الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1127

(2017/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (1) – أمن الخدمات المتنقلة

المتطلبات الأمنية الوظيفية والمعمارية الوظيفية لتدابير مكافحة سرقة الهواتف المتنقلة

التوصية ITU-T X.1127

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
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
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

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

التوصية ITU-T X.1127

المتطلبات الأمنية الوظيفية والمعمارية الوظيفية لتدابير مكافحة سرقة الهواتف المتنقلة

ملخص

تركز التوصية ITU-T X.1127 على المتطلبات الأمنية الوظيفية والمعمارية الوظيفية لآليات مكافحة سرقة الهواتف الذكية استناداً إلى المتطلبات العامة التي وصفتها جمعية النظام العالمي للاتصالات المتنقلة (GSMA).

وإذ تنتشر الهواتف الذكية بسرعة فقد أصبحت جزءاً لا غنى عنه تقريباً من الحياة اليومية. ولسوء الحظ، تُسرق هواتف العديد من مستخدمي الهاتف الذكي. وينبغي للتدابير المضادة لسرقة الهواتف الذكية، أي أداة التبديل المعطِّل المستخدَمة في حالة فقدها أو سرقتها، أن تتيح القدرة على القيام بما يلي:

- الحذف عن بُعد لبيانات المستخدم المخوَّل الموجودة على الهاتف الذكي؛
- جعل الهاتف الذكي غير صالح للعمل على يد مستخدم غير مخوَّل باستخدامه؛
- منع إعادة التفعيل دون إذن المستخدم المخوَّل إلى أقصى حد ممكن من الناحية التكنولوجية؛
- معاودة جعل الهاتف الذكي صالحاً للعمل إذا استعاده المستخدم المخوَّل، واستعادة بيانات المستخدم على الهاتف الذكي إلى أقصى حد ممكن.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1127	2017-09-06	17	11.1002/1000/13259

مصطلحات أساسية

تدابير مكافحة السرقة، الهاتف المتنقل، المتطلبات الأمنية.

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بحرف الهوية الفريد للتوصية. ومثال على 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 "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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1127

المتطلبات الأمنية الوظيفية والمعمارية الوظيفية لتدابير مكافحة سرقة الهواتف المتنقلة

1 مجال التطبيق

تتناول هذه التوصية المتطلبات الأمنية الوظيفية والمعمارية الوظيفية لتدابير مكافحة سرقة الهواتف المتنقلة (أي مفتاح تعطيل)، بما يسمح للمستعملين بالقيام عن بُعد بحذف بياناتهم الشخصية أو تعطيل أجهزة الهاتف الذكي المسروقة أو المفقودة.

وتُتوقع إمكانية أن تنطبق متطلبات الأمن الوظيفي والمعمارية الوظيفية المحددة في هذه التوصية على الهواتف الذكية القادرة على تقديم تدابير مضادة للسرقة تعبِّر عن رغبات عملاء الهواتف الذكية ومصنعي الهواتف الذكية ومشغلي الخدمات المتنقلة.

وتركز هذه التوصية على المتطلبات الوظيفية، والمعمارية الوظيفية، وآليات مكافحة السرقة. وهي تستخدم نموذجاً مرجعياً يتكون من مالك الجهاز، والمخدِّم المخوَّل، والمخدِّم الرديف، والأجهزة المفقودة أو المسروقة. ويرد في التذييل III وصف للتهديدات المحددة في مجال مكافحة السرقة. ولا تعدل هذه التوصية المتطلبات العامة لميزات الهاتف الذكي المضادة للسرقة التي وضعتها جمعية النظام العالمي للاتصالات المتنقلة (GSMA) [b-GSMA].

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية حالياً. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1254] التوصية ITU-T X.1254 (2012)، *إطار ضمان استيقان الكيان*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 تعقيم البيانات (data sanitization) [b-NIST SP 800-88]: الإجراءات المتخذة لجعل البيانات المكتوبة على الوسائط غير قابلة للاسترداد بالوسائل العادية وغير العادية.

2.1.3 ضمان الاستيقان من كيان (EAA) [ITU-T X.1254]: 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]).

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

3.1.3 الهوية (identity) [b-ITU-T X.1250]: تمثيل لكيان على شكل عنصر معلومات واحد أو أكثر يتيح للكيان (الكيانات) أن يكون متميزاً في سياق ما. ويعني مصطلح الهوية لأغراض إدارة الهوية هوية سياقية (مجموعة من النعوت) مثل: يتحدد تنوع النعوت بإطار له شروط حدود معرّفة (السياق) يتواجد فيها الكيان ويتفاعل.

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

4.1.3 مفتاح التعطيل (kill switch) [b-GSMA]: طريقة لتعطيل وظائف حرجة لجهاز متنقل.

ملاحظة – إنه في الأساس وظيفة داخل جهاز المعدات المتنقلة، فإذا فُعِّلت مثلاً برسالة ذات نسق ما تُرسَل إليه، كف الجهاز المتنقل عن العمل على النحو المقصود منه، ولا تتسنى إعادة إعماله أو إعادة استخدامه إلا إذا خوَّل مالك الجهاز بإعادة إعمال الجهاز.

5.1.3 الهاتف المتنقل (mobile phone) [b-ITU-T X-Sup.19]: جهاز إلكتروني يُستخدم لإجراء النداءات الهاتفية وإرسال الرسائل النصية عبر منطقة جغرافية واسعة عن طريق النفاذ الراديوي إلى الشبكات المتنقلة العمومية، مع تمكين المستعمل من التنقل.

6.1.3 الهاتف الذكي (smartphone) [b-ITU-T X-Sup.19]: هاتف متنقل بقدرات حوسبة قوية وتوصيلية بين أطراف غير متجانسة ونظام تشغيل متقدم يوفر منصة لتطبيقات الأطراف الثالثة. ويمكن للمستعملين استناداً إلى نظام التشغيل تثبيت وتشغيل التطبيقات بسهولة. وترتبط الهواتف الذكية بصفة عامة بمنافذ التطبيقات على الخط المتوفرة للمطورين من أجل نشر التطبيقات وللمستعملين من أجل تنزيلها.

7.1.3 تهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب يمكن أن يؤدي إلى ضرر لنظام أو لمنظمة.

8.1.3 النفق (tunnel) [b-ISO/IEC 27033-1]: مسير بيانات بين الأجهزة المترابطة شبكياً المنشأة عبر البنية التحتية الشبكية القائمة.

ملاحظة – يمكن إنشاء الأنفاق باستخدام تقنيات مثل تغليف البروتوكول، أو تبديل الوسوم، أو الدارات الافتراضية.

2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 عتاد الجهاز (device hardware): المكونات المادية التي تجعل معاً جهازاً متنقلاً يعمل، بما في ذلك الشاشة، والمفاتيح، ولوحات الدارات المطبوعة، والرقائق، وبطاقة SIM، والتخزين القابل للإزالة، وما إلى ذلك.

2.2.3 برمجيات الجهاز (device software): جميع برامج البرمجيات على الجهاز وبطاقة SIM، بما في ذلك التطبيقات، ونظام التشغيل، ومحمِّل الإقلاع، وذاكرة ROM للإقلاع، والبرمجيات الثابتة.

3.2.3 مستخدم الجهاز (device user): المستخدم المخوَّل للجهاز المتنقل.

4.2.3 النفق الآمن (secure tunneling): بروتوكول يسمح بالنقل الآمن للبيانات أو الرسائل من موقع شبكة إلى آخر.

ملاحظة – يدعم النفق الآمن عموماً الاستيقان من كيان، وسلامة الرسالة، وكتمان الرسالة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

ATM آلة الصرّاف الآلي *(Automated Teller Machine)*

CRL قائمة إلغاء الشهادة *(Certificate Revocation List)*

DER قواعد التشفير المميزة *(Distinguished Encoding Rules)*

DDoS رفض الخدمة الموزع *(Distributed Denial-of-Service)*

DM إدارة الجهاز *(Device Management)*

EAA ضمان الاستيقان من كيان *(Entity Authentication Assurance)*

GPS النظام العالمي لتحديد الموقع *(Global Positioning System)*

GSMA جمعية النظام العالمي للاتصالات المتنقلة *(Groupe Speciale Mobile Association)*

HTTP بروتوكول نقل النص التشعبي *(Hyper-Text Transfer Protocol)*

LoA مستوى الضمان *(Level of Assurance)*

MAC شفرة الاستيقان من رسالة *(Message Authentication Code)*

OCSP بروتوكول حالة الشهادة على شبكة الإنترنت *(Online Certificate Status Protocol)*

OMA تحالف الاتصالات المتنقلة المفتوحة *(Open Mobile Alliance)*

OTP كلمة مرور لمرة واحدة *(One-Time Password)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable Information)*

PKI البنية التحتية للمفتاح العمومي *(Public-Key Infrastructure)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SMS-SC مركز خدمة – خدمة الرسائل القصيرة *(Short Message Service – Service Centre)*

SSL طبقة مقبس آمن *(Secure Socket Layer)*

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

TFA الاستيقان بثلاثة عوامل *(Three-Factor Authentication)*

TLS أمن طبقة النقل *(Transport Layer Security)*

U شاملة *(Universal)*

UICC بطاقة الدارة المتكاملة الشاملة *(Universal Integrated Circuit Card)*

USSD بيانات الخدمات التكميلية غير المهيكلة *(Unstructured Supplementary Service Data)*

2FA الاستيقان بعاملين *(2-Factor Authentication)*

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 نظرة عامة على تدابير مكافحة السرقة

1.6 تدابير مكافحة السرقة

فيما تنتشر الهواتف الذكية بسرعة فقد أصبحت جزءاً لا غنى عنه من الحياة اليومية. بيد أن هواتف الملايين من مستخدمي الهاتف الذكي تتعرض للسرقة. وينبغي للتدابير المضادة لسرقة الهواتف الذكية، أي أداة التبديل المعطِّل، أن تتيح القدرة على القيام بما يلي:

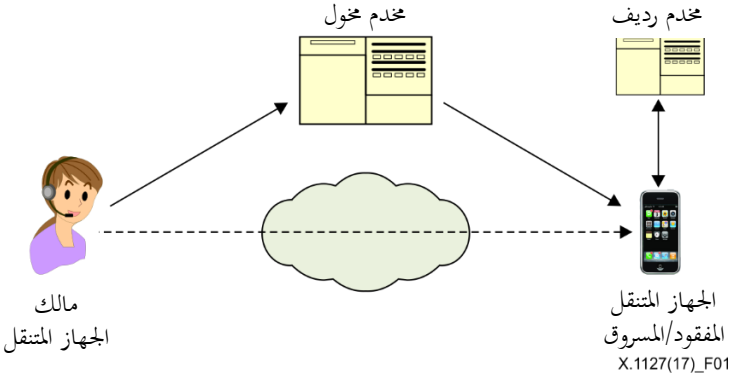
- الحذف عن بُعد لبيانات المستخدم الشخصية الموجودة على الهاتف الذكي في حال فُقد أو سُرق؛
- جعل الهاتف الذكي غير صالح للعمل على يد مستخدم غير مخوَّل باستخدامه؛
- إذا لزم الأمر، تخزين البيانات الشخصية للمستخدم في المخدِّم الرديف الذي يشغِّله مشغلو الخدمة الخلوية أو مصنعو الأجهزة؛
- منع إعادة التفعيل دون إذن المستخدم المخوَّل؛
- معاودة جعل الهاتف الذكي صالحاً للعمل إذا استعاده المستخدم المخوَّل، واستعادة بيانات المستخدم على الهاتف الذكي إلى أقصى حد ممكن من المخدِّم الرديف.

ويمكن لبرمجيات مكافحة السرقة، المثبتة في جهاز متنقل، تعطيل الهاتف المسروق أو المفقود.

وعندما يدرك مالك الجهاز أن جهازه المتنقل قد فُقد أو سُرق، هناك سيناريوهان لبدء تنفيذ ميزات التعطيل:

1) يتصل مالك الجهاز بمشغل الخدمة الخلوية الذي يوعز بتعطيل الجهاز المتنقل؛

2) يشغِّل مالك الجهاز تطبيقاً على جهاز متنقل آخر، أو ينفذ إلى أداة تعطيل تجعل الجهاز المتنقل المفقود/المسروق غير قابل للتشغيل.



الشكل 1 – النموذج المرجعي لتدابير مكافحة السرقة

يصف الشكل 1 النموذج المرجعي لتدابير مكافحة سرقة الأجهزة المتنقلة. ويدعم المخدِّم المخوَّل وظيفة تعطيل الأجهزة المتنقلة، المسروقة أو المفقودة، التي يشغِّلها مقدمو الخدمة الخلوية أو مصنعو الأجهزة. ويرسل المخدِّم المخوَّل تعليمات تعطيل الجهاز المتنقل المسروق/المفقود. ويستعيد المخدِّم الرديف البيانات الشخصية للجهاز المتنقل بناء على طلب مالك الجهاز.

وتنبغي حماية الاتصال بين الجهاز المتنقل المفقود/المسروق والمخدِّم المخوَّل باستخدام نفق آمن (طبقة المقبس الآمن (SSL)، على سبيل المثال). بالإضافة إلى ذلك، تنبغي حماية الاتصال بين الجهاز المتنقل المفقود/المسروق والمخدِّم الرديف باستخدام نفق آمن (طبقة المقبس الآمن (SSL)، على سبيل المثال).

وتستند هذه التوصية إلى إطار ضمان الاستيقان من كيان (EAA) لإدارة هذا الضمان الذي يرد وصفه في التوصية [ITU-T X.1254]. ويحدد إطار ضمان الاستيقان من كيان أربعة مستويات ضمان (LoA) للاستيقان من كيان. 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.

وقد تطلب بعض الولايات القضائية تثبيت برمجيات مكافحة السرقة أو إتاحتها للتنزيل عبر الإنترنت. ففي الولايات المتحدة، على سبيل المثال، تفرض ولاية كاليفورنيا تثبيت برمجيات مكافحة السرقة على الهواتف الجديدة مع تمكين المستخدمين من تعطيل هذه الميزة، على الرغم من أنها مفعَّلة مبدئياً. وبعرض خيار التخلي عن ميزة مكافحة سرقة بدلاً من خيار الاشتراك فيها، يُتوقع أن يستخدم العديد من العملاء تدابير مكافحة سرقة وبالتالي، مما يعزز كثيراً من احتمال حماية أي جهاز متنقل.

2.6 المتطلبات الإجمالية لتدابير مكافحة السرقة

فيما يلي المتطلبات الأمنية الإجمالية لتدابير مكافحة السرقة عند نقل الرسائل المضادة للسرقة من المخدِّم المخوَّل إلى الجهاز المتنقل:

- الاستيقان من الكيان؛
- سلامة الرسالة؛
- كشف التكرار وسلامة التسلسل؛
- إثبات الاستلام وإثبات التنفيذ؛
- كتمان الرسائل؛
- بيان آليات الأمن المستخدمة.

7 المعمارية الوظيفية لتدابير مكافحة سرقة الهاتف المتنقل

1.7 التهديدات لتدابير مكافحة سرقة الهاتف المتنقل

تصف هذه الفقرة مجموعة من تهديدات الأمن المعرَّفة التي تتناولها بعض متطلبات أو آليات هذه التوصية. وقد تم تناول نموذج تهديد الأمن والمواد الأساسية الأخرى طبقاً لتوصيات قطاع تقييس الاتصالات التالية:

- تُعرِف التوصية [b-ITU-T X.800] عناصر المعمارية العامة المعنية بالأمن والتي يمكن تطبيقها بصورة ملائمة في الظروف التي تحتاج إلى حماية الاتصال فيما بين النظم المفتوحة.
- وتُعرِف التوصية [b-ITU-T X.805] معمارية أمن الشبكة لتوفير أمن الشبكة من طرف إلى طرف.

وتحدد التوصيتان [b-ITU-T X.800] و[b-ITU-T X.805] التهديدات الأمنية التالية للشبكات:

- إتلاف المعلومات و/أو الموارد الأخرى؛
- إفساد المعلومات أو تعديلها؛
- سرقة المعلومات و/أو الموارد الأخرى أو إزالتها أو خسارتها؛
- إفشاء معلومات؛
- انقطاع خدمات.

وتحدد هذه التوصية التهديدات التالية الخاصة بتدابير مكافحة سرقة الهاتف المتنقل:

- طلب غير مخوَّل يدعو لحذف بيانات من هاتف متنقل عُطِّل؛
- طلب غير مخوَّل يدعو لتعطيل الهاتف المتنقل؛
- كشف غير مخوَّل عن بيانات حساسة على هاتف متنقل؛
- فقدان بيانات مستخدم على هاتف متنقل؛
- نفاذ غير مخوَّل إلى و/أو تعديل وظائف أو بيانات جهاز عُطِّل؛

– كشف غير مخوَّل عن بيانات وبرمجيات مستخدم يجري تبادلها بين الجهاز ومشغل الشبكة و/أو أداة تعطيل ضمن تدابير مكافحة السرقة.

وتتمثل المخاطر فيما يلي:

– تمكّن القراصنة من العثور على وسيلة لاختطاف تعليمة التعطيل وإيقاف الجهاز المتنقل؛

– إمكانية الكشف عن البيانات الشخصية المخزنة في المخدِّم الرديف أو العابرة بين الجهاز المتنقل والمخدِّم الرديف.

2.7 وظائف الأمن الرئيسية في تدابير مكافحة سرقة الهاتف المتنقل

يجب ألا تنفَّذ وظائف تعطيل جهاز متنقل إلا من مخدِّم مخوَّل أو أداة تعطيل تدعم وظيفة التعطيل. وللإيفاء بهذا المتطلب، يلزم القيام بالوظائف الخمس التالية:

1) توصيلة اتصال آمن بين الجهاز والمخدِّم؛

2) استيقان مخدِّم الجهاز من الكيان؛

3) استيقان جهاز المخدِّم، والمخدِّم الجاري تخويله لأداء الوظيفة، من الكيان؛

4) تتبع موقع الجهاز المتنقل المسروق؛

5) التخزين الرديف للبيانات/حذفها على هاتف متنقل عُطِّل.

وينبغي تقديم آلية من خلال الموقع الإلكتروني الشخصي للسماح لأصحاب الأجهزة بإدارة المعلومات المحددة لهوية شخصهم (PII) ثم تخزينها. ويمكن تزويد مالك الجهاز المتنقل بالتطبيق المثبت في الجهاز. ويمكن أن يسمح تطبيق مكافحة السرقة لأصحاب الأجهزة باختيار البيانات بما في ذلك المعلومات المحددة لهوية شخصهم لمكافحة السرقة وبإشراك الرديف التلقائي للبيانات بما فيها المعلومات المحددة لهوية شخصهم في حل التخزين السحابي. ويتكون إجراء هذه الإدارة من الخطوات الثلاث التالية:

1) تثبيت التطبيقات على الجهاز المتنقل؛

2) قيام مقدمي الخدمة المتنقلة أو مصنعي الأجهزة بتسجيل الجهاز في الموقع الإلكتروني؛

3) إدارة (أي حذف وتنزيل ورفع) المعلومات المحددة لهوية شخص (PII) المخزنة في المخدِّم الرديف من خلال الموقع الإلكتروني الشخصي.

3.7 المعمارية الوظيفية لتدابير مكافحة سرقة الجهاز المتنقل

تستند المعمارية الوظيفية لتدابير مكافحة سرقة الجهاز المتنقل إلى معمارية الأمن الموصوفة في المرجع [b-3GPP TS 33.102]. ويصف الشكل 2 معمارية الأمن المكونة من خمس مجموعات أمنية على النحو التالي:

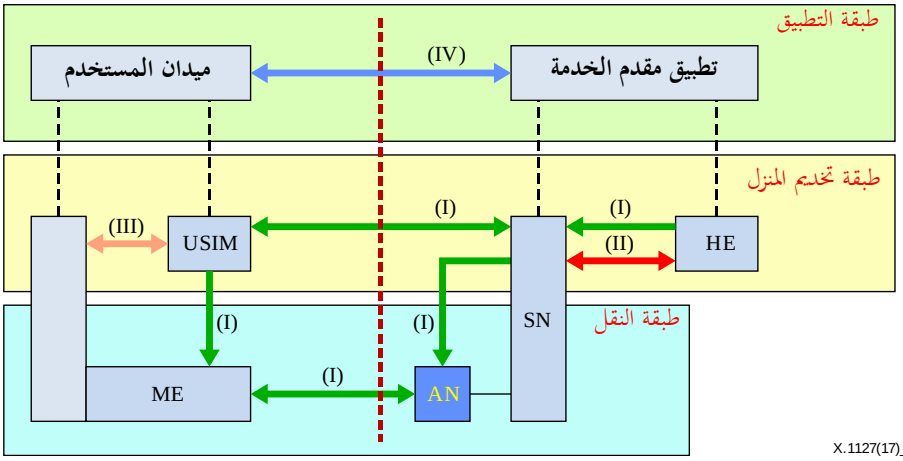
1) أمن النفاذ إلى الشبكة '1': مجموعة الميزات الأمنية التي تزود المستخدمين بالنفاذ الآمن إلى خدمات الجيل الثالث، والتي تحمي بشكل خاص من الهجمات على وصلة النفاذ (الراديوية)؛

2) أمن ميدان الشبكة '2': مجموعة الميزات الأمنية التي تمكن العقد في ميدان مقدم الخدمة من تبادل بيانات التشوير بشكل آمن، ومن اتقاء الهجمات على الشبكة السلكية؛

3) أمن ميدان المستخدم '3': مجموعة الميزات الأمنية التي تضمن النفاذ إلى المحطات المتنقلة؛

4) أمن ميدان التطبيق '4': مجموعة الميزات الأمنية التي تمكن التطبيقات لدى المستخدم وفي ميدان مقدم الخدمة من تبادل الرسائل بشكل آمن؛

5) إمكانية رؤية وإمكانية تشكيل الأمن '5': مجموعة الميزات التي تمكن المستخدم من تبين ما إذا كانت ميزة الأمن قيد التشغيل أم لا، وما إذا كان استخدام الخدمات وتقديمها ينبغي أن يعتمدا على ميزة الأمن.



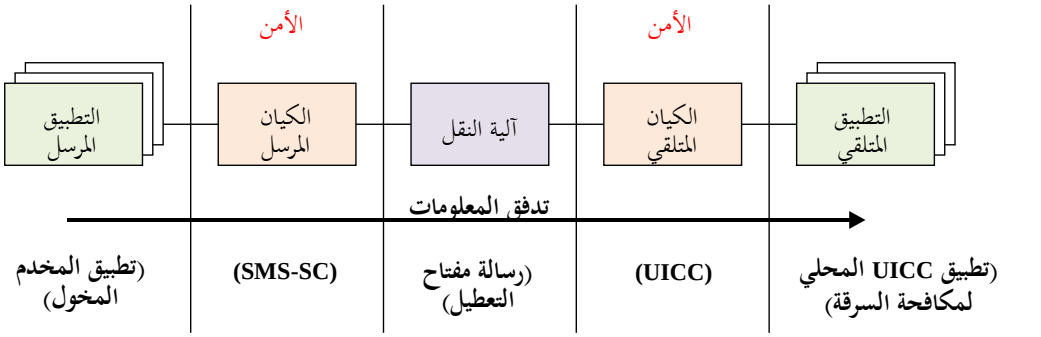
ملاحظة – أُخذ الشكل 2 من المرجع [b-3GPP TS 33.102].

الشكل 2 – معمارية الأمن

يشكل تطبيق تدابير مكافحة السرقة في الجهاز المتنقل جزءاً من مجموعة من التطبيقات التي تقع في ميدان المستخدم، في حين تشكل وظيفة مكافحة السرقة لدى مقدم الخدمة جزءاً من مجموعة من التطبيقات المقيمة في تطبيق مقدم الخدمة.

ويستند النموذج المرجعي الأمني لتدابير مكافحة السرقة إلى نموذج موصوف في المرجع [b-3GPP TS 22.048]. والتطبيق المرسِل هو كيان يولد رسالة تطبيق لإرسالها، في حين أن الكيان المرسِل هو الكيان الذي تنشأ منه الرزمة المؤمَّنة (مثل خدمة الرسائل القصيرة – مركز الخدمة (SMS-SC) أو بطاقة الدارة المتكاملة الشاملة (UICC) أو نقطة إدخال بيانات الخدمة التكميلية غير المهيكلة (USSD) أو مخدِّم مجموعة أدوات وحدة هوية المشترك (SIM) الشاملة (U) المخصصة، وحيث تستدعى آليات الأمن). ويولد الكيان المرسل الرزم المؤمَّنة المراد إرسالها. وتُرسَل الرزم المؤمَّنة من خلال النفق الآمن على مستوى النقل أو النفق الآمن على مستوى التطبيق.

أما التطبيق المستقبِل فهو الكيان الذي تتجه إليه رسالة التطبيق في حين أن الكيان المستقبِل هو الكيان الذي تُستقبل فيه الرزمة المؤمَّنة (مثل خدمة الرسائل القصيرة – مركز الخدمة (SMS-SC) أو بطاقة الدارة المتكاملة الشاملة (UICC) أو نقطة إدخال بيانات الخدمة التكميلية غير المهيكلة (USSD) أو مجموعة أدوات وحدة هوية المشترك (SIM) الشاملة (U) المخصصة).



ملاحظة – أُخذ الشكل 3 من المرجع [b-3GPP TS 22.048]

الشكل 3 – النموذج المرجعي للأمن

تستند معمارية الأمن في هذه التوصية إلى النموذج المرجعي في الشكل 1، ومعمارية الأمن في الشكل 2 والنموذج المرجعي للأمن في الشكل 3.

4.7 آليات لتدابير مكافحة سرقة الهاتف المتنقل

1.4.7 آليات الاتصال الآمن

ينبغي أن يتصرف الجهاز المفقود أو المسروق كمخدِّم استيقان من عميل نفق آمن.

وينبغي أن تستوفي قناة الاتصال بين العميل والمخدِّم المتطلبات الأمنية الستة التالية:

1) الكتمان: ينبغي أن يضمن النفق الآمن عجز الكيانات غير المخوَّلة عن قراءة البيانات. ويُنجز ذلك عن طريق تجفير البيانات باستخدام خوارزمية تجفير ومفتاح سري – أي قيمة لا يعرفها سوى الكيانين اللذين يتبادلان البيانات. ولا يمكن فك تجفير البيانات إلا بواسطة كيان لديه المفتاح السري.

2) السلامة: يجب أن يحدد النفق الآمن ما إذا كانت البيانات قد تغيرت (قصداً أو عن غير قصد) أثناء العبور. ويجب ضمان سلامة البيانات من خلال توليد قيمة لشفرة الاستيقان من رسالة (MAC)، وهي جمع اختباري تجفيري للبيانات يُدخَل عبر لوحة مفاتيح. فإذا غُيرت البيانات وأعيد حساب شفرة الاستيقان من رسالة (MAC)، ستختلف شفرتا MAC القديمة والجديدة.

3) استيقان الأقران: يجب أن تؤكد كل نقطة طرفية هوية النقطة الطرفية الأخرى التي ترغب في الاتصال بها، مما يضمن إرسال حركة الشبكة والبيانات من المضيف المتوقع. ويجرى استيقان النفق الآمن عادة في اتجاه واحد، أي الاستيقان من المخدِّم إلى العميل؛ بيد أن استيقان النفق الآمن يتطلب الاستيقان من كلتا النقطتين الطرفيتين.

4) الحماية من التكرار: لا تسلَّم البيانات نفسها عدة مرات، ويجب أن لا تسلَّم البيانات المخلة إخلالاً جسيماً بترتيبها. ويمكن استخدام رقم تتابع أو عداد في مصدر الرسالة. ويضيف المصدر أو الرسالة رقماً متسلسلاً إلى رزمته أو رزمتها بدءاً من 0 ويتصاعد الرقم في كل مرة تُرسل فيها رسالة أخرى.

5) حماية تحليل الحركة: يجب على شخص يراقب حركة الشبكة ألا يحدد محتوى حركة الشبكة أو كم تبادل المعلومات. ويمكن أيضاً أن يخفي النفق الآمن الأطراف التي تتواصل، في حين أن طبقة المقبس الآمن تترك هذه المعلومات مكشوفة. وتمكن أيضاً حماية تواتر الاتصالات تبعاً للتنفيذ. ومع ذلك، يمكن حساب عدد الرزم الجاري تبادلها.

6) التحكم في النفاذ: يجب أن تقوم النقطتان الطرفيتان في النفق الآمن بإجراء اصطفاء للتأكد من أن المستخدمين المخوَّلين فقط يمكنهم النفاذ إلى موارد معينة للشبكة. ويمكن أيضاً أن تسمح النقطتان الطرفيتان في النفق الآمن أو تمنع أنواع معينة من الحركة في الشبكة، مثل السماح بالنفاذ إلى مخدِّم الإنترنت ولكن منع تبادل الملفات.

ولتلبية المتطلبات المذكورة أعلاه، يوصى باستخدام أمن طبقة النقل (TLS) لتأمين الاتصالات بين الجهاز المتنقل والمخدِّم المخوَّل. وأمن طبقة النقل هو بروتوكول يقدم نفق اتصال آمن عبر الشبكات. وهو يسمح لتطبيقات العميل/المخدِّم بالاتصال بطريقة مصممة لمنع التنصت أو التلاعب أو تزوير الرسائل. ويتربع أمن طبقة النقل على قمة بروتوكولات النقل الموثوق بها (كبروتوكول التحكم في الإرسال (TCP))، ويستخدم لتغليف مختلف البروتوكولات ذات المستوى الأعلى (كبروتوكول نقل النص التشعبي (HTTP)).

ويتكون أمن طبقة النقل (TLS) من ثلاث مراحل أساسية:

1) التفاوض بين الأقران لدعم خوارزمية؛

2) تبادل المفاتيح والاستيقان؛

3) تجفير الشفرة المتناظر والاستيقان من الرسالة.

ويرد في التذييل V ملف تعريف تفصيلي لأمن طبقة النقل.

وبالإضافة إلى ذلك، توصي هذه التوصية أيضاً باستخدام قناة الاتصال الآمنة القائمة على بروتوكول تحالف الاتصالات المتنقلة المفتوحة (OMA).

2.4.7 آليات الاستيقان المتبادل

يعمل الاستيقان على تأكيد هويات الكيانات التي تتواصل. وهناك ثلاثة أنواع من عوامل الاستيقان:

1) عامل المعرفة ("شيء لا يعرفه إلا المستخدم")، مثل كلمات المرور؛

2) عامل الحيازة ("شيء لا يمتلكه إلا المستخدم")، مثل بطاقات آلة الصراف الآلي (ATM)؛

3) عامل التأصل ("شيء متأصل في المستخدم وحده")، مثل القياسات البيومترية.

وتصف التوصية [b-ITU-T X.1158] ثلاثة أنواع من أساليب الاستيقان:

1) الاستيقان بعامل واحد (SFA) هو الأسلوب التقليدي الذي لا يتطلب إلا اسم المستخدم وكلمة المرور قبل منح النفاذ إلى المستخدم؛

2) الاستيقان بعاملين (2FA) يقوم على الجمع بين عاملي استيقان مختلفين. وقد يكون هذان العاملان شيئاً يعرفه المستخدم، أو شيئاً يمتلكه المستخدم أو شيئاً يتسم به المستخدم. وثمة مثال جيد، من الحياة اليومية، عندما يريد المستخدم سحب مال من صراف آلي، فلا يتسنى له القيام بذلك إلا بالجمع الصحيح بين بطاقة مصرفية (شيء يمتلكه المستخدم) ورقم التعريف الشخصي (PIN، أي شيء يعرفه المستخدم)؛

3) الاستيقان بثلاثة عوامل (TFA) يقوم على الجمع بين ثلاثة عوامل مختلفة مستقلة: ما يعرفه المستخدم (كلمة المرور) وما يمتلكه المستخدم (تأشيرة الأمن) وما يتسم به المستخدم (التحقق البيومتري).

ويستند الاستيقان المتعدد العوامل على الجمع بين عاملين مختلفين مستقلين أو أكثر. ويشكل الاستيقان بعاملين والاستيقان بثلاثة عوامل جزءاً من الاستيقان متعدد العوامل.

3.4.7 آليات الحذف الآمن للبيانات

يشير التعقيم إلى عملية تجعل النفاذ إلى البيانات المستهدفة في الوسائط عصياً على مستوى معين من الجهد [b-NIST SP 800-88]. ويقدم المرجع [b-NIST SP 800-88] ثلاث فئات من التعقيم على النحو التالي:

1) عملية إخلاء: تطبق تقنيات منطقية لتعقيم البيانات في جميع مواقع التخزين التي يمكن أن يعنونها المستخدم للحماية من تقنيات استعادة البيانات غير الاقتحامية البسيطة؛ والتي تطبَّق عادةً من خلال أوامر القراءة والكتابة العادية إلى جهاز التخزين، مثل إعادة كتابة قيمة جديدة أو استخدام خيار من قائمة خيارات لإعادة ضبط الجهاز إلى حالة المصنع (حيث لا تُدعم إعادة الكتابة)؛

2) عملية تطهير: تطبق التقنيات المادية أو المنطقية التي تجعل استعادة البيانات المستهدفة غير قابلة للاستعمال باستخدام أحدث التقنيات المختبرية؛

3) عملية تدمير: تجعل استعادة البيانات المستهدفة غير قابلة للاستعمال باستخدام أحدث التقنيات المختبرية وتؤدي إلى عجز لاحق عن استخدام الوسائط لتخزين البيانات.

وتكتب عملية الإخلاء فوق الوسائط باستخدام البرمجيات الموافَق عليها تنظيمياً، وتقوم بالتحقق من البيانات المكتوبة فوق الوسائط. وينبغي أن يمرر نمط الإخلاء تمرير كتابة واحدة على الأقل بقيمة بيانات ثابتة، كقيمة كلها أصفار. ويمكن حسب الاختيار استخدام تمريرات كتابة متعددة أو قيم أكثر تعقيداً.

8 متطلبات الأمن الوظيفي

1.8 نظرة عامة

- يُتطلب أن تعتمد المعمارية الوظيفية على إطار ضمان الاستيقان من كيان (EAA) الموصوف في التوصية [ITU-T X.1254]؛
- يُتطلب أن تقدم المعمارية الوظيفية نفقاً آمناً (مثل أمن طبقة النقل (TLS) الموصوف في المرجع [b-IETF RFC 6460] أو قناة اتصال آمنة تستند إلى بروتوكول OMA) للاتصال بين المكونات؛
- يُتطلب أن تقدم المعمارية الوظيفية إدارة مفاتيح آمنة (بالاستناد، على سبيل المثال، إلى البنية التحتية للمفتاح العمومي (PKI) الموصوفة في التوصية [b-ITU-T X.509]) لدعم مسارات آمنة؛
- يُتطلب أن تدعم المعمارية الوظيفية على الأقل آلية استيقان من كيان بمستويي ضمان (LoA 2) موصوفة في التوصية [ITU-T X.1254]؛
- يُتطلب أن تدعم المعمارية الوظيفية على الأقل التحاق كيان بمستويي ضمان (LoA 2) موصوف في التوصية [ITU-T X.1254]؛
- يُتطلب أن تدعم المعمارية الوظيفية على الأقل إدارة بيانات اعتماد كيان بمستويي ضمان (LoA 2) موصوفة في التوصية [ITU-T X.1254]؛
- يُتطلب أن تدعم المعمارية الوظيفية الاستيقان من الرسالة للرسائل المنقولة؛
- يُتطلب أن تدعم المعمارية الوظيفية مكافحة هجوم التكرار للرسائل المنقولة؛
- يُتطلب أن تدعم المعمارية الوظيفية القدرة على النسخ الرديف لبيانات الجهاز إلى مخدِّم الشبكة الآمن؛
- يُتطلب أن تقدم المعمارية الوظيفية تخويلاً قوياً (التحكم في النفاذ)؛
- يُتطلب أن تدعم المعمارية الوظيفية آليات الأمن الموصوفة في المرجع [b-3GPP TS 22.048]؛
- يُتطلب أن تقدم المعمارية الوظيفية إدارة الهوية لمالك الجهاز المتنقل والمخدِّم المخوَّل والأجهزة المتنقلة المسروقة.

2.8 متطلبات الأمن الوظيفي لمالك الجهاز المتنقل

- يُتطلب الاستيقان من مالك الجهاز المتنقل لدى المخدِّم المخوَّل استناداً إلى استيقان بعاملين على الأقل (على سبيل المثال، هوية/كلمة مرور وكلمة مرور لمرة واحدة (OTP) على النحو الموصوف في التوصية [ITU-T X.1254])؛
- يُتطلب تحديد هوية مالك الجهاز المتنقل باستخدام إجراء التحاق كيان بمستويي ضمان (LoA 2) الموصوف في التوصية [ITU-T X.1254]؛
- يُتطلب أن تدعم المعمارية الوظيفية لمالك الجهاز الاستيقان من مخدِّم التخويل باستعمال آلية استيقان من كيان بمستويي ضمان (LoA 2) على الأقل موصوفة في التوصية [ITU-T X.1254]؛
- يُتطلب أن تدعم المعمارية الوظيفية لمالك الجهاز نفقاً آمناً (مثل أمن طبقة النقل (TLS) الموصوف في المرجع [b-IETF RFC 6460] أو قناة اتصال آمنة تستند إلى بروتوكول OMA) كي تتواصل الرسالة المنقولة مع المخدِّم المخوَّل.

3.8 متطلبات الأمن الوظيفي للمخدِّم المخوَّل

- يُتطلب أن تقدم المعمارية الوظيفية للمخدِّم المخوَّل الاستيقان من مالك الجهاز باستخدام آلية استيقان بعاملين على الأقل (مثل الاستيقانات بثلاثة مستويات ضمان (LoA 3) الموصوفة في التوصية [ITU-T X.1254])؛
- يُتطلب الاستيقان من المعمارية الوظيفية للمخدِّم المخوَّل بواسطة الجهاز المتنقل المسروق باستخدام آلية استيقان بعاملين على الأقل (مثل الاستيقانات بثلاثة مستويات ضمان (LoA 3) الموصوفة في التوصية [ITU-T X.1254])؛

- يُتطلب أن تدعم المعمارية الوظيفية للمخدِّم المخوَّل نفقاً آمناً (مثل أمن طبقة النقل (TLS) الموصوف في المرجع [b-IETF RFC 6460] أو قناة اتصال آمنة تستند إلى بروتوكول OMA) كي تتواصل الرسالة مع مالك الجهاز المتنقل؛
- يُتطلب أن تدعم المعمارية الوظيفية للمخدِّم المخوَّل نفقاً آمناً كي تتواصل الرسالة المنقولة مع الجهاز المتنقل المسروق.

4.8 متطلبات الأمن الوظيفي للجهاز المتنقل المسروق

- يُتطلب أن تدعم المعمارية الوظيفية للجهاز المتنقل المسروق نفقاً آمناً (مثل أمن طبقة النقل (TLS) الموصوف في المرجع [b-IETF RFC 6460] أو قناة اتصال آمنة تستند إلى بروتوكول OMA) كي تتواصل الرسالة المنقولة مع المخدِّم المخوَّل؛
- يُتطلب الاستيقان من المعمارية الوظيفية للجهاز المتنقل المسروق لدى المخدِّم المخوَّل باستخدام آلية استيقان بعاملين على الأقل (مثل الاستيقانات بثلاثة مستويات ضمان (LoA 3) الموصوفة في التوصية [ITU-T X.1254])؛
- يُتطلب أن تقدم المعمارية الوظيفية للجهاز المتنقل المسروق الاستيقان من المخدِّم المخوَّل باستخدام آلية استيقان بعاملين على الأقل (مثل الاستيقانات بثلاثة مستويات ضمان (LoA 3) الموصوفة في التوصية [ITU-T X.1254])؛
- يُتطلب أن تستدعي المعمارية الوظيفية للجهاز المتنقل المسروق ميزة التخزين الرديف لجميع بيانات الجهاز العائد إلى المالك في مخدِّم شبكة آمن؛
- يُتطلب أن تنفِّذ المعمارية الوظيفية للجهاز المتنقل المسروق آليات التحكم في النفاذ لتفعيل التعليمات الواردة من المخدِّم المخوَّل؛
- يُتطلب أن تحمي المعمارية الوظيفية للجهاز المتنقل المسروق البيانات أو الوظائف من نفاذ واستعمال كيان غير مخوَّل؛
- يُتطلب أن تدعم المعمارية الوظيفية للجهاز المتنقل المسروق عملية الإخلاء في حذف البيانات الآمن المذكورة في الفقرة 3.4.7 بمجرد أن تتلقى تعليمات من المخدِّم المخوَّل لحذف البيانات في الجهاز المتنقل.

5.8 متطلبات الأمن الوظيفي للمخدِّم الرديف

- يُتطلب أن تدعم المعمارية الوظيفية للمخدِّم الرديف نفقاً آمناً لنقل المراسلات مع الجهاز المتنقل؛
- يُتطلب أن تقدم المعمارية الوظيفية للمخدِّم الرديف الاستيقان من الجهاز المتنقل باستخدام آلية استيقان حصينة، من أجل التخزين الرديف لبيانات الجهاز، إذا لزم الأمر؛
- يُتطلب أن يستيقن الجهاز المتنقل من المعمارية الوظيفية للمخدِّم الرديف باستخدام آلية استيقان حصينة؛
- يُتطلب أن تدعم المعمارية الوظيفية للمخدِّم الرديف القدرة على التخزين الرديف لبيانات الجهاز المناسبة من الجهاز المتنقل؛
- يُتطلب أن تقدم المعمارية الوظيفية للمخدِّم الرديف موارد (أي موارد تخزين) كافية إلى الجهاز المتنقل.

التذييل I

المتطلبات العامة لتدابير مكافحة السرقة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم المرجع [b-GSMA] متطلبات عامة للمعلومات المتعلقة بتدابير مكافحة السرقة. ويصف هذا التذييل هذه المتطلبات.

1.I مالك الجهاز

- للتأكد من فقدان الجهاز أو سرقته بشكل غير قابل للاسترداد (كأن تُظهر إحداثيات النظام العالمي لتحديد الموقع (GPS) الجهاز في مكان لا يعرفه المالك)، يُتطلب من المالك بدء إجراء تعطيل الخدمة بعد القيام بما يلي:
  - الإيعاز للجهاز بإرسال نغمة صاخبة لفترة طويلة (30 ثانية إلى 3 دقائق) لإتاحة فرصة للمالك لتحديد موقع الجهاز، على افتراض أنه على مرمى السمع؛
  - عرض رسالة على شاشة القفل/الشاشة الرئيسية للجهاز تطلب إعادة الجهاز؛
  - العثور على موقع الجهاز باستخدام النظام العالمي لتحديد المواقع (GPS) (أو أي تكنولوجيا أخرى لتحديد المواقع إذا كان الجهاز يدعم هذه الميزة) وعرض الموقع على خريطة؛
- يُتطلب من المالك "اختيار الاستغناء" صراحةً عن ميزة تعطيل الجهاز ولكن يُتطلب "اختيار الاستفادة" منها كخيار مبدئي؛
- عند أول إقلاع وإعداد للجهاز المتنقل، يوصى بعرض برنامج تعليمي قصير على المالك لتثقيفه بشأن السلوك العام الآمن عند استخدام الجهاز الجديد وتخزينه. وينبغي أن يكون البرنامج التعليمي ضرورياً قبل تفعيل الخدمة؛
- يوصى بأن يكون مالك الجهاز قادراً على النفاذ إلى وظيفة تعطيل الجهاز والاستعانة بها عن طريق استخدام قدرات الخدمة الذاتية دون الحاجة إلى إشراك مشغل الشبكة؛
- يوصى بألا يتمكن مالك الجهاز من إعادة تفعيل الجهاز إذا عطَّله المشغِّل؛
- يجوز للمالك استدعاء ميزة التخزين الرديف لجميع بيانات الجهاز العائدة للمالك (البيانات الشخصية)، في مخدِّم شبكة آمن؛
- يُتطلب من المالك التمكن من أن يمنع عن بُعد النفاذ إلى جميع بيانات الجهاز؛
- يُتطلب من المالك التمكن من أن يحذف من الجهاز عن بُعد بيانات المستخدم (كالصور ومقاطع الفيديو ودليل الهاتف والبريد الإلكتروني). وإذا جُفرت بيانات المستخدم بقوة، يكفي محو مفتاح التجفير من الجهاز؛
- بالنسبة للأجهزة المفقودة أو المسروقة المسجلة على شبكة تزار (تجوال)، يمكن إخطار المالك بأي تكاليف إضافية عند محاولة استدعاء وظائف التخزين الرديف للبيانات أو تعطيل الجهاز أو استعادة إعدادات الجهاز؛
- يُتطلب أن يعجز المستخدم غير المخوَّل عن النفاذ إلى وظائف أو بيانات جهاز عُطِّل؛
- ينبغي أن تتاح للمالك وظيفة عرض رسالة مخصصة على شاشة القفل/الشاشة الرئيسية للجهاز عندما لا يكون الجهاز في حوزة المالك.

2.I المخدِّم

- يُتطلب من مشغل الشبكة الاستيقان من طلب من مالك الجهاز لبدء تعطيل الجهاز؛
- يُتطلب الاستيقان من طلب المالك لتعطيل جهاز، ولا يُتطلب إلا للتحكم في الجهاز المسجَّل لذلك المالك؛
- يُتطلب أمن موقع المخدمات الداعمة لميزة التعطيل، وأمن النفاذ إلى هذه المخدمات؛

- يوصى بألا يسمح بالنفاذ إلى وظائف التعطيل واستدعائها إلا للموظفين المخولين المدربين تدريباً كافياً؛
- يُتطلب من المخدِّم إنشاء سجلات لجميع طلبات التعطيل المستلَمة والاحتفاظ بها؛
- عند إعادة الخدمة إلى جهاز عُطِّل سابقاً وأعيد تفعيله، تُتطلب إعادة بيانات وتطبيقات المالك الرديفة إلى الجهاز؛
- يُتطلب تخزين بيانات المالك الرديفة تخزيناً آمناً، وضمان كتمان البيانات وسلامتها؛
- عندما يطلب المالك تعطيل جهازه، يمكنه أن يتوقع أن تنجِز الوظيفةُ التنفيذَ في أقل من 15 دقيقة، إذا أمكن الاستيقان من الجهاز بنجاح؛
- يتعذر استخدام إعادة ضبط الجهاز إلى حالة المصنع كوسيلة لتجاوز التدابير المضادة للسرقة.

3.I الجهاز المتنقل

- يُتطلب التحقق من صحة طلب تعطيل الجهاز قبل الانتقال إلى الخطوات التالية نحو تعطيل الجهاز؛
- يُتطلب تنفيذ آلية تعطيل جهاز متنقل من مخدِّم مخوَّل يدعم وظيفة التعطيل. ومن أجل الإيفاء بهذا المتطلب، يلزم ما يلي:
  - توصيل آمن بين الجهاز والمخدِّم؛
  - استيقان المخدِّم من الجهاز؛
  - استيقان الجهاز من المخدِّم وكون المخدِّم مخولاً بأداء الوظيفة؛
- يُتطلب من الجهاز المتنقل، عند أول إقلاع وإعداد، أن يطلع المالك صراحةً على ميزات مكافحة السرقة وأي ميزات أمنية أخرى ذات صلة مثل آليات التحكم في النفاذ إلى الجهاز؛
- يُتطلب من الجهاز أن يمتلك القدرة على إعادة تفعيل الخدمة على يد المالك الشرعي بعد أن تم تعطيله. ويُتطلب أن يعجز عن إعادة التفعيل على يد أي شخص غير المالك الشرعي؛
- يوصى بأن تكون وظيفة تعطيل الجهاز قابلة للتشغيل عندما لا يكون الجهاز موصولاً بشبكة اتصالات متنقلة برية عمومية بل موصولاً بالإنترنت؛
- بالنسبة للأجهزة المفقودة أو المسروقة المسجلة على شبكة تزار (تجوال)، يُتطلب أن تعمل بنجاح جميع وظائف التخزين الرديف للبيانات أو تعطيل الجهاز أو استعادة إعدادات الجهاز.

4.I تصنيع الأجهزة

- يوصى مصنعو الأجهزة بالاستمرار في تنفيذ وتطوير تدابير لردع ومنع إعادة التهيئة غير المخوَّلة لجهاز مفقود أو مسروق إلى حالة يمكن بها لشخص آخر غير المالك استخدام الجهاز.

التذييل II

متطلبات أمنية إضافية لتدابير مكافحة السرقة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II متطلبات المخدِّم الرديف

- يُتطلب تنفيذ الآلية من مخدِّم رديف يدعم تخزين المعلومات المحددة لهوية الأشخاص مالكي الأجهزة المتنقلة المسروقة/المفقودة. ومن أجل الإيفاء بهذا المتطلب، يلزم ما يلي:
  - توصيل آمن بين الجهاز والمخدِّم الرديف؛
  - استيقان المخدِّم الرديف من الجهاز المتنقل؛
  - استيقان الجهاز من المخدِّم الرديف.

التذييل III

تهديدات محددة في مجال مكافحة السرقة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.III التهديدات بين مالك الجهاز المتنقل والمخدِّم المخوَّل

- انتحال هوية مالك الجهاز. أي قيام مهاجم ينتحل شخصية مالك الجهاز بإيصال تعليمات تعطيل غير مشروعة إلى المخدِّم المخوَّل. ويمكن للهجوم الذي يستغل هذا التهديد أن يتسبب بتعطيل أجهزة متنقلة سَليمة؛
- العبث برسالة/التنصت عليها/إعادة إرسالها. أي إيصال تعليمات تعطيل غير مشروعة إلى المخدِّم المخوَّل؛ أو إفشاء مضمون رسالة التعليمات لمهاجم قادر على التنصت على الاتصال؛ أو إرسال حركة هائلة إلى المخدِّم المخوَّل تفضي إلى هجمات رفض الخدمة الموزع (DDoS)؛
- انتحال هوية المخدِّم المخوَّل. أي إما إفشاء بيانات اعتماد الاستيقان من مالك الجهاز الشرعي أو إيصال تعليمات مالك الجهاز الشرعي بالتعطيل إلى المخدِّم المخوَّل المنتحَلة هويته. ويمكن للهجوم الذي يستغل هذا التهديد أن يتسبب بتعطيل أجهزة متنقلة سَليمة.

2.III التهديدات بين المخدِّم المخوَّل والوكيل المعطِّل المضاد للسرقة

- انتحال هوية مخدِّم الاستيقان. أي إيصال تعليمات تعطيل غير مشروعة إلى الجهاز المتنقل المسروق؛
- العبث برسالة/التنصت عليها/إعادة إرسالها. أي إيصال تعليمات تعطيل غير مشروعة إلى الوكيل المعطِّل المضاد للسرقة؛ أو إفشاء مضمون رسالة التعليمات لمهاجم قادر على التنصت على الاتصال؛ أو إرسال حركة هائلة إلى الوكيل المعطِّل المضاد للسرقة بحيث تفضي إلى هجمات حرمان من الخدمة موزَّعة (DDoS)؛
- انتحال هوية الوكيل المعطِّل المضاد للسرقة. أي إما إفشاء بيانات اعتماد الاستيقان من المخدِّم المخوَّل الشرعي أو إيصال تعليمات مالك الجهاز الشرعي بالتعطيل إلى الوكيل المعطِّل المضاد للسرقة المنتحَلة هويته.

3.III التهديدات بين الوكيل المعطِّل المضاد للسرقة والمخدِّم الرديف

- انتحال هوية الوكيل المعطِّل المضاد للسرقة. أي إفشاء الرسالة الرديفة المخزنة في المخدِّم الرديف إلى الوكيل المعطِّل المنتحَلة هويته؛
- العبث برسالة/التنصت عليها/إعادة إرسالها. أي تغيير المعلومات الرديفة وإفشاءها للمهاجم القادر على التنصت على الاتصال؛
- انتحال هوية المخدِّم المخوَّل. أي إفشاء المعلومات الرديفة للمخدِّم الرديف المنتحَلة هويته.

التذييل IV

سيناريو لتدابير مكافحة السرقة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.IV أنواع الميزات المعطلة للجهاز المتنقل

هناك نوعان من ميزات التعطيل:

1) ميزة التعطيل "القاسي" الذي يجعل الجهاز المتنقل المسروق غير صالح للاستعمال بشكل دائم؛

2) ميزة التعطيل "اللين" الذي يكتفي بجعل جهاز متنقل غير صالح للاستعمال على يد "مستخدم غير مخوَّل".

2.IV تمكين الجهاز المتنقل المسروق/المفقود

تتطلب ميزات مكافحة السرقة مشاركة نشطة من صاحب الجهاز المتنقل. وعندما يشتري مالك الجهاز جهازاً متنقلاً جديداً، ويشترك لدى مقدم خدمة خلوية، ينبغي أن يشكِّل الجهاز المتنقل لتمكين ميزة مكافحة السرقة.

3.IV سيناريو تعطيل الجهاز المتنقل المسروق/المفقود

إذا سُرق الهاتف المتنقل أو فُقد، يتصل مالك الجهاز بمقدم خدمته الخلوية أو يستخدم موقعاً إلكترونياً يديره مشغِّل الخدمة الخلوية، الذي يُعرف باسم المخدِّم المخوَّل، لإرسال تعليمات "تعطيل الجهاز" إلى الجهاز المتنقل. وستقفل هذه التعليمات الجهاز المتنقل، وإذا رغب مالك الجهاز، يمكنه أيضاً محو بعض البيانات الشخصية من الجهاز المتنقل أو السماح للمخدِّم الرديف بتخزين بعض البيانات الشخصية.

وستؤدي تعليمات تعطيل الجهاز إلى جعل الجهاز غير قابل للتشغيل على شبكة أي مقدم لخدمات متنقلة تجارية أو خدمة بيانات متنقلة تجارية على مستوى العالم، حتى إذا أُوقف تشغيل الجهاز أو أزيلت واسطة تخزين البيانات منه.

ولن يتاح سبيل لاستعادة إعدادات جهاز مقفل إلا بكلمة مرور مورَّدة من مالك الهاتف.

التذييل V

ملف تعريف أمن طبقة النقل في تدابير مكافحة السرقة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل ملف تعريف الحد الأدنى لأمن طبقة النقل في تدابير مكافحة السرقة. ويرد المثال النمطي لملف تعريف أمن طبقة النقل في المرجعين [b-IETF RFC 6460] و[b-ISO/IEC 20648].

1.V متطلَب بروتوكول أمن طبقة النقل

– يوصى لمخطط مكافحة السرقة الذي يعمل كمخدِّم أن ينفِّذ بروتوكول أمن طبقة النقل؛ غير أن استخدامه من جانب العملاء هو أمر اختياري. ويُتطلب تنفيذ الإصدار 1.2 من أمن طبقة النقل (الموصَّف في المرجع [b-IETF RFC 5246]) أو تنفيذ الإصدار الأحدث منه.

2.V مجموعة حالات شفرة أمن طبقة النقل من أجل قابلية التشغيل البيني

– يجب ألا يستخدم مخطط مكافحة السرقة اختزال MD5 أو اختزال SHA-1 كاختزال مبدئي لشفرة الاستيقان من الرسالة المختزلة عبر لوحة المفاتيح (HMAC)؛

– يجب ألا يستخدم مخطط مكافحة السرقة اختزال RC4 كاختزال مبدئي للخوارزمية التجفيرية؛

ملاحظة – يحظر المرجع [b-IETF RFC 7465] استخدام اختزال RC4.

– يُتطلب أن يدعم مخطط مكافحة السرقة: اختيار واستخدام أزواج خوارزمية التوقيع/الاختزال، باستخدام خوارزميات التوقيع المدعومة في الإصدار 1.2 من أمن طبقة النقل واستعمال اختزال SHA-256 أو اختزالات أقوى؛

– يُتطلب أن يستخدم مخطط مكافحة السرقة مجموعة حالات شفرة لديها ما لا يقل عن 112 بتة من قوة الأمن. وبالإضافة إلى ذلك، يُتطلب دعم حالات الشفرة التالية:

- {0x00, 0x3C} TLS_RSA_WITH_AES_128_CBC_SHA256.

3.V الشهادات الرقمية

يُتطلب أن يدعم مخطط مكافحة السرقة شهادات المفتاح العمومي في الإصدار 3 من التوصية [b-ITU-T X.509] التي تلتزم بملف تعريف الشهادة وتوسعة الشهادة المحدد في القسم 4 من المرجع [b-IETF RFC 5280].

– يُتطلب أن يدعم مخدِّم أمن طبقة النقل في مخطط مكافحة السرقة شهادات المخدِّم؛

– يوصى أن يدعم عميل أمن طبقة النقل في مخطط مكافحة السرقة شهادات العميل؛

– يُتطلب أن يدعم مخطط مكافحة السرقة مقاسات المفتاح البالغة 2048 بتة أو أكبر، في شهادات التوصية [b-ITU-T X.509] لمخدِّم RSA/DSA؛

– يُتطلب أن يدعم مخطط مكافحة السرقة أنساق شهادة التوصية [b-ITU-T X.509] بتشفير قواعد التشفير المميزة (DER)، والتوصية [b-ITU-T X.509] بتشفير قاعدته 64، و[b-IETF RFC 7292] PKCS#12؛

– يُتطلب أن يدعم مخطط مكافحة السرقة التحقق من الشهادة على النحو الموضح في القسم 6 من المرجع [IETF RFC 5280]، الذي يعرض شهادة رقمية. وبالإضافة إلى ذلك، يستخدم أحد النهج التالية لتحديد ما إذا كانت الشهادة قد ألغيت:

- الخيار 1: استخدام قوائم إلغاء الشهادات (CRL): قوائم إلغاء الشهادات المدعومة في أنساق شهادة التوصية [b-ITU-T X.509] بتشفير قواعد التشفير المميزة (DER) أو التوصية [b-ITU-T X.509] بتشفير قاعدته 64، وقوائم إلغاء الشهادات الصالحة المخزنة محلياً (التوزيع خارج نطاق هذا المعيار) أو المستخلصة من مصدر خارجي (على سبيل المثال، نقطة توزيع قائمة إلغاء الشهادات (CRLDP))؛
- الخيار 2: استخدام بروتوكول حالة الشهادة مثل بروتوكول حالة الشهادة على الإنترنت (OCSP) بإحدى الطرق التالية: استخدام بروتوكول OCSP مباشرة على النحو الموضح [b-IETF RFC 6960] واستخدام بروتوكول OCSP بشكل غير مباشر من خلال تقديم طلب حالة الشهادة إلى أمن طبقة النقل الموصوفة في القسم 8 من المرجع [b-IETF RFC 6066].

التذييل VI

نظرة عامة على إدارة جهاز بروتوكول تحالف الاتصالات المتنقلة المفتوحة (OMA)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل لمحة عامة عن بروتوكول إدارة الجهاز (DM) الذي يعرِّفه تحالف الاتصالات المتنقلة المفتوحة (OMA) [b-OMA-DM].

1.VI توصيف إدارة جهاز بروتوكول تحالف الاتصالات المتنقلة المفتوحة (OMA)

صُمم توصيف إدارة الجهاز وفق بروتوكول تحالف الاتصالات المتنقلة المفتوحة (OMA DM) لإدارة الأجهزة المتنقلة مثل الهواتف المتنقلة وأجهزة المساعد الرقمي الشخصي وأجهزة الحاسوب اللوحية. وتهدف إدارة الجهاز إلى دعم الاستخدامات التالية:

- التهيئة: تشكيل الجهاز (بما في ذلك استخدام المرة الأولى)، وتفعيل وتعطيل الميزات؛
- تشكيل الجهاز: السماح بإدخال تغييرات على إعدادات ومعلمات الجهاز؛
- ترقيات البرمجيات: تقديم برمجيات جديدة و/أو إصلاحات لشوائب برمجية ليصار إلى تحميلها على الجهاز، بما في ذلك التطبيقات وبرمجيات النظام؛
- إدارة العطل: تقرير عن أخطاء من الجهاز، والاستعلام عن حالة الجهاز.

ويدعم توصيف إدارة الجهاز وفق بروتوكول تحالف الاتصالات المتنقلة المفتوحة جميع الوظائف المذكورة أعلاه، ويمكن أن يطبق الجهاز بشكل اختياري كل هذه الميزات أو مجموعة فرعية منها. وبما أن توصيف إدارة الجهاز وفق بروتوكول تحالف الاتصالات المتنقلة المفتوحة موجه نحو الأجهزة المتنقلة، فإنه مصمم بحساسية لما يلي:

- الأجهزة الصغيرة محدودة الذاكرة وحيز التخزين؛
- تقييد عرض نطاق الاتصالات، كما في التوصيلية اللاسلكية؛
- الأمن المشدد، حيث تتعرض الأجهزة لهجمات البرمجيات؛ ويشكل الاستيقان والصعوبات جزءاً من المواصفات.

بيبليوغرافيا

[b-ITU-T X.509] Recommendation ITU-T X.509 (2012), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

[b-ITU-T X.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*.

[b-ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

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

[b-ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *Supplement on security aspects of smartphones*.

[b-ISO/IEC 20648] ISO/IEC 20648:2016, *Information technology – TLS specification for storage systems*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-3GPP TS 22.048] 3GPP TS 22.048 (2003), *Security mechanisms for the (U)SIM Application Toolkit*, June 2003.

[b-3GPP TS 33.102] 3GPP TS 33.102 (2009), *3G Security; Security architecture (Release 9)*, December 2009.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5280] IETF RFC 5280 (2008), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

[b-IETF RFC 6066] IETF RFC 6066 (2011), *Transport Layer Security (TLS) Extensions: Extension Definitions.*

[b-IETF RFC 6460] IETF RFC 6460 (2012), *Suite B Profile for Transport Layer Security (TLS).*

[b-IETF RFC 6960] IETF RFC 6960 (2013), *ITU-T X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[b-IETF RFC 7292] IETF RFC 7292 (2015), *PKCS #12 Personal Information Exchange Syntax v1.1*.

[b-IETF RFC 7465] IETF RFC 7465 (2015), *Prohibiting RC4 Cipher Suites*.

[b-GSMA] GSMA, *SG.24 Anti-Theft Device Feature Requirements v3.0*, 17 May 2016.

[b-OMA-DM] Open Mobile Alliance, *OMA Device Management V1.2*, April 2013.

[b-NIST SP 800-88] NIST, *NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization*, December 2014.

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، 2018