط حماية الأصول والموارد من النفاذ غير المرخّص والذي يمكن من أجله استخدام آلية التحكم بالنفاذ، و/أو إنفاذ المساءلة عن طريق الاحتفاظ بسجلات تدقيق تخص أحداثاً ذات صلة، وكذلك لأغراض تتعلق بالمحاسبة والترسيم.

وتقدم التوصية ITU-T X.1254 إطاراً لضمان استيقان الكيان. ويشير الضمان الوارد في هذه التوصية إلى الثقة الموضوعة في جميع العمليات وأنشطة الإدارة والتكنولوجيات المستخدمة في تحديد وإدارة هوية كيان ما من أجل استخدامها في معاملات الاستيقان.

الشكل 1 – لمحة عامة عن إطار ضمان استيقان الكيان

تقدم هذه التوصية، باستخدام مستويات الضمان الأربعة المحددة، توجيهات تتعلق بتكنولوجيات التحكم والعمليات وأنشطة الإدارة، فضلاً عن معايير الضمان التي يتعين استخدامها للتخفيف من حدّة التهديدات للاستيقان من أجل تنفيذ مستويات الضمان الأربعة. كما توفر توجيهات بشأن تنفيذ التقابل بين خطط ضمان الاستيقان الأخرى والمستويات الأربعة المحددة، فضلاً عن التوجيهات المتعلقة بتبادل النتائج التي تسفر عنها معاملات الاستيقان. أخيراً، توفر هذه التوصية توجيهات إعلامية تتعلق بحماية المعلومات التي تعرّف بصاحبها شخصياً والمقترنة بعملية الاستيقان.

والهدف من هذه التوصية هو استخدامها بصورة رئيسية من قبل مورّدي خدمة أوراق الاعتماد/الإثباتات وغيرهم من الجهات التي لديها اهتمام بخدماتهم (مثلاً الأطراف المعوّلة وجهات التقييم ومدقّقي الحسابات لهذه الخدمات). ويحدد إطار ضمان استيقان الكيان هذا الحد الأدنى من الشروط التقنية والإدارية والخاصة بالعملية لمستويات الضمان الأربعة من أجل كفالة التكافؤ فيما بين أوراق الاعتماد/الإثباتات التي تصدر عن مختلف مورّدي خدمة أوراق الاعتماد/الإثباتات. كما يقدم بعض الاعتبارات الإدارية والتنظيمية الإضافية التي تؤثر في ضمان استيقان الكيان، دون أن يطرح معايير محددة لتلك الاعتبارات. وقد تجد الأطراف المعوِّلة وغيرها من الجهات هذه التوصية مفيدة لاستيعاب ما يقدمه كل مستوى من مستويات الاستيقان وفهمه. وإضافة إلى ذلك، يمكن اعتمادها بهدف استخدامها ضمن إطار موثوق لتحديد المتطلبات التقنية لمستويات الاستيقان. ويستهدف إطار ضمان استيقان الكيان، على سبيل المثال لا الحصر، حالات استخدام قائمة على الدورات أو تتمحور حول الوثائق باعتماد تكنولوجيات الاستيقان المختلفة. ومن الممكن نشوء كل من تصورات الثقة المباشرة أو المتوسطة وذلك ضمن ترتيبات أو اتحادات قانونية/ ثنائية.

التوصيـــة ITU-T X.1254

إطار ضمانة استيقان الكيان[1]

1 مجال التطبيق

توفر هذه التوصية إطاراً لإدارة ضمان استيقان الكيان ضمن سياق معيّن. فهي تعمل بوجهٍ خاص على:

- تحديد المستويات الأربعة لضمان استيقان الكيان؛
- وتحديد المعايير والمبادئ التوجيهية لتحقيق كل مستوى من المستويات الأربعة لضمان استيقان الكيان؛
- وتوفير التوجيهات لتنفيذ التقابل بين خطط ضمان الاستيقان الأخرى ومستويات الضمان الأربعة؛
- وتوفير التوجيهات لتبادل نتائج الاستيقان التي تستند إلى مستويات الضمان الأربعة؛
- وتقديم التوجيهات فيما يتعلق بعمليات التحكم التي يتعين استخدامها للتخفيف من حدة التهديدات للاستيقان.

2 المراجع المعيارية

لا يوجد.

3 التعاريف

1.3 مصطلحات معرّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 زعم (assertion): بيان أدلى به كيانٌ دون إرفاقه بدليل على صحته [ITU-T X.1252].

ملاحظـــة – من المتفق عليه عموماً أن مصطلحي ادعاء وزعم متشابهان في المعنى بعض الشيء مع اختلاف طفيف في مدلولاتهما. ولأغراض هذه التوصية، يُعتبر الزعم أقوى في دلالته من الادعاء.

2.1.3 استيقان (authentication): تقديم ضمان يؤكد هوية كيان ما [ISO/IEC 18014-2].

3.1.3 عامل الاستيقان (authentication factory): المعلومات و/أو العملية التي تستخدم في استيقان هوية كيان ما أو التحقق من صحتها [ISO/IEC 19790].

ملاحظـــة – تقسم عوامل الاستيقان إلى أربع فئات:

- شيء يملكه الكيان (مثلاً بصمة جهاز، أو جواز سفر، أو تجهيزات تحتوي على أوراق اعتماد/إثباتات، أو مفتاح خاص)؛
- شيء ما يعرفه الكيان (مثلاً كلمة سر، رقم تعريف الهوية الشخصي PIN)؛
- صفة ينفرد بها الكيان نفسه (مثلاً خاصية من خصائص القياس الحيوي)؛
- شيء يفعله الكيان نفسه في المعتاد (مثلاً نمط سلوكي).

4.1.3 ادعاء (claim): القول بأن الأمر على نحو ما دون التمكن من تقديم إثبات على ذلك [ITU-T X.1252].

ملاحظـــة – من المتفق عليه عموماً أن مصطلحي ادعاء وزعم متشابهان في المعنى بعض الشيء مع اختلاف طفيف في مدلولاتهما. ولأغراض هذه التوصية، يُعتبر الزعم أقوى في دلالته من الادعاء.

---

[1] أعربت جمهورية كوريا عن تحفظ ولن تطبق هذه التوصية لأنها مناقضة للوائح التنظيمية في كوريا فيما يتعلق بالمستويات الأربعة المطلوبة لضمان استيقان الكيان والمعايير المرتبطة بها لتحقيق كل من مستويات الضمان الأربعة.

5.1.3 سياق (context) [ITU-T X.1252]: بيئة ذات ظروف حدية محددة توجد فيها الكيانات وتتفاعل.

6.1.3 أوراق اعتماد/إثباتات (credential) [ITU-T X.1252]: مجموعة بيانات تقدّم كدليل على هوية و/أو استحقاقات مدّعاة.

ملاحظـــة – انظر التذييل I للحصول على خصائص إضافية لأوراق الاعتماد/الإثباتات.

7.1.3 كيان (entity) [ITU-T X.1252]: شيء له وجود قائم بذاته ومميز ويمكن تعريفه في سياق ما.

ملاحظـــة – لأغراض هذه التوصية ، يُستخدم الكيان أيضاً في حالات معينة لشيء يدّعي هوية ما.

8.1.3 هوية (Identity) [ISO/IEC 24760]: مجموعة من النعوت المتصلة بكيان ما.

ملاحظـــة – قد يكون للهوية ضمن سياق معين معرّف واحد أو أكثر للتمكن من التعرّف على الكيان بشكل دقيق ومتفرّد ضمن ذلك السياق.

9.1.3 استيقان متعدد العوامل (multifactor authentication) [ISO/IEC 19790]: استيقان يدخل فيه على الأقل عاملان مستقلان للاستيقان.

10.1.3 عدم تنصّل (non-repudiation) [ITU-T X.1252]: القدرة على الحماية من إنكار أحد الكيانات المشاركة في إجراء ما مشاركته في الإجراء كله أو في جزء منه.

11.1.3 تنصّل (repudiation) [ITU-T X.1252]: إنكار أحد الكيانات المشاركة في إجراء ما مشاركته في الإجراء كله أو في جزء منه.

2.3 مصطلحات معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 بروتوكول الاستيقان (authentication protocol): تسلسل محدد من الرسائل بين كيان وجهة التحقق يمكّن جهة التحقق من تأكيد صحة هوية الكيان.

2.2.3 مصدر مُعتمَد (authoritative source): جهة إيداع يُعترف بأنها مصدر دقيق ومصدر لأحدث المعلومات.

3.2.3 مورّد خدمة أوراق الاعتماد/الإثباتات (credential service provider) (CSP): جهة فاعلة موثوقة تُصدر أوراق الاعتماد و/أو تديرها.

4.2.3 ضمان استيقان الكيان (entity authentication assurance) (EAA): درجة الثقة التي تم التوصل إليها في عملية الاستيقان بأن الكيان هو ما هو عليه أو أنه على النحو المتوقع (يستند هذا التعريف إلى تعريف "ضمان الاستيقان" الوارد في [b-ITU-T X.1252]).

ملاحظـــة – تقوم الثقة على أساس درجة الثقة في الربط بين الكيان والهوية المقدّمة.

5.2.3 معرّف الهوية (identifier): نعت واحد أو أكثر يُستعمل للتحديد الدقيق والمتفرد لهوية كيان ضمن سياق محدد.

6.2.3 التحقّق من الهوية (identity information verification): عملية التأكد من معلومات تدقيق الهوية وأوراق الاعتماد/الإثباتات مقابل الجهات المصدِرة لها ومصادر البيانات أو أي من الموارد الخارجية أو الداخلية الأخرى فيما يتعلق بالاستيقان والصلاحية والصحة وإسنادها إلى الكيان.

7.2.3 تدقيق الهوية (identity proofing): العملية التي تقوم هيئة التسجيل (RA) بموجبها بالحصول على معلومات كافية والتحقق منها لتعريف هوية كيان ما وفقاً لمستوى ضمان محدد أو مفهوم.

8.2.3 هجوم لمتطفل بين طرفين (man-in-the-middle attack): الهجوم الذي يكون فيه المهاجم قادراً على قراءة الرسائل وإقحامها وتعديلها بين طرفين دون علم منهما.

9.2.3 استيقان متبادل (mutual authentication): عملية استيقان لهويات الكيانات يستيقن فيها كيانان من بعضهما البعض بحيث يتأكد كل منهما من هوية الآخر.

10.2.3 تصيّد احتيالي (phishing): احتيال ينخدع به مستعمل البريد الإلكتروني للكشف عن معلومات شخصية أو سرية بحيث يستطيع المحتال استخدامها بصورة غير شرعية.

11.2.3 هيئة التسجيل (registration authority) (RA): الجهة الفاعلة الموثوقة التي تحدد هوية الكيان أمام مورّد خدمة أوراق الاعتماد/الإثباتات و/أو تكفل صحتها.

12.2.3 الطرف المعوّل (relying party) (RP): الجهة الفاعلة التي تعتمد على هوية مزعومة أو مدّعاة.

13.2.3 قيمة التظليل (salt): قيمة غير سرية، وغالباً عشوائية، تُستخدم في عملية التظليل.

ملاحظـــة – يُشار إليها أيضاً بالقيمة الملحية (salt) أو الرملية (sand).

14.2.3 سر مشترك (shared secret): سر يُستخدم في عملية الاستيقان يكون معلوماً فقط لدى الكيان وجهة التحقّق.

15.2.3 خاتم الوقت (time stamp): معلمة موثوقة متغيرة مع الزمن تُشير إلى نقطة زمنية بالنسبة لمرجع مشترك.

16.2.3 معاملة (transaction): عملية محددة تتم بين الكيان ومورّد الخدمة تقوم بدعم غرض تجاري أو برنامجي.

17.2.3 إطار ثقة (trust framework): طائفة من الشروط وآليات الإنفاذ للأطراف التي تتبادل معلومات تتعلّق بالهوية.

18.2.3 طرف ثالث موثوق (trusted third party) (TTP): سلطة أو وكيل لها، موثوق بها من قبل الجهات الفاعلة الأخرى فيما يتعلق ببعض (مثلاً الأنشطة المتصلة بالأمن).

ملاحظـــة – يتم الوثوق بطرفٍ ثالث موثوق من قبل كيان و/أو جهة تحقّق لأغراض الاستيقان.

19.2.3 مدة الصلاحية (validity period): الفترة الزمنية التي يمكن خلالها استخدام هوية أو أوراق اعتماد في معاملة واحدة أو أكثر.

20.2.3 تحقّق (verification): عملية تدقيق في معلومات بمقارنة المعلومات المقدمة بمعلومات تم تأكيدها في السابق.

21.2.3 جهة التحقق (verifier): جهة فاعلة تؤكد صحة معلومات الهوية.

ملاحظـــة – يمكن لجهة التحقق أن تشترك في عدة مراحل من إطار ضمان استيقان الكيان وأن تقوم بعملية التحقق من أوراق الاعتماد و/أو تدقيق الهوية.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

CA سلطة إصدار الشهادات (*Certification Authority*)

CSP مورّد خدمة أوراق الاعتماد/الإثباتات (*Credential Service Provider*)

EAA ضمان استيقان الكيان (*Entity Authentication Assurance*)

EAAF إطار ضمان استيقان الكيان (*Entity Authentication Assurance Framework*)

ICT تكنولوجيا المعلومات والاتصالات (*Information and Communication Technology*)

IdM إدارة الهوية (*Identity Management*)

IP بروتوكول الإنترنت (*Internet Protocol*)

LoA مستوى الضمان (*Level of Assurance*)

LoAs مستويات الضمان (*Levels of Assurance*)

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

NPE كيان مادي (غير شخصي) (*Non-Person Entity*)

PDA مساعد رقمي شخصي (*Personal Digital Assistant*)

PII معلومات محدّدة لهوية الشخص (*Personally Identifiable Information*)

PIN رقم تعريف الهوية الشخصي (*Personal Identification Number*)

RA هيئة التسجيل (*Registration Authority*)

RP طرف معوّل (*Relying Party*)

SAML لغة ترميز تأكيد الأمن (*Security Assertion Markup Language*)

TCP/IP بروتوكول مراقبة الإرسال/بروتوكول الإنترنت (*transmission control protocol/Internet protocol*)

TLS أمن طبقة النقل (*transport layer security*)

TPM وحدة منصة موثوقة (TPM) (*trusted platform module*)

TTP طرف ثالث موثوق (*trusted third party*)

URL موقع الموارد الموحّد (*uniform resource locator*)

5 الاصطلاحات

تطبق هذه التوصية الأشكال الشفهية التالية لتعابير النصوص:

أ) "يقوم/يفعل" تشير إلى معنى اشتراطي

ب) "يجب/يتعين على" تشير إلى التوصية بأمر ما

ج) "يجوز" تشير إلى السماح لطرف أو جهة بأمر ما

د) "بإمكان/يمكن لـــ" تشير إلى الإمكانية أو المقدرة على أمر ما.

6 مستويات الضمان

يحدد إطار ضمان استيقان الكيان (EAAF) هذا أربعة مستويات ضمان لاستيقان الهوية. ويعرض كل مستوى من مستويات الضمان وصفاً لدرجة الثقة في العمليات المفضية إلى عملية الاستيقان ذاتها وشاملة لها، الأمر الذي يقدّم ضماناً بأن الكيان الذي يستعمل هوية معينة هو في الواقع الكيان الذي خُصصت له تلك الهوية. ولأغراض هذه التوصية، يمثل مستوى الضمان دالة من دوالّ العمليات والأنشطة الإدارية والضوابط التقنية المنفّذة من قبل مورّد خدمة أوراق الاعتماد/الإثباتات لكل مرحلة من مراحل إطار ضمان استيقان الكيان استناداً إلى المعايير المبيّنة في الفقرة 10. ويتأثر ضمان استيقان الكيان بكل من الاعتبارات الإدارية والتنظيمية، علماً بأن هذه التوصية لا تقدم معياراً نظرياً معلناً لتلك الاعتبارات. وقد يكون الكيان شخصاً أو كياناً مادياً.

فقد يكون مستوى الضمان لشبكة على سبيل المثال دالّة في جميع المكونات التي تكوّن مجتمعةً الشبكة وتتضمّن كيانات مادية أو أجهزة طرفية (مثل الهواتف المتنقلة أو المساعِدات الرقمية الشخصية (PDA) أو أجهزة فك التشفير أو الحواسيب المحمولة). وفي بعض الحالات يمكن للأجهزة الطرفية أن تنتحل شخصية كيانات شرعية. وتبعاً لذلك، فإن القدرة على تمييز جهاز موثوق من جهاز زائف بدرجة معينة من الثقة تُعتبر أساسية بالنسبة لإطار ضمان استيقان الكيان.

ويعتبر مستوى الضمان الأول المستوى الأدنى بين مستويات الضمان، فيما يُعتبر مستوى الضمان الرابع المستوى الأعلى. ويتوقف تحديد مستوى الضمان الأنسب في وضع معين على مجموعة منوعة من العوامل. فتحديد مستوى الضمان اللازم

مرهن بصورة رئيسية بدرجة المخاطر: العواقب المترتبة على خطأ في الاستيقان و/أو إساءة استخدام أوراق الاعتماد/الإثباتات، والأضرار والتأثيرات الناجمة عن ذلك، واحتمال حدوثها. وتُعتمد مستويات ضمان أعلى لدى توقع درجة أعلى من المخاطر.

ويقدم إطار ضمان استيقان الكيان متطلبات وشروطاً وتوجيهات للتنفيذ لكل مستوى من مستويات الضمان الأربعة. كما يطرح بوجه خاص متطلبات لتنفيذ العمليات للمراحل التالية:

أ) الانتساب (مثلاً التحقق من الهوية وتدقيق الهوية والتسجيل)

ب) إدارة وثائق الاعتماد/الإثباتات (مثلاً إصدار أوراق الاعتماد/الإثباتات وتفعيل أوراق الاعتماد/الإثباتات)

ج) الاستيقان.

كما يقدّم توجيهات تتعلق بالاعتبارات الإدارية والتنظيمية (مثلاً، الامتثال القانوني وإدارة أمن المعلومات) التي تؤثر في ضمان استيقان الكيانات.

ويتم تعريف مستويات الضمان الأربعة على النحو المبيّن في الجدول 6-1:

الجدول 6-1 – مستويات الضمان[2]

المستوى	الوصف
1 – منخفض	درجة قليلة من الثقة أو انعدام الثقة بالهوية المزعومة أو المدعاة
2 – متوسط	بعض الثقة بالهوية المزعومة أو المدعاة
3 – مرتفع	درجة عالية من الثقة بالهوية المزعومة أو المدعاة
4 – مرتفع جداً	درجة عالية جداً من الثقة بالهوية المزعومة أو المدعاة

ويتضمن هذا الإطار شروطاً لتحقيق مستوى الضمان المنشود لكل مرحلة من مراحل إطار ضمان استيقان الكيان. أما مستوى الضمان الكلي المحقق باعتماد تنفيذ يستخدم هذا الإطار فسيكون مستوى المرحلة ذات مستوى الضمان الأدنى.

1.6 مستوى الضمان الأول (LoA1)

يوجد عند مستوى الضمان الأول حد أدنى من الثقة بالهوية المزعومة أو المدعاة للكيان، وبعض الثقة بأن الكيان هو الكيان نفسه على مدى حالات استيقان متتالية. ويُستخدم مستوى الضمان الأول هذا حين يرتبط الاستيقان الخاطئ بحد أدنى من المخاطر. ولا توجد شروط محددة لآلية الاستيقان المستخدمة باستثناء أنها توفّر درجة دنيا من الضمان. ويمكن لمجموعة واسعة من التكنولوجيات المتاحة، بما في ذلك أوراق الاعتماد/الإثباتات المقترنة بمستويات ضمان أعلى، أن تفي بشروط ضمان استيقان الكيان لمستوى الضمان هذا. ولا يتطلب هذا المستوى استخدام طرق استيقان تجفيرية (مثلاً بروتوكول التحدي والردّ على أساس التجفير).

فعلى سبيل المثال، قد ينطبق مستوى الضمان الأول على عملية استيقان يعرض فيها الكيان اسم مستعمل مسجلاً ذاتياً أو كلمة سر على موقع الويب لمقدم خدمة لإنشاء صفحة حسب الطلب، أو على معاملات تتضمن مواقع شبكية تستدعي التسجيل من أجل النفاذ إلى المواد والوثائق، من قبيل الأخبار أو الوثائق الخاصة بمنتج ما.

فعند مستوى الضمان الأول مثلاً يمكن لعنوان التحكم في النفاذ إلى الوسائط أن يلبي شروط الاستيقان الخاصة بجهاز ما. ومع ذلك، ثمة درجة ضئيلة من اليقين من أن جهازاً آخر سوف يعجز عن استعمال عنوان التحكم في النفاذ إلى الوسائط نفسه.

---

[2] يُعتبر مستوى الضمان دالة من دوال العمليات والأنشطة الإدارية والضوابط التقنية المنفذة من قبل مورّد خدمة أوراق الاعتماد/الإثباتات لكل مرحلة من مراحل إطار ضمان استيقان الكيان بالاستناد إلى المعايير المبينة في الفقرة 10.

2.6 مستوى الضمان الثاني (LoA2)

يوجد عند مستوى الضمان الثاني بعض الثقة بالهوية المزعومة أو المدعاة للكيان. ويُستخدم مستوى الضمان الثاني هذا حين يرتبط الاستيقان الخاطئ بحد متوسط من المخاطر. ويعتبر الاستيقان الأحادي العامل مقبولاً. ويتوقف نجاح الاستيقان على إثبات الكيان، من خلال بروتوكول استيقان آمن، بأن لديه سلطة رقابية على أوراق الاعتماد/الإثباتات. وتُوضع عمليات التحكم موضع التنفيذ للحد من فعالية هجمات التنصّت والتخمين على الشبكة. وكذلك للحماية من الهجمات على أوراق الاعتماد المخزّنة.

فقد يقوم مقدّم خدمة، على سبيل المثال، بتشغيل موقع ويب يمكّن زبائنه من تغيير عناوين سجلاتهم. ويمكن اعتبار المعاملة التي يغيّر فيها المستفيد عنوان السجل معاملة استيقان ذات مستوى ضمان ثانٍ، نظراً لأن هذه المعاملة تنطوي على قدر متوسط من مخاطر التعرض للمضايقات. وبما أن الإشعارات الرسمية المتعلقة بمبالغ الدفع ووضع الحسابات وسجلات التغييرات تُرسل إلى عنوان سجل المستفيد، يترتب على المعاملة، إضافةً إلى ذلك، درجة متوسطة من مخاطر الإصدار غير المرخّص للمعلومات المحددة لهوية الشخص. ونتيجةً لذلك، يجب أن يحصل مقدم الخدمة على بعض ضمانات الاستيقان على الأقل قبل السماح بإجراء مثل هذه المعاملة.

3.6 مستوى الضمان الثالث (LoA3)

توجد عند مستوى الضمان الثالث درجة عالية من الثقة بالهوية المزعومة أو المدعاة. ويُعتمد مستوى الضمان هذا حين يقترن الاستيقان الخاطئ بمخاطر كبيرة، كما يَستخدم مستوى الضمان هذا الاستيقان المتعدد العوامل. وتتوفر حماية المعلومات السرية التي يتم تبادلها بين بروتوكولات الاستيقان بطريقة التجفير أثناء المرور وفي حالة الراحة (على الرغم من أن مستوى الضمان الثالث لا يتطلب استخدام بروتوكول التحدي والردّ على أساس التجفير). ولا توجد شروط تتعلق بتوليد أو تخزين أوراق الاعتماد/الإثباتات؛ إذ يجوز تخزينها أو توليدها في الحواسيب المتعددة الأغراض أو التجهيزات المعدّة لأغراض خاصة.

فعلى سبيل المثال، إن المعاملة التي تقوم فيها شركة بتقديم معلومات سرية إلى وكالة حكومية بطريقة إلكترونية قد تتطلب معاملة استيقان ذات مستوى ضمان ثالث. فالإفصاح غير المناسب عن المعلومات قد يسفر عن خطر كبير بالتعرض إلى خسارة مالية. ومن الأمثلة الأخرى على معاملات مستوى الضمان الثالث النفاذ الإلكتروني إلى الحسابات التي تسمح للكيان بإجراء معاملات مالية معينة، أو استخدام طرف ثالث متعاقد لنظام بعيد للنفاذ إلى معلومات يُحتمل أن تكون معلومات شخصية وحساسة خاصة بالزبون.

4.6 مستوى الضمان الرابع (LoA4)

يوجد عند مستوى الضمان الرابع درجة عالية جداً من الثقة بالهوية المزعومة أو المدعاة. ويُستخدم مستوى الضمان هذا حين يقترن الاستيقان الخاطئ بمخاطر كبيرة جداً. ويُمثل مستوى الضمان الرابع المستوى الأعلى لضمان استيقان الكيان المعرّف وفقاً لهذه التوصية. ويُعتبر مستوى الضمان الرابع شبيهاً بمستوى الضمان الثالث، لكنه يضيف شروط تدقيق الهوية الشخصية للكيانات البشرية واستخدام أجهزة الحواسيب المقاومة للعبث لتخزين جميع مفاتيح التجفير السرية أو الخاصة. وإضافةً إلى ذلك، تتم بالتجفير حماية جميع المعلومات المعرفة لهوية الشخص والبيانات الحساسة الأخرى المتضمنة في بروتوكولات الاستيقان.

فعلى سبيل المثال، قد تتطلب الخدمات التي تنطوي على خطر محتمل بالتعرض للأذى أو الاستغاثة في حال فشل الاستيقان حماية ذات مستوى ضمان رابع. ويحتاج الطرف المسؤول إلى ضمان تام يؤكد أن الكيان الصحيح قد قدم بعض المعلومات الهامة، وقد يُعتبر الطرف المسؤول مسؤولاً عن ارتكاب جناية في حال عجزه عن التحقق من المعلومات. أخيراً، يمكن اعتبار الموافقة على عملية تنطوي على خطر مرتفع جداً بالتعرض لخسارة مالية بمثابة معاملة ذات مستوى ضمان رابع.

وعند مستوى الضمان الرابع يمكن استخدام شهادات رقمية (مثلاً ITU-T X.509 وشهادات التحقق من البطاقات) لاستيقان كيانات مادية مثل الحواسيب المحمولة والهواتف المتنقلة والطابعات وأجهزة الفاكس وغيرها من الأجهزة الموصولة بشبكة ما. فعلى سبيل المثال، قد تتطلب عملية الانتساب لهاتف ذكي نشر شهادات رقمية للهاتف الذكي. كذلك، ومن أجل الحؤول دون النفاذ غير المرخص إلى شبكة الطاقة، يمكن استخدام شهادات رقمية في عملية نشر تكنولوجيات العدّادات الذكية.

5.6 اختيار مستوى الضمان المناسب

ينبغي أن يستند اختيار مستوى الضمان المناسب إلى عملية تقييم لمخاطر المعاملات أو الخدمات التي سيتم استيقان الكيانات من أجلها. فمن خلال تنفيذ التقابل بين مستويات التأثير ومستويات الضمان، تستطيع الأطراف في معاملة استيقان معينة أن تحدد مستوى الضمان الذي تحتاجه، وشراء الخدمات، والاعتماد على هويات مضمونة وفقاً لذلك. ويشير الجدول 6-2 إلى التبعات والتأثيرات التي يُحتمل أن تنجم عن فشل الاستيقان عند مختلف مستويات الاستيقان.

الجدول 6-2 – التأثيرات المحتملة عند كل مستوى من مستويات الضمان

العواقب المحتملة لفشل الاستيقان	التأثير المحتمل لفشل الاستيقان حسب مستوى الضمان			
	1	2	3	4
المضايقات، أو الاستغاثة، أو تعرض المكانة أو السمعة للضرر	متدني	متوسط	مرتفع	مرتفع جداً
الخسارة المالية أو تحمل الوكالة للمسؤولية	متدني	متوسط	مرتفع	مرتفع جداً
إلحاق الضرر بالكيان أو ببرامجه أو بمصالحه العامة	لا ينطبق	متدني	متوسط	مرتفع جداً
الإفصاح غير المرخّص عن معلومات حساسة	لا ينطبق	متوسط	مرتفع	مرتفع جداً
السلامة الشخصية	لا ينطبق	لا ينطبق	متدني متوسط	مرتفع مرتفع جداً
انتهاكات مدنية أو مخالفات جنائية	لا ينطبق	متدني	مرتفع	مرتفع جداً

يعتمد تقرير الحد الأدنى أو المتوسط أو المرتفع أو المرتفع جداً من المخاطر على معايير المخاطر المحددة من قبل المنظمة التي تستخدم هذه التوصية لكل عاقبة من العواقب المحتملة. بالإضافة إلى ذلك، من الممكن أن يوجد سيناريوهات ذات تأثيرات متعددة (مثلاً، قد تتضمن العواقب إلحاق الأذى بالمنظمة فضلاً عن الإفصاح غير المرخص عن معلومات حساسة).

ويتم تحديد كل مستوى من مستويات الضمان حسب قوة وشدة ضوابط التحكم والعمليات المتضمنة لكل مرحلة من مراحل إطار ضمان استيقان الكيان التي يطبقها مورّد خدمة أوراق الاعتماد/الإثباتات على توفيره للخدمة. ويحدد إطار ضمان استيقان الكيان الحاجة إلى معايير تتعلق بضمان الخدمة التشغيلية عند كل مستوى من مستويات الضمان لمورّدات خدمة أوراق الاعتماد/الإثباتات. وتُعرض معايير ضمان الخدمة في الفقرة 11، علماً بأن ثمة متطلبات معينة تقع خارج نطاق هذه التوصية.

وقد توجد عوامل أخرى تتصل بالأعمال التجارية لا بدّ من أخذها في الاعتبار، تتجاوز نطاق الأمن، لدى استخدام نتائج تقييم المخاطر لتقرير مستوى الضمان المعتمد. ومن بين العوامل التجارية هذه ما يلي:

أ) نهج المنظمة لإدارة المخاطر المتبقية؛

ب) مدى انفتاح المنظمة لتقبّل المخاطر من حيث التأثيرات المبيّنة في الجدول 6-2؛

ج) الأهداف التجارية للخدمة (مثلاً، يمكن لخدمة لديها هدف تجاري يتمثل في دفع وتشجيع ما تستوعبه أن تُلبّى بصورة أفضل بواسطة مستوى ضمان أدنى باعتماد إثبات من قبيل كلمة السر، إذا كان لدى المنظمة عمليات للتخفيف من حدة الاحتيال ولا يضايقها القبول بمخاطر الاحتيال).

ويجوز إجراء تقييم لمخاطر معاملة ما كجزء من تقييم مخاطر معلومات الأمن الكلية (مثلاً ISO/IEC 27001)، وينبغي أن يركز على الحاجة المحددة للأمن في المعاملات التي يتم التفكير بها. ويُشترط بتقييم المخاطر التصدي لأخطار تتصل بضمان استيقان الكيان. ويتوجب مقارنة نتائج عملية تقييم المخاطر بمستويات الضمان الأربعة، على أن يتم اختيار مستوى الضمان الذي يلبي عملية تقييم المخاطر على أفضل وجه.

وعند تصوّر فئات متعددة من المعاملات، من المحتمل أن ينطبق مستوى ضمان مختلف على كل معاملة أو مجموعة من المعاملات. وبكلمات أخرى، يجوز أن تقبل منظمة واحدة بمستويات ضمان متعددة وفقاً للمعاملة المحددة قيد البحث.

6.6 تقابل مستويات الضمان وإمكانية التشغيل البيني

قد تحدد الميادين المختلفة مستويات الضمان على نحو مختلف. ومستويات الضمان تلك لن تقوم بالضرورة بدعم تقابل واحد لواحد لمستويات الضمان الأربعة الوارد وصفها في هذا الإطار. فقد يعتمد ميدان واحد على سبيل المثال نموذجاً رباعي المستوى فيما يعتمد ميدان آخر نموذجاً خماسي المستوى. ويتوجب تعريف المعايير المختلفة لنماذج الاستيقان كلاً على حدة وتوصيلها ونشرها على نطاق واسع.

وفي سبيل تحقيق التشغيل البيني بين نماذج مستويات الضمان المختلفة، يعمد كل ميدان إلى شرح كيفية ارتباط مخطط التقابل الخاص به بمستويات الضمان المعرفة في هذه التوصية عن طريق:

أ) تطوير منهجية محددة بشكل جيد لضمان استيقان الكيان، بما في ذلك فئات محددة بوضوح لمستويات الضمان؛

ب) ونشر هذه المنهجية على نطاق واسع لكي يتسنّى للمنظمات الراغبة في الدخول في اتفاقات تحمل الطابع الموحّد أن تفهم بوضوح عمليات ومصطلحات إحداها الأخرى.

ويُشترط بمنهجية مستويات الضمان أن تراعي وتعرِّف بوضوح مستويات الضمان من الناحية المتعلقة بعملية تقييم المخاطر التي تحدد وتقدّر حجم ما يلي:

أ) التهديدات المتوقعة؛

ب) التأثيرات (أي تحديد ما إذا كانت متدنية أو متوسطة) إذا ما أصبحت التهديدات فعلية؛

ج) التعرّف على التهديدات التي ينبغي التحكم بها عند كل مستوى من مستويات الضمان؛

د) تكنولوجيات وعمليات الأمن الموصى باستخدامها في تنفيذ عمليات التحكم عند كل مستوى من مستويات الضمان، مثل تعيين الإثبات المنفّذ على جهاز حاسوبي (كالبطاقة الذكية) أو تعيين الشروط لتوليد أوراق الاعتماد/الإثباتات وتخزينها؛

هـ) المعايير لتحديد التكافؤ لتوليفات مختلفة من عوامل الاستيقان مع الأخذ في الحسبان كل من تدقيق الهوية وأوراق الاعتماد/الإثباتات ذات الصلة.

ويتمثل أحد النهج المتّبعة للتصدّي لقضية التقابل/الوصل بين نماذج مستويات الضمان المختلفة في استخدام النموذج الرباعي المستوى الوارد تعريفه في هذه الوثيقة ومقارنته بنماذج ذات أخرى متعددة المستويات. فهذه الطريقة تسمح لاتحادات الهويات التي تستخدم نماذج مختلفة لضمان الاستيقان بأن تجري مقارنات بالنموذج الرباعي المستوى. وتعمل عملية التقابل على تحديد كيفية التعامل مع مستويات الضمان التي لم تتم مقارنتها، مما ينطوي على تجاهلها ببساطة أو مقارنتها بالمستوى التالي الأدنى (حيث ترد إمكانية عدم وجود أساس لافتراض مستوى ضمان أعلى إذا لم يكن قد تقرّر ذلك بالتحديد مسبقاً).

7.6 تبادل نتائج الاستيقان استناداً إلى مستويات الضمان الأربعة

قد تحتاج الجهات الفاعلة المشاركة في معاملة استيقان (مثلاً مورّدو خدمة أوراق الاعتماد/الإثباتات والأطراف المعوّلة) إلى تبادل المعلومات من أجل إتمام معاملة أو نشاط.

وتتضمن مجموعة الإجراءات، على سبيل المثال لا الحصر، ما يلي:

أ) السماح لطرف معوّل بالتعبير عن توقعاته بالنسبة لمستوى الضمان الذي يجب عنده أن يتم استيقان الكيان؛

ب) السماح لطرف معوّل أو لمورد خدمة أوراق الاعتماد/الإثباتات بأن يشير في ردوده إلى مستوى الضمان الفعلي؛

ج) السماح لكيان أو لمورّد خدمة أوراق الاعتماد/الإثباتات بالإعلان عن مستويات الضمان تلك التي تم بشأنها التصديق على قدرته على الوفاء بالشروط والمتطلبات المرتبطة بذلك المستوى من مستويات الضمان.

ويُشترط بالجهات الفاعلة التي تشارك في عملية الاستيقان أن توافق على البروتوكول والدلالات ونسق وبنية المعلومات المقرر تبادلها. وقد يضطر الطرف المعوّل إلى تحديد ما إذا كان سيقبل بأي من استجابات الاستيقان خلاف تلك المطلوبة بالتحديد.

ومع أن الشهادات الرقمية تشكل طريقة راسخة لنقل معلومات تتعلق بضمان أوراق الاعتماد ذات الصلة، فإنه يجري بصورة متزايدة استخدام البيانات الوصفية كأسلوب لتوصيل شروط الضمان التي توجد لدى الأطراف القائمة بعملية التبادل. "فصنف السياق"، من قبيل "صنف سياق استيقان لغة ترميز تأكيد الأمن (SAML)" الذي يحمل شكل موقع الموارد المحدد (URL)، يمثل آلية معروفة جداً لدى الأطراف للتعبير عن تلك الأصناف المتعلقة بضمان الاستيقان في طلبات الاستيقان والمزاعم بشأنها. فعلى سبيل المثال، قد يعمل زعم شائع وارد من مورّد الهوية على نقل معلومات كالتالية: "إن المستخدم هو John Doe، وعنوانه البريدي هو john.doe@example.com، وقد تم استيقانه في هذا النظام باستخدام آلية كلمة السر".

وما تبقّى من هذا الإطار يتناول البنية التي يتم فيها إرساء العمليات والشروط للخدمات وكذلك التهديدات والتأثيرات المتصلة باستيقان الكيان. ويُختتم بعرض عام للحاجة إلى معايير ضمان الخدمة مقابل تحديد الخدمات التي قد يتم تقييمها لضمان تعيين مستوى الضمان المناسب من أجل تحقيق خدمات منح أوراق الاعتماد/الإثباتات الكافية.

7 الجهات الفاعلة

من بين الجهات الفاعلة المتضمنة في إطار ضمان استيقان الكيان الكيانات التالية: مورّدو خدمة أوراق الاعتماد/الإثباتات، وهيئات التسجيل، والأطراف المعوّلة، وجهات التحقق، والمعلومات المحددة لهوية الشخص. وقد توجد مجموعة منوعة من العلاقات والقدرات المقدمة من عدد من المنظمات بما في ذلك المكونات والأنظمة والخدمات المتقاسَمة أو المتفاعلة.

1.7 الكيانات

يمكن لكيان ما أن يُجري استيقاناً لهويته. وتعتمد القدرة على استيقان الهوية على عدد من العوامل. وفي سياق هذا الإطار، تنطوي إمكانية استيقان كيان على أن الكيان قد تمّ تسجيله وإصدار أوراق الاعتماد المناسبة له من قبل مورد خدمة أوراق الاعتماد/الإثباتات، وأنه قد تم تحديد بروتوكول للاستيقان. ويجوز أن يشهد الكيان أثناء عملية الاستيقان على صحة هويته. ومن الممكن وجود طرف مستقل يمثّل الكيان لأغراض الاستيقان.

2.7 مورد خدمة أوراق الاعتماد/الإثباتات

يُصدر مورّد خدمة أوراق الاعتماد و/أو يُدير أوراق الاعتماد/الإثباتات أو التجهيزات والبرمجيات والبيانات المرتبطة بها التي يمكن استخدامها لإصدار أوراق الاعتماد/الإثباتات. وتشكل كلمات السر وبيانات القياس الحيوي أمثلة على أوراق الاعتماد/الإثباتات التي قد يصدرها ويديرها مورّد خدمة أوراق الاعتماد/الإثباتات. وتعتبر البطاقات الذكية التي تحتوي على مفاتيح خاصة مثالاً على التجهيزات والبيانات ذات الصلة (التي يمكن أن تُستخدم لإنتاج أوراق الاعتماد) التي قد يصدرها ويديرها مورد خدمة أوراق الاعتماد/الإثباتات. كما يستطيع مورد خدمة أوراق الاعتماد إصدار وإدارة بيانات قد تُستخدم في استيقان أوراق الاعتماد. وإذا ما استُخدمت كلمات السر كإثباتات، قد تمثل هذه البيانات قيم الوظائف الأحادية الاتجاه لكلمات السر. وحين تكون أوراق الاعتماد/الإثباتات مستندة إلى معلومات موقعّة رقمياً، يجوز لموردي خدمة أوراق الاعتماد أن يصدروا شهادات المفتاح العام التي يمكن لجهات التحقّق استخدامها. وتشكل أوراق الاعتماد/الإثباتات تصدرها الجهات الموردة لخدمة أوراق الاعتماد وتوفر الدعم لها، فضلاً عن الضمانات التي ينفذها مورّد خدمة أوراق الاعتماد، عوامل أساسية في تقرير مستوى الضمان الذي يمكن بلوغه أثناء معاملة استيقان معينة (انظر الفقرة 3.10).

ويتم إصدار ورقة أو أكثر من أوراق الاعتماد لكل كيان، أو تزويده بوسائل إنتاج أوراق الاعتماد، لتمكينه من تنفيذ الاستيقان في وقت لاحق. وتُصدر أوراق الاعتماد أو وسائل إصدارها في العادة بعد النجاح في إتمام عملية الانتساب، التي يجري تسجيل الكيان عقب انتهائها.

3.7 هيئة التسجيل

تحدّد هيئة التسجيل (RA) هوية كيان ما و/أو تكفل صحتها أمام مورّد خدمة أوراق الاعتماد. ويتم الوثوق بهيئة التسجيل من قبل مورد خدمة أوراق الاعتماد لتنفيذ العمليات المتصلة بمرحلة الانتساب وكيانات التسجيل بطريقة تُجيز لمورد خدمة أوراق الاعتماد تخصيص أوراق الاعتماد/الإثباتات في وقت لاحق.

وتؤدي كل هيئة تسجيل شكلاً من أشكال تدقيق الهوية والتحقق منها وفقاً لإجراء محدّد. ولتمييز كيان عن بيانات أخرى، يُخصّص للكيان عادة معرّف واحد للهوية أو أكثر، مما يسمح بالتعرف على الكيان في وقت لاحق ضمن السياق المعتمد.

4.7 الطرف المعوّل

الطرف المعوّل هو جهة تعتمد على هوية مزعومة أو مدّعاة. ويجوز للطرف المعوّل المطالبة بهوية مُستيقن منها لأغراض متنوعة، من قبيل إدارة الحسابات والتحكم بالنفاذ وقرارات الترخيص ونحو ذلك. ويجوز أن يؤدي الطرف المعوّل بذاته العمليات اللازمة لاستيقان الكيان، أو يمكنه إسناد تلك العمليات إلى طرف ثالث.

5.7 جهة التحقّق

تؤكد جهة التحقق صحة المعلومات عن الهوية. ويمكن لجهة التحقق أن تشارك في مراحل متعددة من ضمان استيقان الكيان أو أن تقوم بتدقيق أوراق الاعتماد و/أو تدقيق الهوية.

6.7 الطرف الثالث الموثوق

الطرف الثالث الموثوق هو سلطة أو وكيل لها، تثق به الجهات الفاعلة الأخرى فيما يتعلق ببعض الأنشطة (مثل الأنشطة المتصلة بالأمن). وفي هذا الإطار، يتم الوثوق بالطرف الثالث الموثوق من قبل كيان و/أو جهة تحقق لأغراض الاستيقان. ومن بين الأمثلة على الأطراف الثالثة الموثوقة لأغراض استيقان الكيان سلطات التصديق وسلطات خاتم الوقت.

8 مراحل إطار ضمان استيقان الكيان

تعرض هذه الفقرة وصفاً لمراحل ضمان استيقان الكيان وعملياته. وبالرغم من إمكانية اختلاف بعض نماذج ضمان استيقان الكيان عن بنية هذا النموذج، فإن التطابق مع هذا النموذج يستدعي تلبية القدرات الوظيفية للشروط المبينة في هذا الإطار بشكل تام. ويتسم هذا الإطار بأنه محايد من الناحية التكنولوجية.

ويتعين على المنظمات التي تعتمد هذا الإطار أن تحدّد السياسات والإجراءات التي توفر ما يلزم من العمليات الداعمة وتفي بالشروط الواردة في هذا الإطار. وهذه تختلف وفقاً للدور الذي تختاره منظمة معينة وكذلك، على سبيل المثال، وفقاً لمستويات الضمان التي توفر المنظمة عندها أوراق الاعتماد/الإثباتات. وقد تخضع المنظمة على سبيل المثال لما يلي:

أ) المتطلبات الخاصة بإجراءات معينة تقوم بها المنظمة أو ممثليها وتتصل بمستويات ضمان معينة؛

ب) المتطلبات الخاصة بتقييم يجريه طرف خارجي أو ثالث لقدرات المنظمة التشغيلية ضمن إطار ضمان استيقان الكيان؛

ج) السياسات والإجراءات والقدرات الضرورية لتأكيد أمانة العمليات والخدمات والقدرات التي تقدمها المنظمات المعتمدة للإطار وجدارتها بالثقة.

1.8 مرحلة الانتساب

تتألف مرحلة الانتساب من أربع عمليات: تقديم الطلب والاستهلال؛ وتدقيق الهوية؛ والتحقق من الهوية؛ وحفظ السجلات/التسجيل. وقد تُجري منظمة واحدة هذه العمليات بأكملها، أو قد تتكون هذه العمليات من مجموعة متنوعة من العلاقات والقدرات التي يوفرها عدد من المنظمات بما في ذلك عناصر وأنظمة وخدمات متقاسَمة أو متفاعلة.

وتختلف العمليات المطلوبة وفقاً للقوة التي يستدعيها مستوى الضمان المعتمد. ففي الحالة التي ينتسب فيها كيان إلى مستوى الضمان الأول، تكون هذه العمليات في حدّها الأدنى (فقد يقوم فرد مثلاً بالنقر على زر "مستخدم جديد" على صفحة الويب وإنشاء اسم للمستعمل وكلمة سر). وفي حالات أخرى، قد تكون العمليات موسّعة. فالانتساب إلى مستوى الضمان الرابع على سبيل المثال يتطلب حدوث لقاء شخصي بين الكيان وهيئة التسجيل فضلاً عن تدقيق موسّع للهوية.

1.1.8 تقديم الطلب والاستهلال

تُستهل عملية الانتساب باعتماد طرق شتى. فيمكن استهلالها على سبيل المثال عملاً بطلب تتقدّم به كيانات تلتمس الحصول على أوراق اعتماد/إثباتات معينة (مثلاً حين يرغب المستعمل الجديد لصفحة الويب في الحصول على اسم مستخدم وكلمة سر). ويُحتمل بنفس القدر أن تُستهل عملية الانتساب من قبل طرف ثالث نيابة عن الكيان، أو من قبل مورد خدمة أوراق الاعتماد/الإثباتات نفسه (مثلاً بطاقة هوية رسمية أو شارة تعريف الموظفين). ولا يمكن قبول الطلبات المقدمة عند مستويات ضمان أعلى مثلاً إلا حين يكون الكيان قد حظي برعاية من طرف ثالث.

وفي شتى الحالات، قد تتضمن عملية استهلال مرحلة الانتساب الخاصة بالأشخاص تعبئة نموذج تقديم الطلب. ويجب أن يسجل هذا النموذج معلومات كافية لضمان إمكانية التعرف على الكيان بشكل مميز ضمن سياق معين (مثلاً بتدوين الاسم الكامل وتاريخ ومكان الولادة). وفيما يتعلق بالكيانات المادية (غير الأشخاص)، مثل جهاز متنقل، قد تُستهل عملية الانتساب بواسطة نقل أوراق الاعتماد/الإثباتات إلى الجهاز، مما يسمح بالتعرف إلى الجهاز بشكل مميز وتلقي الإعدادات المفصّلة للجهاز من خلال مواصفات تشكيلة مجفّرة.

وعلى مورّدي خدمة أوراق الاعتماد/الإثباتات وضع شروط الانتساب والشروط التي يتم بموجبها استعمال الخدمات المرتبطة بعملية الانتساب تلك. ويمكن تحديد شروط الخدمات المقترنة بالانتساب وفقاً لإطار موثوق. ويتعين، حسب الاقتضاء، أن يقبل الكيان أو من يمثله إخلاء المسؤولية القانونية قبل متابعة عمليات الانتساب.

2.1.8 تدقيق الهوية والتحقق منها

يتمثل تدقيق الهوية بعملية الحصول على المعلومات التي تكفي للتعرف إلى هوية ضمن مستوى ضمان محدد أو مفهوم والتحقق منها. ويتمثل التحقق من الهوية بعملية التدقيق في المعلومات عن الهوية وأوراق الاعتماد لدى الجهات المصدرة أو مصادر البيانات أو الموارد الداخلية أو الخارجية الأخرى فيما يتعلق بالتيقن والصلاحية والدقة والإسناد إلى الكيان. ورهناً بالسياق المعتمد، يمكن لمجموعة منوعة من المعلومات عن الهوية (بطاقات الهوية الرسمية، ورخص القيادة، ومعلومات القياس الحيوي، والشهادات المستندة إلى الآلة، وشهادات الميلاد) المأخوذة من مصادرة رسمية أو معتمدة أن تفي بشروط تدقيق الهوية. أما المعلومات الفعلية المتعلقة بالهوية المقدمة للوفاء بشروط تدقيق الهوية فتختلف باختلاف مستوى الضمان.

وقد تتضمن عملية تدقيق الهوية التدقيق المادي في وثائق تتعلق بالهوية تم تقديمها لكشف إمكانية الاحتيال أو التلاعب أو التزييف. كما قد تشتمل عملية تدقيق الهوية على التدقيق للتأكد من أن الهوية تُستخدم في سياقات أخرى (أي مُتحقق منها من قبل هيئات تسجيل أخرى). وتكون شروط تدقيق الهوية أكثر صرامةً كلما ارتفع مستوى الضمان. كما أن عملية تدقيق الهوية للكيانات التي تزعم أو تدعي وجود هويات لها عن بعد (مثلاً عبر قنوات الإنترنت) تكون أكثر صرامة من تلك التي تتم محلياً (من خلال اللقاء الشخصي مع هيئة التسجيل على سبيل المثال).

ويستند مدى صرامة شروط تدقيق الهوية إلى الأهداف التي يتوجب تحقيقها لكل مستوى من مستويات الضمان. فعند مستوى الضمان الأول، يتمثل الهدف الوحيد في التأكد من أن الهوية هي هوية ينفرد بها الكيان ضمن السياق المقصود. ويجب ألا ترتبط الهوية بكيانين مختلفين. ويوجد عند المستوى الثاني هدفان: أولاً، يجب أن تكون الهوية فريدة ضمن سياق معين. وثانياً، يجب أن يكون الكيان الذي يملك الهوية موجوداً في الواقع، مما يعني أنها ليست هوية وهمية أو ملفّقة بشكل متعمد لأغراض التزوير والاحتيال[3]. ويمكن أن يشتمل تدقيق هوية إنسان عند مستوى الضمان الثاني، على سبيل المثال، على التدقيق

[3] ولا يستثني ذلك استعمال الأسماء المستعارة.

في سجلات المواليد والوفيات لضمان وجود بعض الأوراق الثبوتية الأصلية (بالرغم من أنها لا تثبت أن الكيان الحائز على شهادة ميلاد هو الكيان نفسه الذي تخصه شهادة الميلاد بالفعل). وبالمثل، قد يتضمن تدقيق الهوية عند مستوى الضمان الثاني بالنسبة للكيانات المادية التدقيق في الرقم التسلسلي لدى الجهة المصنّعة لها.

ويتضمن مستوى الضمان الثالث أهداف مستويي الضمان الأول والثاني، فضلاً عن هدف التحقق من صحة المعلومات عن الهوية من خلال الرجوع إلى مصدر أو أكثر من المصادر المعتمدة، مثل قاعدة بيانات خارجية. ويبين التحقق من الهوية أن الهوية قيد الاستعمال وأنها مرتبطة بالكيان. المستعملة ولا توجد مع ذلك ضمانات تؤكد أن المعلومات المتعلقة بالهوية هي في حوزة المالك الفعلي أو الحقيقي للهوية. وفيما يتعلق بالأشخاص، يضيف مستوى الضمان الرابع هدفاً إضافياً إلى مستوى الضمان الثالث من خلال طلب الإدلاء بالشهادة الشخصية على وجود الكيان تلافياً لخطر انتحال صفة أو شخصية.

أما عمليات تدقيق الهوية عند مستويات ضمان أعلى فتتضمن العمليات التي تشملها مستويات ضمان أدنى. فمن المفترض أن يكون تدقيق الهوية عند مستوى الضمان الثالث على سبيل المثال قد استوفى شروط ضوابط تدقيق الهوية عند مستويي الضمان الأول والثاني.

الجدول 8-1 – تطبيق أهداف تدقيق الهوية على مستويات الضمان

مستوى الضمان	الوصف	الهدف	عناصر التحكم	طريقة المعالجة[4]
LoA1 – متدني	درجة ضئيلة من الثقة أو انعدام الثقة بالهوية المزعومة أو المدعاة	الهوية متفرّدة ضمن سياق معين	مزعومة أو مدّعاة ذاتياً	محلية أو عن بُعد
LoA2 – متوسط	بعض الثقة بالهوية المزعومة أو المدعاة	الهوية متفرّدة ضمن السياق، والكيان الحائز على الهوية موجود في الواقع	تدقيق الهوية عن طريق استخدام معلومات عن الهوية مستمدة من مصدر رسمي	محلية أو عن بُعد
LoA3 – مرتفع	درجة عالية من الثقة بالهوية المزعومة أو المدعاة	الهوية متفرّدة ضمن السياق، والكيان الحائز على الهوية موجود في الواقع، والهوية متحقق منها، وتُستخدم في سياقات أخرى	تدقيق الهوية عن طريق استخدام معلومات عن الهوية مستمدة من مصدر رسمي + التحقق من الهوية	محلية أو عن بُعد
LoA4 – مرتفع جداً	درجة عالية جداً من الثقة بالهوية المزعومة أو المدعاة	الهوية متفرّدة ضمن السياق، والكيان الحائز على الهوية موجود في الواقع، والهوية متحقق منها، وتُستخدم في سياقات أخرى	تدقيق الهوية عن طريق استخدام معلومات عن الهوية مستمدة من مصادر رسمية متعددة + التحقق من الهوية + الشهادة الشخصية على وجود الكيان[5]	محلية فقط

وتتحدد عمليات التحكم اللازمة لمستوى الضمان للحماية من التهديدات لمرحلة الانتساب عن طريق استخدام عناصر التحكم المدرجة في الفقرة الفرعية 2.1.10.

ويعتمد أي تنفيذ لإطار ضمان استيقان الكيان على (مجموعة فرعية من) المعلومات المتعلقة بالهوية والمصادر المتاحة للكيانات المرتقبة و/أو هيئة التسجيل.

---

4 يُنجز تدقيق الهوية عن بعد من خلال شبكة وبذلك ينطوي على العجز عن رؤية الكيان بأم العين، في حين أن تدقيق الهوية محلياً يتم بطريقة تستدعي رؤية الكيان شخصياً.

5 تنطبق شروط الشهادة الشخصية على الكيانات البشرية أي الأشخاص فقط.

وتشكل موثوقية ودقة أوراق الاعتماد/الإثباتات والمعلومات عن الهوية والمصادر تلك الضمان الفعلي الذي تقدمه مرحلة الانتساب. وتبعاً لذلك، على الجهات المنفذة لإطار ضمان استيقان الكيان أن تنظر بحرص في الضمان المقدّم من البنى التحتية للهوية (وإدارة الهوية) التي تُستخدم من قبل مختلف المصادر وجهات الإصدار عند تحديد أوراق الاعتماد والمعلومات المتعلقة بالهوية و/أو المصادر التي يجب الاعتماد عليها لأغراض تدقيق الهوية والتحقق منها. ويجب أن تتضمن أي عملية تنفيذ لإطار ضمان استيقان الكيان نشر وثيقة (وثيقة تدقيق الهوية مثلاً على النحو الوارد في الفقرة الفرعية 1.2.1.10) تعرض لمحة عامة عن المعلومات عن الهوية والمصادر و/أو الجهات المصدِرة التي يُعتمد عليها لدعم مرحلة الانتساب.

3.1.8 حفظ السجلات/التسجيل

وهي عملية إتمام انتساب الكيان. وتمثل عملية حفظ السجلات لمرحلة الانتساب التي يتم فيها إنشاء سجل عملية الانتساب. ويحتوي هذا السجل على معلومات ووثائق تم جمعها (ويمكن الاحتفاظ بها)، ومعلومات عن عملية التحقق من الهوية، ونتائج هذه الخطوات، وغير ذلك من المعطيات ذات الصلة. ومن ثمّ يصدر القرار بهذا الشأن ويُسجّل للقبول به أو إنكاره أو إحالة عملية الانتساب للخضوع لمزيد من الفحص أو إجراءات المتابعة الأخرى.

4.1.8 التسجيل

التسجيل هو العملية التي يطلب فيها الكيان استخدام خدمة أو مورد. ومع أن التسجيل يُعتبر عموماً جزءاً من عملية الانتساب، حيث إنها تُنفّذ عند انتهاء مرحلة الانتساب، فمن الممكن أيضاً تنفيذه في وقت لاحق. وخلافاً للعمليات الأخرى المتضمنة في الانتساب التي يُحتمل أن تلزم لمرة واحدة فقط، قد يكون التسجيل ضرورياً حين يطلب الكيان النفاذ إلى أي خدمة أو مورد للمرة الأولى.

2.8 مرحلة إدارة أوراق الاعتماد/الإثباتات

تشمل مرحلة إدارة أوراق الاعتماد/الإثباتات جميع العمليات ذات الصلة بإدارة دورة حياة أوراق الاعتماد، أو الوسائل المعتمدة لإنتاج أوراق الاعتماد، التي تمكّن المستخدم من المشاركة في نشاط أو سياق معين. وقد تتضمّن مرحلة إدارة أوراق الاعتماد بعضاً من العمليات التالية أو كلها: إنشاء أوراق الاعتماد، وإصدار أوراق الاعتماد أو وسائل إنتاجها، وتفعيل أوراق الاعتماد أو وسائل إنتاجها، وتخزين أوراق الاعتماد و/أو إلغاؤها و/أو إتلافها أو وسائل إنتاج أوراق الاعتماد، وتجديد أوراق الاعتماد و/أو استبدالها أو وسائل إنتاج أوراق الاعتماد، وحفظ السجلات بشأنها. وتتوقف بعض هذه العمليات على ما إذا كانت أوراق الاعتماد محمولة على جهاز من التجهيزات.

1.2.8 إنشاء أوراق الاعتماد/الإثباتات

تضم عملية إنشاء أوراق الاعتماد/الإثباتات كل العمليات التي تلزم من أجل ذلك، أو وسائل إنتاجها للمرة الأولى. وقد تتضمّن هذه العمليات المعالجة المسبقة لأوراق الاعتماد واستهلالها وإسنادها لجهة ما.

1.1.2.8 المعالجة المسبقة لأوراق الاعتماد/الإثباتات

تتطلب بعض أوراق الاعتماد أو وسائل إنتاجها معالجة مسبقة قبل إصدارها، من قبيل إضفاء الطابع الشخصي عليها عندما يتم إعدادها بحسب هوية الكيان. وقد تتخذ عملية التخصيص أشكالاً مختلفة وفقاً لأوراق الاعتماد/الإثباتات المعنية. فتخصيص البطاقة الذكية على سبيل المثال التي تحمل إثباتات قد يتضمن طبع (على الجانب الخارجي من البطاقة) أو كتابة (على رقاقة البطاقة) اسم الكيان الذي ستُصدّر البطاقة له. وهنالك أيضاً أوراق اعتماد لا تستدعي إضفاء الطابع الشخصي عليها أو تخصيصها ككلمة السر.

2.1.2.8 استهلال أوراق الاعتماد/الإثباتات

تشمل عملية استهلال أوراق الاعتماد/الإثباتات كل ما يلزم من خطوات لضمان تمكّن وسيلة إنتاج أوراق الاعتماد في وقت لاحق من دعم الوظائف التي يتوقع أن تقدم الدعم لها. فقد تكون رقاقة البطاقة الذكية على سبيل المثال لازمة لحساب أعداد

أزواج مفاتيح التجفير الضرورية من أجل الدعم اللاحق لتوليد التواقيع الرقمية. وبشكل مماثل، قد تُصدّر البطاقة الذكية وهي في حالة "مقفلة"، الأمر الذي يستدعي استخدام رقم تعريف الهوية الشخصي أثناء عملية التفعيل.

3.1.2.8 إسناد أوراق الاعتماد/الإثباتات

يمثل الإسناد عملية إرساء صلة الارتباط بين أوراق الاعتماد/الإثباتات أو وسائل إنتاجها وبين الكيان التي ستصدُر من أجله. وتختلف كيفية تنفيذ الإسناد وإرساء الثقة بوصلات الارتباط المقترنة بالإسناد باختلاف مستوى الضمان. ففي إطار سيناريو يتم على الشبكة مثلاً، وعند إسناد معرّف الهوية الدائم لاسم مستعار لكيانٍ ما إلى سجل الزبائن الخاص بالكيان، يمكن استخدام "شفرة تفعيل" للمرة الأولى من خلال عملية الإسناد ضمن بصمة مجفّرة لدورة واحدة فقط على قناة مأمونة. وبالمقابل، يمكن تجفير شفرة التفعيل في نهاية العملية فور إنجاز خطوة الربط بين معرّف الهوية الدائم وبين الكيان من أجل ربط معرّف الهوية الدائم بسجل الزبون.

2.2.8 إصدار أوراق الاعتماد/الإثباتات

إن عملية إصدار أوراق الاعتماد/الإثباتات هي عملية تزويد الكيان بأوراق اعتماد/إثباتات معينة أو بوسائل إنتاج أوراق الاعتماد، أو ربطها بالكيان،. ويتفاوت مدى تعقيد هذه العملية وفقاً لمستوى الضمان المطلوب. ففي حالة مستويات الضمان الأعلى، قد تتضمن العملية تسليماً مأموناً لجهاز ما (البطاقة الذكية مثلاً) يختزن إحدى أوراق الاعتماد وتتطلب تسليم الجهاز بصورة شخصية. إما في حالة مستويات الضمان الأكثر انخفاضاً، قد تكون عملية الإصدار غاية في البساطة كالقيام بإرسال كلمة السر أو رقم تعريف الهوية الشخصي إلى العنوان المادي للكيان أو إلى عنوان بريده الإلكتروني.

وفيما يتعلق بالكيانات المادية (غير الأشخاص) مثل الأجهزة، تبدأ عمليات الإصدار عند مستويات ضمان أعلى في العادة حين تطلب الجهة المصنّعة للجهاز شهادات رقمية بالجملة من خلال تزويد مورّد خدمة أوراق الاعتماد بقائمة بأرقام تعريف هوية خاصة بالجهاز وذلك لكل شهادة من الشهادات الرقمية. ويستجيب مورد خدمة أوراق الاعتماد بتقديم الشهادات والمفاتيح الخاصة إلى الجهة المصنعة في نسق مجفّر. ويجوز أن تقوم الجهة المصنعة إبّان عملية التصنيع بدمج شهادة رقمية في كل جهاز من الأجهزة، مما يؤدي إلى إنشاء معرّف هوية مميز ينفرد به الجهاز.

3.2.8 تفعيل أوراق الاعتماد/الإثباتات

يمثل تفعيل أوراق الاعتماد/الإثباتات عملية يتم بموجبها تهيئة أوراق الاعتماد أو وسائل إنتاجها لتصبح جاهزة للاستعمال. وقد تتضمن عملية التفعيل مجموعة منوعة من التدابير حسب وضع أوراق الاعتماد. فقد تكون إحدى أوراق الاعتماد أو وسائل إنتاجها على سبيل المثال قد "أُقفِلت" بعد استهلالها إلى أن تحين لحظة إصدارها إلى الكيان منعاً لإساءة الاستعمال المؤقتة. وفي حالات كهذه، قد يتضمن التفعيل "إزالة الإقفال" عن ورقة الاعتماد (باستخدام كلمة السر مثلاً). كذلك يمكن إعادة تفعيل أوراق الاعتماد أو وسائل إنتاجها بعد تعليقها عندما تكون صلاحيتها قد أوقفت بشكل مؤقت.

4.2.8 تخزين أوراق الاعتماد/الإثباتات

يقصد بتخزين أوراق الاعتماد/الإثباتات العملية التي يتم بموجبها تخزين أوراق الاعتماد أو وسائل إنتاجها بطريقة آمنة بهدف الحماية من الإفشاء أو الاستعمال أو التعديل أو الإتلاف غير المرخص لها. ويتضمن تخزين أوراق الاعتماد الكيان المقترن بورقة الاعتماد والإجراءات اللازمة للحؤول دون الاستعمال غير المرخص لها.

ولا يشمل تخزين أوراق الاعتماد بالضرورة حماية المعلومات التي تستخدم للتأكد من أن أوراق الاعتماد قانونية إذا لم تكن تلك المعلومات تشكل جزءاً من أوراق الاعتماد. كما أن حماية المعلومات، من قبيل جداول كلمات السر المظلّلة اللازمة للاستيقان، تُطلب عند مستويات الضمان الأعلى.

5.2.8 تعليق أوراق الاعتماد و/أو إلغاؤها و/أو إتلافها

الإلغاءُ هو العملية التي تنهي صلاحية أوراق الاعتماد/الإثباتات بشكل دائم. أما التعليق فهي عملية ذات صلة يتم بموجبها وقف صلاحية أوراق الاعتماد بشكل مؤقت. وقد يكون الإلغاء مناسباً في حالات مختلفة كثيرة. ويتم الإلغاء في الحالات التالية:

أ) حين يتم التبليغ عن أن أوراق الاعتماد أو وسائل إنتاجها قد فُقدت أو تعرضت للسلب أو للضرر؛

ب) أو عند انتهاء صلاحية أوراق الاعتماد؛

ج) أو عند انتهاء وجود الأساس لصدور أوراق الاعتماد (حين يترك الموظف مكان عمله مثلاً)؛

د) أو عند استعمال أوراق الاعتماد لأغراض غير مرخصة؛

هـ) أو حين تُصدَر أوراق اعتماد مختلفة لتحل محل أوراق الاعتماد قيد البحث.

ويتحدد الإطار الزمني الممتد بين التبليغ عن حدث ما يستدعي الإلغاء وبين إنجاز عملية الإلغاء بواسطة السياسة التنظيمية المتبعة. فعند مستويات الضمان الأعلى، تكون الفترة المسموح بها للإلغاء عادة أقصر. كما أن بعض أوراق الاعتماد، من قبيل تلك التي تختزنها البطاقات الذكية، يمكن إتلافها فور إلغائها. ومع ذلك، لا يمكن دائماً إتلاف المعلومات المرتبطة بأوراق الاعتماد.

6.2.8 تجديد أوراق الاعتماد/الإثباتات و/أو استبدالها

التجديد هو عملية يتم بموجبها إطالة أمد أوراق الاعتماد/الإثباتات القائمة. أما الاستبدال فهي العملية التي تُصدَر بها أوراق اعتماد جديدة، أو وسائل إنتاج أوراق الاعتماد، لتحل محل أوراق الاعتماد التي صدرت في السابق وتمّ إبطالها. وأحد الأمثلة على استبدال أوراق الاعتماد هو حين يقوم مورد خدمة أوراق الاعتماد بإرسال كلمة سر مؤقتة إلى عنوان البريد الإلكتروني للكيان لتمكينه من استحداث كلمة سر جديدة بعد تقديم كلمة السر المؤقتة. ومن الأمثلة الأخرى شفرة فتح رقم تعريف الهوية الشخصي التي ينبغي معاملتها كما لو أنها شفرة رقم تعريف الهوية الشخصي. وتختلف صرامة العمليات المتعلقة بتجديد أوراق الاعتماد أو استبدالها باختلاف مستوى الضمان.

7.2.8 حفظ السجلات

يجب الحفاظ على السجلات المناسبة طوال دورة حياة أوراق الاعتماد/الإثباتات. وكحد الأدنى يُحتفظ بالسجلات من أجل توثيق المعلومات التالية:

أ) ما يؤكد حقيقة أن أوراق الاعتماد قد استُحدِثت؛

ب) معرّف هوية أوراق الاعتماد (عند الاقتضاء)؛

ج) الكيان الذي أُصدرت وثائق الاعتماد من أجله (عند الاقتضاء)؛

د) وضع أوراق الاعتماد (عند الاقتضاء).

ويجب حفظ السجلات لكل عملية (منطبقة) من العمليات التي تدخل في مرحلة إدارة أوراق الاعتماد/الإثباتات. وعند إصدار أوراق الاعتماد لكيانات بشرية (لأشخاص)، من المرجح أن يتضمن حفظ السجلات معالجة المعلومات المحددة لهوية الشخص. انظر التذييل I.

3.8 مرحلة استيقان الكيان

أثناء مرحلة استيقان الكيان، يَستخدم الكيان أوراق اعتماده ليشهد على هويته أمام هيئة التسجيل. وتكون عملية الاستيقان معنية حصرياً بتوطيد الثقة (أو عدم توطيدها) بالهوية المزعومة أو المدعاة، ولا يوجد تأثير لها على الإجراءات التي قد يختار الطرف المعوّل اتخاذها استناداً إلى زعم أو ادعاء، كما لا تربطها علاقة بتلك الإجراءات.

1.3.8 الاستيقان

تشمل عملية الاستيقان استخدام بروتوكول لإثبات تملّك أوراق الاعتماد أو السيطرة عليها من أجل إرساء الثقة بالكيان. وتتغير متطلبات بروتوكول الاستيقان وفقاً لمستويات الضمان المعتمدة. فبالنسبة لمستوى ضمان أدنى على سبيل المثال، قد يتضمن الاستيقان استخدام كلمة سر. أما في حالة مستويات الضمان الأعلى، فقد يتضمن الاستيقان استخدام بروتوكول التحدي والرد على أساس التجفير. ويكون الاستيقان المتعدد العوامل لازماً عند مستويات الضمان الأعلى. ولا تبدي جميع عوامل الاستيقان نفس القدر من القوة، وتُستخدم عوامل متعددة لتعزيز الضمان. انظر الفقرة 10.

2.3.8 حفظ السجلات

قد تكون عمليات مراقبة الأحداث وحفظ سجلات بشأنها في مرحلة الاستيقان ضرورية لأغراض متنوعة، من قبيل توفير الخدمة والامتثال والمحاسبة و/أو المتطلبات القانونية.

وحين يكون الأمر متعلقاً بالكيانات البشرية (الأشخاص)، قد تحتوي المعلومات الواردة في تلك السجلات على معلومات حساسة. ويجب أن تُدار تلك السجلات بطريقة تراعي الحاجة إلى حماية المعلومات المحددة لهوية الشخص وتقليلها إلى حدها الأدنى. انظر أيضاً التذييل I.

9 الاعتبارات الإدارية والتنظيمية

لا يرد ضمان استيقان الكيان من عوامل تقنية فقط، بل من أنظمة ولوائح واتفاقات تعاقدية ومن دراسة لطريقة إدارة توفير الخدمة وتنظيمها. فالحل القوي من الناحية التقنية الذي لا يكون مصحوباً بإدارة وتشغيل كفؤين قد يعجز عن استغلال قدراته الكامنة لتوفير الأمن في سياق تقديم ضمان استيقان الكيان.

وتعتبر هذه الفقرة إعلامية وتعرض وصفاً للاعتبارات الإدارية والتنظيمية التي تؤثر في ضمان استيقان الكيان. وهي لا تقدم معايير محدّدة لكل مستوى من مستويات الضمان. ومع أن المعايير المحددة وعمليات تقييم الامتثال للاعتبارات الإدارية والتنظيمية تقع خارج نطاق هذه التوصية، إلا أن توفيرها ينبغي أن يتم ضمن إطار موثوق.

1.9 إرساء الخدمة

يتصدى إرساء الخدمة لكل من الوضع القانوني لمورّد الخدمة ووضع توفير الخدمة الوظيفية. فالمعرفة مثلاً بأن مورّد خدمات إدارة واستيقان الهوية هو كيان قانوني مسجّل تمنح الثقة بأن مورد خدمة أوراق الاعتماد/الإثباتات هو بمثابة شركة حسنة النوايا ضمن الولاية القضائية التي تعمل فيها. وتزداد أهمية ذلك حين يتم تشغيل مكونات الخدمة من قبل كيانات قانونية مختلفة (التسجيل كوظيفة مستقلة مثلاً).

ومع أن الشروط الأساسية هي نفسها بالنسبة لجميع مستويات الضمان، فإن مستويات الضمان الأعلى ينبغي أن تعتمد بصورة أكبر على اكتمال توفير الخدمة وموثوقيتها. فعند مستوى الضمان الثالث وما فوق على سبيل المثال، يجب أن يُستمد قدر أكبر من الضمان بشأن توفير الخدمة من معرفة صلاته وعلاقاته التجارية ومن فهم مستوى الاستقلالية المسموحة له في تنفيذ عملياته.

2.9 الامتثال القانوني والتعاقدي

ينبغي لجميع الجهات الفاعلة في إطار ضمان استيقان الكيان أن تتفهّم الشروط القانونية الواقعة على عاتقها فيما يتعلق بتشغيل الخدمة وتنفيذها وأن تمتثل لهذه الشروط. وينطوي ذلك على تأثيرات تشمل، على سبيل المثال لا الحصر، أنواع المعلومات التي يمكن التماسها وكيفية إجراء تدقيق الهوية وتحديد المعلومات التي يمكن الاحتفاظ بها. ويعتبر التعامل مع المعلومات المحددة لهوية الشخص من الشواغل القانونية (انظر الملحق ألف). ولا بدّ من مراعاة جميع السلطات القضائية التي تعمل الجهات الفاعلة في إطارها. وعند مستوى الضمان الثاني وما فوق، ينبغي تحديد السياسات والشروط التعاقدية أيضاً.

3.9 أحكام مالية

حين يشكل توفر الخدمات الطويل الأجل اعتباراً من الاعتبارات في توقعات الكيان والأطراف المعوّلة على السواء، ينبغي إظهار الاستقرار المالي بقدر يكفي لضمان استمرار تشغيل الخدمة ولتحمل درجة المسؤولية القانونية التي تتعرض لها. فبالنسبة لخدمات مستوى الضمان الأول وموثوقيته، من غير المرجح أن تشكل هذه الأحكام أحد الاعتبارات، في حين أن الخدمات التي تدعم معاملات أكثر أهمية عند مستوى الضمان الثاني وما فوق ينبغي أن تتصدى لمثل هذه الاحتياجات.

4.9 إدارة وتدقيق أمن المعلومات

عند مستوى الضمان الثاني وما فوق، يجب على الجهات الفاعلة في إطار ضمان استيقان الكيان أن تضع موضع التنفيذ ما تمّ توثيقه من ممارسات إدارة أمن المعلومات وسياساتها ونهجها المتبعة بشأن إدارة المخاطر، والضوابط الأخرى المعترف بها، وذلك من أجل توفير الضمان بأن الممارسات الفعالة هي موضع التنفيذ. وبالنسبة لمستوى الضمان الثالث وما فوق، يتعين استخدام نظام رسمي لإدارة أمن المعلومات (مثلاً، السلسلة ISO/IEC 27000-b).

ورهناً بالاتفاقات المتعلقة بالامتثال القانوني والتعاقدي والتقني، يتعين على الجهات الفاعلة أن تضمن تقيّد الأطراف بالالتزامات، ويجوز لها أن توفر سبل الانتصاف والتعويض في حال عدم قيامها بذلك. وعند مستوى الضمان الثاني وما فوق، ينبغي أن يكون هذا الضمان مدعوماً بعمليات تدقيق أمنية، خارجية وداخلية على السواء، وكذلك بالاحتفاظ الآمن بسجلات الأحداث البارزة بما في ذلك عمليات التدقيق تلك. ويمكن استخدام التدقيق للتأكد من أن الممارسات التي تتبعها الأطراف تتمشى مع ما تمّ الاتفاق عليه. ويجوز استخدام خدمات تسوية الخلافات في حالات التضارب في الآراء.

5.9 مكونات الخدمة الخارجية

حين تعتمد منظمة ما على أطراف ثالثة من أجل أجزاء من خدمتها، فإن الطريقة التي توجّه بها الإجراءات التي تتخذها تلك الأطراف وتشرف عليها ستسهم في الضمان الكلي لتوفير الخدمة. وينبغي أن تكون طبيعة الترتيبات ودرجتها متناسبة مع مستوى الضمان المطلوب ونظام إدارة أمن المعلومات المطبّق. فعند مستوى الضمان الأول، ينبغي أن يكون لهذا الضمان حد أدنى من التأثير، علماً بأن هذه التدابير تسهم، انطلاقاً من مستوى الضمان الثاني فما فوق، في الضمان الكلي المقدّم.

6.9 البنية التحتية التشغيلية

من أجل المساعدة في قيام شبكات الثقة الواسعة النطاق، يجوز استخدام إطار ثقة. وضمن إطار الثقة، تقوم الجهات الفاعلة بدعم تدفق المعلومات فيما بينها. ووفقاً للاتفاقات المبرمة، يجوز دعوة الجهات الفاعلة الإضافية إلى ضمان تقيّد جميع الأطراف بالالتزامات، ويجوز لها أن توفر سبل الانتصاف في حال عدم قيامها بذلك.

7.9 قياس القدرات التشغيلية

يطرح واضعو السياسات الشروط التقنية والتعاقدية لأطر الثقة. وقد تتضمن الشروط التقنية على سبيل المثال مستويات إصدار المنتج، وتشكيلة الأنظمة، والإعدادات، والبروتوكولات، فيما قد يتم توجيه الشروط التعاقدية نحو الممارسات الإعلامية المعقولة. وينبغي لواضعي السياسات، عند تحديد تلك الشروط، أن يدرجوا فيها المعايير التي يمكن بواسطتها قياس كيانات أطر الثقة. فبدلاً من قيام واضعي السياسات بوضع المعايير بأنفسهم، قد يرغبون في الاستفادة من المعايير القياسية التي سبق أن بلورها الخبراء، مثل هذه التوصية. وكلما زاد استخدام واضعي السياسات للمعايير القياسية في أطر الثقة المختلفة، ازدادت سهولة فهم الكيانات لتلك المعايير وتطبيقها بشكل متسق. وعلاوة على ذلك، يمكن أن تفيد مجموعات المعايير المعينة كوسيلة مختزلة للإشارة إلى مختلف درجات أو أنواع الصرامة المتضمنة في الشروط أو القدرات عند مختلف مستويات الضمان.

10 التهديدات وعمليات التحكم

تعرض هذه الفقرة وصفاً لكل مرحلة من مراحل استيقان الكيان وتحدد عمليات التحكم اللازمة لكل مستوى من مستويات الضمان.

1.10 التهديدات لمرحلة الانتساب وعمليات التحكم بها

1.1.10 التهديدات لمرحلة الانتساب

يحدد الجدول 10-1 التهديدات التي تتعرض مرحلة الانتساب لها ويقدم وصفاً لها.

الجدول 10-1 – التهديدات لمرحلة الانتساب

التهديد	الوصف والأمثلة
انتحال الشخصية	تتجسد بعض الأمثلة على انتحال الشخصية عند قيام كيان ما بطريقة غير مشروعة باستخدام معلومات تخص هوية كيان آخر، أو حين يتم تسجيل جهاز في شبكة باعتماد عنوان مخادع للتحكم في النفاذ إلى الوسائط.

2.1.10 عمليات التحكم اللازمة لمستوى الضمان للحماية من التهديدات لمرحلة الانتساب

يحدد الجدول 10-2 عمليات التحكم اللازمة لمرحلة الانتساب وفقاً لمستوى الضمان.

الجدول 10-2 – عمليات التحكم بمرحلة الانتساب لكل مستوى من مستويات الضمان

التهديدات	عمليات التحكم	عمليات التحكم اللازمة			
		LoA1	LoA2	LoA3	LoA4
انتحال الشخصية	تدقيق الهوية: التقيّد بالسياسة	الرقم 1	الرقم 1	الرقم 1	الرقم 1
	تدقيق الهوية: بشكل شخصي				الرقم 2
	تدقيق الهوية: معلومات رسمية موثوقة	الرقم 3	الرقم 4	الرقم 5	الرقم 6

ملاحظـــة – في الجدول أعلاه، تقابل معرفات الهوية من الرقم 1 إلى الرقم 6 عمليات تحكم محددة لازمة لتوفير الحماية عند كل مستوى من مستويات الضمان. ويرد وصف كلّ من عمليات التحكم تلك بشكل مفصّل في الفقرة الفرعية 1.2.1.10. أما الخانات في الجدول التي تحتوي على خط قطري فتشير إلى أن عملية التحكم ذات الصلة لا تنطبق على مستوى الضمان المشار إليه.

1.2.1.10 عمليات التحكم للحماية من التهديدات لمرحلة الانتساب

تقابل عمليات التحكم التالية للحماية من التهديدات لمرحلة الانتساب العمليات من رقم 1 إلى رقم 6 المدرجة في الجدول 10-2.

تدقيق الهوية: التقيّد بالسياسة

الرقم 1. نشر سياسة تدقيق الهوية وإجراء كل عمليات تدقيق الهوية بما يتوافق مع وثيقة تدقيق الهوية التي تم نشرها.

تدقيق الهوية: بشكل شخصي

الرقم 2. تدقيق الهوية بشكل شخصي يُستخدم للأشخاص.

تدقيق الهوية: معلومات رسمية موثوقة

الرقم 3. المعلومات المتعلقة بالهوية يمكن أن تكون مزعومة أو مدعاة ذاتياً.

الرقم 4. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 3.

إضافةً إلى ما يلي:

- يقدم الكيان معلومات عن الهوية مأخوذة مما لا يقل عن مصدر موثوق واحد وممتثل للسياسات لمعلومات تتعلق بالهوية.

أ) للكيانات البشرية (الأشخاص):

'1' بشكل شخصي:

- التأكد من أن في حوزة الكيان وثيقة تعريف هوية مأخوذة مما لا يقل عن مصدر موثوق واحد وممتثل للسياسات وتحمل صورة فوتوغرافية لصاحبها مطابقة لشكل الكيان؛
- والتأكد من أن وثيقة تعريف الهوية المقدمة هي وثيقة أصلية، صادرة حسب الأصول وصالحة في وقت استخدامها.

'2' بشكل غير شخصي:

- يقدم الكيان دليلاً على أنه يملك معلومات عن الهوية الشخصية ممتثلة للسياسات. (من بين الأمثلة على المعلومات المقبولة المتعلقة بالهوية رخصة القيادة أو جواز السفر)؛
- ويتم إثبات وجود الدليل المقدّم وصلاحيته وفقاً لمتطلبات السياسة المحلية.

ب) للكيانات المادية (غير الأشخاص)

- تسجيل معلومات مستقاة من مصدر موثوق لمعلومات تتعلق بالهوية، مثل الاسم الشائع والأوصاف ورقم التسلسل وعنوان التحكم في النفاذ إلى الوسائط والمالك والموقع وجهة التصنيع ونحو ذلك.

الرقم 5. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 4.

إضافةً إلى ما يلي:

أ) للكيانات البشرية (الأشخاص):

'1' بشكل شخصي:

- التحقق من دقة المعلومات المتعلقة بالعنوان الواردة في وثيقة تعريف الهوية باستخدامها للاتصال بالكيان؛
- والتحقق مما لا يقل عن وثيقة واحدة من وثائق تعريف الهوية (مثلاً شهادة الميلاد أو الزواج أو وثائق الهجرة) بمقارنتها بسجلات المصدر الموثوق ذي الصلة؛
- وتأكيد صحة المعلومات الشخصية بمقارنتها بمصادر معلومات موثوقة ومصادر (حيثما أمكن) مأخوذة من سياقات أخرى، تكفي لضمان انفراد الكيان بالهوية؛
- والتحقق من معلومات قدمت في السابق من قبل الكيان أو يحتمل أن تكون معروفة من الكيان فقط دون غيره.

'2' بشكل غير شخصي:

- التأكد من صحة التدقيق من قبل طرف ثالث موثوق في زعم/ادعاء الكيان لامتلاكه الحالي لأوراق اعتماد/إثباتات من مستوى الضمان الثالث (أو أعلى) مأخوذة من مصدر موثوق؛
- التحقق من معلومات قدمت في السابق من قبل الكيان أو يحتمل أن تكون معروفة من الكيان فقط دون غيره.

ب) للكيانات المادية (غير الأشخاص):

- تُستخدم تجهيزات موثوقة (مثلاً وحدة TPM) عند مستوى الضمان الثالث؛
- بالنسبة للكيانات المادية المتداولة، يتم تسجيل الكيان المادي مادياً مع هيئة تسجيل تحمل شكل الجهاز باستخدام أوراق اعتماد/إثباتات من مستوى الضمان الثالث صادرة عن أشخاص. وعند استخدام معدات موثوقة، يتعين تمكينها؛
- وبالنسبة للكيانات المادية التي لم يتم اقتناؤها بعد يقدّم طلب باعتماد الاستيقان البشري من مستوى الضمان الثالث أو التوقيع الرقمي لإثبات أن الكيان مقدّم الطلب مخول بتقديم طلب الحصول على الكيان المادي. وتقوم هيئة التسجيل لدى جهة التصنيع بتسجيل الكيان المادي وتمكين أي تجهيزات موثوقة والتحكّم بإصدار الكيان المادي وإعطائه الطابع الشخصي. ويجري بدء تشغيل التجهيزات الموثوقة فور توصيلها بالشبكة؛
- وبالنسبة للكيانات المادية خلاف الحواسيب، يتأمن الربط بين الجهاز أو المالك أو الشبكة أو ناقل الاتصال وبين هيئة التسجيل بطريقة تجفيرية شبيهة بتلك الخاصة بأجهزة الحاسوب الموثوقة؛
- وعند استخدام البرمجيات، تُوقع الشفرة رقمياً قبل الإصدار باعتماد أوراق اعتماد/إثباتات من المستوى الثالث صادرة عن أشخاص، وتضع هيئة التسجيل التوقيع الثاني عليها كإثبات لقبولها قبل إدخالها حيز التشغيل.

الرقم 6. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 5.

إضافةً إلى ما يلي:

أ) للكيانات البشرية (الأشخاص):

- يقدم الكيان معلومات عن الهوية مأخوذة مما لا يقل عن مصدر إضافي واحد موثوق وممتثل للسياسات.

ب) للكيانات المادية (غير الأشخاص):

- يجري تسجيل الأجهزة الإضافية الموصولة بحاسوب أو هاتف ذكي أو معالج مماثل عند إصدارها، ويتم ربطها بالتجفير بجهاز الإرساء (مثل جهاز حاسوب موثوق ومخول، وقارئ القياسات الحيوية، والبطاقات الذكية، وجهة استيقان أرضية للنظام العالمي لتحديد المواقع)؛
- وتُدار أية تغييرات تطرأ على ترتيبات الربط بين الأجهزة عن طريق هيئة التسجيل. ويجب على قدرة إدارة الشبكة، كلما أمكن ذلك، تنبيه هيئة التسجيل أو إدارة الشبكة بشأن أية تغييرات تجري في العلاقات بين الأجهزة والإجراء التصحيحي المتخذ؛
- وتُوضع القدرات موضع التشغيل للحؤول دون تشغيل العلاقات بين الأجهزة التي تم تبديلها؛
- وتوقّع شفرة برمجيات مستوى الضمان الرابع رقمياً باعتماد أوراق اعتماد/إثباتات من مستوى الضمان الرابع صادرة عن أشخاص، على أن يتم التوقيع عليها ثانيةً من قبل هيئة التسجيل كإثبات لقبولها قبل إدخالها حيز التشغيل.

2.10 التهديدات لمرحلة إدارة أوراق الاعتماد/الإثباتات وعمليات التحكم بها

1.2.10 التهديدات لإدارة أوراق الاعتماد/الإثباتات

يُدرج الجدول 10-3 التهديدات لمرحلة إدارة أوراق الاعتماد/الإثباتات.

الجدول 10-3 – التهديدات لمرحلة إدارة أوراق الاعتماد/الإثباتات	
نوع التهديد	**الوصف والأمثلة**
إنشاء أوراق الاعتماد: التلاعب بها	قيام المهاجم بتغيير المعلومات لدى مرورها من عملية الانتساب إلى عملية إنشاء أوراق الاعتماد.
إنشاء أوراق الاعتماد: إنشاء غير مرخص	تسبّب المهاجم في قيام مورد خدمة أوراق الاعتماد بإنشاء أوراق اعتماد استناداً إلى هوية وهمية.
إصدار أوراق الاعتماد: الكشف عنها	قيام المهاجم بنسخ أوراق الاعتماد التي أنشأها مورد خدمة أوراق الاعتماد أثناء نقلها من مورد الخدمة إلى الكيان أثناء إنشاء أوراق الاعتماد.
تفعيل أوراق الاعتماد: تملّك غير مرخّص	حيازة المهاجم على أوراق اعتماد لا تخصه والادّعاء بأنها الهوية الصحيحة له، مما يدفع مورد خدمة أوراق الاعتماد إلى تفعيل أوراق الاعتماد.
تفعيل أوراق الاعتماد: عدم التوفر	1 عدم تواجد الكيان الذي تخصه أوراق الاعتماد، أو الوسيلة لإنتاج أوراق الاعتماد، في الموقع المعتاد وعدم التمكن من استيقان هويته بصورة كافية أمام مورد خدمة أوراق الاعتماد. 2 تأخير تجهيز أوراق الاعتماد أو الوسيلة لتوليد أوراق الاعتماد، وتعذّر عملية التفعيل أثناء الفترة المحدّدة.
تخزين أوراق الاعتماد: الكشف عنها	الكشف عن أوراق الاعتماد المختزنة في ملف نظام ما. مثلاً نفاذ المهاجم إلى سجل مختزن بأسماء المستعملين وكلمات المرور.
تخزين أوراق الاعتماد: التلاعب بها	تعرّض الملف الذي يقابل بين أسماء المستعملين وأوراق الاعتماد للضرر بحيث يتم تحوير عمليات التقابل، واستبدال أوراق الاعتماد القائمة بأخرى باستطاعة المهاجم النفاذ إليها.
تخزين أوراق الاعتماد: الاستنساخ	استخدام المهاجم لمعلومات مختزنة لاستحداث أوراق اعتماد مُستنسخة (مثلاً بإصدار نسخة طبق الأصل عن بطاقة ذكية يمكنها توليد أوراق الاعتماد) يمكن استخدامها من قبل الكيان غير المرخص.
تخزين أوراق الاعتماد: الكشف عن طريق الكيان	احتفاظ الكيان بسجل خطي باسم المستعمل وكلمة السر في مكان يستطيع الآخرون النفاذ إليه.
إلغاء أوراق الاعتماد: الإلغاء المؤجّل	عدم نشر معلومات الإلغاء في الوقت المناسب، ما يؤدي إلى خطر بقاء الكيانات ذات أوراق الاعتماد الملغاة قادرة على الاستيقان قبل قيام جهة التحقق بتحديث المعلومات الأخيرة المتعلقة بالإلغاء.
إلغاء أوراق الاعتماد: الاستعمال بعد وقف التشغيل	عدم حذف حسابات المستعملين عند ترك الموظفين للشركة أو لمكان العمل، ما يؤدي إلى احتمال إساءة استخدام الحسابات القديمة من قبل أشخاص غير مرخص لهم بذلك. – استخدام أوراق اعتماد مختزنة في أجهزة حاسوبية بعد إلغاء مفاتيح التجفير الخاصة بها.
تجديد أوراق الاعتماد: الكشف عنها	قيام المهاجم بنسخ أوراق الاعتماد التي أعاد تجديدها مورد خدمة أوراق الاعتماد أثناء نقلها.
تجديد أوراق الاعتماد: التلاعب بها	قيام المهاجم بتحوير أوراق الاعتماد الجديدة التي استحدثها الكيان أثناء تقديمها إلى مورد خدمة أوراق الاعتماد لتحل محل أوراق الاعتماد المنتهية صلاحيتها.
تجديد أوراق الاعتماد: التجديد غير المرخص	تمكّن المهاجم من الاستفادة من ضعف بروتوكول تجديد أوراق الاعتماد من أجل تمديد فترة صلاحية أوراق الاعتماد للكيان الحالي. خداع المهاجم لمورد خدمة أوراق الاعتماد بحيث يصدر الأخير أوراق اعتماد جديدة للكيان الحالي، وتعمل أوراق الاعتماد الجديدة على ربط هوية الكيان الحالي بأوراق اعتماد جديدة قدمها المهاجم. وفيما يتعلق بالكيانات المادية (غير الأشخاص)، يتجسد أحد الأمثلة في إعادة وسم (إعادة إصدار) مكون من مكونات النظام بوصفه مكوناً جديداً حتى بعد استعماله (مثلاً ذاكرة النفاذ العشوائي).
حفظ سجلات أوراق الاعتماد: التنصّل	زعم الكيان أو ادّعاؤه بأن بعض أوراق الاعتماد القانونية هي أوراق اعتماد زائفة أو تحتوي على معلومات غير صحيحة بهدف النفي الكاذب لقيامه باستعمال أوراق الاعتماد.

2.2.10 عمليات التحكم اللازمة لمستوى الضمان للحماية من التهديدات لمرحلة إدارة أوراق الاعتماد/الإثباتات

يحدد الجدول 10-4 عمليات التحكم اللازمة لمواجهة التهديدات لإدارة أوراق الاعتماد وفقاً لمستوى الضمان.

الجدول 10-4 – عمليات التحكم بإدارة أوراق الاعتماد لكل مستوى من مستويات الضمان

نوع التهديد	عمليات التحكم	عمليات التحكم اللازمة			
		LoA1	LoA2	LoA3	LoA4
إنشاء أوراق الاعتماد: التلاعب بها	الإنشاء الملائم لأوراق الاعتماد	الرقم 1	الرقم 1	الرقم 2	الرقم 2
	التجهيزات فقط				الرقم 3
	إقفال الحالة				الرقم 4
إنشاء أوراق الاعتماد: الإنشاء غير المرخص	أعمال جرد متتبّعة	الرقم 5	الرقم 5	الرقم 5	الرقم 5
إصدار أوراق الاعتماد: الكشف عنها	الإصدار الملائم لأوراق الاعتماد	الرقم 6	الرقم 7	الرقم 7	الرقم 8
تفعيل أوراق الاعتماد: تملك غير مرخص تفعيل أوراق الاعتماد: عدم التوفر	التفعيل من قبل الكيان	الرقم 9	الرقم 9	الرقم 10	الرقم 11
تخزين أوراق الاعتماد: الكشف عنها تخزين أوراق الاعتماد: التلاعب بها تخزين أوراق الاعتماد: الاستنساخ تخزين أوراق الاعتماد: الكشف عنها من قبل الكيان	التخزين الآمن لأوراق الاعتماد	الرقم 12	الرقم 13	الرقم 14	الرقم 15
إلغاء أوراق الاعتماد: تأخير الإلغاء إلغاء أوراق الاعتماد: استعمالها بعد وقف التشغيل	الإلغاء الآمن لأوراق الاعتماد وإتلافها	الرقم 16	الرقم 16	الرقم 16	الرقم 16
تجديد أوراق الاعتماد: الكشف عنها تجديد أوراق الاعتماد: التلاعب بها تجديد أوراق الاعتماد: التجديد غير المرخص	التجديد الآمن لأوراق الاعتماد	الرقم 17	الرقم 17	الرقم 18	الرقم 19
حفظ سجلات أوراق الاعتماد: التنصّل	الاحتفاظ بالسجلات	الرقم 20	الرقم 20	الرقم 21	الرقم 21

ملاحظـــة – في الجدول أعلاه، تقابل معرفات الهوية من الرقم 1 إلى الرقم 21 عمليات تحكم محددة لازمة لتوفير الحماية عند كل مستوى من مستويات الضمان. ويرد وصف كلّ من عمليات التحكم تلك بشكل مفصّل في الفقرة الفرعية 1.2.2.10. أما الخانات في الجدول التي تحتوي على خط قطري فتشير إلى أن عملية التحكم ذات الصلة لا تنطبق على مستوى الضمان المشار إليه.

1.2.2.10 عمليات التحكم لمواجهة التهديدات لمرحلة إدارة أوراق الاعتماد/الإثباتات

تقابل عمليات التحكم التالية للتهديدات لمرحلة إدارة أوراق الاعتماد الأرقام المدرجة في الجدول 4.10.

الإنشاء الملائم لأوراق الاعتماد

الرقم 1. تنطبق عمليات التحكم التالية:

تُستخدم العمليات الرسمية والموثقة في إنشاء أوراق الاعتماد.

قبل الانتهاء من إسناد أوراق الاعتماد إلى الكيان، يجب أن يكون لدى مورد خدمة أوراق الاعتماد الضمان الكافي بأن أوراق الاعتماد مسندة إلى الكيان الصحيح وتبقى مسندة إليه.

الرقم 2. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 1.

إضافة إلى ما يلي:

- إسناد أوراق الاعتماد يوفر الحماية من التلاعب باستخدام إما:

أ) التواقيع الرقمية؛

ب) أو الآليات الموصوفة في إقفال الحالة لأوراق الاعتماد المحفوظة في التجهيزات.

التجهيزات فقط

الرقم 3. يتم تضمين أوراق الاعتماد في وحدة أمن التجهيزات[6].

إقفال الحالة

الرقم 4. تُحفظ أوراق الاعتماد المحتجزة في التجهيزات في حالة مقفلة عند انتهاء عملية الإنشاء.

أعمال الجرد المتتبّعة

الرقم 5. حين تُحفظ أوراق الاعتماد أو وسيلة إنتاجها في جهاز من التجهيزات، يتم الحفاظ على الأمن المادي للجهاز وتتبّع أعمال الجرد. فعلى سبيل المثال، ينبغي تخزين البطاقات الذكية غير المشخصنة في مكان آمن وتسجيل أرقام التسلسل الخاصة بها لحمايتها من السرقة ومن المحاولات اللاحقة لإنشاء أوراق اعتماد غير مرخصة.

الإصدار الملائم لأوراق الاعتماد

الرقم 6. تُستخدم العمليات الرسمية والموثقة في إصدار أوراق الاعتماد.

الرقم 7. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 6.

إضافة إلى ما يلي:

- يجب أن تتضمن عملية الإصدار آلية تكفل توفير أوراق الاعتماد للكيان المناسب أو من يمثله. فإن لم يتم تسليم أوراق الاعتماد شخصياً، تُستخدم آلية للتحقق من أن عنوان التوصيل موجود وأنه مرتبط بالكيان بصورة مشروعة.

الرقم 8. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 7.

إضافة إلى ما يلي:

- إذا لم يتم تسليم أوراق الاعتماد شخصياً، ينبغي تسليمها باعتماد قناة آمنة على أن يوقع الكيان أو من يمثله على وثيقة استلام تعترف باستلام أوراق الاعتماد.

التفعيل من قبل الكيان

الرقم 9. يتعين وجود إجراء لضمان تفعيل أوراق الاعتماد، أو وسيلة توليدها، فقط إذا كانت تحت سيطرة الكيان المقصود. ولا توجد شروط محددة لهذا الإجراء.

الرقم 10. يتعين وجود إجراء لضمان تفعيل أوراق الاعتماد، أو وسيلة توليدها، فقط إذا كانت تحت سيطرة الكيان المقصود. ويجب أن يثبت هذا الإجراء أن الكيان مرتبط بتفعيل أوراق الاعتماد (مثلاً بروتوكول التحدي والردّ).

الرقم 11. يتعين وجود إجراء لضمان تفعيل أوراق الاعتماد، أو وسيلة توليدها، فقط إذا كانت تحت سيطرة الكيان المقصود. وعلى هذا الإجراء أن:

أ) يثبت أن الكيان مرتبط بتفعيل أوراق الاعتماد (مثلاً بروتوكول التحدي والردّ)،

ب) ويسمح بالتفعيل فقط ضمن الفترة الزمنية التي تقررها السياسة.

---

6 يرد تعريف حدود وحدة أمن التجهيزات في التوصية ISO/IEC 19790:2012.

التخزين الآمن لأوراق الاعتماد

الرقم 12. تنطبق عمليات التحكم التالية:

- يجب حماية أوراق الاعتماد المستندة إلى أسرار مشتركة من خلال عمليات التحكم بالنفاذ التي تحصر النفاذ في جهات الإدارة والتطبيقات التي تحتاج إلى النفاذ؛
- ويجب أن توصف سياسة الحماية لأوراق الاعتماد المختزنة في الوثائق المقترنة باستخدام أوراق الاعتماد تلك والتي يتم توفيرها للكيانات.

الرقم 13. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 12.

إضافة إلى ما يلي:

- يجب أن لا تحتوي الملفات السرية المشتركة هذه على كلمات سر أو على أسرار النص المكتوب؛ وقد تُستخدم طريقة بديلة لحماية السر المشترك.

الرقم 14. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 13.

إضافة إلى ما يلي:

- يجب حماية الأسرار المشتركة من خلال عمليات التحكم بالنفاذ التي تحصر النفاذ في جهات الإدارة والتطبيقات التي تحتاج إلى النفاذ. ويجب تجفير الأسرار المشتركة هذه. أما مفتاح التجفير للسر المشترك فيُجفر بحد ذاته ويُخزن في وحدة تجفير (تجهيزات أو برمجيات). ولا يتم فك تجفير مفتاح تجفير السر المشترك إلا في الوقت الذي يطلب فيه ذلك من أجل عملية استيقان؛
- يُطلب إلى الكيانات أو من يمثلها الإقرار بفهم هذه الشروط والموافقة على حماية أوراق الاعتماد وفقاً لتلك الشروط.

الرقم 15. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 14.

إضافة إلى ما يلي:

- يُطلب إلى الكيانات أو من يمثلها التوقيع على وثيقة للإقرار بفهم الشروط اللازمة لتخزين أوراق الاعتماد والموافقة على حماية أوراق الاعتماد تبعاً لذلك.

الإلغاء الآمن لأوراق الاعتماد وإتلافها

الرقم 16. يلغي مورّد خدمة أوراق الاعتماد أو يتلف (إن أمكن ذلك) أوراق الاعتماد (بما في ذلك تلك القائمة على أسرار مشتركة) ضمن فترة زمنية محددة لكل مستوى من مستويات الضمان على النحو المحدد في السياسة التنظيمية.

التجديد الآمن لأوراق الاعتماد

الرقم 17. تنطبق عمليات التحكم التالية:

- قيام مورد خدمة أوراق الاعتماد بإرساء سياسات مناسبة لتجديد أوراق الاعتماد واستبدالها؛
- تأكيد إثبات تملك الكيان لأوراق الاعتماد الحالية غير المنتهية الصلاحية قبل قيام مورد خدمة أوراق الاعتماد بالسماح بتجديدها و/أو استبدالها؛
- استيفاء كلمات السر للحد الأدنى من شروط سياسة مورد خدمة أوراق الاعتماد المتعلقة بقوة كلمة السر وإعادة استعمالها؛
- عدم السماح بتجديد أوراق الاعتماد عقب انتهاء صلاحية أوراق الاعتماد الحالية؛
- إتمام جميع عمليات التفاعل عبر قناة محمية.

الرقم 18. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 17.

إضافةً إلى ما يلي:

- إجراء تدقيق للهوية عند مستوى الضمان الثاني وفقاً للفقرة الفرعية 1.2.1.10 (تدقيق الهوية: التقيّد بالسياسات، تدقيق الهوية: معلومات معتمدة).

الرقم 19. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 18.

إضافة إلى ما يلي:

- إجراء تدقيق الهوية عند مستوى الضمان الثاني وفقاً للفقرة الفرعية 1.2.1.10 (تدقيق الهوية: التقيد بالسياسات، تدقيق الهوية: معلومات معتمدة).

الاحتفاظ بالسجلات

الرقم 20. يحتفظ مورد خدمة أوراق الاعتماد بسجل يتضمن تسجيل وتاريخ ووضع كل ورقة من أوراق الاعتماد (بما في ذلك إلغاءها). وتحدد سياسة مورد خدمة أوراق الاعتماد فترة الاحتفاظ بالسجلات.

الرقم 21. تنطبق عمليات التحكم التالية:

- جميع عمليات التحكم بدءاً بالرقم 20.
- وضع إجراءات رسمية وموثقة من أجل تسلسل عهدة كل سجل من السجلات.

3.10 التهديدات لمرحلة الاستيقان وعمليات التحكم بها

1.3.10 التهديدات لمرحلة الاستيقان

تتضمن التهديدات لمرحلة الاستيقان كلاً من التهديدات المرتبطة باستخدام أوراق الاعتماد/الإثباتات أثناء عملية الاستيقان والتهديدات العامة للاستيقان. ومن بين التهديدات العامة لعملية الاستيقان التهديدات التالية على سبيل المثال لا الحصر: البرمجيات الضارة (مثلاً الفيروسات والفيروسات المتخفّية ومسجّلات ضربات المفاتيح)؛ والتحايل الاجتماعي (مثل اختلاس النظر فوق كتف المشترك، وسرقة أجهزة معدات الحاسوب، وأرقام تعريف الهوية الشخصية)؛ وأخطاء يرتكبها المستعملون (مثل كلمات السر الضعيفة، والعجز عن حماية استيقان المعلومات)؛ والتنصّل الزائف؛ والاعتراض و/أو التحوير غير المرخّص للبيانات أثناء الإرسال؛ ومنع الخدمة؛ وضعف الإجراءات. وباستثناء استخدام الاستيقان المتعدد العوامل، فإن عمليات التحكم بالتهديدات العامة للاستيقان تقع خارج نطاق هذه التوصية. وتركز هذه الفقرة على التهديدات المرتبطة باستخدام أوراق الاعتماد من أجل الاستيقان، وتقدم وصفاً لهذه التهديدات وتُدرج عمليات التحكم بكل نوع منها.

وإذا ما وضعنا جانباً الشرط القاضي باستخدام الاستيقان المتعدد العوامل لمستويي الضمان الثالث والرابع، يتبين أنه من غير الملائم تحديد وتتبع عمليات تحكم محددة من حيث الصلة بمستوى الضمان لمرحلة الاستيقان. فقد تكون بعض عمليات التحكم غير ملائمة لجميع السياقات. فعلى سبيل المثال، من المحتمل أن تكون عمليات التحكم الخاصة باستيقان المستخدمين الساعين إلى النفاذ إلى الاشتراكات في مجلات إلكترونية مختلفة عن عمليات التحكم الخاصة بالأطباء الساعين إلى النفاذ إلى الملفات الطبية للمرضى. وبناء على ذلك، وبالنظر إلى التزايد المطّرد في حدة المخاطر والتبعات المترتبة على الاستغلال، ينبغي لمورّد خدمة أوراق الاعتماد/الإثباتات أن ينظر في قضية الأمن بتعمّق (أي القيام بترتيب طبقات عمليات التحكم الملائمة للبيئة التشغيلية والتطبيق ومستوى الضمان). أما اتخاذ القرارات المتعلقة بكيفية استخدام عمليات التحكم هذه، وتحديد الوقت لذلك وضمن أي توليفات، فــتُلقى على عاتق مصممي النظام بالاستناد إلى عملية تقييم للمخاطر.

وثمة الكثير من الأخطار التي تتهدّد أوراق الاعتماد المستخدمة للاستيقان. ويُدرج الجدول 10-5 بعض الفئات العريضة للتهديدات التي تواجه استخدام أوراق الاعتماد ويقدم أمثلة محددة لتوضيح تلك التهديدات.

الجدول 10-5 – موجز للتهديدات لاستخدام أوراق الاعتماد/الإثباتات في مرحلة الاستيقان

التهديد	الوصف والأمثلة
التهديدات العامة	تتضمن التهديدات العامة للاستيقان الكثير من فئات تهديدات الأمن المشتركة والشائعة لدى أي نوع من أنواع تكنولوجيا المعلومات والاتصالات. ومن بعض الأمثلة على ذلك تسجيل ضربات المفاتيح، والتحايل الاجتماعي والأخطاء التي يرتكبها المستعملون. وتتجاوز عمليات التحكم بتلك التهديدات نطاق هذا المعيار، باستثناء استخدام الاستيقان المتعدد العوامل. وتجدر الإشارة إلى أن الاستيقان المتعدد العوامل لا يوفر حماية ضد جميع التهديدات العامة المحتملة.
التخمين على الشبكة	إجراء المهاجم لمحاولات تسجيل متكررة بتخمين القيم المحتملة لأوراق الاعتماد.
التخمين خارج الشبكة	كشف الأسرار المرتبطة بتوليد أوراق الاعتماد باستخدام طرق تحليلية تقع خارج معاملة الاستيقان. ففك كلمة السر يعتمد في الغالب على طرق هجمات القوة المفرطة من قبيل استخدام الهجمات القاموسية. فباعتماد الهجمات القاموسية يستخدم المهاجم برنامجاً لتصفح واستعراض جميع الكلمات الواردة في قاموس (أو قواميس متعددة بلغات مختلفة)، وحساب قيمة التظليل لكل كلمة، والتدقيق في قيمة التظليل الناتجة إزاء قاعدة للبيانات. ويُعتبر استخدام جداول قوس قزح (رينبو) طريقة أخرى لفك كلمة السر. فجداول قوس قزح هي جداول محوسبة مسبقاً لأزواج النص الواضح/قيمة التظليل. وتتسم هجمات جداول قوس قزح بأنها أسرع من هجمات القوة المفرطة لأنها تستخدم دوالّ اختزال لتقليل حيز البحث. وبمجرد توليد جداول قوس قزح أو الحصول عليها، يمكن استخدامها بشكل متكرر من قبل المهاجم.
استنساخ أوراق الاعتماد	الاستنساخ غير المشروع لأوراق اعتماد الكيان أو وسائل توليد أوراق الاعتماد. ومن أمثلة ذلك النسخ غير المرخص للمفتاح الخاص.
التصيّد الاحتيالي	استدراج الكيان للتفاعل مع جهة تحقق مزيفة والتحايل عليه للكشف عن كلمة السر الخاصة به أو عن بيانات شخصية حساسة يمكن استخدامها للتنكر وانتحال شخصية الكيان. مثال ذلك إرسال رسالة إلكترونية إلى كيان لتوجيهه نحو موقع ويب مزوّر والطلب إليه التسجيل باستخدام اسمه وكلمة السر الخاصة به.
التنصّت	قيام المهاجم بالتنصت على معاملة استيقان لالتقاط معلومات يمكن استخدامها في هجوم فعال لاحق للتنكر والتظاهر بأنه الكيان نفسه.
هجوم إعادة التنفيذ	قدرة المهاجم على إعادة الرسائل الملتقطة في السابق (بين كيان مشروع وهيئة تسجيل) ليظهر بمظهر ذلك الكيان المستيقن منه أمام هيئة التسجيل.
اختطاف الدورة	قدرة المهاجم على إقحام نفسه بين الكيان وجهة التحقق عقب نجاح تبادل الاستيقان بين الطرفين الأخيرين. وقدرة المهاجم على الظهور بمظهر الكيان أو الادعاء بأنه الكيان أمام الطرف المعوّل أو بالعكس للتحكم بتبادل معلومات الدورة. مثال ذلك حين يتمكن المهاجم من الاستيلاء على دورة تمّ استيقانها عن طريق التنصت أو التنبؤ بقيمة بصمة الاستيقان المستخدمة لوضع علامة أو إشارة على الطلبات المتعلقة ببروتوكول نقل النصوص التشعبية من قبل الكيان.
هجوم لمتطفل بين طرفين	تموضع المهاجم في موقع بين الكيان والطرف المعوّل للتمكن من اعتراض وتغيير محتوى رسائل بروتوكول الاستيقان. فينتحل المهاجم في العادة هوية الطرف المعوّل أمام الكيان وهوية الكيان أمام جهة التحقق بشكل متزامن. وقد يؤدي إجراء التبادل الفعال مع كلا الطرفين بصورة متزامنة إلى السماح للمهاجم باستخدام رسائل الاستيقان المرسلة من طرف مشروع واحد للتمكن من الاستيقان الناجح أمام الطرف الآخر.
سرقة أوراق الاعتماد	قيام المهاجم بسرقة جهاز يولد أوراق الاعتماد أو يحتوي عليها.
الاحتيال والتنكر	يشير الاحتيال أو التنكر إلى أوضاع ينتحل فيها المهاجم هوية كيان آخر مما يسمح للمهاجم بالقيام بأمور يعجز عن تأديتها لولا ذلك (مثلاً من خلال الحصول على إمكانية النفاذ إلى أصول وموجودات يتعذر النفاذ إليها في حالات خلاف ذلك). وقد يُنفّذ ذلك بالاستفادة من أوراق الاعتماد الخاصة بالكيان أو الادعاء بأنه الكيان (بتزوير أوراق الاعتماد على سبيل المثال). ومن الأمثلة على ذلك انتحال المهاجم لهوية كيان والتحايل على خاصية أو أكثر من خصائص القياس الحيوي بخلق بصمة "اصطناعية" تماثل البصمة الخاصة بالكيان؛ أو ينتحل المهاجم عنوان التحكم في النفاذ إلى الوسائط (MAC) عن طريق جعل جهازه يبث عنواناً للتحكم في النفاذ إلى الوسائط يخصّ جهازاً آخر يملك تراخيص بهذا الشأن على شبكة معينة؛ أو حين يدعي المهاجم بأنه ناشر شرعي للبرمجيات ومسؤول عن التنزيل الإلكتروني لتطبيقات البرمجيات و/أو تحديثاتها.

2.3.10 عمليات التحكم اللازمة لمستوى الضمان للحماية من التهديدات لاستخدام أوراق الاعتماد

يحدد الجدول 10-6 عمليات التحكم اللازمة لمواجهة التهديدات لاستخدام أوراق الاعتماد وفقاً لمستوى الضمان.

الجدول 10-6 – موجز لعمليات التحكم بالتهديدات لاستخدام أوراق الاعتماد وفقاً لمستوى الضمان

نوع التهديد	عمليات التحكم	*LoA	LoA1	LoA2	LoA3	LoA4
تهديدات عامة	استيقان متعدد العوامل				الرقم 1	الرقم 1
التخمين على الشبكة	كلمة سر قوية إغلاق أوراق الاعتماد استعمال الحساب المبدئي التدقيق والتحليل	الرقم 2 الرقم 3 الرقم 4 الرقم 5				
التخمين خارج الشبكة	كلمة سر مظللة مع قيمة تظليل	الرقم 6				
استنساخ أوراق الاعتماد	مكافحة التزوير	الرقم 7				
التصيّد الاحتيالي	الكشف عن انتحال الهوية من الرسائل اعتماد ممارسة مكافحة انتحال الهوية الاستيقان المتبادل	الرقم 8 الرقم 9 الرقم 10				
التنصّت	عدم إرسال كلمة السر الاستيقان المجفّر معلمات استيقان مختلفة	الرقم 11 الرقم 12 الرقم 13				
هجوم إعادة التنفيذ	معلمات استيقان مختلفة خاتم الوقت الأمن المادي	الرقم 13 الرقم 14 الرقم 15				
اختطاف الدورة	دورة مجفرة ضبط مواطن ضعف البروتوكول إقامة اتصال متبادلة مجفرة	الرقم 16 الرقم 17 الرقم 18				
هجوم لمتطفل بين طرفين	الاستيقان المتبادل دورة مجفرة	الرقم 10 الرقم 16				
سرقة أوراق الاعتماد	تفعيل أوراق الاعتماد	الرقم 19				
الاحتيال والتنكر	توقيع الشفرة رقمياً كشف الجوانب الحية	الرقم 20 الرقم 21				
*LoA – يجب تطبيق عمليات التحكم هذه وفق ما تقتضي ضرورته عملية تقييم المخاطر.						

ملاحظـــة – في الجدول أعلاه، تقابل معرفات الهوية من الرقم 1 إلى الرقم 21 عمليات تحكم محددة لازمة لتوفير الحماية عند كل مستوى من مستويات الضمان. ويرد وصف كل من عمليات التحكم تلك بشكل مفصّل في الفقرة الفرعية 1.2.3.10.

1.2.3.10 عمليات التحكم بالتهديدات لاستخدام أوراق الاعتماد/الإثباتات في مرحلة الاستيقان

تقابل عمليات التحكم التالية لمواجهة التهديدات لاستخدام أوراق الاعتماد/الإثباتات أثناء مرحلة الاستيقان الأرقام المدرجة في الجدول 10-6.

MultiFactorAuthentication

الرقم 1. استخدام ورقتي اعتماد أو أكثر لتنفيذ عوامل الاستيقان المختلفة (مثلاً، شيء قمت بضمه لشيء آخر تعرفه).

StrongPassword

الرقم 2. إنفاذ استعمال كلمات السر القوية (مثلاً، سلسلة معقدة غير مرتبة بحسب القاموس تحتوي على مزيج من الأحرف الكبيرة والصغيرة الحجم والأرقام والأحرف الخاصة).

CredentialLockout

الرقم 3. استخدام آلية إغلاق أو إبطاء بعد عدد معين من محاولات فاشلة في استعمال كلمة السر.

DefaultAccountUse

الرقم 4. عدم استعمال أسماء وكلمات سر الحساب المبدئي (مثلاً، إعدادات خاصة بجهة التصنيع).

AuditAndAnalyze

الرقم 5. استخدام سلسلة سجل تدقيق لعمليات تسجيل فاشلة من أجل تحليل أنماط محاولات تخمين كلمات السر على الشبكة.

HashedPasswordWithSalt

الرقم 6. استخدام كلمات سر مظللة لردع هجمات القوة المفرطة وهجمات جداول قوس قزح.

Anticounterfeiting

الرقم 7. استخدام تدابير مكافحة التزوير (مثل الصور المجسمة الثلاثية الأبعاد والبطاقات الصغرية) على الأجهزة التي تحتفظ بأوراق الاعتماد.

DetectPhishingFromMessages

الرقم 8. تطبّق عمليات التحكم المصمّمة خصيصاً للكشف عن هجمات التصيد الاحتيالي (على سبيل المثال، مرشح بايز، والقائمة السوداء لبروتوكول الإنترنت، والمراشيح القائمة على موقع الموارد الموحد، والمراشيح الحدسية، وأنماط بصمات الأصابع).

AdoptAntiPhishingPractice

الرقم 8. استخدام ممارسات من قبيل صور التعطيل والوصلات التشعبية المعطلة من مصادر غير موثوقة، وتوفير تلميحات وإشارات مرئية في الرسائل الإلكترونية للزبون من أجل حماية الكيانات من هجمات التصيّد الاحتيالي.

MutualAuthentication

الرقم 9. اعتماد الاستيقان المتبادل.

NoTransmitPassword

الرقم 11. استخدام آليات الاستيقان التي لا ترسل كلمات السر على الشبكة (مثلاً بروتوكول كيربيروس).

EncryptedAuthentication

الرقم 12. حين يكون تبادل الاستيقان عبر الشبكة ضرورياً، يتم تجفير البيانات قبل عبورها.

DifferentAuthenticationParameter

الرقم 13. استخدام معلمة استيقان مختلفة لكل معاملة من معاملات الاستيقان (كلمة سر تُستخدم لمرة واحدة فقط، وأوراق اعتماد قائمة على الدورة).

Timestamp

الرقم 14. يتم وضع خاتم الوقت على كل رسالة باعتماد خاتم وقت غير قابل للتزوير.

PhysicalSecurity

الرقم 15. استخدام آليات الأمن المادي (أي الدليل على التلاعب والكشف والاستجابة).

EncryptedSession

الرقم 16. استخدام الدورات المجفرة.

FixProtocolVulnerabilities

الرقم 17. استخدام البرمجيات التصحيحية للمنصة لضبط مواطن ضعف البروتوكول (مثلاً بروتوكول الإنترنت TCP/IP).

CryptographicMutualHandshake

الرقم 18. استخدام إقامة اتصال متبادلة قائمة على التجفير (مثلاً، أمن طبقة النقل TLS).

CredentialActivation

الرقم 19. يتعين وجود سمة من سمات التفعيل من أجل استخدام أوراق الاعتماد (مثلاً، إدخال رقم تعريف الهوية الشخصي أو معلومات القياس الحيوي في تجهيزات تحتوي على أوراق الاعتماد).

CodeDigitalSignature

الرقم 20. يتم التحقق من التواقيع الرقمية باعتماد مصدر موثوق لمواجهة تنزيل البرمجيات التي تم تحويرها من قبل أطراف غير مرخصة.

LivenessDetection

الرقم 21. يتم استخدام تقنيات الكشف عن الجوانب الحية لتحديد هوية استخدام خصائص القياس الحيوي الاصطناعية (البصمات المزوّرة على سبيل المثال).

11 معايير ضمان الخدمة

يتعين على مشغلي إطار الثقة الساعين إلى الامتثال لهذا الإطار القيام بوضع معايير محددة تفي بشروط كل مستوى من مستويات الضمان التي ينوون دعمها، وعليهم تقييم موردي خدمة أوراق الاعتماد/الإثباتات الذين يدعون الامتثال للإطار إزاء تلك المعايير. وبالمثل، يحدد موردو خدمة أوراق الاعتماد/الإثباتات مستوى الضمان الذي تمتثل عنده خدماتهم لهذا الإطار عن طريق تقييم العمليات التجارية الكلية والآليات التقنية الخاصة بها إزاء معايير محددة.

الملحق ألف

مواصفات أوراق الاعتماد/الإثباتات

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية.)

أ) أوراق الاعتماد/الإثباتات هي عبارة عن معطيات.

لا تحتوي أوراق الاعتماد على أي مُستوعب مادي أو جهاز يختزن البيانات، كما لا تتضمن مولّداً للبيانات التي تؤلّف معاً أوراق الاعتماد. وعليه، فإن مولّد شفرة المرور لا يشكل على الإطلاق جزءاً من أوراق الاعتماد، وليس ببطاقة ذكية يمكنها توقيع المعطيات أو برمجيات تولّد التواقيع الرقمية أو ورقة يمكن كتابة أشياء عليها.

ب) يجب أن تشتمل أوراق الاعتماد على بيانات تشكل دليلاً على هوية و/أو استحقاقات.

ومن الأمثلة على هذا الدليل ما يلي:

1) شيء معروف (كلمة سر ثابتة)؛

2) أو خاصية قياس حيوي أو تمثيل لما يشبهها؛

3) أو بيانات تنتج عن شيء تملكه جهة (مثلاً شفرات مرور لمرة واحدة تنتج عن مولد لشفرة المرور، وبيانات موقعة رقمياً من قبل تجهيزات أو برمجيات تستخدم مفتاحاً خاصاً يُفترض أن يكون في حوزة كيانٍ ما).

ج) قد تكون أوراق الاعتماد مصحوبة ببيانات أخرى يمكن الاستفادة منها في عمليات الاستيقان والتعرف على الهوية، دون أن تشكّل جزءاً من أوراق الاعتماد الفعلية.

ومن الأمثلة على هذه البيانات اسم الكيان وشهادة المفتاح العام. ولا يكون أي من هذين ضرورياً كدليل يثبت هوية أو استحقاقات، علماً بأنه مفيد في بروتوكولات الاستيقان. وتجدر الإشارة إلى أن ربط اسم الكيان بأوراق الاعتماد يؤكد الهوية. أما ربط شهادة المفتاح العام بأوراق الاعتماد فيقدم معلومات تساعد في إخضاع الدليل للاختبار فضلاً عن إمكانية توفير معلومات عن هوية الكيان أو استحقاقاته.

د) قد تكون أوراق الاعتماد أيضاً أوراق اعتماد مشتقة.

وفي هذه الحالة يمكن أن تكون أوراق الاعتماد المشتقة هذه عبارة عن مجموعة من المعلومات المشتقة من مجموعة أوراق اعتماد يستحدثها كيان في العادة ويرسلها إلى جهة التحقق من أوراق الاعتماد لاستيقانها. وعلى سبيل المثال، ففي بعض أنواع الاستيقان المغفل، يحول الكيان أوراق الاعتماد التي أصدرها مورد خدمة أوراق الاعتماد إلى أوراق اعتماد مشتقة تستعمل في عملية الاستيقان.

هـ) ليس من الضروري إبقاء جميع البيانات التي تتضمن أوراق اعتماد سرية.

و) يمكن استعمال أوراق الاعتماد لأغراض استيقان الكيان أو تعريف هويته أو ترخيصه أو لهذه الأغراض الثلاثة معاً.

ز) يتعين التحقق من أوراق الاعتماد قبل قبولها كأوراق مُستيقن منها وجديرة بالثقة للغرض الخاص المتعلق بها (كالاستيقان وتعريف الهوية والترخيص).

ح) يجب أن تجتاز أوراق الاعتماد خطوات عدة قبل التحقق منها. ومن الأمثلة على تلك الخطوات ما يلي:

1) التدقيق في أن أوراق الاعتماد مستيقن منها للتأكد من أنها صادرة عن الجهة المصدِرة المزعومة لها؛

2) إثبات صلاحية وموثوقية أوراق الاعتماد (مثلاً، تحديد ما إذا كان هنالك صلة مباشرة مع جذر أو منشأ موثوق منبثق عن الجهة المصدِرة لأوراق الاعتماد؛

3) تأكيد الدقة الحسابية للعمليات الرياضية/التجفير.

ط) قد تكون أوراق الاعتماد مستيقناً منها وأصلية دون أن تكون ذات صلاحية في جميع السياقات (على سبيل المثال، قد تكون الإثباتات الموجودة في بطاقة ذكية، مثل رقاقة البطاقة الهاتفية المدفوعة مسبقاً، مستيقناً منها وأصلية علماً بأنها قد لا تكون صالحة إلا للمكالمات التي تُجرى باستخدام المرافق الخاصة بالجهة المصدِرة لها).

التذييل I

الخصوصية وحماية المعلومات المحددة لهوية الشخص

(لا يشكّل هذا الملحق جزءاً أساسياً من هذه التوصية.)

لا يتوقف مدى ملاءمة نهج استيقان مُعتمد من أجل استخدام معين على تقييم لفعالية الاستيقان فحسب، بل يعتمد أيضاً على المخاطر التي تعترض المنظمة المعنية ومدى تحمّلها للمخاطر. فسوء استخدام المعلومات المحددة لهوية الشخص والخاصة بالكيانات ، أو الافتقار إلى الحماية الكافية لها، يستتبع نشوء مخاطر ملحوظة على المنظمات تتراوح بين إلحاق الأذى بسمعتها والتعرض لمسؤوليتها القانونية. وبناء على ذلك، لا بد من القيام بدراسة متأنية لاستخدام المعلومات المحددة لهوية الشخص لأغراض الاستيقان وحماية تلك المعلومات. ويقدم هذا التذييل توجيهات إعلامية مفيدة تتصل ببعض اعتبارات الخصوصية التي يتعين أن تراعيها المنظمات عند البتّ في استخدام نهج استيقان معين وتطبيقه.

وعندما يكون الكيان شخصاً، تتضمّن غالبية نُهُج الاستيقان معالجة المعلومات المحددة لهوية الشخص أثناء عملية أو أكثر من العمليات التالية:

أ) أثناء عملية الانتساب وذلك عند جمع معلومات تتعلق بالكيان وتدقيقها والتحقق من هوية الكيان؛

ب) أثناء عملية إنشاء أوراق الاعتماد/الإثباتات لكيان ما وإصدارها وإدارتها؛

ج) أثناء استخدام أوراق الاعتماد من قبل كيان والتحقّق منها من جانب الأطراف المعوِّلة وجهات التحقق.

ومن الممكن إجراء عملية استيقان متينة والتمتع بخصوصية تتسم بالقوة. ويوجد الكثير من نهج الاستيقان القوية من ناحية التجفير التي تنطوي على تأثير سلبي محدود على الخصوصية (مثلاً أوراق اعتماد يتعذر تحديد هوية الكيان الخاص بها، وتواقيع جماعية). وتجدر الإشارة إضافةً إلى ذلك إلى أن تزايد قوة مستوى الضمان (مستوى الضمان الرابع مقابل مستوى الضمان الثاني على سبيل المثال) يمكنه، وليس من المحتـــّم بالضرورة، أن يؤثر بصورة سلبية على خصوصية فرد ما. فثمة أمور كثيرة تعتمد على نهج الاستيقان الذي تم اختياره وكيفية تنفيذه. ولدى وضع هذه القرارات، يتعين على كل منظمة أن تأخذ بعين الاعتبار ضرورة حماية المعلومات المحددة لهوية الشخص والخاصة بالكيانات، إضافةً إلى ضرورة حماية مواردها واعتبار الكيانات عرضة للمحاسبة في حالة القيام بأنشطة غير مرخصة.

وتتضمن غالبية نُهُج الاستيقان استخدام معرّفات مميزة للهوية للتمييز بصورة لا لبس فيها بين كيانٍ وكيانات محتملة أخرى في سياق عملية الاستيقان. ويُعد استخدام المعرّفات المميزة للهوية عادة ضرورياً أيضاً لأغراض متنوعة أخرى، من قبيل إدارة الحسابات والحفاظ على تسجيل تدقيق ملائم. أما الاهتمامات المرتبطة بالخصوصية والمتعلقة باستخدام المعرّفات المميزة للهوية فلا تتصل باستخدام معرّف مميز للهوية على هذا النحو، بل بإعادة استخدام المعرّف المميز للهوية نفسه في إطار إعدادات مختلفة كثيرة. فعلى سبيل المثال، يعتبر رقم الحساب المخصّص لغرض واحد عموماً أقل حساسية من مرجع إداري حكومي يُستخدم لأغراض متعددة (مثلاً، الضرائب والرعاية الصحية والتقاعد). وقد توجد في بعض الولايات القضائية أيضاً تشريعات تقيّد استخدام معرّفات هوية معيّنة.

في ضوء الاعتبارات السابقة، يتعين على المنظمات تنفيذ ضمانات فعالة لحماية المعلومات المحددة لهوية الشخص والخاصة بالكيانات في المراحل والعمليات الوارد وصفها في إطار ضمان استيقان الكيان هذا. ويتعين بوجه خاص تصميم نهج الاستيقان الذي تم اختياره وتنفيذه بطريقة تعمل بوجه عام على التقليل إلى الحد الأدنى من معالجة المعلومات المحددة لهوية الشخص. إضافة إلى ذلك، ينبغي أن يكون استخدام المعرّفات المميزة للهوية التي تُستُعمل أيضاً في سياقات وميادين أخرى مقتصراً على الحالات التي تستدعي ضرورة استعماله، وحيثما تجيزه قوانين الولاية (الولايات) القضائية ذات الصلة.

ويمكن العثور على توجيهين إضافيين صادرين عن منظمة التقييس الدولية/اللجنة الكهرتقنية (ISO/IEC) بشأن حماية المعلومات المحددة لهوية الشخص في مصدرين اثنين:

أ) التوجيه [b-ISO/IEC 29100] ويصف الشروط الأساسية للخصوصية من الناحية المتعلقة بالعوامل الرئيسية الثلاثة: (1) الشروط القانونية والتنظيمية لضمان خصوصية الفرد وحماية المعلومات المحددة لهوية الشخص والخاصة به، (2) والمتطلبات الخاصة بالعمل وحالات الاستخدام، (3) والأفضليات المتعلقة بالخصوصية الفردية للمعلومات المحددة لهوية الشخص والخاصة بالكيان. ويعرض التوجيه ISO/IEC 29100 المبادئ الأساسية التالية للخصوصية: الموافقة والاختيار، وتوصيف وتحديد الغرض، وتقييدات عملية الجمع، والاستخدام، وتقييدات الاحتفاظ والكشف، والتقليل من البيانات إلى الحد الأدنى، والدقة والجودة المتسمة بالانفتاح، والشفافية والإشعارات، والمشاركة الفردية والنفاذ، والمساءلة، وعمليات التحكم الأمنية، والامتثال. وإضافة إلى وجوب إجراء تقييم للمخاطر لتحليل التهديدات، يتعين على المنظمات إجراء تقييم لأثر نهج الاستيقان على الخصوصية من أجل تحديد مكونات أنظمتها التي تستدعي اهتماماً خاصاً من الناحية المتعلقة بتدابير حماية الخصوصية.

ب) التوجيه [b-ISO/IEC 29101] ويقدم إطاراً معمارياً لأنظمة تكنولوجيا الاتصالات والمعلومات التي تعالج المعلومات المحددة لهوية الشخص. ويعبر عن هذا الإطار في شكل اهتمامات وعدة آراء معمارية. وتتوفر فيه مجموعة من المكونات اللازمة لتنفيذ أنظمة تكنولوجيا الاتصالات والمعلومات التي تعالج المعلومات المحددة لهوية الشخص. والغرض من هذا الإطار هو بناء معماريات للأنظمة تتقيد بمبادئ الخصوصية التي تم التطرق إليها في التوجيه [b-ISO/IEC 29100].

وللحصول على توجيهات مُفصّلة بشأن الشروط والمبادئ وتصاميم الأنظمة فيما يتعلق بحماية المعلومات المحددة لهوية الشخص، يُطلب إلى القارئ الرجوع إلى المعايير الواردة أعلاه.

بيبليوغرافيا

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

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

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

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

[b-ITU-T Y.2722] التوصية ITU–T Y.2722 (2010)، *آليات إدارة الهوية في شبكات الجيل التالي*.

[b-ISO/IEC 9798] المعيار ISO/IEC 9798-1998، *تكنولوجيا المعلومات – تقنيات الأمن – استيقان الكيانات*.

[b-ISO/IEC 18014-2] المعيار ISO/IEC 18014-2: 2009، *تكنولوجيا المعلومات – تقنيات الأمن – خدمات خاتم التوقيت – الجزء 2: آليات توليد الأذنات المستقلة*.

[b-ISO/IEC 19790] المعيار ISO/IEC 19790: 2012، *تكنولوجيا المعلومات – تقنيات الأمن – متطلبات أمنية للوحدات التجفيرية*.

[b-ISO/IEC 19792] المعيار ISO/IEC 19792: 2009، *تكنولوجيا المعلومات – تقنيات الأمن – التقييم الأمني للقياس الحيوي*.

[b-ISO/IEC 27000] المعيار ISO/IEC 27000: 2012، *تكنولوجيا المعلومات – تقنيات الأمن – نظام رسمي لإدارة أمن المعلومات – لاستكشاف مجال استعراض ومفردات*.

[b-ISO/IEC 27001] المعيار ISO/IEC 27001: 2005، *تكنولوجيا المعلومات – تقنيات الأمن – نظام رسمي لإدارة أمن المعلومات – المتطلبات*.

[b-ISO/IEC 29100] المعيار ISO/IEC 29100: 2011، *تكنولوجيا المعلومات – تقنيات الأمن – إطار الخصوصية*.

[b-ISO/IEC 29101] المعيار ISO/IEC 29101، *تكنولوجيا المعلومات – تقنيات الأمن – إطار لمعمارية الخصوصية*.

[b-ISO/IEC 24760-1] المعيار ISO/IEC 24760-1: 2011، *تكنولوجيا المعلومات – تقنيات الأمن – إطار لإدارة الهوية – الجزء 1: المصطلحات والمفاهيم*.

[b-ISO/IEC 19790] المعيار ISO/IEC 19790: 2012، *تكنولوجيا المعلومات – تقنيات الأمن – متطلبات أمنية للوحدات التجفيرية*.

[b-INIST SP800-36] المنشور الخاص 800-36 للمعهد العالي للمعايير والتكنولوجيا (2003): *دليل اختيار منتجات أمن تكنولوجيا المعلومات*.
http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[b-INIST SP800-63] المنشور الخاص 800-63 للمعهد العالي للمعايير والتكنولوجيا (2006): *مبادئ توجيهية للاستيقان الإلكتروني.، الإصدار 2.0.1*.
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[b-AGGPKI] *Australian Government Gatekeeper Public Key Infrastructure*.
http://www.gatekeeper.gov.au/

[b-DuD] Van Alsenoy B., and De Cock, D. (2008), *'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', Datenschutz und Datensicherheit*, Vol.32, No.3, pp.178-183.

[b-EoI] New Zealand Standard: *Evidence of Identity Standard Version 2.0, 2009.* <http://www.dia.govt.nz/EOI/pdf/EOIv2.0.pdf>

[b-ENISA] ENISA, *Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0*.

[b-IAF] *Kantara Initiative Identity Assurance Framework v2.0*. http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework

[b-MOV] Menezes, A., van Oorschot, P., and Vanstone, S. (1997), *'Handbook of Applied Cryptography*', pp. 3-4. <http://www.cacr.math.uwaterloo.ca/hac/>

[b-NeAF] *The National e-Authentication Framework*. <http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>

[b-OECD] OECD (2007), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*. <http://www.oecd.org/dataoecd/32/45/38921342.pdf>

[b-OMB] OMB M-04-04 (2003), *e-Authentication Guidance for Federal Agencies* <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

[b-PEA] Industry Canada (2004), *Principles for Electronic Authentication: A Canadian Framework*. <http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html

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