الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1256
(2016/03)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

مبادئ توجيهية وإطار من أجل تبادل نتائج استيقان الشبكات مع تطبيقات الخدمات

التوصية ITU-T X.1256

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
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029-X.1000
أمن الشبكة	X.1049-X.1030
إدارة الأمن	X.1069-X.1050
القياسات البيومترية عن بُعد	X.1099-X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109-X.1100
أمن الشبكة المحلية	X.1119-X.1110
أمن الخدمات المتنقلة	X.1139-X.1120
أمن الويب	X.1149-X.1140
بروتوكولات الأمن	X.1159-X.1150
الأمن بين جهتين نظيرتين	X.1169-X.1160
أمن معرفات الهوية عبر الشبكات	X.1179-X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199-X.1180
آمن الفضاء السيبراني	
الأمن السيبراني	X.1229-X.1200
مكافحة الرسائل الاقتحامية	X.1249-X.1230
إدارة الهوية	**X.1279-X.1250**
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339-X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349-X.1340
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.1256

مبادئ توجيهية وإطار من أجل تبادل نتائج استيقان الشبكات مع تطبيقات الخدمات

ملخص

إن الارتفاع الكبير في أعداد الأجهزة والتطبيقات التي تنفذ إلى الإنترنت يقترن بتزايد التعقيد الذي يكتنف بيئة الشبكات والخدمات. ويفضي ذلك إلى حاجة ملحة إلى تبسيط آلية استيقان المستعملين من أجل تحسين تجربة المستعمل وجودة الخدمة.

وقد أجرت منظمات تقييس عديدة، منها قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات، الكثير من الأعمال البحثية بشأن آلية الاستيقان الموحَّدة (أي تسجيل الدخول الوحيد). بيد أن كل الأعمال الحالية تركِّز من حيث الأساس على الاستيقان الموحَّد فيما بين تطبيقات الخدمات، دون النظر إلى علاقة ذلك باستيقان الشبكات.

ومن منظور مشغِّلي الشبكات، يخضع المستعملون لبعض أشكال استيقان الشبكات عند النفاذ إليها، لكن استيقان الشبكات الأول منهم لا يُستعمل قط مرة ثانية عند تسجيلهم للدخول مجدَّداً لطلب النفاذ إلى خدمة من الخدمات. وعند اعتماد آلية لتبادل نتائج الاستيقان بين الخدمات والشبكات، يمكن لتطبيقات الخدمات التعرف على هوية المستعمل بواسطة نتائج الاستيقان الآتية من الشبكة. وتتيح هذه الآلية تمتع المستعمل بالنفاذ إلى الخدمة مباشرة على أساس استيقان الشبكة منه مرة واحدة فقط.

وتقدِّم التوصية ITU-T X.1256 لمشغِّلي الشبكات وموفِّري الخدمات مبادئ توجيهية لتبادل نتائج استيقان الشبكات، وتهيئ إطاراً لتبادل قدر أدنى من النعوت فيما بين خدمات متعددة في نطاق علاقة قائمة على الثقة الراسخة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1256	2016-03-23	17	11.1002/1000/12605

مصطلحات أساسية

الاستيقان، نعوت الهوية، الاستيقان على مستوى الشبكة.

* للنفاذ إلى التوصية، يرجى 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 "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/.

© ITU 2017

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

جدول المحتويات

الصفحة

1 مجال التطبيق 1

2 المراجع 1

3 التعاريف 1

1.3 المصطلحات المعرَّفة في وثائق أخرى 1

2.3 مصطلحات معرّفة في هذه التوصية 1

4 المختصرات والأسماء المختصرة 1

5 الاصطلاحات 2

6 آليات تبادل نعوت الاستيقان 3

1.6 الإطار 3

2.6 آلية إصدار الشبكة لنعوت الاستيقان 4

3.6 آلية استصدار نعوت الاستيقان في سياق الخدمة 5

7 الاعتبارات الأمنية 6

التذييل I – حالتا استعمال 7

1.I حالة استعمال تصدر فيها الشبكة نعوت الاستيقان 7

2.I حالة استعمال تُستصدر فيها نعوت الاستيقان في سياق الخدمة 8

بيبليوغرافيا 11

التوصية ITU-T X.1256

مبادئ توجيهية وإطار من أجل تبادل نتائج استيقان الشبكات مع تطبيقات الخدمات

1 مجال التطبيق

تقدِّم هذه التوصية لمشغِّلي الشبكات وموفِّري الخدمات مبادئ توجيهية لتبادل نتائج استيقان الشبكات، وتهيئ إطاراً لتبادل قدر أدنى من النعوت فيما بين خدمات متعددة في نطاق علاقة قائمة على الثقة الراسخة.

أما الطرائق التي يتّبعها مشغِّلو الشبكات لإجراء الاستيقان أو إدماجه أو إعماله على مستوى الشبكات فتخرج عن نطاق هذه التوصية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكِّل من خلال الإشارة إليها في هذا النص جزءاً من هذه التوصية. وإبّان النشر كانت الطبعات المذكورة سارية الصلاحية. ولمّا كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة فيرجى من جميع مستعملي هذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى المشار إليها أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي عليها، كوثيقة قائمة بذاتها، صفة التوصية.

[ITU-T X.1254] التوصية ITU-T X.1254 (2012)، *إطار ضمان الاستيقان من كيان*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

لا يوجد.

2.3 مصطلحات معرّفة في هذه التوصية

لا يوجد.

4 المختصرات والأسماء المختصرة

تُستعمل في هذه التوصية المختصرات والأسماء المختصرة التالية:

2G/3G الجيل الثاني/الجيل الثالث *(Second/Third Generation)*

AC المتحكم في النفاذ *(Access Controller)*

AKA اتفاق الاستيقان والمفتاح *(Authentication and Key Agreement)*

AN شبكة النفاذ *(Access Network)*

AP نقطة النفاذ *(Access Point)*

API الواجهة البينية لبرمجة التطبيقات *(Application Programming Interface)*

AUG بوّابة الاستيقان *(Authentication Gateway)*

BRAS مخدم النفاذ العريض النطاق البعيد *(Broadband Remote Access Server)*

EAP-SIM طريقة بروتوكول الاستيقان الموسَّع لوحدة هوية المشترك (في النظام العالمي للاتصالات المتنقلة (GSM)) *(Extensible Authentication Protocol Method for (GSM) Subscriber Identity Modules)*

GGSN عقدة دعم بوّابة الخدمة العامة للاتصالات الراديوية بأسلوب الرزم (GPRS) *(Gateway GPRS Support Node)*

GPRS الخدمة العامة للاتصالات الراديوية بأسلوب الرزم *(General Packet Radio Service)*

HTTP بروتوكول نقل النصوص الإلكترونية *(Hyper Text Transfer Protocol)*

IMPI هوية خاصة للوسائط المتعددة القائمة على بروتوكول الإنترنت *(IP Multimedia Private Identity)*

IMPU هوية مستعمل عام للوسائط المتعددة القائمة على بروتوكول الإنترنت *(IP Multimedia Public User Identity)*

IMS النظام الفرعي المتعدّد الوسائط القائم على بروتوكول الإنترنت *(IP Multimedia Subsystem)*

IMSI الهوية الدولية للمشترك المتنقل *(International Mobile Subscriber Identity)*

IP بروتوكول الإنترنت *(Internet Protocol)*

ISDN الشبكة الرقمية للخدمات المتكاملة (Integrated Services Digital Network)

LoA مستوى الضمان *(Level of Assurance)*

MSISDN الرقم الدولي للمشترك المتنقل في الشبكة الرقمية للخدمات المتكاملة/الشبكة الهاتفية العمومية التبديلية *(Mobile Subscriber International ISDN/PSTN Number)*

PSTN الشبكة الهاتفية العمومية التبديلية (Public Switched Telephone Network)

RADIUS خدمة الاستيقان عن بُعد للمستعملين الداخلين *(Remote Authentication Dial-In User Service)*

SGSN عقدة دعم GPRS القائمة بالخدمة *(Serving GPRS Support Node)*

SIM وحدة هوية المشترك *(Subscriber Identity Protocol)*

SIP بروتوكول استهلال الدورة *(Session Initiation Protocol)*

SNS خدمة شبكات التواصل الاجتماعي (Social Network Service)

UE جهاز المستعمل *(User Equipment)*

USIM وحدة هوية المشترك العالمية *(Universal Subscriber Identity Module)*

URI محدِّدُ المورد الموحَّدُ *(Uniform Resource Identifier)*

WAP بروتوكول التطبيق اللاسلكي *(Wireless Application Protocol)*

WLAN شبكة المنطقة المحلية اللاسلكية *(Wireless Local Area Network)*

5 الاصطلاحات

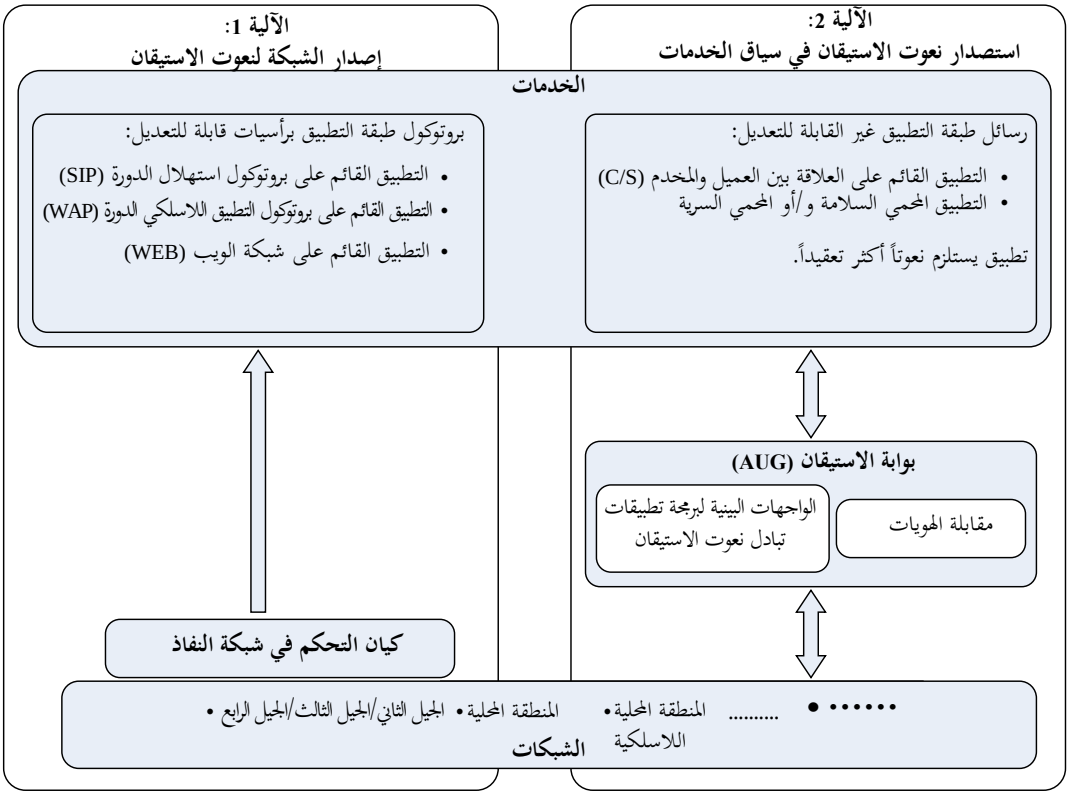
لا يوجد.

6 آليات تبادل نعوت الاستيقان

1.6 الإطار

عندما ينفذ المستعملون إلى شبكة لإحدى الجهات التي تتولى التشغيل، يتعين أن يتم في إطار شبكة النفاذ الاستيقان منهم على نحو شديد. بيد أن وظيفة الاستيقان هذه لا تسهِّل الخدمات عادة. ففي معظم الحالات يجري الاستيقان من المستعملين النهائيين في الشبكة وفي نظام الخدمات، على الترتيب. فعلى سبيل المثال تقوم شبكة الجيل الثالث (3G) بالاستيقان من المستعملين النهائيين استناداً إلى بطاقة وحدة هوية المشترك العالمية (USIM) داخل هواتفهم الخلوية (ماذا لديهم)، لكن يتعيَّن عند تصفحهم إحدى خدمات الشبكات الاجتماعية (SNS) استيقانُ مخدم شبكة الويب منه مرة ثانية على أساس الزوج "اسم المستعمل، كلمة السر" المسجَّل من ذي قبل (ماذا يعرفون).

إن المفهوم الأساسي لتبادل نعوت الاستيقان يتمثل في تمكين الخدمات من استعمال نعوت استيقان الشبكة. ويُبيَّن إطار تبادل نعوت الاستيقان في الشكل 6-1.



الشكل 6-1 – إطار تبادل نعوت استيقان الشبكات مع تطبيقات الخدمات

ينطوي هذا الإطار على نوعين من آليات تبادل نعوت الاستيقان:

- الآلية 1 – الآلية القائمة على إصدار الشبكة لنعوت الاستيقان: تحويل نعوت استيقان الشبكة إلى تطبيقات الخدمات مباشرة

عندما يفهم كيان التحكم في النفاذ إلى الشبكة بروتوكول طبقة التطبيق في الخدمة (مثل بروتوكول استهلال الدورة (SIP)، وبروتوكول التطبيق اللاسلكي (WAP)، وبروتوكول نقل النصوص الإلكترونية (HTTP)، إلخ)، يكون بإمكانه أن يُدرج نعوت استيقان الشبكة ضمن رسائل طبقة التطبيق وأن يحوِّلها مباشرة إلى منصة الخدمة. وفي هذه الحالة لا يتعيَّن تعريف أي من الواجهات البينية لبرمجة التطبيق (API) لكي تبادر تطبيقات الخدمة إلى طلب الحصول على نعوت الاستيقان لأنها تكتفي على نحو منفعل بتلقي هذه المعطيات التي تتضمنها رأسيات الرسائل.

ويمكن أن تقرر تطبيقات الخدمة تحليل الرأسيات التي أدرجتها الشبكة واستعمال هذه الرأسيات أو أن تتجاهلها تماماً. وإذا احتاجت تطبيقات الخدمة إلى نعوت أكثر مما أصدرته الشبكة فينبغي لها أن تستخدم آلية استصدار نعوت الاستيقان في سياق الخدمات.

انظر التذييل I.1 للاطّلاع على حالة استعمال ملموسة.

- الآلية 2 – آلية استصدار نعوت الاستيقان في سياق الخدمات: تبادل نعوت استيقان الشبكة عبر بوّابة الاستيقان (AUG).

إذا تعذر على كيان التحكم في النفاذ إلى الشبكة تحليل أو تعديل رسائل طبقة التطبيق (كما تكون عليه الحال مثلاً عندما يخضع بروتوكول طبقة التطبيق لحقوق الملكية، أو عندما تكون رسائل طبقة التطبيق محمية السلامة و/أو محمية السرية)، يتعين أن تُضمَّ إلى الشبكة بوّابة استيقان مستقلة من أجل تبادل نعوت الاستيقان. وتُعْمِل بوّابة الاستيقان واجهاتٍ بينيةً لبرمجة التطبيقات جيدةَ التعريف خاصة بالشبكة يمكن لتطبيقات الخدمات أن تتصل بها للحصول على نعوت الاستيقان من الشبكة.

ويضاف إلى ذلك أنه، إذا كانت تطبيقات الخدمة تحتاج على النحو المذكور في صدد آلية إصدار الشبكة لنعوت الاستيقان إلى نعوت أكثر مما تم إصداره فينبغي لها أيضاً أن تستخدم استصدار نعوت الاستيقان في سياق الخدمات بغية الحصول على نعوت استيقان إضافية من الشبكة.

انظر التذييل I.2 للاطّلاع على حالة استعمال ملموسة.

2.6 آلية إصدار الشبكة لنعوت الاستيقان

1.2.6 إرشادات بشأن التنفيذ

عندما يتصفح المستعمل الشبكة، يقوم كيان التحكم في النفاذ إلى الشبكة الموجود على حدودها بالاستيقان من هوية المستعمل. ومن الأمثلة المعتادة على كيانات التحكم في النفاذ إلى الشبكات جهاز مراقبة النفاذ في شبكة المنطقة المحلية اللاسلكية (WLAN)، وعقدة دعم الخدمة العامة للاتصالات الراديوية بأسلوب الرزم (SDSN) أو عقدة دعم بوّابة الخدمة العامة للاتصالات الراديوية بأسلوب الرزم في شبكة الخدمة العامة للاتصالات الراديوية بأسلوب الرزم (GGSN)، ومخدّم النفاذ العريض النطاق البعيد (BRAS) في الشبكات الثابتة. ويَعْرِف كيان التحكم في النفاذ إلى الشبكة هوية المستعمل نتيجة لاستيقان الشبكة.

فإذا فهم كيان التحكم في النفاذ إلى الشبكة بروتوكول طبقة التطبيق في الخدمة (مثل بروتوكول استهلال الدورة (SIP)، وبروتوكول التطبيق اللاسلكي (WAP)، وبروتوكول نقل النصوص الإلكترونية (HTTP)، إلخ)، فيمكنه أن يدرج هوية المستعمل وبعض المعلومات المصاحبة في رسائل طلب الخدمة وأن يحوِّلها إلى منصة خدمة.

وإذا كانت منصة الخدمة تثق بكيان التحكم في النفاذ إلى الشبكة فيمكنها أن تستخرج بصورة مباشرة هوية المستعمل من طلبات الخدمة فتعتبر أنه تم بالفعل الاستيقان من المستعمل.

وفي هذه المعمارية يتعين على منصة الخدمة أن تتبين ما إذا كان يمكن الثقة بنعوت الاستيقان التي أدرجها كيان التحكم في النفاذ إلى الشبكة. ودعماً لذلك ينبغي على مشغِّل الشبكة أن يبرم اتفاقاً مع موفِّر الخدمات، وأن يقدم قائمة بأجهزة التحكم في النفاذ التي يمكن الثقة بها أو آلية (تتمثل في مفاتيح متبادلة مسبقاً أو في شهادات رقمية، على سبيل المثال) لاستبانة ماهية أجهزة التحكم في النفاذ الممكن الثقة بها. وتنبغي حماية المعلومات المتعلقة بالمستعمل التي تُنقل بين جهاز التحكم في النفاذ ومنصة الخدمة. وينبغي لأجهزة التحكم في النفاذ إلى الشبكة أن تتدبر أيضاً قائمة بالمنصات المجازة من منصات الخدمة المتعاقد معها. فينبغي أن لا تُحال نعوت استيقان الشبكة إلا إلى منصات الخدمة المدرجة في هذه القائمة المجازة. ولا تندرج المبادئ التوجيهية بشأن كيفية التوصل إلى إقامة هذه العلاقة القائمة على الثقة ضمن نطاق هذه التوصية.

2.2.6 وصف الواجهة البينية

تُحَمَّل نعوت استيقان الشبكة ضمن رأسية رسائل طلب الخدمة المعدة وفق بروتوكول التطبيق (مثل بروتوكول استهلال الدورة (SIP)، أو بروتوكول نقل النصوص الإلكترونية (HTTP))، وتُنْقَل من كيان التحكم في النفاذ إلى الشبكة إلى منصة الخدمة.

ويجب أن يشمل ذلك النعوت التالية:

1) هوية المستعمل:

يُدْرَج في هذه الخانة بيان هوية مستعمل الشبكة (مثل محدِّد المورد الموحَّد (URI) في بروتوكول استهلال الدورة (SIP)، والرقم الدولي للمشترك المتنقل في الشبكة الرقمية للخدمات المتكاملة/الشبكة الهاتفية العمومية التبديلية (MSISDN)، واسم المستعمل (Username)، إلخ). ويمكن أن تستعمل منصة الخدمة هذا البيان لاستبانة هوية المستعمل.

2) طريقة للاستيقان بمستوى ضمان معروف (LoA) [ITU-T X.1254]:

يُدْرَج في هذه الخانة مميِّز طريقة الاستيقان (مثل اتفاق الاستيقان والمفتاح (AKA) للجيل الثاني/الثالث/الرابع، واتفاق الاستيقان والمفتاح للنظام الفرعي المتعدد الوسائط القائم على بروتوكول الإنترنت (ISM)، واستيقان النفاذ المختصر في بروتوكول نقل النصوص الإلكترونية (HTTP)/بروتوكول استهلال الدورة (SIP)، إلخ.).

وينبغي أن يتفق مشغِّل الشبكة وموفِّرو الخدمات على قائمة بمميِّزات طرائق الاستيقان الممكن التعرف عليها ومستوى الضمان (LoA) الذي يقابلها.

وينبغي لكل منصة خدمة معيَّنة أن تبتّ فيما إذا كان يتعيَّن قبول نعوت الاستيقان التي تصدرها الشبكة استناداً إلى مستوى ضمان طريقة الاستيقان وسياستها فيما يخص الأمن.

3) سائر النعوت المطلوبة بموجب العقد بين المشغِّل وموفِّر الخدمات.

3.6 آلية استصدار نعوت الاستيقان في سياق الخدمة

1.3.6 إرشادات بشأن التنفيذ

لا يمكن إعمال آلية إصدار الشبكة لنعوت الاستيقان إذا لم يكن بمقدور كيان التحكم في النفاذ إلى الشبكة تحليل رسائل طبقة تطبيق الخدمات أو تعديلها، كما تكون عليه الحال مثلاً عندما يخضع بروتوكول طبقة التطبيق لحقوق الملكية، أو عندما تكون رسائل الخدمة مشفَّرةً أو محميةَ السلامة. وفي هذه الحالة يمكن أن توضع بوّابة استيقان بين الشبكة ومنصة الخدمة لتعمل بصفة وكيل لمنصة الخدمة بغية الحصول على نعوت استيقان الشبكة.

كما إن لنموذج استصدار نعوت الاستيقان في سياق الخدمة مبرِّراً آخر يتمثل في أن النعوت المدرجة ضمن الرسائل التي تصدرها الشبكة قد لا تكون ملائمة لطلب خدمة معيَّن. وفي هذه الحالة قد يتعين على منصة الخدمة أن تبادر إلى الاتصال بالشبكة للحصول على معلومات إضافية بشأن نعوت استيقان الشبكة.

ولإتاحة إعمال نموذج استصدار نعوت الاستيقان في سياق الخدمة، يتعيَّن أن تعرض بوّابة الاستيقان مجموعة من الواجهات البينية لبرمجة التطبيق يمكن أن تتصل بها تطبيقات الخدمة للحصول من الشبكة على شتى المعلومات المتعلقة بنتائج الاستيقان. ويمكن أن تستعمل الشبكة ومنصات الخدمات هويات (مميِّزات) مختلفة لاستبانة هوية المستعملين. ولذا ينبغي أن تتضمن بوّابة الاستيقان وظيفة للمقابلة بين الهويات تقرن هوية المستعمل الخاصة بالخدمات بهويته الخاصة بالشبكة، والعكس بالعكس.

وفي هذه المعمارية تلزم الثقة المتبادلة بين منصة الخدمة وبوّابة الاستيقان. ودعماً لذلك ينبغي لمشغِّل الشبكة أن يبرم اتفاقاً مع موفِّر الخدمة، وأن يقدِّم قائمةً بما يمكن أن يوثق به من أجهزة بوّابة الاستيقان أو آليةً (من قبيل المفاتيح المتبادلة مسبقاً أو الشهادات الرقمية) لتمييز ما يمكن أن يوثق به من هذه الأجهزة. وتنبغي حماية المعلومات التي تُنْقَل بين جهاز بوّابة الاستيقان ومنصة الخدمة. وينبغي أن تُعْمِل أجهزة بوّابة الخدمة آلية ترخيص (مثل قائمة منصات الخدمة المجازة) على الواجهات البينية المعروضة لبرمجة التطبيق

بحيث لا يمكن تبادل نعوت استيقان الشبكة إلا مع منصات الخدمة المتعاقد معها. ولا تندرج المبادئ التوجيهية بشأن كيفية التوصل إلى إقامة هذه العلاقة القائمة على الثقة ضمن نطاق هذه التوصية.

2.3.6 وصف الواجهة البينية

إن آلية الاستيقان تُعمِل واجهاتٍ بينيةً لبرمجة التطبيق جيدةَ التحديد خاصة بالشبكة يمكن لتطبيقات الخدمة أن تتصل بها للحصول من الشبكة على نعوت الاستيقان.

ويمكن لمشغِّلي الشبكات أن يُعمِلوا واجهات بينية لبرمجة التطبيق في أشكال معيَّنة بحسب تفضيلاتهم. أما تعريف هذه الواجهات البينية لبرمجة التطبيق فيخرج عن نطاق هذه التوصية.

ويمكن أن تشمل نعوت الاستيقان التي يجوز تبادلها على هذا النحو أي معلومة متصلة بمستعمل للشبكة مُستَيْقَن منه، مثل مكان وجود المستعمل، والمعلومات المتعلقة باشتراكه، وإحصائيات استعماله للشبكة، وهكذا دواليك.

7 الاعتبارات الأمنية

عندما تطبَّق الحلول التقنية المتعلقة بالإطار المذكور في القسم 6، تتعيَّن الإحاطة ببعض الاعتبارات الأمنية:

- من المهم أهميةً حيوية حماية عناصر الاستيقان على الشبكة، والتكفل بكون وظيفة استيقان الشبكة جديرة بالثقة ومأمونة.
- ينبغي أن تقيم نظم الخدمات علاقة مع الشبكة قائمة على الثقة، بحيث تتسنى ثقة نظم الخدمات المعتمدة على الشبكة بالنعوت الاستيقانية المنقولة منها. فينبغي أن لا تثق منصة الخدمة إلا بمعلومات الهوية الصادرة عن مخدم استيقان معروف وذلك تفادياً لانتحال صفة مخدم الاستيقان.
- من المهم أهمية حيوية السهر على أمن إحالة نعوت الاستيقان إلى منصة الخدمة. فينبغي ضمان سريةِ وسلامةِ المعلومات المتعلقة بهوية المستعمل وحماية إرسالها من عمليات الاستنساخ التدليسي والتزييف.
- ينبغي أن تتقيد الشبكة، عند تقديم نتائج الاستيقان وغيرها من المعلومات المتعلقة بالمستعملين إلى منصة الخدمة، بالقوانين واللوائح المتعلقة بحماية الخصوصية والواجب تطبيقها في إطار الولاية القضائية للمكان الذي تُوفَّر فيه الخدمة.
- وينبغي لمنصة الخدمة أن تتناول على نحو سليم المعلومات المتعلقة بالاستيقان من المستعملين التي يُحصل عليها من الشبكة، كأن تحفظها على نحو مأمون من أجل استعمالها، وأن تتلفها سريعاً بعد استعمالها. وينبغي منع إساءة استعمال المعلومات المتعلقة بالمستعملين وتسربها.

التذييل I

حالتا استعمال

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I حالة استعمال تصدر فيها الشبكة نعوت الاستيقان

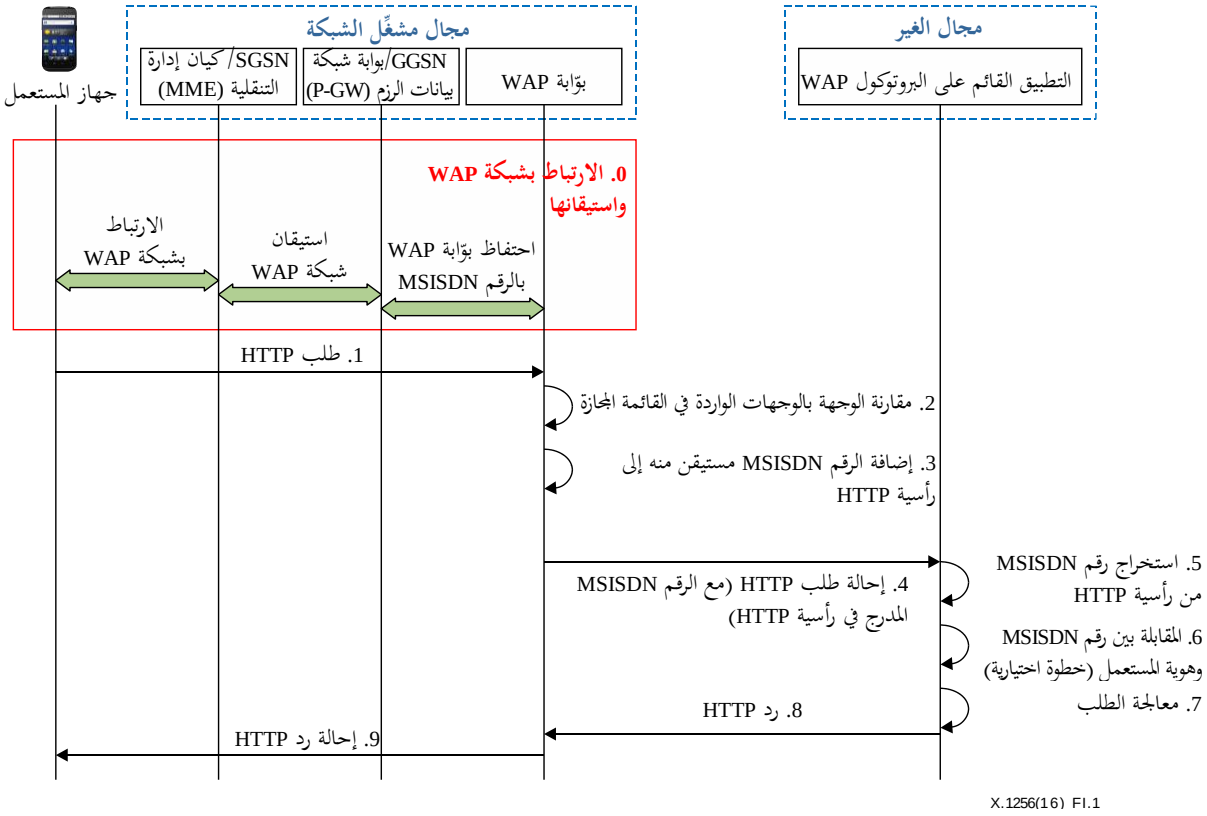
1.1.I إصدار شبكة من شبكات الجيل الثاني/الجيل الثالث/الجيل الرابع نعوت الاستيقان إلى خدمة بروتوكول التطبيق اللاسلكي

إن خدمة بروتوكول التطبيق اللاسلكي (WAP) هي خدمة بيانات متنقلة تحظى بالإقبال يمكن للمستعملين أن ينفذوا إليها عن طريق شبكات الجيل الثاني/الجيل الثالث/الجيل الرابع. وبعد الارتباط بالشبكة واستيقانها يكون بمقدور بوّابة بروتوكول التطبيق اللاسلكي (WAP GW) إدراج الرقم الدولي للمشترك المتنقل في الشبكة الرقمية للخدمات المتكاملة/الشبكة الهاتفية العمومية التبديلية (MSISDN) في طلبات WAP القادمة. ويكون بمقدور مخدم WAP استخراجُ الرقم MSISDN من الطلبات فاستبانةُ هوية المستعمل انطلاقاً من هذا الرقم مباشرة، أو المقابلةُ بين هذا الرقم وهوية المستعمل المسجَّلة.

ومن الأمثلة المعتادة على هذه التطبيقات القائمة على WAP التطبيقُ الذي يستعين به الناس لحجز سيارة تكسي. فيمكن للمستعمل المغْفَل الهوية الولوج إلى موقع من مواقع WAP هذه على هاتفه الخلوي دون إبراز اسمه الحقيقي. ويكون بمقدور مخدم WAP أن يستعمل الرقم MSISDN لاستبانة هوية المستعمل والاستجابة لطلبه. وإذا احتاج سائق التاكسي إلى الاتصال بالمستعمل المعني فيمكن له الاتصال بالرقم MSISDN المقابل.

كما يكون بمقدور مخدم WAP أن يطلب من المستعمل أن يتسجّل مقدَّماً وأن يحدِّد هوية مستعمل ويربطها بواحد أو أكثر من أرقام MSISDN. وفي هذه الحالة يحتاج مخدم WAP، قبل معالجة الطلب، إلى المقابلة بين رقم MSISDN الذي أصدرته الشبكة وهوية المستعمل المسجَّلة.

ويعرَّف الإجراء التقني المفصّل ذو الصلة على النحو المبيَّن أدناه (انظر الشكل 1.I):



الشكل 1.I – تبادل نتائج الاستيقان في حالة خدمة بروتوكول التطبيق اللاسلكي (WAP) عبر شبكة من شبكات الجيل الثاني/الجيل الثالث/الجيل الرابع

0. يرتبط جهاز المستعمل (UE) بشبكة الجيل الثاني/الجيل الثالث/الجيل الرابع. وتحتفظ بوّابة خدمة بروتوكول التطبيق اللاسلكي (WAP GW) بالرقم MSISDN لكل مستعمل مُستيْقن منه.
1. يبدأ جهاز المستعمل طلباً ببروتوكول نقل النصوص الإلكترونية (HTTP) للنفاذ إلى خدمة بروتوكول التطبيق اللاسلكي (WAP).
2. تتلقى بوّابة WAP الطلب، فتتحقق مما إذا كانت وجهة الخدمة من الوجهات المدرجة في القائمة المجازة.
3. إذا كان عنوان الوجهة مدرجاً في القائمة المجازة فإن بوّابة WAP تدرج خانة لرأسية جديدة في البروتوكول HTTP ("x-up-calling-line-id"، مثلاً) ضمن الطلب، تتضمن رقم MSISDN الخاص بالمستعمل.
4. تحيل بوّابة WAP الطلب ببروتوكول HTTP المعدَّل إلى مخدم WAP.
5. يستخرج مخدم WAP رقم MSISDN الخاص بالمستعمل من رأسية HTTP.
6. يكون لمخدم WAP خيار المقابلة بين رقم MSISDN وهوية المستعمل المسجَّلة.
7. يقوم مخدم WAP بمعالجة الطلب وفقاً لرقم MSISDN أو لهوية المستخدم المقابلة لهذا الرقم.
8. يرسل مخدم WAP رد HTTP إلى بوّابة WAP.
9. تحيل بوّابة WAP رد HTTP إلى جهاز المستعمل.

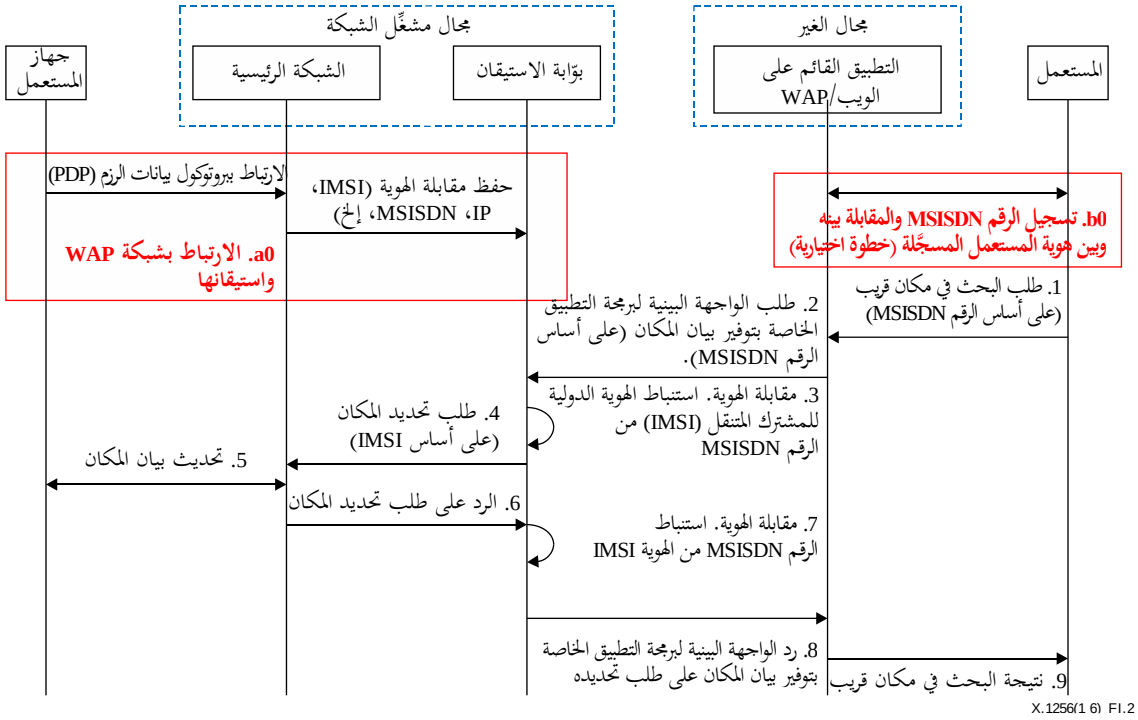
2.I حالة استعمال تُستصدر فيها نعوت الاستيقان في سياق الخدمة

1.2.I استعمال نعوت الموقع من أجل تحديد المكان في شبكة من شبكات الجيل الثاني/الجيل الثالث/الجيل الرابع

يتوفَّر على الإنترنت والإنترنت المتنقلة كثير من الخدمات المستندة إلى تحديد المكان. فعلى سبيل المثال يمكن للمستعمل أن يتصفح خدمة لبروتوكول التطبيق اللاسلكي (WAP) انطلاقاً من هاتفه الخلوي فيبحث عن مصرف أو فندق أو مطعم أو متجر قريب. وإذا كان الهاتف مجهَّزاً بالنظام العالمي لتحديد المواقع فإنه يمكن أن يرسل بيان مكان المستعمل إلى مخدم WAP في إطار طلب

البحث. أما إذا لم يكن الهاتف مجهَّزاً بالنظام العالمي لتحديد المواقع أو لم يعمل هذا النظام عند اللزوم (بسبب الوجود ضمن المباني مثلاً)، فقد يحتاج مخدم WAP إلى دعم من شبكة الجيل الثاني/الجيل الثالث/الجيل الرابع الرئيسية لتحديد مكان وجود المستعمل.

ويعرَّف الإجراء التقني المفصَّل لاستعمال خدمة الإنترنت لنتائج تحديد المكان في شبكة من شبكات الجيل الثاني/الجيل الثالث/الجيل الرابع على النحو المبيَّن أدناه (انظر الشكل 2.I):



الشكل 2.I – استعمال خدمة الإنترنت لنعوت تحديد المكان في شبكات من شبكات الجيل الثاني/الجيل الثالث/الجيل الرابع

a0. يرتبط جهاز المستعمل (UE) بشبكة الجيل الثاني/الجيل الثالث/الجيل الرابع. وتقوم عقدة دعم بوّابة الخدمة العامة للاتصالات الراديوية بأسلوب الرزم (GGSN)/بوابة شبكة بيانات الرزم (P-GW) بإرسال علاقة المقابلة بين الهوية الدولية للمشترك المتنقل (IMSI) والرقم MSISDN وعنوان بروتوكول الإنترنت إلى بوّابة الاستيقان بواسطة بروتوكول خدمة الاستيقان عن بُعد من المستعملين الداخلين (RADIUS)؛

b0. يكون للمستعمل خيار التسجل على مخدم التطبيقات المستند إلى شبكة الويب/بروتوكول التطبيق اللاسلكي (WAP) وربط هوية المستعمل الخاصة به بواحد أو أكثر من أرقام MSISDN.

1. يستهل المستعمل طلب بحث في مكان قريب، يتضمن رقم MSISDN الخاص به بمثابة أحد المعطيات. ويمكن أن تدرج بوّابة WAP الرقم MSISDN على النحو المبيَّن في 1.1.I، أو أن يدخله المستعمل بنفسه وأن يتحقق منه المخدم على نحوٍ ما يخرج عن نطاق التوصية الحالية.

2. يقوم مخدم WAP/شبكة الويب بتحليل الرقم MSISDN الوارد في الطلب ويتصل بالواجهة البينية لبرمجة التطبيق الخاصة بتوفير بيان المكان (Get Location API) لإرسال طلب إلى بوّابة الاستيقان يتضمن الرقم MSISDN المحدَّد.

3. تقوم بوّابة الاستيقان بالمقابلة بين الرقم MSISDN (الهوية في الخدمة) والهوية IMSI (الهوية في الشبكة).

4. تسأل بوّابة الاستيقان الشبكة الرئيسية عن المكان الحالي المقابل للهوية الدولية للمشترك المتنقل (IMSI).

5. تتصل الشبكة الرئيسية بجهاز المستعمل المقابل للهوية IMSI وتنجز تحديث بيان المكان.

6. ترد الشبكة الرئيسية على طلب بوّابة الاستيقان توفير بيان المكان.

7. تستنبط بوّابة الاستيقان الرقم MSISDN من الهوية IMSI.

8. تجيب بوّابة الاستيقان على اتصال مخدم WAP/شبكة الويب الرامي إلى الحصول على بيان المكان عن طريق الواجهة البينية لبرمجة التطبيق.

9. يقوم مخدم WAP/شبكة الويب بالرد على طلب البحث في مكان قريب الصادر عن المستعمل بواسطة المعلومات المتعلقة بالمكان المستقاة من الشبكة ويبين نتائج البحث للمستعمل.

بيبليوغرافيا

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 4186] IETF RFC 4186 (2006), *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).*

[3GPP TS 33.328] 3GPP TS 33.328 V12.6.0 (2014), *IP Multimedia Subsystem (IMS) media plane security (Release12).*

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، 2017