الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1254
(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

إطار ضمان استيقان الكيان

التوصية ITU-T X.1254

الاتحاد الدولي للاتصالات

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
الدليل	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 (1)	
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 (1)	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 (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
أمن شبكات الجيل الخامس	X.1819–X.1800

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

التوصية ITU-T X.1254

إطار ضمان استيقان الكيان

ملخص

توصف التوصية ITU-T X.1254 ثلاثة مستويات لضمان استيقان الكيان (AAL) والمعايير والتهديدات الخاصة بكل مستوى.

بالإضافة إلى ذلك فهي تعمل على:

- تحدد إطار لإدارة مستويات ضمان استيقان الكيان؛
- توفر التوجيهات فيما يتعلق بتكنولوجيات التحكم التي يتعين استخدامها للتخفيف من حدة التهديدات للاستيقان، استناداً إلى تقييم المخاطر؛
- توفر التوجيهات بشأن تنفيذ التقابل بين مستويات ضمان استيقان الكيان الثلاثة ومخططات ضمان الاستيقان الأخرى؛
- توفر التوجيهات بشأن تبادل نتائج الاستيقان التي تستند إلى مستويات ضمان استيقان الكيان الثلاثة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1254	2012-09-07	17	11.1002/1000/11608
2.0	ITU-T X.1254	2020-09-03	17	11.1002/1000/14260

مصطلحات أساسية

مستوى ضمان الاستيقان (AAL)، ضمان، استيقان، مستوى ضمان الاستيقان، إدارة الهوية (IdM)، مستوى الضمان (LOA).

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

الهوية الرقمية هي التمثيل الوحيد لكيان يشارك في إجراء معاملة عبر الإنترنت. والضمان – أو الثقة – بأن الهوية الرقمية التي يتم التفاعل معها متسقة مع الهوية المدعاة هو في صميم الثقة والأمان ومراقبة النفاذ عبر الإنترنت. ويتم تعريف ثلاثة أنواع من الضمان للمساهمة في إرساء الثقة في الهوية الرقمية، وهي: ضمان الهوية، وضمان الاستيقان، وضمان الاتحاد.

توفر هذه التوصية إطاراً لضمان الاستيقان. ولأغراض هذه التوصية، فإن الاستيقان هو العملية التي يتم فيها التحقق من الهوية المدعاة بهدف إجراء معاملة عبر الإنترنت. وبالنسبة للخدمات التي تطبق فيها زيارات متكررة، يوفر الاستيقان الناجح تأكيدات معقولة قائمة على المخاطر تفيد بأن المستعمل الذي ينفذ اليوم إلى الخدمة هو نفسه الذي نفذ إليها سابقاً.

يزود الإطار المحدد في هذه التوصية مقدمي الخدمات عبر الإنترنت – الأطراف المعولة (RP) ومقدمو خدمات أوراق الاعتماد (CSP) – بنهج منتظم لفهم المخاطر المتعلقة بهم وتحديد الضوابط التي تساعد في التخفيف من حدتها. وهو مصمم لتسهيل الاختيار المنهجي للضوابط واستراتيجيات التخفيف من حدة المخاطر باستخدام عملية من ثلاث خطوات:

1 تحديد الأدوار والخدمات اللازمة لتعيين فئات التهديدات؛

2 تطبيق عملية محددة الهدف لإدارة المخاطر من أجل تحديد قوة الضوابط المطلوبة؛

3 وتحديد التكنولوجيات – البروتوكولات وأنواع أوراق الاعتماد وما إلى ذلك – المستخدمة في زيادة تنقيح الضوابط.

نموذج قائم على التهديدات

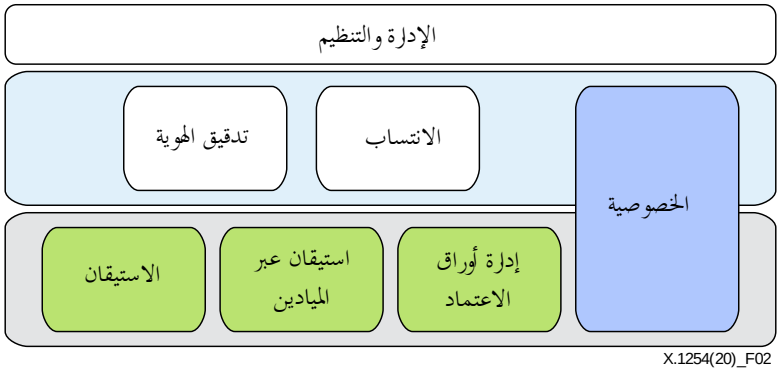
هذه التوصية مصممة لتسهيل الاختيار المنهجي للضوابط والاستراتيجيات القائمة على المخاطر. وإحدى الخطوات الأولية للتمكن من اختيار الضوابط المناسبة واستراتيجيات التخفيف تتمثل في تحديد أنواع المخاطر والتهديدات المرتبطة بدور (أدوار) وخدمات أي من موردي الخدمات عبر الإنترنت. انظر الشكل 0-1.

الشكل 0-1 – الخدمات والمخاطر والضوابط

وقد نُظّم هذا الإطار على أساس فئات المخاطر والتهديدات، ما يزود مقدمي الخدمات عبر الإنترنت برابطة وظيفية بين عمليات تقييم المخاطر وأنشطة التحكم بالمخاطر والتخفيف من حدتها.

وقد يوفر مقدمو خدمات الهوية جميع المكونات الوظيفية لمراحل الهوية الرقمية هذه، أو بعض هذه المكونات أو واحدة منها فقط. وبناءً على ذلك، قد يكون من المناسب إجراء تقدير المخاطر ومعالجة الضوابط ونُهُج التخفيف من حدة المخاطر على أساس نهج مجزأ إلى عدة مكونات مماثل للنهج المتبع في دورة حياة المعاملة الرقمية. وتتناول هذه التوصية المخاطر والضوابط المتعلقة بمراحل إدارة واستيقان أوراق الاعتماد في دورة الحياة هذه. وهناك وثائق أخرى (مثلاً التوصية [ISO/IEC TS 29003]) تتناول المخاطر والضوابط المتعلقة بأنشطة الانتساب وتدقيق الهوية، والضوابط التنظيمية والإدارية. ومن المرتقب أن تكون هذه الوثائق، وغيرها، متوائمة من أجل تمثيل مجموعة منسقة من المعايير الأساسية لإدارة الهوية (كما هو مبين في الشكل 0-2) التي توفر، عند استعمالها معاً، العمليات والمخاطر والضوابط من أجل دورة حياة معاملة الهوية الرقمية.

وتقدم هذه التوصية أيضاً فهرساً بالتهديدات المتعلقة بالخصوصية، وبالاعتبارات وضوابط التخفيف الخاصة بمجال تطبيقها (استيقان وإدارة أوراق الاعتماد). ولا تشمل الاعتبارات المتعلقة بالخصوصية فيما يتعلق بتدقيق الهوية أو الانتساب.



الشكل 0-2 – مجموعة منسقة من المعايير الأساسية لإدارة الهوية

علاقة هذه التوصية بصيغتها السابقة

قدم الإصدار الأول من هذه التوصية [b-ITU-T X.1254 (2012)] دورة حياة معاملات الهوية الرقمية خلال ثلاث مراحل: الانتساب وتدقيق الهوية، وإدارة أوراق الاعتماد، واستيقان الكيان. ومنذ عام 2012 تطورت الصناعة وظهرت مفاهيم ونُهُج جديدة، من قبيل الاستيقان من دون كلمة سرّ والاستيقان المعزّز. وبناء على ذلك، انتقلت الصناعة من مفهوم مستوى الضمان (LOA) باعتباره ترتيباً فريداً يحدد متطلبات خاصة بالتنفيذ. وبدلاً من ذلك، وبالجمع بين إدارة مناسبة للأعمال والمخاطر ذات الصلة بالخصوصية جنباً إلى جنب مع احتياجات المهمة، يختار المنفّذون مستويات ضمان الهوية (IAL) ومستويات ضمان الاستيقان (AAL) ومستويات ضمان الاتحاد (FAL) بوصفها خيارات متميزة. وتركز هذه التوصية على مستويات ضمان الاستيقان. أما مستويات ضمان الهوية ومستويات ضمان الاتحاد فتقع خارج نطاق هذه التوصية.

التوصية ITU-T X.1254

إطار ضمان استيقان الكيان

1 مجال التطبيق

توفر هذه التوصية إطاراً لإدارة ضمان استيقان الكيان (EAA) ضمن سياق معيّن. وهي تعمل بوجهٍ خاص على:

- تحديد ثلاثة مستويات لضمان استيقان الكيان (AAL)؛
- تقديم مبادئ توجيهية لفهم المستويات AAL هذه؛
- تحديد المعايير والمبادئ التوجيهية لتحقيق مستويات محددة لضمان استيقان الكيان؛
- توفير التوجيهات لمقارنة وتنفيذ التقابل عبر خطط ضمان الاستيقان؛
- توفير التوجيهات لتبادل نتائج الاستيقان التي تستند إلى مستويات ضمان محددة؛
- تقديم التوجيهات فيما يتعلق بالضوابط التي يتعين استخدامها للتخفيف من حدة التهديدات المتعلقة بالاستيقان، استناداً إلى تقييم المخاطر.

2 المراجع

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

ملاحظة – من المتفق عليه عموماً أن مصطلحي "ادعاء" و"زعم" 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) [ISO/IEC 18014-2]: تقديم ضمان يؤكد الهوية المدعاة من كيان ما.

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

ملاحظة – 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 يعرفه الكيان (مثلاً كلمة سرّ، رقم تعريف الهوية الشخصي (PIN))؛
- صفة ينفرد بها الكيان (مثلاً خاصية من خصائص القياس الحيوي)؛
- شيء يفعله الكيان في المعتاد (مثلاً نمط سلوكي).

4.1.3 بروتوكول الاستيقان (authentication protocol) [b-ISO/IEC 29115]: تتابع محدد من الرسائل بين كيان وجهة من جهات التحقق يمكّن جهة التحقق من أجراء استيقان الكيان.

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

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

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

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

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

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

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

9.1.3 هوية (Identity) [ISO/IEC 24760-1]: مجموعة من النعوت المتصلة بكيان ما.

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

10.1.3 التحقّق من معلومات الهوية (identity information verification) [b-ISO/IEC 29115]: عملية التأكد من معلومات الهوية والإثباتات مقابل الجهات المصدِرة لها أو مصادر البيانات أو أي من الموارد الخارجية أو الداخلية الأخرى فيما يتعلق بالاستيقان والصلاحية والصحة وإسنادها إلى الكيان.

11.1.3 تدقيق الهوية (identity proofing) [b-ISO/IEC 29115]: العملية التي تقوم هيئة التسجيل (RA) بموجبها بالحصول على معلومات كافية والتحقق منها لتعريف هوية كيان ما وفقاً لمستوى ضمان محدد أو مفهوم.

12.1.3 هجوم لمتطفل بين طرفين (man-in-the-middle attack) [b-ISO/IEC 29115]: الهجوم الذي يكون فيه المهاجم قادراً على قراءة الرسائل وإقحامها وتعديلها بين طرفين دون علم منهما.

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

14.1.3 استيقان متبادل (mutual authentication) [b-ISO/IEC 29115]: استيقان من هويات الكيانات يستيقن فيها كيانان من بعضهما البعض بحيث يتأكد كل منهما من هوية الآخر.

15.1.3 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.

16.1.3 تصيّد احتيالي (phishing) [b-ISO/IEC 29115]: احتيال ينخدع به مستعمل البريد الإلكتروني للكشف عن معلومات شخصية أو سرية بحيث يستطيع المحتال استخدامها بصورة غير شرعية.

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

18.1.3 تقييم المخاطر (risk assessment) [ISO/IEC 27000]: العملية الكاملة لتحديد المخاطر وتحليلها وتقييمها.

19.1.3 سرّ مشترك (shared secret) [ITU-T X.29115]: سر يُستخدم في عملية الاستيقان يكون معلوماً فقط لدى الكيان وجهة التحقّق.

20.1.3 معاملة (transaction) [ITU-T X. 29115]: عملية محددة تتم بين الكيان ومورد الخدمة تقوم بدعم غرض تجاري أو برنامجي.

21.1.3 تحقّق (verification) [ITU-T X. 29115]: عملية تدقيق في معلومات بمقارنة المعلومات المقدمة بمعلومات تم تأكيدها في السابق.

22.1.3 جهة التحقق (verifier) [ITU-T X. 29115]: جهة فاعلة تؤكد صحة معلومات الهوية.

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

2.3 مصطلحات معرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 مقدم خدمة أوراق الاعتماد/الإثباتات (credential service provider) (CSP): جهة فاعلة موثوقة تُصدر أوراق الاعتماد أو تديرها.

ملاحظة – يستند هذا التعريف إلى التعريف الوارد في المعيار [b-ISO/IEC 29115].

2.2.3 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.

ملاحظة 1 – تقوم الثقة على أساس درجة الثقة في الربط بين الكيان والهوية المقدّمة.

ملاحظة 2 – يستند هذا التعريف إلى تعريف "ضمان الاستيقان" الوارد في التوصية [ITU-T X.1252]

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

ملاحظة – يستند هذا التعريف إلى التعريف الوارد في التوصية [b-ITU-T X.1252].

4.2.3 هيئة التسجيل (registration authority) (RA): جهة فاعلة موثوقة تحدد هوية الكيان أمام مقدّم خدمة أوراق الاعتماد/الإثباتات و/أو تكفل صحتها.

ملاحظة – يستند هذا التعريف إلى التعريف الوارد في المعيار [b-ISO/IEC 29115].

5.2.3 الطرف المعوّل (relying party) (RP): جهة فاعلة تعتمد على هوية مزعومة أو مدّعاة.

ملاحظة – يستند هذا التعريف إلى التعريف الوارد في المعيار [b-ISO/IEC 29115].

4 المختصرات

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

AAL مستوى ضمان الاستيقان *(Authentication Assurance Level)*

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

EAA ضمان استيقان الكيان (*Entity Authentication Assurance*)

FAL مستوى ضمان الاتحاد *(Federation Assurance level)*

FIDO الهوية الرقمية السريعة *(Fast Identity On-line)*

HTML لغة وسم النصوص الترابطية *(Hypertext Markup Language)*

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

HTTPS أمن بروتوكول نقل النصوص الترابطية *(Hypertext Transfer Protocol Secure)*

IAL مستوى ضمان الهوية *(Identity Assurance Level)*

IdM إدارة الهوية (*Identity Management*)

IDP مورد الهوية *(Identity Provider)*

LoA مستوى الضمان (*Level of Assurance*)

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

MITM متطفل بين طرفين *(Man-In-the-Middle)*

MITB متطفل في متصفّح الويب *(Man-In-the-Browser)*

OAuth الاستيقان المفتوح *(Open Authentication)*

OpenID الهوية المفتوحة *(Open Identity)*

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

PIA تقييم أثر الخصوصية *(Privacy Impact Assessment)*

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*)

TLS أمن طبقة النقل (*transport layer security*)

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 لـ" تشير إلى الإمكانية أو المقدرة على أمر ما.

6 سير عملية الاستيقان الرقمي

1.6 معلومات عامة

الهوية الرقمية هي التمثيل الوحيد لكيان يشارك في إجراء معاملة عبر الإنترنت. ويتضمن الاستيقان الرقمي، في أبسط أشكاله، التحقق بدرجة معينة من الثقة من الهوية المدّعاة لكيان بهدف منحه حق النفاذ إلى خدمة عبر الإنترنت. ويحاول الكيان المسجّل الاستيقان من خدمة عبر الإنترنت بإثبات حيازته على مستيقن، يعرف أيضاً باسم أوراق الاعتماد، تم إصداره في وقت التسجيل. بعد ذلك تقوم الخدمة عبر الإنترنت – وتعرف أيضاً في المعاملة باسم الطرف المعوّل (RP) – بمحاولة للتحقق من صحة المستيقن بواسطة مقدم خدمة الهوية أو مقدم خدمة أوراق الاعتماد أو جهة التحقق. وبعد أن يتحقق مقدم خدمة أوراق الاعتماد أو جهة التحقق من أوراق الاعتماد يمنح الكيان حق النفاذ إلى الخدمة عبر الإنترنت.

ويوضح الشكل 6-1 سير عملية الاستيقان الرقمي التالية:

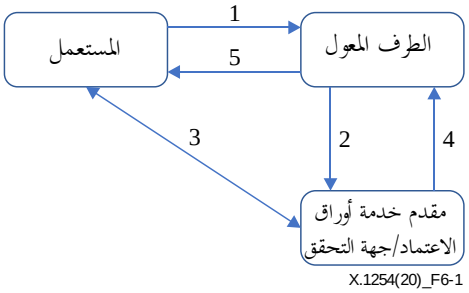
1 يقوم الكيان بالنفاذ إلى خدمة عبر الإنترنت تابعة للطرف المعوّل؛

2 يحيل الطرف المعوّل الكيان إلى مقدم خدمة أوراق الاعتماد لأغراض الاستيقان؛

3 يتحقق مقدم خدمة أوراق الاعتماد من امتلاك الكيان للمستيقن أو المستيقنات المسجلة؛

4 يرسل مقدم خدمة أوراق الاعتماد تأكيد الاستيقان إلى الطرف المعوّل للتأكد من حالة استيقان الكيان؛

5 وتقام دورة مستيقن منها بين الكيان والطرف المعوّل.



الشكل 6-1 – سير عملية الاستيقان الرقمي

يوفر توضيح سير عملية الاستيقان الرقمي بهذه الطريقة منهجية لفهم المخاطر المرتبطة بمختلف الأدوار والوظائف المتضمنة في عملية الاستيقان الرقمي.

وبالرغم من إمكانية امتلاك الطرف المعوّل حلاً خاصاً به لإدارة الهوية (IdM) وأنه يتصرف مثل مقدم خدمة أوراق الاعتماد الخاص به، فإن هذه التوصية تقدم الطرف المعول ومقدم خدمة أوراق الاعتماد على أنهما يقومان بأدوار متمايزة. ومع ذلك، فإن وظائف كل دور هي نفسها في الحالتين.

بالإضافة إلى ذلك، يجمع الشكل 6-1 أدوار مقدم خدمة أوراق الاعتماد إلى أدوار جهة التحقق. وبالرغم من أن مقدمي خدمة أوراق الاعتماد يقومون عادة بوظيفة التحقق، إلا أنه يمكن في بعض الحالات لمقدم خدمة أوراق الاعتماد أن يستخدم جهة تحقق قائمة بذاتها.

ويفترض سير عملية الاستيقان الرقمي الوارد وصفها هنا أن انتساب الكيانات لمقدم خدمة أوراق الاعتماد قد تم بالفعل وأنها تملك واحداً أو أكثر من المستيقنات المسجلة. ولا تندرج عمليات الانتساب والتسجيل ضمن نطاق هذه التوصية.

2.6 ضمان الهوية الرقمية

من الضروري فهم الكيفية التي تتفاعل بها الخدمات التي تتصدى لمراحل دورة حياة الهوية الرقمية ومكوناتها الوظيفية لدعم الثقة والأمان العام في معاملة عبر الإنترنت. ويعبر عن هذه الثقة عادة بأنها مستوى الأمان عبر درجات أو مستويات الضمان. وتقدم هذه التوصية المتطلبات والتوجيهات اللازمة لمرحلة ضمان استيقان الهوية الرقمية ووظائف مكونات الهوية الرقمية الكاملة وإطار ضمان الاستيقان. ويبين الشكل 6-2 المكونات ووصف الضمان والأنشطة الوظيفية المتعلقة بمجموعة من الوثائق الأساسية المتوائمة لإدارة الهوية التي تتناول الضمان والضوابط في هذا الإطار الكامل للهوية الرقمية.

مكونات الضمان	المواصفات	الأنشطة
IA *ضمان الهوية*	متانة عملية تدقيق الهوية والربط بين المستيقن والشخص الذي تم التدقيق في هويته	• تدقيق الهوية • الوضوح • إقرار الصلاحية • التدقيق • الانتساب • الربط
AA *ضمان الاستيقان*	الثقة بأن مدعي معين هو نفسه المشترك الذي تم الاستيقان منه سابقًا	• الاستيقان • إدارة أوراق الاعتماد • إصدار أوراق الاعتماد • تعليق أوراق الاعتماد و/أو إبطالها و/أو إتلافها • تجديد أوراق الاعتماد و/أو استبدالها
FA *ضمان الاتحاد*	يجمع بين جوانب نموذج الاتحاد، وقوة حماية التأكيد، وعرض التأكيد	• إدارة المفاتيح • قرارات وقت التنفيذ • إدارة النعوت

X.1254(20)_F6-2

الشكل 6-2 – مستويات ضمان الهوية الرقمية

ضمان الهوية (Identity assurance): يشمل هذا الضمان العمليات التي وضعت للتحقق من ارتباط الشخص بهويته في العالم الحقيقي. وتتناول التوصية [ISO/IEC TS 29003] ضمان الهوية.

ضمان الاستيقان (Authentication assurance): ينص الاستيقان على أن الشخص الذي يسعى للنفاذ إلى خدمة رقمية يتحكم بالتكنولوجيات المستخدمة للاستيقان. يشمل هذا الضمان العمليات المستخدمة للتحقق من أن الهوية المدعاة هي نفسها التي شاركت في عملية التسجيل وأن النظام قد استيقن منها سابقاً.

ضمان الاتحاد (Federation assurance): يشمل هذا الضمان العملية (العمليات) المستخدمة لإبلاغ تأكيدات الهوية التي يجري توفيرها من خلال ميادين أمنية مختلفة، وحمايتها والتحقق من صلاحيتها. واتحاد الهوية هو تقاسم معلومات الهوية والاستيقان عبر الإنترنت بين طرفين أو أكثر.

ولا تندرج مكونات وأنشطة ضمان الهوية التي تدعم ضمان الاتحاد ضمن نطاق مراجعة هذه التوصية.

3.6 الأدوار

1.3.6 معلومات عامة

يساعد سير عمليات الاستيقان الرقمي، بوصفه نموذجاً متمحوراً حول المخاطر، في تحديد فئات التهديدات المرتبطة بثلاثة أدوار رئيسية: مقدمو خدمات أوراق الاعتماد (CSP)، والأطراف المعوّلة (RP)، والكيانات.

2.3.6 مقدمو الخدمات عبر الإنترنت

مقدمو الخدمات عبر الإنترنت هم عبارة عن مؤسسات تقدم خدمات وتطبيقات ومعلومات عبر الإنترنت تتطلب نفاذاً مقيّداً، من قبيل الخدمات المصرفية وخدمات مقدمي الرعاية الصحية وتجار التجزئة. وتبعاً لكيفية تنفيذ الخدمة، يمكن أن يؤدي مقدمو الخدمات عبر الإنترنت دوراً أو اثنين من الأدوار التالية:

- مقدم خدمة أوراق الاعتماد
- مقدم خدمة الهوية

- جهة التحقق
- الطرف المعوّل.

3.3.6 مقدم خدمة أوراق الإعتماد/الإثباتات (CSP)

يضطلع مقدمو خدمة أوراق الاعتماد بمسؤولية التحقق من أوراق الاعتماد (أي المستيقن) التي قدمها الكيان. وتتحدد العملية، ودرجة الصرامة، التي يفعلون ذلك بواسطتها بمستوى المخاطر المرتبطة بالمعاملة عبر الإنترنت وبالبيئة التي ستستعمل فيها الهوية. ويمكن أن يؤدي وظيفة مقدم خدمة أوراق الاعتماد إما نظام داخلي لإدارة الهوية لدى مقدم الخدمة عبر الإنترنت أو خدمة الهوية التي يقدمها طرف ثالث. بالإضافة إلى ذلك، كثيراً ما يكون دور مقدم خدمة أوراق الاعتماد مسؤولاً عن أنشطة إدارة أوراق الاعتماد.

4.3.6 مقدم خدمة الهوية (IDP)

يضطلع مقدمو خدمة الهوية بمسؤولية تدقيق الهوية المدعاة لكيان ما والتأكد من أن هذه الهوية المدعاة مرتبطة بأوراق الاعتماد التي يستخدمها الكيان. وتتحدد العملية، ودرجة الصرامة، التي يفعلون ذلك بواسطتها بمستوى المخاطر المرتبطة بالمعاملة عبر الإنترنت وبالبيئة التي ستستعمل فيها الهوية. وقد يكون مقدم خدمة الهوية أيضاً مسؤولاً عن تسجيل الكيانات في برامج وخدمات محددة وانتسابها إليها. ولا تندرج المخاطر والضوابط التي تتناول وظائف مكونات مقدم خدمة الهوية هذه ضمن نطاق هذه التوصية.

بالإضافة إلى ذلك، قد يؤدي مقدم خدمة الهوية دور مقدم خدمة أوراق الاعتماد. وبما أن تركيز هذه التوصية ينصب على الاستيقان وإدارة أوراق الاعتماد، فعند استعمال مصطلح مقدم خدمة أوراق الاعتماد، يقصد به أيضاً تمثيل مقدم خدمة الهوية الذي يؤدي هذا الدور في المعاملة.

5.3.6 جهة التحقق

تكون جهات التحقق مسؤولة عن تأكيد هوية الكيان بالتحقق من امتلاك الكيان لمستيقن أو مستيقنات والتحكم بها باستخدام أحد بروتوكولات الاستيقان. ولتحقيق ذلك، قد يتعين أيضاً على جهة التحقق التثبت من صلاحية أوراق الاعتماد التي تربط المستيقن (المستيقنات) بمعرّف هوية الكيان والتحقق من حالتها. وكثيراً ما يؤدي دور جهة التحقق مقدم خدمة أوراق الاعتماد أو مقدم خدمة الهوية الذي يقدم خدمات أوراق الاعتماد.

6.3.6 الطرف المعوّل (RP)

تقبل الأطراف المعوّلة (أو تعتمد على) وتستعمل تأكيدات حالة استيقان الكيان من الخدمات الخاصة بها لإدارة الهوية أو من مقدمين خارجيين لخدمات أوراق الاعتماد. ويجب أن تتمكن الأطراف المعوّلة من الثقة في معلومات الهوية التي تردها من هذه الخدمات من أجل اتخاذ قرارات قائمة على المخاطر بشأن ما إذا كانت تسمح لكيانات محددة بالنفاذ إلى خدماتها ومنتجاتها الخاصة عبر الإنترنت.

7.3.6 الكيانات

لأغراض هذه التوصية، الكيانات هي عبارة عن مستعملي الخدمات التي يوفرها مقدمو الخدمات عبر الإنترنت.

وتكون الكيانات مسؤولة عن حماية هوياتها وأوراق الاعتماد الرقمية الخاصة بها من الاحتيال وإساءة الاستعمال، وعن استعمال أوراق الاعتماد الخاصة بها بالطريقة التي وضعت من أجلها.

4.6 مكونات عمليات الاستيقان

تزود هذه التوصية مقدمي الخدمات بمنهجية لتحديد التهديدات والمخاطر المرتبطة بالخدمات التي يقدمونها، وذلك استناداً إلى دورهم (أدوارهم) – كما هو محدد في الفقرة 3.6 – والتكنولوجيات التمكينية.

ولتيسير تقدير المخاطر والتهديدات المحددة المرتبطة بخدمة عبر الإنترنت، من المهم تحديد الوظائف والتكنولوجيات الداعمة المشاركة في عملية الاستيقان.

وتشمل مكونات العملية ما يلي:

- المستيقنات، مثل الأسرار المحفوظة عن غيب (مثل كلمات السرّ)، والأجهزة التي تنتج كلمة سرّ تستعمل لمرة واحدة (OTP)، والبطاقات الذكية، والشهادات الرقمية، والقياسات الحيوية (مثل البصمات).
- برمجيات مخدمات العملاء.
- بروتوكولات الاتصالات والاستيقان، مثل لغة وسم النصوص الترابطية (HTML)، ولغة وسم تأكيد الأمن (SAML)، وأمن طبقة النقل (TLS)، والاستيقان المفتوح (OAuth)، والهوية المفتوحة (Open ID).

وتتعرض معاملات الاستيقان لهجمات اختراق المعاملات، التي تستهدف مواطن الضعف المرتبطة بمكون واحد أو أكثر من المكونات المذكورة في الفقرة السابقة. وترتبط بمعظم تكنولوجيات الاستيقان، بما في ذلك المعدات والبرمجيات وبروتوكولات الاتصالات، تهديدات ومواطن ضعف محددة. وكجزء من أنشطتهم لتقدير المخاطر، يجب على مقدمي الخدمات عبر الإنترنت أن يأخذوا في الاعتبار مواطن الضعف المرتبطة بكل مكون من المكونات. ويرد في الفقرة 8 وصف لفئات محددة من التهديدات والمخاطر والضوابط.

1.4.6 المستيقنات

المستيقن هو شيء يملكه الكيان ويتحكم به يستخدم لاستيقان هوية الكيان. وقد يكون للكيان أكثر من مستيقن واحد مرتبط به. وتشمل **عوامل** الاستيقان *شيئاً تعرفه*، مثل كلمة السرّ؛ و*شيئاً تملكه*، مثل بطاقة ذكية؛ و*شيئاً تنفرد به*، مثل القياس الحيوي. وتزداد قوة معاملة الاستيقان باستخدام واحد أو أكثر من العوامل المختلفة.

ويجب على مقدم الخدمات عبر الإنترنت أن يأخذ في الاعتبار مواصفات مخاطر الخدمة عند اختيار المستيقنات التي يمكن قبولها لاستيقان هذه الخدمة. بالإضافة إلى ذلك، يجب على الطرف المعوّل أن يأخذ في الاعتبار متطلبات ضمان الخدمة الخاصة به قبل قبول الخدمات من مقدم خدمة أوراق الاعتماد.

وتشمل أنواع المستيقنات ما يلي:

- الأسرار المحفوظة عن غيب
- أسرار مسترجعة
- أجهزة خارج النطاق
- أجهزة إنتاج كلمة سرّ لمرة واحدة (OTP) بعامل وحيد
- أجهزة إنتاج كلمة سرّ لمرة واحدة متعددة العوامل
- برمجيات تجفير بعامل وحيد
- أجهزة تجفير بعامل وحيد
- برمجيات تجفير متعددة العوامل
- أجهزة تجفير متعددة العوامل.

2.4.6 المستيقن

جسم أو هيكل بيانات يربط الهوية – عبر معرّف أو معرفات الهوية – والنعوت الإضافية (بصورة اختيارية) بمستيقن واحد على الأقل يملكه ويتحكم به المشترك. ومع أن الاستخدام المشترك يفترض غالباً أن الكيان يحافظ على المستيقن، فإن هذه التوصية تستخدم المصطلح أيضاً للإشارة إلى سجلات إلكترونية يحتفظ بها مقدم خدمة أوراق الاعتماد وتربط بين مستيقن (مستيقنات)

المشترك والهوية. والشكل الأكثر شيوعاً للمستيقن هو اسم المستعمل وسجل المستعمل المصاحب له الذي يرتبط بكلمة سرّ أو بمستيقن آخر.

7 تطبيق إدارة المخاطر على إطار ضمان الاستيقان

1.7 معلومات عامة

يعتمد النظام الفاعل لإدارة الهوية على فهم مستويات المخاطر المرتبطة بأنواع الخدمات عبر الإنترنت التي تقدمها المؤسسة. ولفهم هذه المخاطر، يجب على مقدمي الخدمات عبر الإنترنت أن يراعوا دورهم أو أدوارهم المحددة ضمن الإطار، وطبيعة مستخدمي هذه الخدمات، وأنواع البيانات والمعاملات التي تعالجها تطبيقاتهم.

ينتج عن تطبيق منهجية منظمة لإدارة المخاطر ما يلي: تعريف المخاطر والتهديدات؛ والقرارات بشأن الطريقة التي ينبغي معالجتها بها؛ والمدخلات اللازمة لاختيار وتنفيذ الضوابط. وفي مجال إدارة الهوية، توجد توجيهات محددة لمساعدة المؤسسات على فهم كيفية معادلة مستويات المخاطر هذه لمستويات الضمان؛ أي للمدى النسبي للثقة في سلامة الهويات على الإنترنت.

ويتعين على مقدمي الخدمات عبر الإنترنت استخدام منهجية لإدارة المخاطر ووضع خطة لإدارة المخاطر الرقمية المتعلقة بالاستيقان.

ويتعين على مجال تطبيق تقدير المخاطر المرتبطة بالهوية الرقمية أن يأخذ في الاعتبار، بالحد الأدنى، نوع ومستوى الأثر المرتبط بكل واحد من المخاطر المحددة. كما يمكن النظر في احتمال وقوع أي خطر من المخاطر.

2.7 مخاطر الاستيقان

عند النظر في مخاطر الاستيقان، يكون السؤال الأساسي "ما هي التحديات التي تنطوي عليها؟" في حالة فشل الاستيقان، أي ما هو الأثر إذا أعطيت إمكانية النفاذ إلى كيان ليس المالك الشرعي لأوراق الاعتماد والحساب المرتبط بها؟

ويتعين أن ينظر مقدمو الخدمات عبر الإنترنت فيما يلي عند تقدير المخاطر المرتبطة بفشل الاستيقان:

- البيانات – يعتبر تحديد أنواع البيانات التي تتم معالجتها وحمايتها ضمن حدود النظام عنصراً أساسياً في تحديد "التحديات التي ينطوي عليها ذلك". وتشمل أنواع البيانات المعلومات المحددة لهوية الشخص (PII)، والمعلومات المالية، ومعلومات الملكية، المتاحة للجمهور والشديدة الحساسية.
- المستعملون – يعتبر تعريف هوية مستعملي نظام معين أو مؤسسة وفهمهم أساسياً للتمكن من تعريف وتصنيف مخاطر محددة. وتشمل الفئات المستعملين الداخليين والخارجيين والمميزين. وينبغي أن تنظر المؤسسات في ما إذا مان المستعملون التابعون لها ملزمين باتفاقات تعاقدية أو قانونية أو بأنواع أخرى من الاتفاقات.
- الدوافع للهجمات – بتعريف المؤسسة أولاً لمستعمليها وأنواع البيانات الخاصة بها، تصبح في موقع أفضل لفهم الدوافع وراء الهجمات، مثلاً، إذا كان النظام يعالج معلومات الحسابات المصرفية ويوفر حمايتها، فقد يكون المهاجم مدفوعاً للنفاذ إلى النظام بطريقة احتيالية بهدف الكسب المالي.

ويتعين على مقدمي الخدمات عبر الإنترنت أن يختاروا الضوابط، وغيرها من خيارات التخفيف من حدة التهديدات، استناداً إلى المخاطر المقدرة.

8 فئات التهديدات، المخاطر والضوابط

تقدم هذه الفقرة فهرساً بالتهديدات والمخاطر منظماً حول فئات التهديات. وينبغي أن يعرّف مقدمو خدمات الهوية فئات التهديدات المحددة التي يتعرضون لها، استناداً إلى دورهم (أدوارهم) وخدمتهم (خدماتهم) المتعلقة بالاستيقان. وتجمع الضوابط بحسب فئات التهديدات التالية:

- اختراق الاستيقان

- اختراق المعاملات
- انتحال هوية مقدم خدمة أوراق الاعتماد
- انتحال هوية الكيان
- اختراق خدمة الاستيقان

وتتقاسم الأطراف المعولة ومقدمو خدمة أوراق الاعتماد مسؤولية الحماية من التهديدات التي يتعرض لها الاستيقان. ويجب أن تكون الأدوار والمسؤوليات ضمن معاملة الاستيقان محددة بوضوح ومتفق عليها من جميع الأطراف.

ويعرض الجدول 8-1 فئات التهديدات التي يتعرض لها الاستيقان والمسؤولية عادة للتخفيف من حدة هذه التهديدات.

الجدول 8-1 – الأدوار وفئات التهديدات

الدور	فئات التهديدات
الأطراف المعولة	• انتحال هوية جهة التحقق • اختراق المعاملة • الخصوصية • الاتحاد
مقدمو خدمات أوراق الاعتماد	• انتحال هوية جهة التحقق • اختراق المعاملة • انتحال هوية المشترك • اختراق المستيقن • اختراق خدمة الاستيقان • الخصوصية • الاتحاد

1.8 مستويات الضمان

في هذه التوصية، الاستيقان هو العملية التي يتم بواسطتها التحقق من هوية مدعاة لأغراض إجراء معاملة عبر الإنترنت. وتؤدي الصرامة المتزايدة في العمليات المستخدمة للتحقق من الهويات المدعاة إلى ثقة متزايدة بأن الهوية المستيقن منها تمثل الصاحب المقصود لهذه الهوية. وضمان الاستيقان هو قياس لتلك الثقة، وهناك أنظمة – أو مخططات – تحدد مجموعة من المستويات النسبية للثقة، وتعرف باسم مستويات ضمان الاستيقان.

وتصف هذه التوصية نموذجاً لضمان الاستيقان يقوم على مفهوم تحديد التهديدات والمخاطر التي تتعرض لها معاملات الاستيقان. في الكثير من الحالات، قد تختار المؤسسات والهيئات الوطنية والمجتمعات إنشاء مخطط لمستويات ضمان الاستيقان يجمع المخاطر والتهديدات والضوابط ذات الصلة بالبيئات التي تعمل فيها. ومن شأن القيام بذلك توفير فوائد ملموسة عديدة، بما في ذلك تحديد المتطلبات اللازمة للمشاركة في المعاملات عند مستويات محددة عادة، والقدرة على استحداث مجموعات معيارية من المنتجات لتلبية احتياجات المجتمعات.

وتتراجع هذه التوصية عن مفهوم مستوى الضمان (LOA) بوصفه ترتيباً فريداً يحدد المتطلبات الخاصة بالتنفيذ. وبدلاً من ذلك، فالجمع بين الإدارة المناسبة للمخاطر المتعلقة بالخصوصية والأعمال واحتياجات المهمة، يقوم المنفذون باختيار مستوى ضمان الهوية (IAL) ومستوى ضمان الاستيقان (AAL) ومستوى ضمان الاتحاد (FAL) كخيارات متميزة. ومع أن عدداً كبيراً من الأنظمة سيكون لها المستوى الرقمي نفسه بالنسبة لكل مستوى من مستويات IAL وAAL وFAL، فإن هذا ليس شرطاً وعلى المنفذين عدم الافتراض بأن هذه المستويات ستكون هي نفسها في أي نظام معين.

وفيما يلي مكونات ضمان الهوية المفصلة في هذه المبادئ التوجيهية على النحو التالي:

- المستوى IAL هو عملية تدقيق الهوية.
- المستوى AAL هو عملية ضمان الاستيقان.
- المستوى FAL هو قوة التأكيد في بيئة اتحادية، ويستعمل لإرسال الاستيقان ومعلومات النعوت (حسب الاقتضاء) إلى الطرف المعوّل.

يوفر الفصل بين هذه الفئات للمنفذين المرونة في اختيار الحلول لمسألة الهوية ويزيد من القدرة على إدراج أساليب معززة للخصوصية باعتبارها عناصر أساسية لأنظمة الهوية عند أي مستوى من مستويات الضمان. وعلى سبيل المثال، يدعم هذا النموذج سيناريوهات تسمح بتفاعلات ذات أسماء مستعارة حتى عند استخدام مستيقنات قوية متعددة العوامل.

وفي البيئة المعاصرة، لا حاجة لأن يكون حل مسألة هوية المؤسسة كتلة واحدة، حيث يوفر نظام أو بائع واحد جميع العناصر الوظيفية. وقد تتألف خدمات الهوية من مكونات متعددة، ما يسمح للمؤسسات والوكات باستخدام حلول قابلة للتوصيل وقائمة على المعايير لمسألة الهوية مبنية على احتياجات المهمة.

تحدد المستويات AAL الثلاثة المجموعات الفرعية للخيارات التي يمكن أن يختارها المنفذون استناداً إلى مواصفاتهم للمخاطر والضرر المحتمل الذي يسببه مهاجم يتحكم بأحد المستيقنات وينفذ إلى أنظمة الوكالات. وفيما يلي مستويات ضمان الاستيقان (AAL):

AAL1: يوفر المستوى AAL1 درجة من الضمان بأن الكيان يتحكم بمستيقن مرتبط بحساب الكيان. ويتطلب المستوى AAL1 استيقاناً بعامل وحيد أو متعدد العوامل باستخدام مجموعة واسعة من تكنولوجيات الاستيقان المتوفرة. ويتطلب الاستيقان الناجح أن يثبت المدعي ملكية المستيقن والتحكم به من خلال بروتوكول استيقان آمن.

AAL2: يوفر المستوى AAL2 ثقة كبيرة بأن الكيان يتحكم بالمستيقن أو المستيقنات المرتبطة بحساب الكيان. ولا بد أن يكون هناك إثبات بملكية عاملي استيقان متميزين والتحكم بهما من خلال بروتوكول أو بروتوكولات استيقان آمنة. ويحتاج الأمر إلى أساليب تجفير مقبولة عالمياً عند المستوى AAL2 فما فوق.

AAL3: يوفر المستوى AAL3 ثقة كبيرة جداً بأن الكيان يتحكم بالمستيقن أو المستيقنات المرتبطة بحساب الكيان. ويستند الاستيقان بالمستوى AAL3 على إثبات ملكية مفتاح من خلال أحد بروتوكولات التجفير. ويتعين على الاستيقان بالمستوى AAL3 استخدام مستيقن تجفير قائم على المعدات ومستيقن يوفر مقاومة لانتحال هوية جهة التحقق؛ وقد يستوفي الجهاز نفسه هذين المتطلبين. ولإجراء استيقان بالمستوى AAL3، يجب أن يثبت المدعون أنهم يمتلكون عاملي استيقان متميزين ويتحكمون بهما من خلال بروتوكول أو بروتوكولات استيقان آمنة. ويحتاج الأمر إلى أساليب تجفير مقبولة عالمياً.

لا تقترح هذه الطبعة من هذه التوصية مجموعة وحيدة من مستويات الضمان المعيارية والمقيّسة. فمحاولة استحداث هيكل ضمان مقيّس ووحيد لجميع المجتمعات تؤدي إلى الحد من قدرة مجتمعات محددة على إدارة المخاطر بما يتناسب مع بيئاتها. ومع ذلك فهي تعترف بوجود مخططات الضمان المختلفة هذه وبأن مقدمي خدمة الهوية يجب أن يكونوا قادرين على إثبات التزامهم بمجموعة واحدة أو أكثر من المستويات AAL.

وبما أن مخططات مستويات ضمان الاستيقان تمثل مستويات متزايدة من الثقة في التحقق من هوية مدعاة، مع مستويات متزايدة نسبياً من الصرامة في عملية الاستيقان، فإن مواصفات الضوابط في هذه التوصية تستخدم مصطلحات نسبية بدلاً من المستويات AAL المتمايزة. وبالنسبة لهذه الضوابط التي يمكن تعديلها لتوفير زيادة في الثقة، يشار إلى الظروف التي توفر أقل قدر من الثقة بعبارة "أدنى مستويات AAL"؛ بعد ذلك يشار إلى المزيد من الثقة بعبارة "مستويات عالية AAL"؛ ويشار إلى الظروف التي ينتج عنها أعلى قدر من الثقة بعبارة "أعلى مستويات AAL". ويقدم الجدول 8-2 فكرة تصورية عن كيفية معادلة هذا الاصطلاح لبعض المخططات الأكثر شيوعاً لضمان الاستيقان. (يرجى ملاحظة أن المواءمة الواردة في الجدول 2.8 ليس الغرض منها بأي حال من الأحوال إنشاء تكافؤ مباشر بين المخططات المختلفة.)

الجدول 8-2 – مستويات ضمان الاستيقان

AAL	المخطط 4-AAL	المخطط 3-AAL	مخطط من 3 مستويات
أعلى مستوى	AAL 4	AAL 3	مرتفع
مستوى مرتفع	AAL 3	AAL 2	واقعي
	AAL 2		
أدنى مستوى	AAL 1	AAL 1	منخفض

يوفر القسم المتبقي من هذه الفقرة مجموعة فوقية من الضوابط المعيارية مجمعة وفقاً للتهديدات التي تخفف من حدتها. ويجب على مقدمي خدمة الهوية أن يعرفوا التهديدات المحددة التي يتعرضون لها استناداً إلى الأدوار والخدمات المنوطة بهم، على النحو الوارد في هذه التوصية. وبمجرد تحديد ذلك، وللتمكن من تقدير المطابقة مع هذه التوصية، يجب على مقدمي خدمات الهوية توثيق التهديدات، ومواصفات الضوابط المقابلة والنتائج المرجوة، على النحو الوارد في الجزء المتبقي من هذه الفقرة

2.8 اختراق المستيقن

1.2.8 مخاطر اختراق المستيقن

اختراق المستيقن هو عبارة عن أي هجوم يكرر معلومات أوراق الاعتماد التي يمكن استخدامها لتمكين نظام معلومات من الاستيقان عنها بنجاح والحصول على نفاذ غير مرخص به، أو يتلاعب بها أو يؤدي إلى الإفشاء غير المصرح به عنها. وقد يحدث اختراق المستيقنات في أي وقت من دورة حياة إدارة الهوية. ومع ذلك، فإن التهديدات والضوابط المندرجة في نطاق هذه التوصية لا تهدف إلا إلى معالجة الاستيقان.

ويمكن اختراق أوراق الاعتماد بواسطة عدد من نواقل الهجوم، بما في ذلك التصيّد الاحتيالي، والسرقة، ونسخ أوراق الاعتماد، وهجوم التكرار، والهجمات الشاملة لجميع الاحتمالات عبر الإنترنت أو بدون توصيل بالإنترنت. ولا تقتصر الحماية من مخاطر اختراق أوراق الاعتماد على الضوابط في فئة التهديدات هذه. وتجدر الإشارة إلى أن إحدى نتائج إخفاقات الضوابط في أي فئة من فئات التهديدات يمكن أن تؤدي إلى اختراق أوراق الاعتماد. فعلى سبيل المثال، إذا كان مقدم خدمة الاستيقان يعاني من خرق للبيانات، فيمكن استخدام المعلومات المتحصل عليها لاكتساب نفاذ غير مصرح به إلى نظام المعلومات.

2.2.8 ضوابط اختراق المستيقن

يدرج الجدول 8-3 قائمة بضوابط اختراق المستيقن.

الجدول 8-3 – ضوابط اختراق المستيقن

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
AC-1	في حالة أعلى مستوى AAL، ينبغي للاستيقان أن يستخدم مستيقنَ تجفير قائم على المعدات ومستيقناً يوفر مقاومة لانتحال هوية جهة التحقق – ويمكن للجهاز نفسه أن يلبي هذين الشرطين.	استخدام المستيقنات المناسبة لتحقيق المستوى المطلوب لضمان الاستيقان.
AC-2	في حالة أعلى مستوى AAL، ينبغي أن يثبت المدعون امتلاكهم لعاملي استيقان مختلفين من خلال بروتوكول (بروتوكولات) استيقان آمنة وتحكمهم بهما.	اتباع بروتوكولات الاستيقان المناسبة لتحقيق المستوى المطلوب لضمان الاستيقان.
AC-3	ينبغي التثبت من صلاحية المستيقنات المتعددة العوامل المستخدمة عند أعلى مستوى AAL بالقدر المطلوب لبرنامج معتمد للتحقق من وحدة التجفير.	التثبت من صلاحية تجفير المستيقن حسبما تقتضيه الضرورة لتحقيق المستوى المطلوب لضمان الاستيقان.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
AC-4	ينبغي التثبت من صلاحية المستيقنات التي يحصل عليها مقدمو خدمات الهوية لتلبية متطلبات برنامج معتمد للتحقق من وحدة التجفير.	استخدام تجفير معتمد.
AC-5	ينبغي لجهة التحقق أن تطبق ضوابط للحماية من هجمات التخمين على الإنترنت إذا كانت تنطبق على نوع المستيقن.	قيام جهة التحقق بتطبيق ضوابط لحماية المستيقنات من هجمات التخمين على الإنترنت.
AC-6	ما لم يحدد خلاف ذلك في مواصفات مستيقن معين، ينبغي لجهة التحقق أن تحد من محاولات الاستيقان الفاشلة المتتالية من حساب واحد بحيث لا تزيد على 100 محاولة.	قيام جهة التحقق بتطبيق ضوابط لحماية المستيقنات من هجمات التخمين على الإنترنت.
AC-7	ينبغي لمستيقنات التجفير استعمال تجفير معتمد.	استخدام تجفير معتمد.
AC-8	في حالة استعمال أكثر من مستيقن واحد للاستيقان، ينبغي أن يكون واحد منها على الأقل مقاوماً للتكرار.	أن تكون المستيقنات محمية من هجمات التكرار.
AC-9	ينبغي أن تكون جميع مستيقنات أجهزة التجفير مقاومة للتكرار.	استخدام الضوابط لحماية المستيقنات من هجمات التكرار.
AC-10	ينبغي أن تكون هجمات لقنوات الجانبية ذات الصلة محددة بواسطة تقدير للمخاطر يجريه مقدم خدمة أوراق الاعتماد.	إجراء مقدم خدمة أوراق الاعتماد للعمليات المناسبة لتقدير المخاطر.
AC-11	ينبغي أن يتم الاتصال بين المدعي وجهة التحقق (باستخدام القناة الأولية في حالة مستيقن خارج النطاق) عن طريق قناة محمية ومستيقن منها.	يكون الاتصال بين بين المدعي وجهة التحقق محمياً.
AC-12	ينبغي التثبت من صلاحية أجهزة التجفير بعامل وحيد إلى المدى المطلوب من برنامج معتمد للتحقق من وحدة التجفير.	التثبت من صلاحية تجفير المستيقن حسبما تقتضيه الضرورة لتحقيق المستوى المطلوب لضمان الاستيقان.
AC-13	عند استعمال جهاز مثل الهاتف الذكي في عملية الاستيقان، ينبغي ألا يعتبر فتح هذا الجهاز (الذي يتم عادة باستعمال رقم تعريف الهوية الشخصي (PIN) أو قياس حيوي) عاملاً من عوامل الاستيقان.	استعمال المستيقنات المناسبة لتحقيق المستوى المطلوب لضمان الاستيقان.
AC-14	ينبغي لنظام القياسات الحيوية ألا يسمح بأكثر من 10 محاولات فاشلة متتالية للاستيقان. وبمجرد بلوغ هذا الحد، ينبغي للمستيقن البيومتري أن يقوم بأي مما يلي: • فرض مهلة لا تقل عن 30 ثانية قبل المحاولة التالية (مثلاً دقيقة واحدة قبل القيام بالمحاولة الثانية التالية)، • أو إبطال الاستيقان البيومتري للمستعمل وتقديم عامل آخر (مثل طريقة بيومترية مختلفة أو رقم تعريف الهوية الشخصي/كلمة السرّ إذا لم يكن بالفعل أحد العوامل المطلوبة) إذا كانت هذه الطريقة البديلة متاحة بالفعل.	قيام النظام البيومتري بتطبيق ضوابط لحماية المستيقنات من هجمات التخمين.

3.8 اختراق المعاملة

1.3.8 مخاطر اختراق المعاملة

اختراق المعاملة هو هجوم يخرق سرية البيانات في طور العبور عند تبادلها بين طرفين أو يعرقل إتاحتها. والهجمات الشائعة التي يمكن أن تؤدي إلى اختراق المعاملة هي عبارة هجمات متطفل بين طرفين (MItM)، أو هجمات في متصفح الويب (MItB)، أو تنصت، أو اختطاف الدورة.

2.3.8 ضوابط اختراق المعاملة

يدرج الجدول 8-4 قائمة بضوابط اختراق المعاملة.

الجدول 8-4 – ضوابط اختراق المعاملة

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
TC-1	في الحالات التي تكون فيها جهة التحقق ومقدم خدمة أوراق الاعتماد كيانين منفصلين، ينبغي أن تجري الاتصالات بين جهة التحقق ومقدم خدمة أوراق الاعتماد من خلال قناة آمنة يجري فيها استيقان متبادل (مثل توصيلة لأمن طبقة النقل يجري فيها الاستيقان من العملاء) باستخدام تجفير معتمد.	حماية الاتصالات بين جهة التحقق ومقدم خدمة أوراق الاعتماد.
TC-2	ينبغي تبادل سر الدورة بين برمجيات المشترك والخدمة التي يجري النفاذ إليها.	تنفيذ وحماية أسرار الدورة.
TC-3	ينبغي أن يتضمن محتوى مواقع الموارد المحددة (URL) أو الرابط HTTP POST، [b-IETF RFC 7231] معرّف هوية الدورة الذي ينبغي أن يتحقق منه الطرف المعول للتأكد من أن الإجراءات المتخذة خارج الدورة لا تؤثر على الدورة المحمية.	قيام الطرف المعوّل بالتحقق من معرفات هوية الدورات.
TC-4	ينبغي عرض السر مباشرة بواسطة برمجيات المستعمل أو البرهان على امتلاك السر باستخدام آلية تجفير.	توليد أسرار الدورة بصورة عشوائية، وتنفيذها بشكل مناسب والتخلص منها بشكل سليم بعد الاستعمال.
TC-5	ينبغي ألا تكون الأسرار المستعملة لربط الدورات متاحة للاتصالات غير المؤمنة بين المضيف ونقطة المشترك الطرفية. وبعد الاستيقان، ينبغي ألا تتراجع الدورات المستيقن منها إلى نقل عير مؤمن، كأن تنتقل من استعمال بروتوكول نقل النصوص الترابطية المؤمن (HTTPS) إلى استعمل بروتوكول نقل النصوص الترابطية (HTTP).	حماية إرسال أسرار الدورة.
TC-6	ينبغي أن يقوم مضيف الدورة بتوليد أسرار روابط الدورات أثناء تفاعل معين، وعادة بعد الاستيقان من المستعمل مباشرة.	توليد أسرار الدورة بصورة عشوائية، وتنفيذها بشكل مناسب والتخلص منها بشكل سليم بعد الاستعمال.
TC-7	ينبغي توليد الأسرار المستخدمة في روابط الدورات بواسطة مولد معتمد للبتات العشوائية وأن تتضمن أنتروبية لا تقل عن 64 بتة.	توليد أسرار الدورة بصورة عشوائية، وتنفيذها بشكل مناسب والتخلص منها بشكل سليم بعد الاستعمال.
TC-8	ينبغي أن يقوم صاحب الدورة بمحو الأسرار المستخدمة في روابط الدورات أو إبطال صلاحيتها عند خروج المستعمل من الدورة.	توليد أسرار الدورة بصورة عشوائية، وتنفيذها بشكل مناسب والتخلص منها بشكل سليم بعد الاستعمال.
TC-9	ينبغي إرسال الأسرار المستخدمة في روابط الدورات إلى الجهاز أو استقبالها منه باستخدام قناة محمية ومستيقنة.	حماية إرسال أسرار الدورة.
TC-10	ينبغي إيقاف الأسرار المستخدمة في روابط الدورات وعدم قبولها بعد أوقات يحددها مقدم خدمة أوراق الاعتماد.	حماية إرسال أسرار الدورة.
TC-11	ينبغي أن يقوم مضيف الدورة بتوليد الأسرار المستخدمة في روابط الدورات كاستجابة مباشرة لحدث استيقان.	توليد أسرار الدورة بصورة عشوائية، وتنفيذها بشكل مناسب والتخلص منها بشكل سليم بعد الاستعمال.
TC-12	ينبغي وسم ملفات ارتباط متصفح الويب كي لا يكون النفاذ إليها متاحاً إلا في دورات HTTPS.	حماية إرسال أسرار الدورة.
TC-13	ينبغي أن تكون ملفات ارتباط متصفح الويب متاحة للمجموعة العملية الدنيا من أسماء المضيفين والمسارات.	حماية إرسال أسرار الدورة.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
TC-14	ينبغي أن تستند استمرارية الدورات المستيقنة إلى امتلاك سر الدورة الذي تصدره جهة التحقق في وقت الاستيقان ويتم تجديده بصورة اختيارية خلال الدورة.	توليد أسرار الدورة بصورة عشوائية، وتنفيذها بشكل مناسب والتخلص منها بشكل سليم بعد الاستعمال.
TC-15	إذا أجريت المقارنة بطريقة مركزية، ينبغي أن يتم إرسال جميع القياسات البيومترية عبر قناة محمية ومستيقنة.	حماية إرسال المعلومات البيومترية.
TC-16	ينبغي إنشاء قناة محمية ومستيقنة بين المستشعر (أو نقطة طرفية تحتوي على مستشعر يقاوم استبدال المستشعرات) وجهة التحقق.	حماية الاتصالات بين جهة التحقق والنقاط الطرفية.

4.8 انتحال هوية جهة التحقق

1.4.8 مخاطر انتحال هوية جهة التحقق

انتحال هوية جهة التحقق هو هجوم يحدث عندما يتفاعل كيان مع جهة تحقق مزيفة ويتم التحايل عليه للكشف عن معلومات أوراق الاعتماد. وقد تشكل المعلومات التي يحصل عليها المهاجم خطراً كبيراً على فئتي التهديدات المتمثلتين بانتحال هوية المشترك أو اختراق أوراق الاعتماد. ويعتبر التصيد الاحتيالي أحد أكثر الهجمات شيوعاً المرتبطة بانتحال هوية جهة التحقق. ويكون المهاجم قادراً على استدراج الكيان لإرسال معلومات أوراق الاعتماد الخاصة بالمشترك إلى مستعمل أو مخدّم غير موثوق أو خدمة غير موثوقة، واستخدام معلومات أوراق الاعتماد التي حصل عليها للتوصل إلى نفاذ غير مصرح به إلى نظام المعلومات.

2.4.8 ضوابط انتحال هوية جهة التحقق

يدرج الجدول 8-5 قائمة بضوابط انتحال هوية جهة التحقق.

الجدول 8-5 – ضوابط انتحال هوية جهة التحقق

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
VI-1	ينبغي التحقق من صلاحية جهات التحقق لتلبية متطلبات برنامج معتمد للتحقق من وحدة التجفير.	استعمال تجفير معتمد.
VI-2	ينبغي لبروتوكول الاستيقان المقاوم لانتحال الهوية أن ينشئ قناة محمية ومستيقنة مع جهة التحقق.	حماية خرج المستيقن.
VI-3	ينبغي للقناة المحمية والمستيقنة أن تربط بشكلٍ وثيق ونهائي معرف هوية القناة الذي تم التفاوض بشأنه عند إنشاء القناة المحمية التي استيقن منها خرج المستيقن.	حماية خرج المستيقن.
VI-4	ينبغي أن تتحقق جهة التحقق من صلاحية التوقيع أو المعلومات الأخرى المستخدمة في إثبات مقاومة انتحال هوية جهة التحقق.	إقرار جهات التحقق للصلاحية بشكل فعّال.
VI-5	ينبغي استعمال خوارزميات تجفير معتمدة لإنشاء مقاومة لانتحال هوية جهة التحقق.	استعمال تجفير معتمد.
VI-6	ينبغي أن توفر لمفاتيح المستخدمة لإنشاء مقاومة لانتحال هوية جهة التحقق قوة الأمن الدنيا على الأقل المحددة في معيار تجفير مطبق.	عدم انتحال هوية جهات التحقق.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
VI-7	لكي تعتبر المفاتيح العمومية التي تختزنها جهة التحقق مقاومة لاختراق جهة التحقق، ينبغي أن تكون مرتبطة باستخدام خوارزميات تجفير معتمدة وأن توفر على الأقل قوة الأمن الدنيا المحددة في معيار تجفير مطبق.	عدم اختراق جهات التحقق.
VI-8	ينبغي أن تستخدم الأسرار المقاومة لانتحال هوية جهة التحقق خوارزميات اختزال معتمدة وأن يكون للأسرار الأساسية قوة الأمن الدنيا على الأقل المحددة في معيار تجفير مطبق.	عدم اختراق جهات التحقق.
VI-9	ينبغي للمستيقنات التي تشمل الإدخال اليدوي لخرج المستيقن، من قبيل المستيقنات خارج النطاق التي تستعمل كلمة سرّ لمرة واحدة، ألا تعتبر مقاومة لانتحال هوية جهة التحقق لأن الإدخال اليدوي لا يربط خرج المستيقن بالدورة المحددة التي يجري استيقانها.	عدم استعمال مستيقنات تتطلب إدخالاً يدوياً للحماية من انتحال هوية جهة التحقق.

5.8 انتحال هوية المشترك

1.5.8 مخاطر انتحال هوية المشترك

انتحال هوية المشترك هو هجوم يتضمن تزييف هوية مشروعة لتخريب عملية الاستيقان والحصول على نفاذ غير مصرح به إلى شبكة أو نظام للمعلومات. وتشمل الهجمات لشائعة لانتحال هوية المشترك انتحال الصفة واختطاف الدورة. ومن الأمثلة على هجمة انتحال الصفة قيام مهاجم ينتحل هوية الطرف المعوّل بانتحال صفة عنوان التحكم في النفاذ إلى الوسائط (MAC) الذي يخص جهازاً مستيقناً منه حصل على نفاذ مصرح به إلى الشبكة. وهناك مثال آخر هو التنكّر، حيث ينتحل المهاجم هوية مستعمل مشروع من خلال توفير أدلة مزيفة أو مسروقة ويكون قادراً على اتباع بروتوكول إعادة تعيين أوراق الاعتماد بنجاح.

2.5.8 ضوابط انتحال هوية المشترك

يدرج الجدول 8-6 قائمة بضوابط انتحال هوية المشترك.

الجدول 8-6 – ضوابط انتحال هوية المشترك

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
SI-1	تكون نتيجة عملية الاستيقان عبارة عن معرّف هوية ينبغي استخدامه في كل مرة يستيقن بها الطرف المعوّل من المشترك.	ربط المستيقن (المستيقنات) بالمشترك المناسب.
SI-2	لتلبية متطلبات مستوى AAL معين، ينبغي أن يتم الاستيقان من المدعي بمستوى معين من القوة على الأقل لكي يتم الاعتراف به كمشترك.	استيقان المشترك باستخدام المستيقن أو المستيقنات المناسبة بالمستوى المناسب من القوة لتحقيق المستوى المطلوب لضمان الاستيقان.
SI-3	ينبغي أن تبين جميع عمليات الاستيقان وإعادة الاستيقان الهدف من الاستيقان انطلاقاً من مستيقن واحد على الأقل.	إثبات هدف المستيقن.
SI-4	ينبغي أن يوفر مقدمو خدمات أوراق الاعتماد تعليمات للمشترك عن كيفية حماية المستيقن من السرقة أو الفقدان بشكل مناسب.	تمكين المشترك من استعادة المستيقن (المستيقنات) من دون الالتفاف على المستوى المطلوب لضمان الاستيقان.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
SI-5	ينبغي أن يجري الاستيقان بأدنى مستوى AAL باستخدام أي من أنواع المستيقنات التالية: • سر محفوظ عن غيب • سر مسترجع • أجهزة خارج النطاق • جهاز إنتاج كلمة سرّ لمرة واحدة بعامل وحيد • جهاز إنتاج كلمة سرّ لمرة واحدة متعددة العوامل • برمجيات تجفير بعامل وحيد • جهاز تجفير بعامل وحيد • برمجيات تجفير متعددة العوامل • جهاز تجفير متعدد العوامل	الاستيقان من المشترك باستخدام المستيقن أو المستيقنات المناسبة بالمستوى المناسب من القوة لتحقيق المستوى المطلوب لضمان الاستيقان.
SI-6	ينبغي أن يجري الاستيقان بأعلى مستوى AAL باستخدام مستيقن متعدد العوامل أو توليفة من مستيقنين بعامل وحيد. عند استخدام مستيقن متعدد العوامل، يمكن استعمال أيّ مما يلي: • جهاز إنتاج كلمة سرّ لمرة واحدة متعدد العوامل • برمجيات تجفير متعددة العوامل • جهاز تجفير متعدد العوامل	الاستيقان من المشترك باستخدام المستيقن أو المستيقنات المناسبة بالمستوى المناسب من القوة لتحقيق المستوى المطلوب لضمان الاستيقان.
SI-7	عند استعمال توليفة من مستيقنين بعامل وحيد، ينبغي أن تشمل التوليفة مستيقناً بسر محفوظ عن غيب ومستيقناً قائماً على الامتلاك (أي شيء تمتلكه) مستمداً من القائمة التالية: • سرّ مسترجع • جهاز خارج النطاق • جهاز إنتاج كلمة سرّ لمرة واحدة بعامل وحيد • برمجيات تجفير بعامل وحيد • جهاز تجفير بعامل وحيد	الاستيقان من المشترك باستخدام المستيقن أو المستيقنات المناسبة بالمستوى المناسب من القوة لتحقيق المستوى المطلوب لضمان الاستيقان.
SI-8	ينبغي أن يجري الاستيقان بأعلى مستوى AAL باستخدام واحدة من توليفات المستيقنات التالية. وتشتق التوليفات المحتملة من: • جهاز تجفير متعدد العوامل • جهاز تجفير بعامل وحيد يستخدم بالاقتران مع سر محفوظ عن غيب • جهاز (برمجيات أو معدات) إنتاج كلمة سرّ لمرة واحدة متعدد العوامل يستخدم بالاقتران مع جهاز تجفير بعامل وحيد • جهاز (معدات فقط) إنتاج كلمة سرّ لمرة واحدة متعدد العوامل يستخدم بالاقتران مع جهاز تجفير بعامل وحيد • جهاز (معدات فقط) إنتاج كلمة سرّ لمرة واحدة بعامل وحيد يستخدم بالاقتران مع مستيقن برمجيات التجفير متعدد العوامل • جهاز (معدات فقط) إنتاج كلمة سرّ لمرة واحدة بعامل وحيد يستخدم بالاقتران مع مستيقن برمجيات التجفير بعامل وحيد وسر محفوظ عن غيب	الاستيقان من المشترك باستخدام المستيقن أو المستيقنات المناسبة بالمستوى المناسب من القوة لتحقيق المستوى المطلوب لضمان الاستيقان.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
SI-9	ينبغي أن يوفر مقدم خدمة أوراق الاعتماد آلية لإبطال أو تعليق المستيقن فور ورود إشعار من المشترك بالاشتباه بفقدان أو سرقة المستيقن.	عدم إمكانية استعمال مستيقنات غير صالحة للاستيقان من شخص بنجاح.
SI-10	لتسهيل الإبلاغ الآمن عن فقدان مستيقن أو سرقته أو تضرره، ينبغي لمقدم خدمة أوراق الاعتماد أن يزود المشترك بالطريقة التي يستيقن بها من المشترك باستخدام مستيقن رديف أو بديل. وينبغي أن يكون المستيقن الرديف عبارة عن سر محفوظ عن غيب أو مستيقن مادي.	تمكين المشترك من استعادة المستيقن (المستيقنات) من دون الالتفاف على المستوى المطلوب لضمان الاستيقان.
SI-11	ينبغي أن يكون التعليق قابلاً للرجوع عنه إذا نجح مقدم خدمة أوراق الاعتماد في الاستيقان من المشترك باستخدام مستيقن صالح (أي غير معلق) وطلب المشترك إعادة تفعيل مستيقن معلق بهذه الطريقة.	تمكين المشترك من استعادة المستيقن (المستيقنات) من دون الالتفاف على المستوى المطلوب لضمان الاستيقان.
SI-12	إذا ومتى انتهت صلاحية أحد المستيقنات، ينبغي ألا يكون استعماله صالحاً للاستيقان.	عدم إمكانية استعمال مستيقنات غير صالحة للاستيقان من شخص بنجاح.
SI-13	ينبغي لمقدم خدمة أوراق الاعتماد أن يطلب من المشتركين التخلي عن أو إتلاف أي مستيقن مادي يتضمن شهادات نعوت موقعة من مقدم خدمة أوراق الاعتماد في أقرب وقت ممكن بعد أن يصبح المستيقن غير صالح بسبب انتهاء المدة أو الإبطال أو الإنهاء أو التجديد أو أي وسيلة أخرى يحددها مقدم خدمة أوراق الاعتماد.	عدم إمكانية استعمال مستيقنات غير صالحة للاستيقان من شخص بنجاح.
SI-14	ينبغي لمقدمي خدمة أوراق الاعتماد إبطال ربط المستيقنات فوراً عندما لا تعود الهوية موجودة على الإنترنت، بناء لطلب المشترك، أو عندما يقرر مقدم خدمة أوراق الاعتماد أن المشترك لم يعد يلبي متطلبات أهليته.	عدم إمكانية استعمال مستيقنات غير صالحة للاستيقان من شخص بنجاح.
SI-15	ينبغي إلا تستخدم القياسات البيومترية إلا كجزء من استيقان متعدد العوامل بواسطة مستيقن مادي (شيء تملكه).	استعمال القياسات الحيوية بشكل مناسب كمستيقنات.
SI-16	عند أعلى مستوى AAL، ينبغي لمقدم خدمة أوراق الاعتماد أن يربط مستيقناً مادياً (شيئاً تملكه) واحداً على الأقل، وينبغي أن يربط مستيقنين على الأقل، بهوية المشترك على الإنترنت، بالإضافة إلى سر محفوظ عن غيب أو قياس بيومتري واحد أو أكثر.	ربط المستيقن (المستيقنات) بالمشترك المناسب.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
SI-17	بالنسبة لأعلى مستوى AAL، إذا تعذر إكمال الانتساب والربط خلال مقابلة مادية أو معاملة إلكترونية، ينبغي استخدام الأساليب التالية للتأكد من أن الطرف نفسه يتصرف مثل مقدم الطلب خلال العمليات: في حالة المعاملات التي تتم عن بُعد: 1) ينبغي أن يعرّف مقدمو الطلبات أنفسهم في كل معاملة جديدة من خلال تقديم سر مؤقت أنشئ خلال معاملة سابقة، أو أرسل إلى رقم هاتف مقدم الطلب، أو عنوان بريده إلكتروني، أو عنوان بريدي للسجل. 2) ينبغي أن لا يتم إصدار أسرار المستيقنات الطويلة الأجل إلى مقدم الطلب إلا ضمن دورة محمية. وفي حالة المعاملات التي تتم بشكل شخصي: 1) ينبغي أن يعرّف مقدمو الطلبات أنفسهم شخصياً إما باستخدام سر على النحو الوارد في حالة المعاملات عن بُعد (النقطة 1) في الفقرة السابقة، أو عبر استعمال قياس بيومتري تم تسجيله خلال مقابلة سابقة. 2) ينبغي عدم إعادة استعمال الأسرار المؤقتة. 3) إذا أصدر مقدم خدمة أوراق الاعتماد أسرار مستيقنات طويلة الأجل خلال معاملة مادية، ينبغي عندئذ تحميلها محلياً في جهاز مادي يتم إصداره مباشرة إلى مقدم الطلب أو تسليمه بطريقة تؤكد عنوان السجل.	ربط المستيقن (المستيقنات) بالمشترك المناسب.
SI-18	عند ربط مستيقن إضافي بحساب مشترك، ينبغي لمقدم خدمة أوراق الاعتماد أن يطلب أولاً الاستيقان من المشترك بالمستوى AAL الذي سيستعمل فيه المستيقن على الأقل.	ربط المستيقن (المستيقنات) بالمشترك المناسب.
SI-19	بالنسبة لمستوى AAL مرتفع، إذا فقد المشترك جميع المستيقنات المتعلقة بعامل ضروري لإكمال الاستيقان متعدد العوامل وكان على هذا المشترك تكرار عملية تدقيق الهوية.	تمكين المشترك من استعادة المستيقن (المستيقنات) من دون الالتفاف على المستوى المطلوب لضمان الاستيقان.
SI-20	عند الاستعاضة عن عامل استيقان مفقود بمستوى AAL مرتفع، ينبغي لمقدم خدمة أوراق الاعتماد أن يشترط على المدعي الاستيقان باستخدام مستيقن من أي عامل متبقي، لتأكيد الإسناد إلى الهوية القائمة.	تمكين المشترك من استعادة المستيقن (المستيقنات) من دون الالتفاف على المستوى المطلوب لضمان الاستيقان.
SI-21	ينبغي إجراء إعادة دورية للاستيقان من الدورات لتأكيد استمرار وجود المشترك في دورة مستيقن منها.	قيام المشترك بإعادة الاستيقان بصورة دورية بواسطة المستيقن أو المستيقنات المناسبة بالقوة اللازمة لتحقيق المستوى المطلوب لضمان استيقان.

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
SI-22	ينبغي إجراء إعادة استيقان دورية من دورات المشترك: أ) عند أدنى مستوى AAL، ينبغي أن تتكرر إعادة الاستيقان من المشترك بمعدل مرة واحدة على الأقل كل 30 يوماً خلال دورة ممتدة من الاستعمال، بصرف النظر عن نشاط المستعمل. ب) عند أدنى مستوى AAL، ينبغي إنهاء الدورة (أي الخروج منها) عند انتهاء الفترة المحددة. ج) عند مستوى AAL مرتفع، ينبغي أن تتكرر إعادة الاستيقان من المشترك بمعدل مرة واحدة على الأقل كل 12 ساعة خلال دورة ممتدة من الاستعمال، بصرف النظر عن نشاط المستعمل. د) عند مستوى AAL مرتفع، ينبغي أن تتكرر إعادة الاستيقان من المشترك بعد أي فترة خمول تدوم 30 دقيقة أو أكثر. هـ)عند مستوى AAL مرتفع، ينبغي إنهاء الدورة (أي الخروج منها) عند انتهاء أي من هاتين الفترتين. و) عند أعلى مستوى AAL، ينبغي أن تتكرر إعادة الاستيقان من المشترك بمعدل مرة واحدة على الأقل كل 12 ساعة خلال دورة ممتدة من الاستعمال، بصرف النظر عن نشاط المستعمل. ز) عند أعلى مستوى AAL، ينبغي أن تتكرر إعادة الاستيقان من المشترك بعد أي فترة خمول تدوم 15 دقيقة أو أكثر. ح) عند أعلى مستوى AAL، ينبغي إنهاء الدورة (أي الخروج منها) عند انتهاء أي من هاتين الفترتين ((و) أو (ز)). ط) عند أعلى مستوى AAL، ينبغي إجراء إعادة استيقان دورية من المشترك باستخدام جميع عوامل الاستيقان الأصلية.	قيام المشترك بإعادة الاستيقان بصورة دورية بواسطة المستيقن أو المستيقنات المناسبة بالقوة اللازمة لتحقيق المستوى المطلوب لضمان استيقان.
SI-23	ينبغي عدم تمديد الدورة بناء على تقديم سر الدورة وحده.	قيام المشترك بإعادة الاستيقان بصورة دورية بواسطة المستيقن أو المستيقنات المناسبة بالقوة اللازمة لتحقيق المستوى المطلوب لضمان استيقان.
SI-24	عند إنهاء دورة ما، بسبب انتهاء المهلة أو أي إجراء آخر، ينبغي أن يطلب من المستعمل إقامة دورة جديدة بإجراء الاستيقان من جديد.	قيام المشترك بإعادة الاستيقان بصورة دورية بواسطة المستيقن أو المستيقنات المناسبة بالقوة اللازمة لتحقيق المستوى المطلوب لضمان استيقان.
SI-25	ينبغي أن تكون أسرار الدورة غير مستمرة. أي أنه ينبغي عدم الاحتفاظ بها خلال إعادة بدء التطبيق المرتبط بها أو إعادة تشغيل الجهاز المضيف.	قيام المشترك بإعادة الاستيقان بصورة دورية بواسطة المستيقن أو المستيقنات المناسبة بالقوة اللازمة لتحقيق المستوى المطلوب لضمان استيقان.

6.8 اختراق خدمة الاستيقان، المخاطر والضوابط

1.6.8 مخاطر اختراق خدمة الاستيقان

اختراق خدمة الاستيقان هو هجوم على الكيان الذي يوفر خدمة الهوية التي تجعله غير صالح، أو غير دقيق، أو غير متاح، أو غير قادر على القيام بوظيفته على النحو المقصود. وينطوي أي مكمن ضعف يمكن استغلاله في بيئة التحكم بنظام معلومات النظام على

إمكانية اختراق خدمة الاستيقان. وأحد الأمثلة على ذلك هو حين يكون المهاجم قادراً على استغلال أحد مواطن الضعف في البرمجيات والذي لم يتم تصحيحه بعد ويتمكن من الحصول على نفاذ مميز غير مصرح به إلى نظام معلومات خدمة الاستيقان.

2.6.8 ضوابط اختراق خدمة الاستيقان

يدرج الجدول 8-7 قائمة بضوابط اختراق خدمة الاستيقان.

الجدول 8-7 – ضوابط اختراق خدمة الاستيقان

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
ASC-1	ينبغي لمقدم خدمة أوراق الاعتماد أن يستخدم ضوابط أمنية مصممة على نحو مناسب لمستوى معين من الأمن على النحو الموصف في المعيار [ISO/IEC 27002] أو في معيار مكافئ.	حماية سلامة خدمة الاستيقان من الاختراق.
ASC-2	ينبغي لمقدم خدمة أوراق الاعتماد أن يضمن استيفاء الحد الأدنى من الضوابط المتعلقة بالضمان بالنظر إلى سياق المخاطر الإجمالية للأنظمة.	حماية سلامة خدمة الاستيقان من الاختراق.
ASC-3	عند إجراء مقارنة بطريقة مركزية، ينبغي تنفيذ إبطال القياسات البيومترية، المشار إليه في التوصية [ISO/IEC 24745] باسم حماية النماذج البيومترية.	حماية خدمة الاستيقان للمعلومات البيومترية.
ASC-4	ينبغي أن يحدد المستيقن نفسه الهدف من الاستيقان، رغم أن بإمكان أجهزة التجفير متعددة العوامل تحديد الهدف عن طريق إعادة إدخال العامل الآخر للاستيقان في النقطة الطرفية التي يستعمل معها المستيقن.	تحديد الهدف من الاستيقان بواسطة المستيقن فقط.
ASC-5	طوال حياة الهوية الرقمية، ينبغي لمقدمي خدمة أوراق الاعتماد الاحتفاظ بسجل بجميع المستيقنات التي ترتبط أو ارتبطت بكل هوية.	تسجيل معلومات المستيقن والاحتفاظ بها.
ASC-6	ينبغي لمقدم خدمة أوراق الاعتماد أو جهة التحقق الاحتفاظ أيضاً بالمعلومات اللازمة لإعاقة محاولات الاستيقان عند الاقتضاء.	تسجيل معلومات المستيقن والاحتفاظ بها.
ASC-7	ينبغي أن يتضمن السجل الذي أنشأه مقدم خدمة أوراق الاعتماد تاريخ ووقت ربط المستيقن بالحساب.	تسجيل معلومات المستيقن والاحتفاظ بها.
ASC-8	ينبغي ربط المستيقنات بحسابات المشتركين عن طريق: • إصدار من مقدم خدمة أوراق الاعتماد كجزء من الانتساب؛ • أو ربط مستيقن مقدم من المشترك يمكن ان يقبله مقدم خدمة أوراق الاعتماد.	ربط المستيقنات بحسابات المشتركين بشكل مناسب.
ASC-9	عند ربط مستيقن جديد بحساب مشترك، ينبغي لمقدم خدمة أوراق الاعتماد أن يضمن تنفيذ بروتوكول الربط والبروتوكول اللازم لتوفير المفتاح أو المفاتيح المرتبطة بالمستيقن بمستوى أمن يتناسب مع مستوى ضمان الاستيقان الذي سيستخدم عنده المستيقن.	ربط المستيقنات بحسابات المشتركين بشكل مناسب.
ASC-10	ينبغي أن يتطلب ربط مستيقنات متعددة العوامل استيقاناً متعدد العوامل أو ارتباطا بالدورة التي استكمل فيها تدقيق الهوية للتو من أجل ربط المستيقن.	ربط المستيقنات بحسابات المشتركين بشكل مناسب.

7.8 الخصوصية، المخاطر والضوابط

1.7.8 مخاطر الخصوصية

يدعم الاستيقان الرقمي حماية الخصوصية من خلال التخفيف من حدة المخاطر المتعلقة بالنفاذ غير المصرح به إلى معلومات الأشخاص. في الوقت نفسه، وبما أن عمليات تدقيق الهوية والاستيقان والترخيص والاتحاد تشمل معالجة معلومات الأشخاص، يمكن لهذه الوظائف أن تنطوي أيضاً على مخاطر متعلقة بالخصوصية. وبالتالي فإن هذه المبادئ التوجيهية تشتمل على متطلبات واعتبارات متعلقة بالخصوصية تساعد في التخفيف من المخاطر المحتملة المرتبطة بالخصوصية.

ويجب على مقدم خدمة أوراق الاعتماد أن يجري تقديراً لمخاطر الاحتفاظ بالسجلات المتعلقة بالخصوصية. وقد يتضمن محتوى تقدير المخاطر المتعلقة بالخصوصية ما يلي:

1 احتمال أن يؤدي الاحتفاظ بالسجلات إلى التسبب بمشكلة للمشترك، من قبيل غزو المعلومات أو النفاذ غير المصرح إليها.

2 الأثر في حال حدوث هذه المشكلة.

ينبغي لمقدمي خدمة أوراق الاعتماد أن يتمكنوا من تقديم مبرر معقول لأي استجابة صادرة عنهم بشأن مخاطر الخصوصية المحددة، بما في ذلك قبول المخاطر وتخفيفها وتقاسمها. واستخدام موافقة المشترك هو شكل من تقاسم المخاطر وبالتالي فمن المناسب استخدامه فقط عندما يكون من المعقول توقع أن يكون لدى المشترك القدرة على تقييم المخاطر المتقاسَمة وقبولها.

2.7.8 ضوابط الخصوصية

يدرج الجدول 8-8 قائمة بضوابط الخصوصية.

الجدول 8-8 – ضوابط الخصوصية

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
P-1	ينبغي أن يختار مقدم خدمة الهوية بالحد الأدنى مستوى مناسباً لضمان الاستيقان عندما تكون المعلومات المحدّدة لهوية الشخص أو المعلومات الشخصية الأخرى متاحة على الإنترنت.	إنفاذ مقدم خدمة أوراق الاعتماد لسياسات الخصوصية وضوابط الخصوصية فيما يتعلق بالاستيقان.
P-2	ينبغي لمقدم أوراق الاعتماد أن يمتثل لسياسات الاحتفاظ بالسجلات الخاصة به وفقاً للقوانين واللوائح والسياسات المعمول بها التي يمكن تطبيقها. وإذا اختار مقدم خدمة أوراق الاعتماد أن يحتفظ بالسجلات بغياب أي متطلبات إلزامية، ينبغي عليه أن يجري عملية إدارة المخاطر، بما في ذلك عمليات تقدير المخاطر المتعلقة بالخصوصية والأمن، من أجل تحديد إلى أي مدى ينبغي الاحتفاظ بالسجلات، وينبغي يبلغ المشترك بسياسة الاحتفاظ هذه.	استيقان مقدم خدمة أوراق الاعتماد من المشتركين وفقاً للقوانين واللوائح والسياسات المعمول بها.
P-3	ينبغي توخي الحرص على ضمان أن يقتصر استعمال المعلومات المحدّدة لهوية الأشخاص على الغرض الأصلي من جمعها.	قيام مقدم خدمة أوراق الاعتماد بجمع أدنى قدر من المعلومات المحددة لهوية الأشخاص لتحقيق المستوى المطلوب لضمان الاستيقان.
P-4	في الحالة التي لا يندرج فيها استعمال المعلومات المحدّدة لهوية الشخص ضمن الاستعمالات المتعلقة بالاستيقان أو لا يمتثل للقوانين أو الإجراءات القانونية، ينبغي لمقدم خدمة أوراق الاعتماد أن يوفر أشعاراً بذلك وأن يحصل على موافقة المشترك.	استيقان مقدم خدمة أوراق الاعتماد من المشتركين وفقاً للقوانين واللوائح والسياسات المعمول بها..

رقم الضوابط	مواصفات الضوابط	النتيجة المرجوة
P-5	ينبغي لمقدم خدمة الهوية أن يجري أو ينشر تقييماً لأثر الخصوصية لتغطية جمع المعلومات المحدّدة لهوية الشخص أو المعلومات الشخصية الأخرى وفقاً للقوانين واللوائح المعمول بها.	إجراء مقدم خدمة أوراق الاعتماد لعمليات تقييم أثر الخصوصية.
P-6	ينبغي لمقدمي خدمة أوراق الاعتماد عدم استخدام أو إفشاء معلومات عن المشتركين لأي غرض غير إجراء الاستيقان، أو التخفيف من الاحتيال المتعلق بها، أو الامتثال للقوانين أو الإجراءات القانونية، إلا إذا قدم مقدم خدمة أوراق الاعتماد إشعاراً واضحاً وحصل على موافقة المشترك بشأن الاستخدامات الإضافية.	استيقان مقدم خدمة أوراق الاعتماد من المشتركين وفقاً للقوانين واللوائح والسياسات المعمول بها.
P-7	ينبغي لمقدم خدمة أوراق الاعتماد أن يستخدم ضوابط الخصوصية المصممة بشكل مناسب والمحددة في المعيار [ISO/IEC 27002] أو في معيار آخر.	إنفاذ مقدم خدمة أوراق الاعتماد لسياسات الخصوصية وضوابط الخصوصية فيما يتعلق بالاستيقان.
P-8	ينبغي لمقدمي خدمة أوراق الاعتماد أن لا يجعلوا الموافقة شرطاً للخدمة.	استيقان مقدم خدمة أوراق الاعتماد من المشتركين وفقاً للقوانين واللوائح والسياسات المعمول بها.
P-9	مع أن بإمكان مقدم خدمة أوراق الاعتماد إسناد مستيقن ذي مستوى AAL منخفض إلى هوية ذات مستوى AAL مرتفع، فإذا تم الاستيقان من المشترك بمستوى AAL منخفض، ينبغي لمقدم خدمة أوراق الاعتماد ألا يعرض للمشترك المعلومات الشخصية حتى وإن تم التأكيد عليها.	قيام مقدم خدمة أوراق الاعتماد بجمع أدنى قدر من المعلومات المحددة لهوية الشخص أو المعلومات الشخصية لتحقيق المستوى المطلوب لضمان الاستيقان.
P-10	ينبغي ألا تكون موافقة المشترك على الاستخدامات الإضافية شرطاً لتوفير خدمات الاستيقان.	استيقان مقدم خدمة أوراق الاعتماد من المشتركين وفقاً للقوانين واللوائح والسياسات المعمول بها.

التذييل I

مثال على الاستيقان القوي باستخدام التوصية [b-ITU-T X.1278]

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I مقدمة

يعرض الإطار العالمي للاستيقان [b-ITU-T X.1277] والبروتوكول من العميل إلى المستيقن/إطار شامل من عاملين [b-ITU-T X.1278] نُهُجاً للاستيقان وضمان الاستيقان توفر استيقاناً قوياً يستند إلى توصيات مفتوحة وصالحة للتشغيل البيني. ويقدم هذا التذييل مثالاً على الاستيقان القوي باستخدام التوصية [b-ITU-T X.1278].

2.I فئات التهديديات

تُعرض التهديدات في فئتين:

1 التهديدات القابلة للتوسع – سواء تمت مهاجمة 1 000 أو 000 000 1 هدف، فليس لذلك أي تأثير على تكاليف الهجمات.

أ) هجمات على المخدّمات عن بُعد وسرقة كلمة السرّ. هذا الهجوم خطير جداً نظراً لعد تمكّن المستعملين من حماية أنفسهم منه – ويتعين على الأطراف المعوّلة القيام بذلك. ولكن المستعملين يمكن أن يزيدوا الأمر سوءاً: فإذا تبادلوا كلمات السرّ عبر عدة أطراف معوّلة، يمكن قرصنة الطرف المعوّل الأقل أمناً ما يؤثر على جميع الأطراف الأخرى.

ب) هجمات على كثير من أجهزة المستعمل عن بُعد. وعلى سبيل المثال، محاولة سرقة البيانات من جهاز بهدف انتحال هوية المستعمل.

ج) يمكن أيضاً أن تؤدي الهجمات على أجهزة المستعمل عن بُعد إلى إساءة استعمال البيانات على أجهزة المستعمل بهدف انتحال هوية المستعمل.

د) هجمات على كثير من أجهزة المستعمل عن بُعد بهدف إساءة استعمال دورة مستيقنة بقوة. ويعرف ذلك باسم هجوم متطفل في متصفّح الويب (MITB).

من المثير للاهتمام أن نلاحظ أن البطاقات الذكية وحدها لا تحمي من إساءة استعمال أوراق الاعتماد نظراً لأنها لا تستطيع معرفة ما إذا كان رقم تعريف الهوية الشخصي قد أدخل من جانب المستعمل أو تم ضخه بواسطة برمجيات ضارة عملت على تصيده احتيالياً من المستعمل قبل ذلك.

2 الهجمات المادية – حيث يطلب النفاذ المادي للجهاز. والهجمات المادية ليست قابلة للتوسع لان سرقة الهواتف الذكية (النشطة) تنطوي على تكاليف كبيرة لكل هدف.

أ) هجمات مادية على أجهزة المستعمل لسرقة البيانات بهدف انتحال الهوية.

ب) هجمات مادية على أجهزة المستعمل لإساءة استعمال البيانات بهدف انتحال الهوية.

3.I التمكن من "الاستيقان القوي بضمان مرتفع" بواسطة التوصية [b-ITU-T X.1278]

يقصد بالاستيقان القوي بضمان مرتفع ما يلي:

1 استخدام عاملين أو أكثر

2 استفادة أحدها على الأقل من تجفير المفتاح العمومي

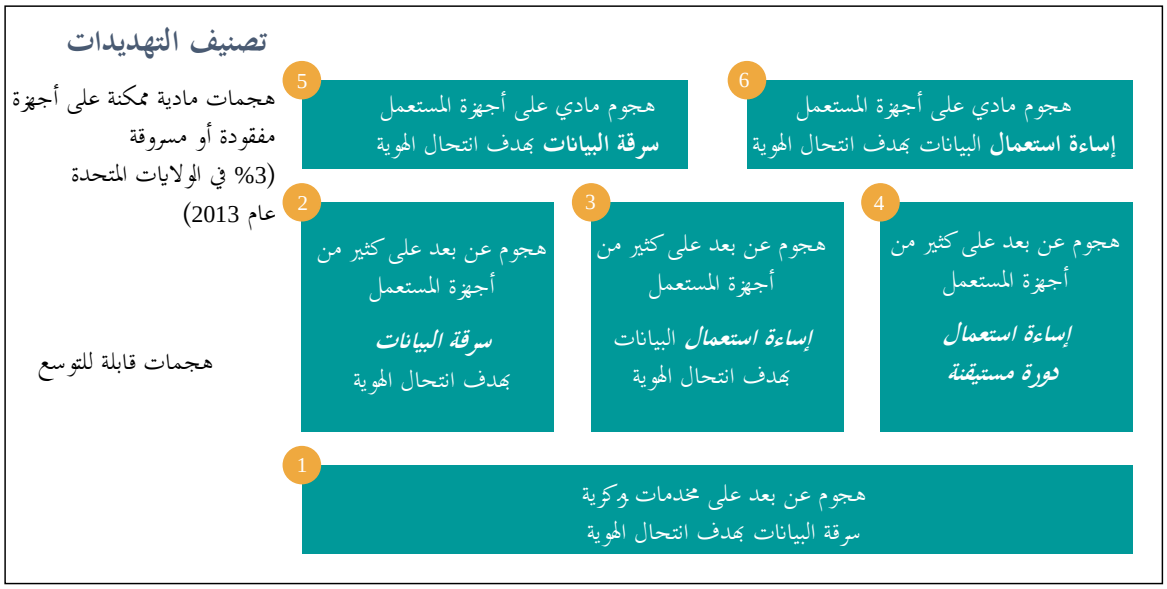
3 عدم التعرض للتصيد الاحتيالي و/أو لمتطفل بين طرفين و/أو لهجمات أخرى تستهدف أوراق الاعتماد

وتشمل المميزات الرئيسية لنهج الهوية السريعة على الإنترنت (FIDO) ما يلي:

- عدم تشارك الأسرار – استعمل ما في حوزتك (مثل أجهزة المعدات) وما أنت عليه (مثل البصمات)؛
- واستعمال تجفير المفتاح العمومي بدلاً من الأسرار المشتركة التناظرية؛
- والتحقق من المستعمل بواسطة مستيقن، وبعد ذلك يستيقن المستيقن بواسطة الطرف المعول؛
- واستيقان متعدد العوامل مقاوم للتصيد الاحتيالي.

تدعم هذه النهج المبادئ التالية للأمن والخصوصية:

- عدم إمكانية الربط بين الخدمات أو الحسابات؛
- عدم وجود طرف ثالث في البروتوكول؛
- عدم خروج القياسات البيومترية، عند استعمالها، من الجهاز؛
- بقاء مفاتيح التجفير في الجهاز؛
- عدم وجود أسرار مشتركة على جانب المخدم؛
- أساس التجفير القائم على المفتاح العمومي.



X.1254(20)_FI.1

الشكل 1.I – تصنيف التهديدات

4.I الاستيقان القديم بواسطة كلمات السرّ

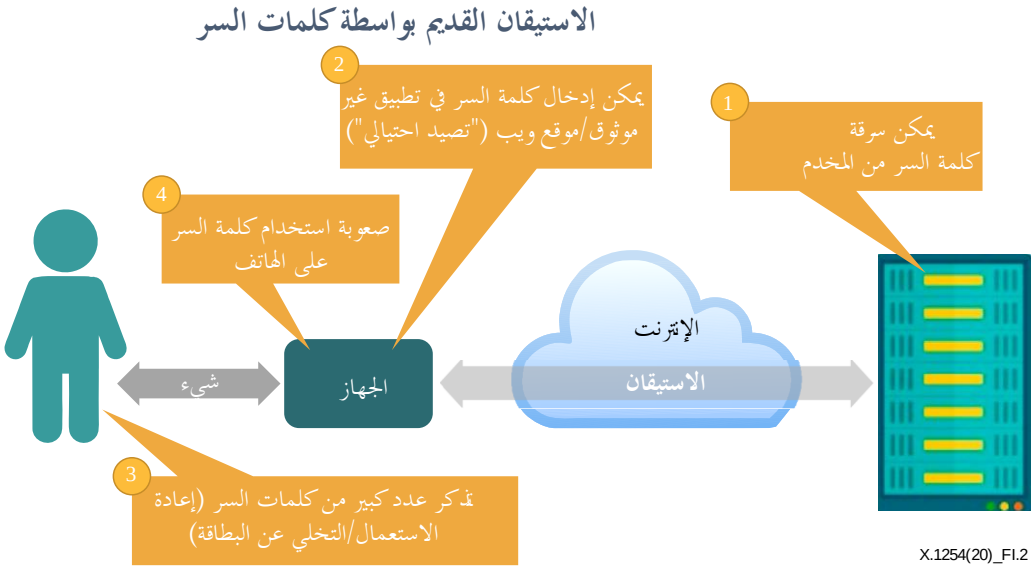
تنطوي عمليات الاستيقان العادية القائمة على كلمات السرّ على مخاطر متأصلة كما هو مبين في الشكل I-2:

1 إمكانية سرقة كلمات السرّ من المخدّم (انتهاك البيانات)؛

2 إمكانية إدخال كلمات السرّ في تطبيقات أو مواقع ويب غير موثوقة (التصيد الاحتيالي)؛

3 العدد الكبير من كلمات السرّ التي يجب تذكرها مما يؤدي إلى إعادة استعمالها بشكل أكبر (من الأسهل تخمين كلمات السرّ عبر المواقع)؛

4 صعوبة طباعة كلمات السرّ على الهواتف (يختار المستعملون كلمات سرّ يسهل تخمينها).



الشكل 2.I – الاستيقان القديم بواسطة كلمات السرّ

5.I الاستيقان الجديد بواسطة التوصية [b-ITU-T X.1278]

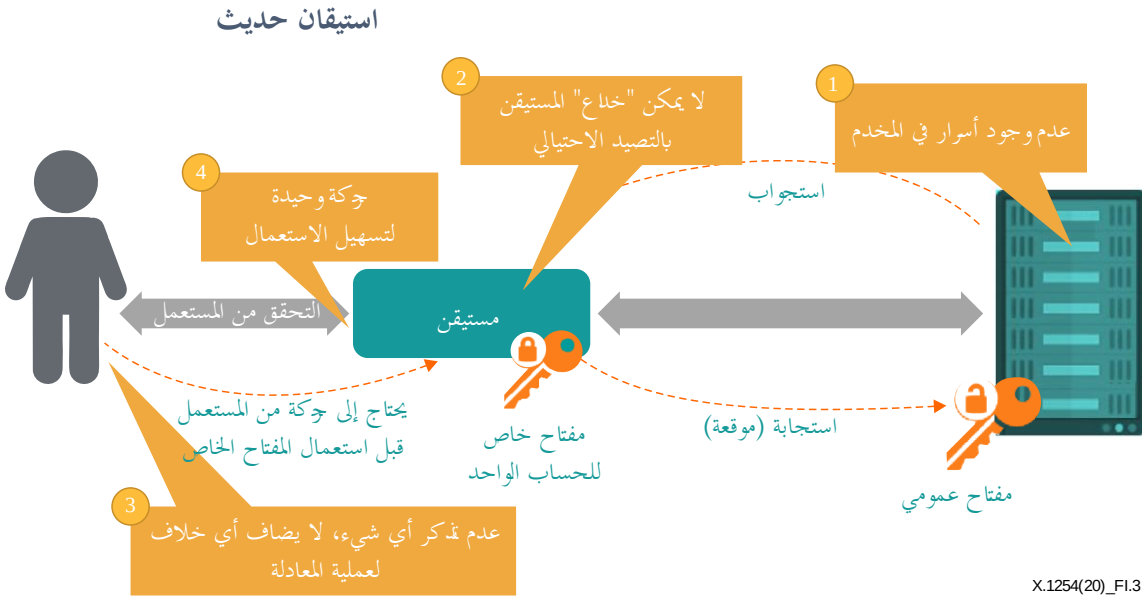
يفصل نهج الهوية السريعة على الإنترنت جانب الاستيقان عن جانب الهوية. ويبين الشكل 3.I فوائد هذا النهج:

1 عدم تخزين الأسرار في المخدّم (حماية من انتهاك البيانات)؛

2 عدم القدرة على خداع المستيقنات بواسطة التصيد الاحتيالي؛

3 عدم الاضطرار لتذكر كلمات السرّ وعدم إضافة احتكاك إلى عملية الاستيقان؛

4 وحركة وحيدة لتسهيل الاستعمال.



الشكل 3.I – الاستيقان الجديد مع التوصية [b-ITU-T X.1278]

6.I قابلية التشغيل البيني وإصدار الشهادات

بالإضافة إلى استحداث طرق جديدة للاستيقان، تزداد قوة الحلول المتعلقة بالاستيقان عن طريق اختبار قابلية التشغيل البيني وإصدار الشهادات.

- زيادة قبول المستعمل أو المستهلك للاستيقان القوي.
- انخفاض مخاطر وآثار سرقة الهوية من خلال انتشار أوسع للاستيقان القوي.
- السهولة وتحسين تجربة المستعمل من خلال مجموعة واسعة من أجهزة وخدمات الاستيقان.
- زيادة اعتماد الاستيقان القوي عن طريق خفض التكاليف.

بيبليوغرافيا

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1254 (2012)] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework*.

[b-ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework*.

[b-ITU-T X.1278] Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework.*

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 24745] ISO/IEC 24745:2011, *Information technology — Security techniques — Biometric information protection*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT security and privacy – A framework for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2018), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

[b-ISO/IEC TS 29003] Technical Specification ISO/IEC TS 29003:2018, *Information technology – Security techniques – Identity proofing*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework*.

[b-IETF RFC 7231] IETF RFC 7231 (2014), *Hypertext transfer protocol (HTTP/1.1): Semantics and content*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021