الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1812

(2022/05)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الاتصالات المتنقلة الدولية–2020

إطار الأمن القائم على علاقة الثقة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

التوصية ITU-T X.1812

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 (1)	X.1149-X.1140
أمن التطبيق (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.1350
أمن أنظمة النقل الذكية (ITS)	X.1399-X.1370
أمن تكنولوجيا سجل الحسابات الموزع (DLT)	X.1429-X.1400
أمن التطبيق (2)	X.1459-X.1450
أمن الويب (2)	X.1489-X.1470
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
الدفاع السيبراني	X.1599-X.1590
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
مولِّد 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
حماية البيانات	X.1789–X.1770
أمن شبكات الاتصالات المتنقلة الدولية–2020	**X.1819–X.1800**

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

التوصية ITU-T X.1812

إطار الأمن القائم على علاقة الثقة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

ملخص

تحدد التوصية ITU-T X.1812 أصحاب المصلحة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 (IMT-2020، المعروفة أيضاً باسم الجيل الخامس) وتحلل علاقات الثقة بينهم وتحدد التهديدات وتوضح المسؤوليات الأمنية لكل من أصحاب المصلحة، وتحدد حدود الأمن بين أصحاب المصلحة وتنشئ إطاراً أمنياً يستند إلى علاقات الثقة هذه.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1812	2022-05-20	17	11.1002/1000/14808

مصطلحات أساسية

النظام الإيكولوجي، الإطار، الاتصالات المتنقلة الدولية–2020، الثقة.

* 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-ar.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة 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 https://www.itu.int/ar/ITU-T/ipr/Pages/default.aspx.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 مصطلحات معرَّفة في مصادر أخرى 1
2.3 المصطلحات المعرفة في هذه التوصية 2
4 المختصرات والأسماء المختصرة 3
5 الاصطلاحات 4
6 لمحة عامة 4
7 إطار الأمن المدعوم بالنموذج الموثوق 6
8 دور أصحاب المصلحة في سيناريوهات النظام الإيكولوجي للاتصالات المتنقلة الدولية-2020 7
1.8 اعتبارات عامة 7
2.8 السيناريو 1: التمثيل الافتراضي لنشر الشبكة في ميدان مشغِّل الشبكة 7
3.8 السيناريو 2: التوصيل البيني والتجوال 9
4.8 السيناريو 3: استئجار سيارة مع التشغيل عن بُعد 10
5.8 السيناريو 4: انفتاح قدرات الشبكة لدوائر الصناعة 11
6.8 السيناريو 5: سلاسل التوريد 12
7.8 أصحاب المصلحة في النظام الإيكولوجي للاتصالات المتنقلة الدولية-2020 14
9 مستوى الثقة ومعايير الثقة ونموذج الثقة 15
1.9 اعتبارات عامة 15
2.9 مستويات الثقة 15
3.9 معايير الثقة 17
4.8 نموذج الثقة القائم على خارطة ارتباطات علاقة الثقة 18
10 متطلبات الأمن المدعوم بنموذج الثقة القائم على علاقات الثقة 20
1.10 اعتبارات عامة 20
2.10 متطلبات الأمن من مستوى الثقة 20
3.10 تفسير الثقة بمتطلبات ضمان تفصيلية 23
بيبليوغرافيا 25

مقدمة

إن مجموعة أصحاب المصلحة في نظام الاتصالات المتنقلة الدولية–2020 (نظام IMT-2020 المعروف أيضاً باسم الجيل الخامس (5G)) أكبر وأكثر تنوعاً منها في أنظمة الاتصالات السابقة. ففي الجيل الثاني والثالث والرابع (2G و3G و4G)، يمكن تلخيص أصحاب المصلحة الرئيسيين كمقدمي الخدمة ومشغلي الشبكات وبائعي المعدات والمشتركين. ولكن تشارك جهات فاعلة تخصصية أيضاً في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020، مثل المؤسسات الصناعية والتجارية. ويمكن أيضاً تقسيم مقدمي الخدمات إلى مشغلي المنصات السحابية وشركات تحليل البيانات وموردي التطبيقات وما إلى ذلك. وعلاوة على ذلك، فإن المشتركين في النهاية الطرفية، ليسوا هم المستعملين النهائيين فحسب كما كان الحال من قبل. ويمكن أن تندرج في عداد المشتركين مجموعة من أنواع مختلفة من أصحاب المصلحة، خاصة بالنسبة للمطاريف التجارية، ومثال ذلك في حالة الاستعمال المشترك لاتصالات المركبة. وتقيم هذه التغييرات علاقات معقدة بين مختلف أصحاب المصلحة، وتثير مجموعة من الإشكالات الأمنية الجديدة للأنظمة الإيكولوجية للاتصالات المتنقلة الدولية–2020.

وتقدم شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020) أيضاً ميزات جديدة أيضاً. فعلى سبيل المثال، يؤدي إدخال التمثيل الافتراضي للشبكة في الاتصالات المتنقلة الدولية–2020 إلى قطع التوصيلات الثابتة بين كيانات الشبكة وتمكين الشبكات المعرفة بالبرمجيات. وثمة مثال آخر تقدمه معمارية الخدمات القائمة على الخدمة. وبمثل هذه المعمارية، يمكن تضمين المزيد من الميزات المتصلة بالحوسبة السحابية في شبكة الاتصالات المتنقلة الدولية–2020. ويمكن للتقسيم إلى شرائح أيضاً أن يمكّن من تحقيق تعاون أكثر فعالية بين شبكة الاتصالات المتنقلة الدولية–2020 وخدماتها.

وبمرور الوقت، ستُطبق أعداد متزايدة من تقنيات تكنولوجيا المعلومات (IT) على أنظمة الاتصالات المتنقلة الدولية–2020، ليس على خدماتها فحسب، بل أيضاً على شبكتها. وتقوم شبكة الاتصالات المتنقلة الدولية–2020 على بروتوكول الإنترنت بالكامل. ويعتمد توصيف معماريتها على الخدمات بدلاً من النقاط المرجعية، كما كان الحال في معماريات الشبكات السابقة. وتنتقل الإشارات بشكل متزايد من الإنترنت وليس من شبكات مخصصة. وقد تغيّر بروتوكول النقل في شبكات الاتصالات المتنقلة الدولية–2020 من بروتوكول القطر [b-IETF RFC 6733]، وهو أقل شيوعاً من بروتوكول نقل النصوص المترابطة المستعمل على نطاق واسع عالمياً. وستجلب هذه التغييرات كلها فوائد لنشر وتشغيل شبكات الاتصالات المتنقلة الدولية–2020 وخدماتها.

ولكن يمكن لاستعمال البروتوكولات الرائجة وبيئة التوصيل المفتوحة أن يعود بفوائد على المهاجمين أيضاً. ولن يحتاج المهاجم إلى قضاء الكثير من الوقت لدراسة بروتوكولات الاتصالات المعقدة، ولعل من الأسهل عليه العثور على ثغرة في الشبكة لينسل منها. ونتيجة لذلك، ليس من المعقول أن نفترض في شبكات الاتصالات المتنقلة الدولية–2020 أن الاتصالات الداخلية جديرة بالثقة بعدئذ. وهكذا، فإن التغيرات من الجيل الرابع إلى الاتصالات المتنقلة الدولية–2020 تحطم علاقة الثقة بين مشغلي الشبكات.

وبالإضافة إلى ذلك، صُممت شبكة الاتصالات المتنقلة الدولية–2020 لتكون أكثر مرونة من أجل الإيفاء بمتطلبات الخدمة المختلفة. وعلى وجه الخصوص، أُدخل التقسيم إلى شرائح في شبكات الاتصالات المتنقلة الدولية–2020. ويمكن لشبكات الاتصالات المتنقلة الدولية–2020 أن تعرض أيضاً بعض القدرات على الخدمات. وستمكِّن تجربةُ هذه القدرات خدمة الاتصالات المتنقلة الدولية–2020 من التحكم في بعض وظائف الشبكة. وستزيد هذه الميزات الجديدة من التباس حدود الأمن بين شبكات الاتصالات المتنقلة الدولية–2020 وخدماتها الأكثر غموضاً.

وتحدد هذه التوصية أصحاب المصلحة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 وتحلل علاقات الثقة بينهم وتحدد التهديدات وتوضح المسؤوليات الأمنية لكل أصحاب المصلحة وتعرّف حدود الأمن بين أصحاب المصلحة وتضع إطاراً أمنياً قائماً على علاقات الثقة هذه.

التوصية ITU-T X.1812

إطار الأمن القائم على علاقة الثقة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

1 مجال التطبيق

توصِّف هذه التوصية إطار الأمن القائم على علاقات الثقة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 (IMT-2020). وتصف هذه التوصية نهجاً عاماً إزاء ما يلي:

- تحديد سيناريوهات تقديم خدمات الاتصالات المتنقلة الدولية–2020؛
- تحديد أصحاب المصلحة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020؛
- تحليل علاقات الثقة بين أصحاب المصلحة؛
- تحديد التهديدات المطبقة على كل صاحب مصلحة؛
- توضيح المسؤوليات الأمنية لكل صاحب مصلحة؛
- تحديد حدود الأمن بين أصحاب المصلحة؛
- توصيف متطلبات الأمن القائمة على نموذج الثقة؛
- إنشاء إطار أمني يقوم على علاقات الثقة بين أصحاب المصلحة.

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 إلى المراجعة، 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. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا يوجد.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تَستعمل هذه التوصية المصطلحات التالية المعرّفة في مصادر أخرى:

1.1.3 وحدة أعمال (business unit) [b-ISO/TS 21089]: وظيفة أو وظيفة فرعية مستقلة وخاضعة للمساءلة ضمن منظمة ما.

ملاحظة – يمكن أن تشمل وحدة الأعمال دائرة أو خدمة أو تخصص ضمن منظمة تقدم الرعاية الصحية.

2.1.3 النشر (deployment) [b-ISO/IEC/IEEE 24765]: مرحلة في مشروع يجري فيها تشغيل نظام وحل إشكالات الانتقال إلى المرحلة التالية.

3.1.3 المطوِر (developer) [b-NIST SP 800-53]: الكيان الذي يشمل: '1' مطوري أو مصنعي أنظمة المعلومات أو مكونات النظام أو خدمات نظام المعلومات؛ و'2' مجمعي الأنظمة؛ و'3' الباعة؛ و'4' موزعي المنتجات.

4.1.3 الميدان (domain) [b-ISO/IEC 14888-1]: مجموعة من الكيانات تعمل بموجب سياسة أمنية واحدة.

مثال – شهادات المفتاح العمومي التي تنتجها سلطة واحدة أو مجموعة من السلطات تستعمل سياسة الأمن نفسها.

5.1.3 نظام المعلومات (information system) [b-ISO/IEC 27000]: مجموعة تطبيقات أو خدمات أو أصول تكنولوجيا المعلومات أو غيرها من مكونات تداول المعلومات.

6.1.3 دورة الحياة (lifecycle) [b- ISO/IEC/IEEE 15288]: تطور نظام أو منتج أو خدمة أو مشروع أو أي كيان آخر من صنع الإنسان، من النشأة الأولى حتى التقاعد.

7.1.3 وظيفة الشبكة (network function) [b-ITU-T Y.3100]: في سياق الاتصالات المتنقلة الدولية–2020، هي وظيفة المعالجة في الشبكة.

الملاحظة 1 – تشمل وظائف الشبكة على سبيل المثال لا الحصر وظائف عقدة الشبكة، مثل إدارة الدورة وإدارة التنقلية ووظائف النقل التي يعرّف سلوكها الوظيفي وسطوحها البينية.

الملاحظة 2 – يمكن تنفيذ وظائف الشبكة على عتاد مخصص أو كوظائف برمجيات ممثَّلة افتراضياً.

الملاحظة 3 – لا تعتبر وظائف الشبكة موارد وإنما يمكن تمثيل حالة أي من وظائف الشبكة باستعمال الموارد.

8.1.3 صاحب المصلحة (stakeholder) [b-ISO/PAS 19450]: فرد أو منظمة أو مجموعة من الأشخاص لديهم مصلحة، أو قد يتأثرون، بالنظام الجاري التفكير فيه أو تطويره أو نشره.

9.1.3 المورِّد (supplier) [b-ISO 10393]: منظمة أو شخص يقدم منتجاً أو خدمة.

10.1.3 تطوير النظام (system development) [b-ISO/IEC 2382]: عملية تتضمن عادة تحليل المتطلبات وتصميم النظام وتنفيذه وتوثيقه وضمان جودته.

11.1.3 الثقة (trust) [b-ISO/IEC 25010]: درجة ثقة المستعمل أو أي صاحب مصلحة آخر بأن المنتج أو النظام سيتصرف على النحو المقصود.

12.1.3 مستوى الثقة (trust level) [b-ISO 28598-1]: تقدير العميل لوزن الأدلة السابقة والتكميلية وغير المباشرة على قدرة المورد على الإيفاء بمتطلبات الجودة المحددة.

2.3 المصطلحات المعرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 مقدم الخدمة الخارجي: مجموعة من الكيانات تشمل أ) كيانات ضمن المنظمة ولكن خارج حدود التخويل الأمني الموضوعة لأنظمة معلومات المنظمة؛ أو ب) كيانات خارج المنظمة إما في القطاع العام (مثل الوكالات الفيدرالية) أو القطاع الخاص (مثل مقدمي الخدمات التجارية)؛ أو ج) توليفة ما من خيارات القطاعين العام والخاص.

ملاحظة – مقتبس من المرجع [b-NIST SP 800-53].

2.2.3 سلسلة التوريد: شبكة من المنظمات المعنية من خلال الوصلات باتجاه المصدر وباتجاه المقصد في العمليات والأنشطة التي تنتج قيمة في شكل منتجات وخدمات في أيدي المستهلك النهائي.

3.2.3 دورة حياة تطوير النظام: نهج مهيكَل تجاه تخطيط نظام المعلومات وإنشائه واختباره ونشره وصيانته.

4.2.3 نموذج الثقة: نموذج يتكون من المكونات التي تصف علاقات الثقة والسلاسل بين أصحاب المصلحة.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

2G الجيل الثاني *(second Generation)*

3G الجيل الثالث *(third Generation)*

4G الجيل الرابع *(fourth Generation)*

5G الجيل الخامس *(fifth Generation)*

5GC شبكة الجيل الخامس الأساسية *(fifth Generation Core)*

BS محطة القاعدة *(Base Station)*

CAB هيئة تقييم المطابقة (*Conformity Assessment Body*)

E2E من طرف إلى طرف (*End to End*)

HO المشغِّل المحلي *(Home Operator)*

ICP مقدِّم محتوى الإنترنت *(Internet Content Provider)*

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

IMT-2020 الاتصالات المتنقلة الدولية−2020 *(International Mobile Telecommunications-2020)*

IoT إنترنت الأشياء (*Internet of Things*)

IoV إنترنت المركبات (*Internet of Vehicles*)

IPX تبادل الرزم بين الشبكات (*Internetwork Packet Exchange*)

ISP مقدم خدمة الإنترنت *(Internet Service Provider)*

IT تكنولوجيا المعلومات (*Information Technology*)

NE عنصر الشبكة (*Network Element*)

NESAS خطة ضمان أمن معدات الشبكة (*Network Equipment Security Assurance Scheme*)

NF وظيفة الشبكة (*Network Function*)

NFV التمثيل الافتراضي لوظائف الشبكة (*Network Functions Virtualization*)

NPN شبكة غير عمومية *(Non-Public Network)*

PII المعلومات المحدِّدة لهوية الشخص (*Personal Identifiable Information*)

PLMN شبكة الاتصالات المتنقلة البرية العمومية (*Public Land Mobile Network*)

SCAS توصيف ضمان الأمن (*Security Assurance Specification*)

SDL دورة حياة تطوير الأمن (*Security Development Lifecycle*)

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

VNF وظيفة الشبكة الممثَّلة افتراضياً (*Virtualized Network Function*)

VO المشغِّل المزار *(Visited Operator)*

5 الاصطلاحات

يتعين فهم الاصطلاحات الأساسية التالية في هذه التوصية على النحو التالي:

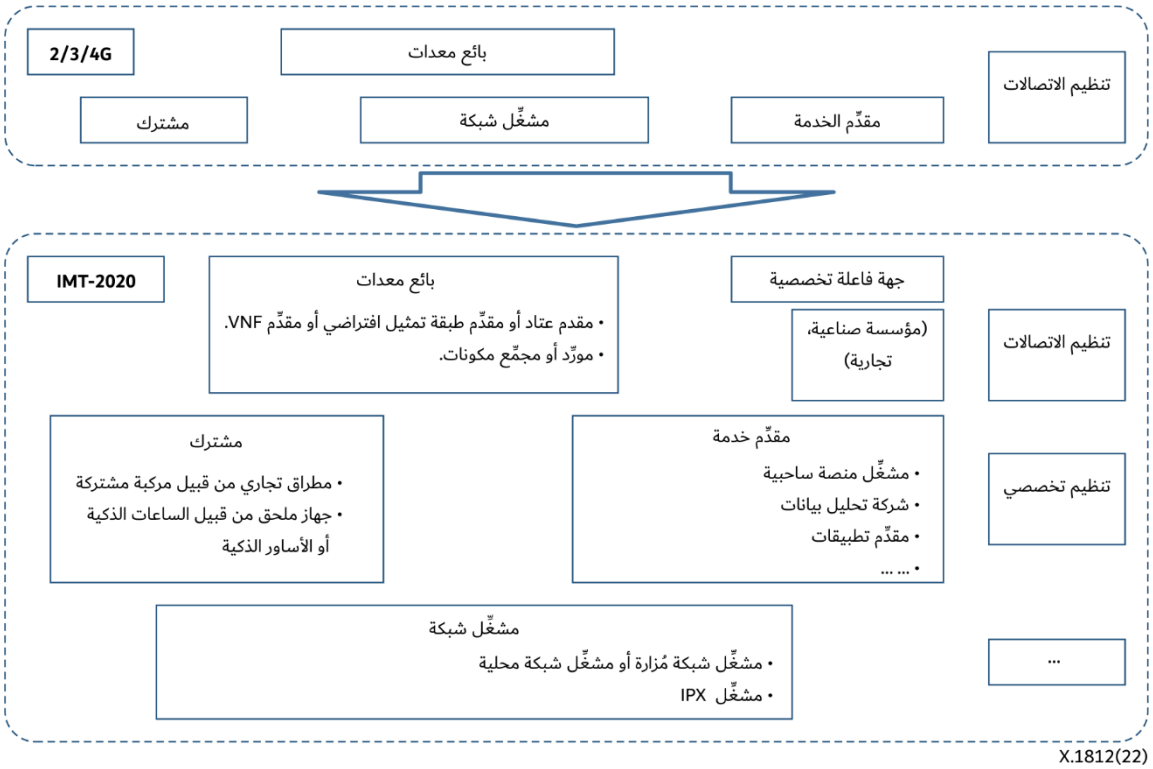
"**يوصى**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

وعبارة "**يمكن اختيارياً**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

6 لمحة عامة

قبل عصر الجيل الخامس (5G)، كانت أنظمة الاتصالات تُستعمل أساساً لتقديم المهاتفة والنفاذ إلى الإنترنت والخدمات ذات الصلة. ونتيجة لقدرات هذه الأنظمة وقيود معدلها، كانت حالات الاستعمال بسيطة عموماً. وعلى وجه الخصوص، لم يتضمن نظام الاتصالات سوى عدد قليل من الأدوار. ففي خدمة النداء، تكون الأطراف الفاعلة هي الطالب والمطلوب وشبكة الاتصالات المتنقلة. وفي خدمة البيانات، تكون الأطراف الفاعلة هي المطراف وشبكة الاتصالات المتنقلة ومقدمي الخدمات/التطبيقات. بالإضافة إلى ذلك، يشارك البائعون لدعم بناء الشبكات وأنظمة التطبيقات. ويُعتبر مصنعو المطاريف ومقدمو بطاقة الدارة المتكاملة الشاملة (UICC) ذوي صلة عند المطراف. وهذه هي الأدوار الرئيسية التي تضطلع بها أنظمة الاتصالات من الجيل الثاني والثالث والرابع (2G و3G و4G).

ولكن تختلف الأشياء في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 (IMT-2020). فلا يشتمل النظام الإيكولوجي على جميع أصحاب المصلحة في نظام الاتصالات في المطاريف والشبكات والخدمات فحسب، بل يشمل أيضاً أصحاب المصلحة الآخرين. وفي المطراف، المشتركون ليسوا المستعملين النهائيين وحدهم، كما كان الحال من قبل، لأن الجهاز المتنقل يمكن أن يكون أحد الأنواع المختلفة العديدة من المعدات التي قد تتشارك فيها أطراف متعددة، وليس الهاتف فحسب. وفي الشبكة، تُدخل الاتصالات المتنقلة الدولية–2020 مجموعة من الميزات الجديدة. فعلى سبيل المثال، يقطع التمثيل الافتراضي للشبكة في الاتصالات المتنقلة الدولية–2020 التوصيل الثابت بين كيانات الشبكات، ويُمكّن الشبكات المعرّفة بالبرمجيات التي يخرق حدود أمن نشر الشبكات. ويُطبَّق المزيد فالمزيد من تقنيات تكنولوجيا المعلومات (IT) في شبكات الاتصالات المتنقلة الدولية–2020 التي يمكن للمهاجمين أيضاً استغلالها. فتفتح خدمة انكشاف الشبكة للمهاجم سطوحاً بينية في مستوي التحكم بدلاً من مستوي المستعمل. ففي الخدمات، تشارك جهات فاعلة تخصصية، مثل المؤسسات الصناعية والتجارية. وهذا يقسم مقدمي الخدمات إلى مشغلي المنصات السحابية وشركات تحليل البيانات ومقدمي التطبيقات وما إلى ذلك، على النحو المبين في الشكل 1.



X.1812(22)

الشكل 1 – تطور النظام الإيكولوجي من الجيل الثاني والثالث والرابع (2G و3G و4G) إلى الاتصالات المتنقلة الدولية–2020

وفي هذه الحالة، تختلف علاقة الثقة في نظام الاتصالات المتنقلة الدولية–2020. إذ إن المستعملين والمشتركين وأنظمة الشبكات والخدمات أقرب كثيراً من ذي قبل. وسلسلة التوريد المعقدة وطويلة الذيول تدفع المشغلين إلى النظر أكثر في تقييم الموردين. فالروابط الشديدة بين الخدمات والشبكات تحمل الصناعات التخصصية إلى الاعتماد كثيراً على الشبكة وتتطلب صرامة أكبر في الثقة والأمن. ويحتاج تقديم نموذج ثقة جديد للنظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 إلى النظر في صياغة متطلبات أمنية وحدود أمنية واضحة بين أصحاب المصلحة. وبهذه الطريقة، يمكن تحسين كفاءة الاتصالات قدر الإمكان مع ضمان أمن البيانات.

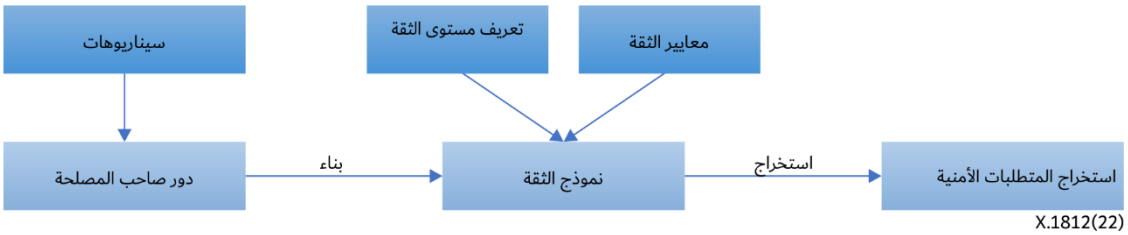
وهناك خمس خصائص تؤثر على جدارة نظام الاتصالات المتنقلة الدولية–2020 (IMT-2020) بالثقة، وهي الصمود، وأمن الاتصالات، وإدارة الهوية، وحماية المعلومات المحددة لهوية شخص (PII) وضمان الأمن:

- الصمود: الصمود هو قدرة المنظمة على مقاومة التأثر بالأعطال. ويمكن لمجموعة متنوعة من الميزات التكميلية والمتداخلة جزئياً في الاتصالات المتنقلة الدولية–2020 أن تساعد على تحقيق قدرة نظام الاتصالات المتنقلة الدولية–2020 على الصمود أمام الهجمات السيبرانية والحوادث غير الخبيثة.
- أمن الاتصالات: يطبق أمن الاتصالات على اتصالات البيانات في الاتصالات المتنقلة الدولية–2020. وتعد الاتصالات الآمنة للأجهزة ولبنيتها التحتية الخاصة أمراً حيوياً في نظام للاتصالات المتنقلة الدولية–2020.
- إدارة الهوية: يتألف نظام إدارة الهوية من عمليات وسياسات تتعلق بإدارة دورة الحياة والقيمة والنوع والبيانات الشرحية الاختيارية للنعوت التي تشكل هويات الكيانات في نظام الاتصالات المتنقلة الدولية–2020. ويوصى بتقديم إدارة هوية آمنة لتعرف واستيقان المشتركين أو التجوال أو عدمه، وضمان أن يقتصر النفاذ إلى خدمات الشبكة على المشتركين الحقيقيين. وتبنى هذه الأنظمة على بدائيات تجفيرية وخصائص أمنية قوية.
- حماية المعلومات المحددة لهوية شخص (PII): تعرّف حرمة البيانات في المعيار [b-ISO/TS 21719-2] بأنها حقوق والتزامات الأفراد والمنظمات فيما يتعلق بجمع المعلومات الشخصية واستعمالها والاحتفاظ بها والإفصاح عنها والتخلص منها. وتنطوي حماية المعلومات المحددة لهوية شخص على حماية المعلومات التي لا يمكن أن تستعملها أطراف غير مخولة لتحديد هوية المشتركين.

- ضمان الأمن: يقدم ضمان الأمن أسباباً للثقة المبررة بأن الادعاء بشأن تحقيق أهداف الأمن قد تحقق أو سيتحقق. وضمان الأمن هو وسيلة لضمان تلبية معدات الشبكة لمتطلبات الأمن وتحقيقها من خلال اعتماد عمليات آمنة للتطوير ودورة حياة المنتج.

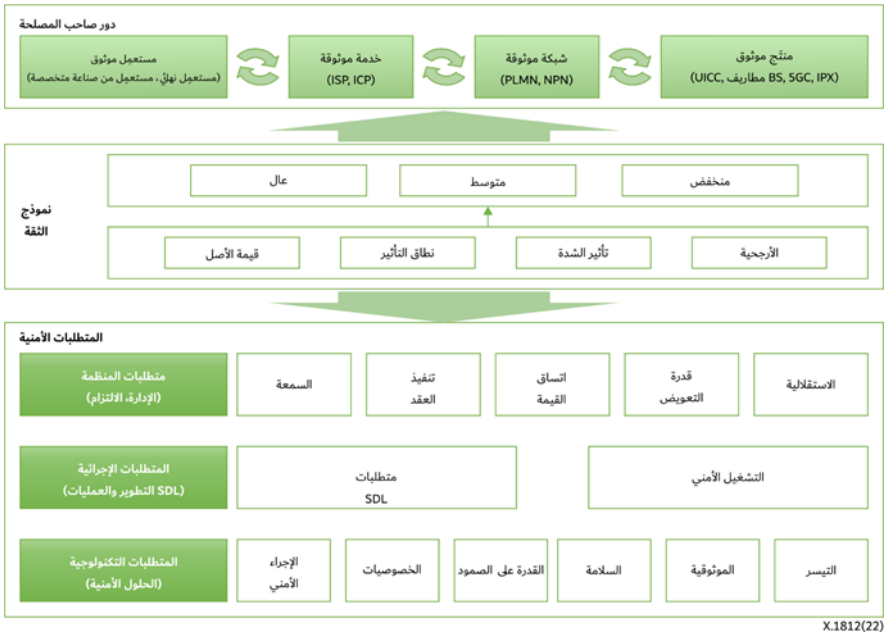
7 إطار الأمن المدعوم بالنموذج الموثوق

تحلل هذه التوصية وتحدد أصحاب المصلحة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 وعلاقات الثقة بين الأدوار بتحليل عدة سيناريوهات نمطية. وهي تسعى بعد ذلك لتحديد مستوى الثقة مع العوامل الرئيسية التي يتعين النظر فيها. وهي على هذا الأساس، تقدم توصيات بشأن كيفية تحديد متطلبات أمنية تقوم على مستوى الثقة، وتشكيل إطار أمني يقوم على علاقة الثقة، على النحو الموضح في الشكل 2.



الشكل 2 – الأفق المستقبلي لبناء إطار الأمن القائم على علاقات الثقة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

يوضَّح في الشكل 3 إطار الأمن الذي يدعمه نموذج الثقة المحدد في هذه التوصية استناداً إلى الدور والعلاقة ونموذج الثقة والمتطلبات الأمنية لجميع أصحاب المصلحة. ويرد وصف جميع مكونات الإطار في الفقرة 8 بشأن دور أصحاب المصلحة؛ والفقرة 9 بشأن نموذج الثقة؛ والفقرة 10 بشأن المتطلبات الأمنية.



الشكل 3 – إطار الأمن المدعوم بالنموذج الموثوق على أساس علاقة الثقة بين أصحاب المصلحة

5GC: شبكة الجيل الخامس الأساسية؛ BS: محطة القاعدة؛ ICP: مقدِّم محتوى الإنترنت؛ ISP: مقدم خدمة الإنترنت؛ NPN: شبكة غير عمومية؛ SDL: دورة حياة تطوير الأمن

8 دور أصحاب المصلحة في سيناريوهات النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

1.8 اعتبارات عامة

يمكن تقسيم نظام الاتصالات الحالي من ثلاثة أنظمة فرعية: مطراف وشبكة وخدمة. وتقتضي الضرورة النظر في العلاقات الممكنة بين كل نظام فرعي وآخر، وضمن نظام فرعي. وبما أن المنظمات الأخرى المعنية بوضع المعايير مثل مشروع شراكة الجيل الثالث (3GPP) قد سبق أن درست العلاقة بين مطراف وشبكة، فإن هذه الفقرة لن تتناولها بمزيد من البحث.

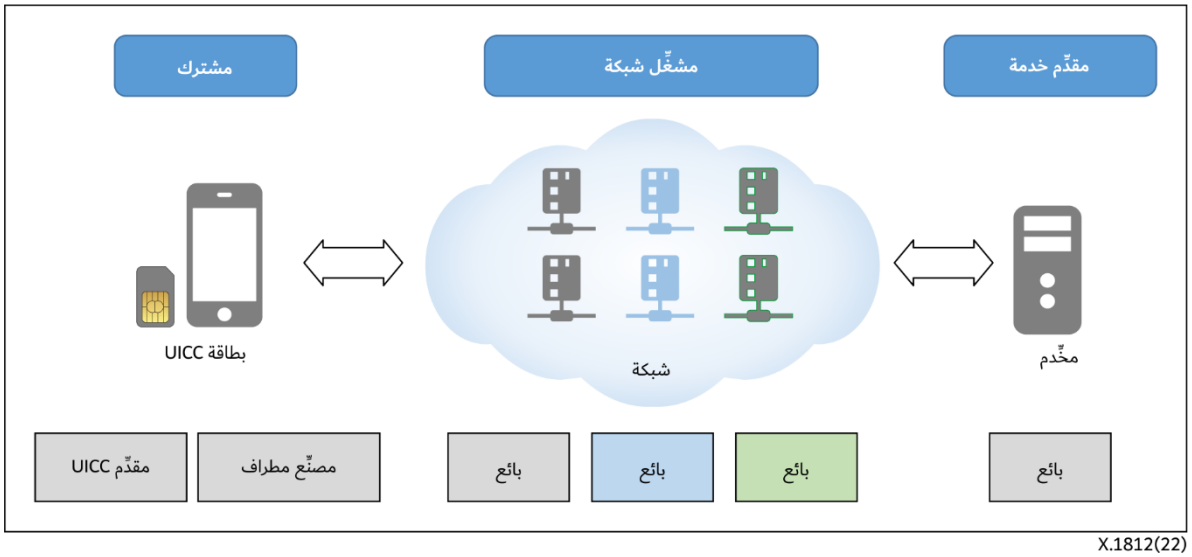
وبشكل جماعي، تغطي مجموعة السيناريوهات الخمسة التي تتناولها هذه الفقرة جميع العلاقات الممكنة بين الأنظمة باستثناء العلاقة بين مطراف وشبكة.

2.8 السيناريو 1: التمثيل الافتراضي لنشر الشبكة في ميدان مشغِّل الشبكة

1.2.8 اعتبارات عامة

يركز هذا السيناريو في المقام الأول على علاقة الشبكة الداخلية.

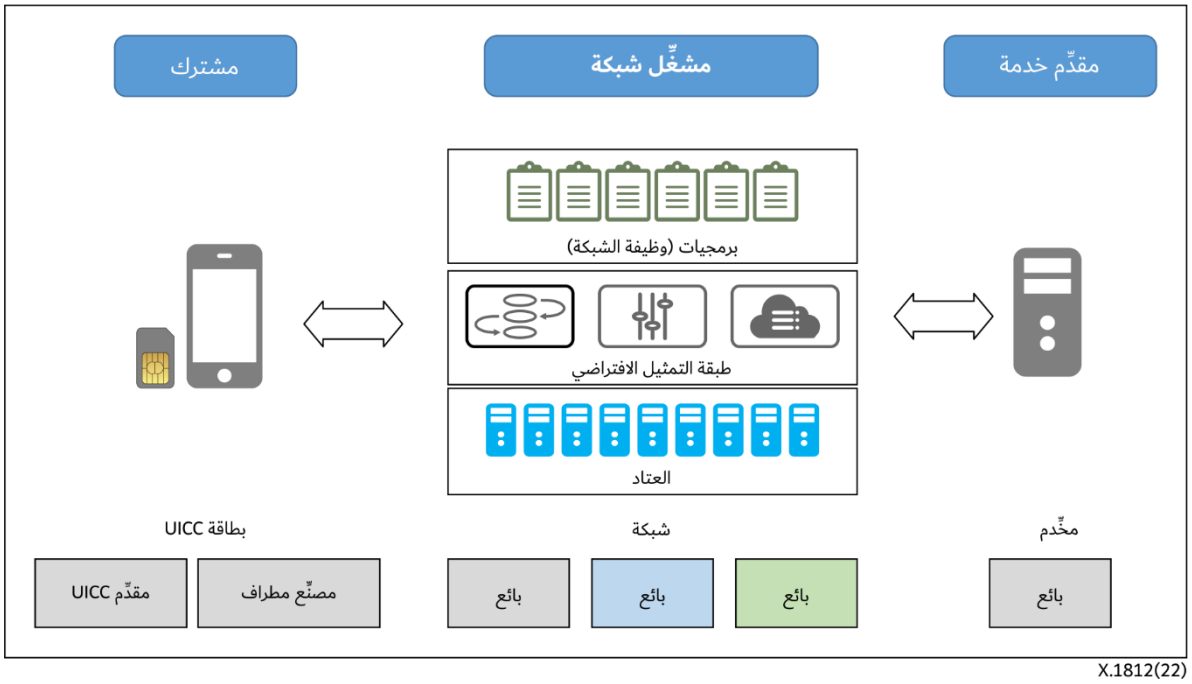
وعادةً ما تنفَّذ عناصر الشبكة (NE) المنشورة في شبكة ما في شبكات الاتصالات الحالية كأجهزة مادية مكرَّسة. ويجري تنفيذ كل عنصر شبكة في شكل واحد أو أكثر من مخدمات الكيانات المادية، بناءً على قدرته. وتستعمل الكبلات والألياف والبدالات والمسيّرات لتوصيل هذه الأجهزة الشبكية من خلال السطوح البينية المادية. وفي هذا السيناريو، فإن أصحاب المصلحة الرئيسيين هم المستعملون أو المشتركون، ومصنعو المطاريف المتنقلة، وبطاقة الدارة المتكاملة الشاملة (UICC)، ومقدمو الخدمات وباعة أجهزة الشبكات والمشغلون، ويرد توضيح ذلك في الشكل 4.



الشكل 4 – أصحاب المصلحة الرئيسيون في ميدان مشغِّل الشبكة

وفي الاتصالات المتنقلة الدولية–2020، تطورت تكنولوجيا الشبكات المعرفة بالبرمجيات (SDN) والتمثيل الافتراضي لوظائف الشبكة (NFV) تطوراً كبيراً، وقد بدأ نشرها تدريجياً في الشبكة. وتتطور شبكات الاتصالات أيضاً مع زيادة استعمال تكنولوجيا المعلومات. وعند تصميم معمارية شبكة الاتصالات المتنقلة الدولية–2020، أُدخلت معمارية جديدة قائمة على الخدمة للاستفادة بشكل أفضل من تكنولوجيا المعلومات في النشر والصيانة. ويستعاض عن عنصر الشبكة بوظيفة الشبكة (NF) التي تتسم بقدر أكبر من المرونة في التشغيل والصيانة. ويمكن تنفيذ وظيفة الشبكة كوظيفة الشبكة الممثَّلة افتراضياً (VNF) حتى في شكل تطبيقات برمجيات تعمل على آلة افتراضية. وهذا يشير إلى أن التمثيل الافتراضي للشبكة سيُستعمل على نطاق واسع في نشر شبكات الاتصالات المتنقلة الدولية–2020. وبهذه الطريقة، تغير التنفيذ من الأجهزة الأصلية ذات العتاد والبرمجيات المتكاملة إلى توليفة

ثلاثية الطبقات من العتاد والطبقة الافتراضية ووظيفة الشبكة الافتراضية. ونتيجة لذلك، فإن أصحاب المصلحة الرئيسيين المشاركين في هذا السيناريو هم: المستعملون أو المشتركون ومصنّعو المطاريف المتنقلة ومقدمو بطاقة الدارة المتكاملة الشاملة (UICC) وباعة عناصر الشبكة (مقدمو المعدات، مقدمو طبقة التمثيل الافتراضي، مقدمو وظيفة الشبكة الممثَّلة افتراضياً (VNF))، ومشغِّلو الشبكة. ويوجز الشكل 5 أصحاب المصلحة هؤلاء.



الشكل 5 – أصحاب المصلحة الرئيسيون في نشر شبكة التمثيل الافتراضي لميدان مشغِّل الشبكة

2.2.8 أدوار أصحاب المصلحة في هذا السيناريو

يقوم أصحاب المصلحة هؤلاء بالأدوار التالية في هذا السيناريو:

- المستعملون أو المشتركون: هؤلاء هم المستعملون النهائيون، أي العملاء، لخدمات الاتصالات. وتتكون معدات المشترك من مطراف متنقل يقدمه مصنّع وبطاقة الدارة المتكاملة الشاملة (UICC) مقدمة من بائع البطاقات.
- مصنّع المطراف المتنقل: يقدم هذا الكيان مطاريف يمكن للمستعملين أو المشتركين المتصلين بشبكة ما استعمالها.
- مقدِّم بطاقة الدارة المتكاملة الشاملة (UICC): يقدم هذا الكيان بطاقات الدارة المتكاملة الشاملة لتي يمكن استعمالها لتمثيل هويات المشتركين.
- بائع عناصر الشبكة: يقدم هذا الكيان أجهزة أو مكونات في الأجهزة التي يمكن تكوينها لإنشاء نظام اتصالات أو منصة/نظام خدمة.

  ملاحظة – في حال تقديم مكونات، يمكن تصنيفه كذلك كمقدِّم عتاد أو مقدم طبقة تمثيل افتراضي أو مقدم وظيفة الشبكة الممثَّلة افتراضياً (VNF).
- مشغِّل الشبكة: يمتلك هذا الكيان أو يتحكم في جميع العناصر اللازمة لبيع خدمات الاتصالات وإيصالها للمشتركين ولمقدمي الخدمات.

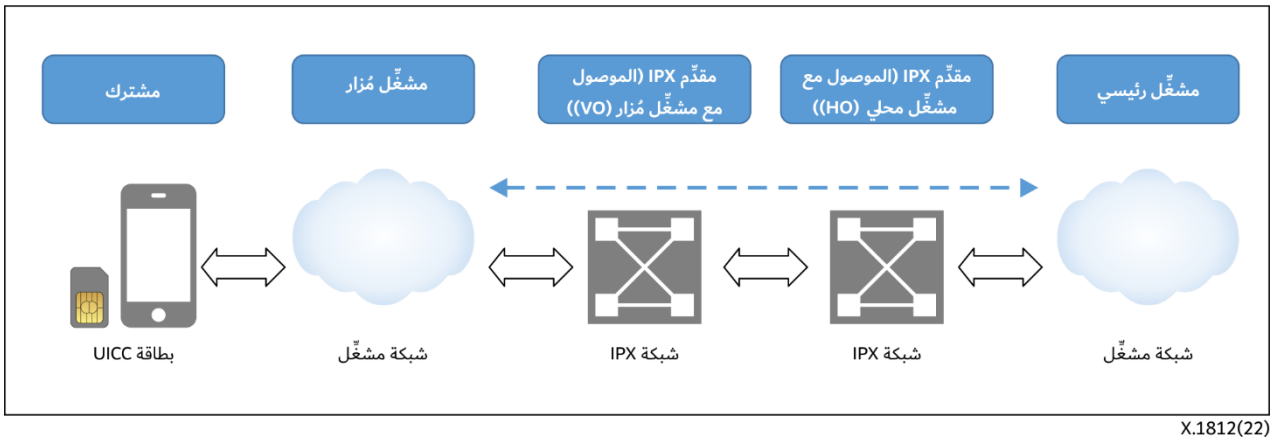
3.8 السيناريو 2: التوصيل البيني والتجوال

1.3.8 اعتبارات عامة

يركز هذا السيناريو في المقام الأول على علاقة الشبكة الداخلية.

ويمكن لشبكة الاتصالات المتنقلة أن تقدم الخدمات للمستعملين في جميع أنحاء العالم استناداً إلى التوصيل البيني والتنسيق بين المشغلين العالميين. ويشمل هذا التوصيل البيني والتنسيق بين المشغلين التنسيق والتعاون في طبقتي الخدمة والنقل.

وحتى الآن، افترض مبدأ التصميم للتوصيل البيني بين شبكة الاتصالات المتنقلة البرية العمومية (PLMN)، أن المشغلين (على مستوى الخدمة) يمكن أن يثقوا تماماً في بعضهم البعض، وتمكن أيضاً الثقة بإرسال بيانات التشوير وبيانات المستعمل. ولضمان إعادة تسيير رسائل التشوير إلى مشغل معين بشكل صحيح، أُدخل مقدِّم تبادل الرزم بين الشبكات (IPX). ولكن مع نمو الشبكة واستعمال الإنترنت، أصبحت توصيلات IPX معقدة بشكل متزايد، وأصبح تعرضها للهجوم عبر الإنترنت ممكناً أيضاً. ونتيجة لذلك، لا يمكن للمشغلين ضمان إلا أمن توصيلات IPX الموصولة بهم مباشرة، وليس أمن الوصلات بين المشغلين وجميع الوصلات الأخرى. وهذا مبيَّن في الشكل 6.



X.1812(22)

الشكل 6 – أصحاب المصلحة الرئيسيون في سيناريو التوصيل البيني والتجوال

HO: المشغِّل المحلي؛ VO: المشغِّل المزار

وأيضاً يتبين وجود العديد من نقاط الضعف لدى المشغلين ويجري استغلالها، مما يسمح للمهاجمين بشن هجمات على المشغلين الآخرين باستعمال أجهزة مخترقة كنقطة انطلاق. ونتيجة لذلك، لم يعد المشغلون موثوقين أيضاً في طبقة الخدمات [b-3GPP TS 33.501].

وفي مثل هذا السيناريو، تكون الجهات الفاعلة الرئيسية المعنية هي المستعملين أو المشتركين والمشغلين المزارين والمشغلين المحليين، ومشغِّلي تبادل الرزم بين الشبكات (IPX): (بما في ذلك تبادل الرزم بين الشبكات الواصل إلى المشغل المزار وتبادل الرزم بين الشبكات الواصل إلى المشغل المحلي).

2.3.8 أدوار أصحاب المصلحة في هذا السيناريو

يقوم أصحاب المصلحة هؤلاء بالأدوار التالية في هذا السيناريو:

- المستعمل أو المشترك: هو المستعمل النهائي لخدمات الاتصالات، أي العميل.
- المشغلين المزارون: يقدم هؤلاء المشغلون خدمات النفاذ إلى المشترك عندما يكون المشترك خارج نطاق تغطية مشغل شبكته المحلية.
- المشغل المحلي: يمتلك هذا المشغل اشتراكات المشتركين ويقدم الخدمات لهم.

- مشغل تبادل الرزم بين الشبكات (IPX) (تبادل الرزم بين الشبكات الواصل إلى المشغل المزار، أو تبادل الرزم بين الشبكات الواصل إلى المشغل المحلي): يقدم هذا الكيان خدمة تبادل رزم التوصيل الشبكي بين المشغلين.

4.8 السيناريو 3: استئجار سيارة مع التشغيل عن بُعد

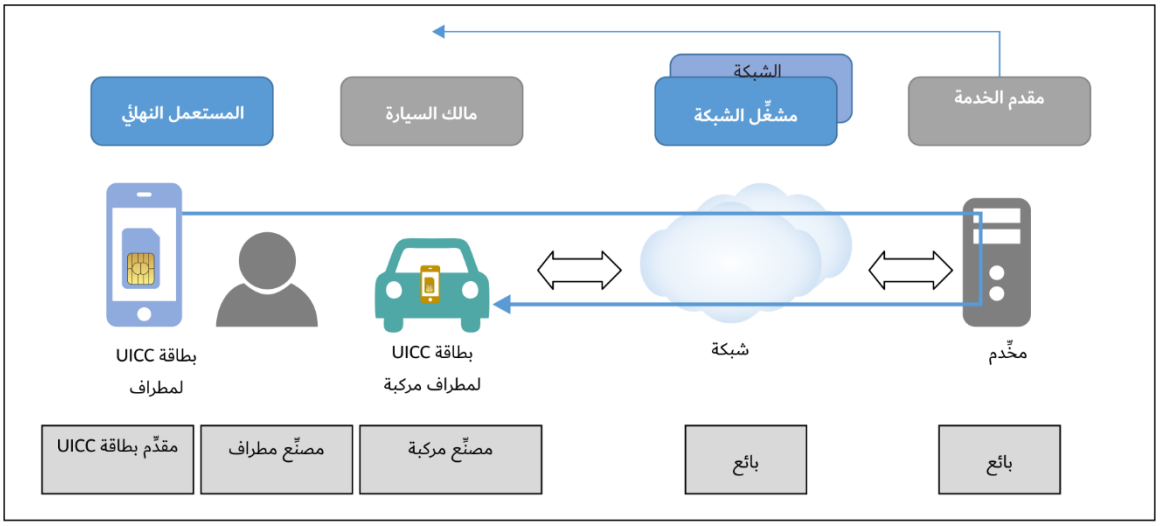
1.4.8 اعتبارات عامة

يركز هذا السيناريو بالدرجة الأولى على العلاقة بين المطراف الداخلي وخدمة المطراف.

وهناك عدد متزايد من المركبات التي تتواصل مع المنصة عن بُعد باستعمال وحدة اتصالات مدمجة أو مثبَّتة لاحقاً. ويمكن لهذه المركبات رفع حالة محددة إلى منصة بعيدة أو الحصول على تعليمات منها. وفي هذه الحالة، تتألف المركبة من جزأين: الأول يتعلق بالاتصالات، ويقدمه مصنِّع المطراف، والآخر هو المركبة نفسها التي صنعها مصنِّع المركبة.

وتقدم شبكة الاتصالات المتنقلة التقليدية للمشتركين أساساً خدمات النفاذ إلى شبكة الاتصالات الصوتية أو الرسائل القصيرة أو البيانات. والمشترك هو المستعمل النهائي للمطراف. وفي خدمات استئجار السيارات، فإن السائقين الذين يستعملون مركبات تحتوي على مطاريف اتصالات ليسوا مشتركين. وفي جانب آخر، يحتاج المستأجر عادة إلى استعمال تطبيق على مطرافه المتنقل للتفاعل مع المنصة عبر شبكة اتصالات، من أجل الحصول على معلومات المركبة عن بُعد أو تشغيل مركبة مستأجرَة عن بُعد، مثل تحديد موقع المركبة، وفتح قفل أو إغلاق الباب بدون مفاتيح، أو تشغيل أو إيقاف تكييف الهواء.

وبالتالي، في هذه الحالة، وعلى النحو المبين في الشكل 7، أصحاب المصلحة المعنيون هم مستأجرو السيارات، والمركبة (كالمطراف المتنقل)، ومصنعو المطراف المتنقل، ومقدِّمو بطاقة الدارة المتكاملة الشاملة (UICC)، ومصنِّعو السيارات، وبائعو عناصر الشبكات، ومشغلو الشبكات، ومقدِّمو التطبيقات.



X.1812(22)

الشكل 7 – أصحاب المصلحة الرئيسيون في سيناريو استئجار سيارة مع التشغيل عن بُعد

2.4.8 أدوار أصحاب المصلحة في هذا السيناريو

يقوم أصحاب المصلحة هؤلاء بالأدوار التالية في هذا السيناريو:

- مستأجر سيارة: مستعمل معين يستأجر سيارة من شركة تأجير سيارات. وهذا الشخص هو أيضاً مشترك في شبكة اتصالات متنقلة بواسطة مطراف متنقل.
- مركبة: مركبة تعود إلى شركة تأجير سيارات بها مطراف متنقل محدد مدمج، ويمكن اعتبارها مشتركةً في الشبكة.
- مصنّع المطراف المتنقل: يقدم هذا الكيان مطاريف يمكن أن يستعملها مشتركون على اتصال مع الشبكة.

- مقدِّم بطاقة الدارة المتكاملة الشاملة (UICC): يقدم هذا الكيان بطاقات الدارة المتكاملة الشاملة التي يمكن استعمالها لتمثيل هويات المشتركين.
- مصنّع السيارات: الكيان الذي ينتج مركبات قد تحتوي أو لا تحتوي على مطراف متنقل.
- بائع عناصر الشبكة: يقدم هذا الكيان أجهزة أو مكونات في الأجهزة التي يمكن تكوينها لإنشاء نظام اتصالات أو منصة أو نظام خدمة.
- مشغِّل الشبكة: يملك هذا الكيان أو يتحكم في جميع العناصر اللازمة لبيع خدمات الاتصالات وتقديمها للمشتركين ولمقدمي الخدمات.
- مقدِّم التطبيق: يقدم هذا الكيان تطبيقات لخدمة تأجير السيارات للمستعملين.

5.8 السيناريو 4: انفتاح قدرات الشبكة لدوائر الصناعة

1.5.8 اعتبارات عامة

يركز هذا السيناريو بشكل أساسي على علاقة خدمة الشبكة وعلاقة الخدمة الداخلية.

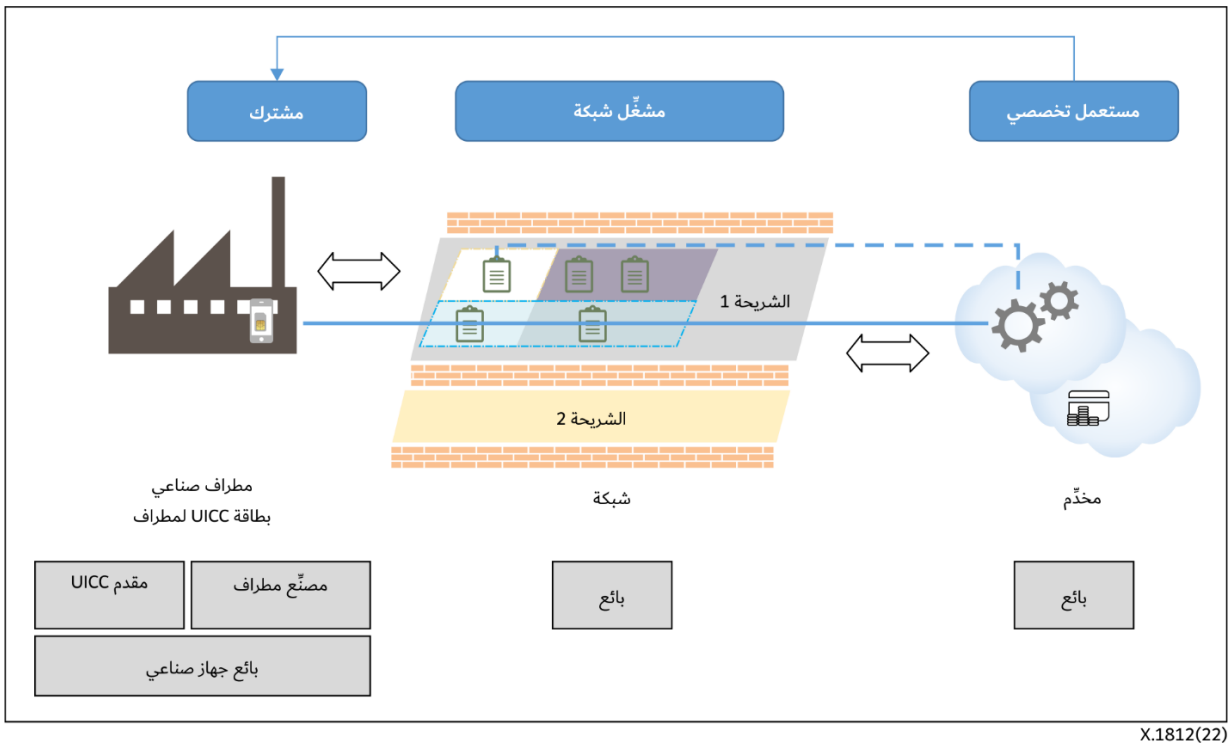
وتمتلك الاتصالات المتنقلة الدولية–2020 ميزات جديدة من قبيل النطاق العريض المتنقل المحسّن (eMBB)، وتوصيل إنترنت الأشياء (IoT) الكثيفة، والاتصالات فائقة الموثوقية منخفضة الكمون. وبهذه الميزات، يمكن لشبكة الاتصالات المتنقلة الدولية–2020 أن تقدم دعماً أفضل لتوصيل الشبكة في مجالات تخصصية مثل الصناعة.

ومقارنة بالاتصالات الشخصية، تختلف احتياجات الاتصالات في صناعة تخصصية، من قبيل تنوع الخدمات، والتمايز الوظيفي، وعدم تجانس التكنولوجيا. فللاتصالات التخصصية في طبقة التطبيق متطلبات أمنية صارمة عادةً، مثل عزل الاتصالات مع المستعملين الآخرين في دوائر الصناعة، وزيادة قدرة الإدارة أو التعاون مع مشغلي الشبكات ذوي الميزات الخاصة مثل الانفتاح على قدرات.

ومقارنة بالخدمات التقليدية، يمكن لخدمات الصناعة التخصصية أن تتعاون مع مشغلي الشبكات، لذلك يعرَّف بمقدمي التطبيقات، ويشارك أيضاً مقدمو مخدمات التطبيقات ذات الصلة أو مقدمو المنصات السحابية.

ومن جانب المطراف، كما في السيناريو 3، قد يحتوي الجهاز المطرافي أيضاً على جزأين، يتعلق أحدهما بالاتصالات التي يقدمها مصنع المطراف، والآخر بتطبيقات تخصصية مكرسة يقدمها مصنعو المطاريف الصناعية الأخرى.

وفي مثل هذه الحالة، وعلى النحو المبين في الشكل 8، أصحاب المصلحة المعنيون هم: مستعملو الصناعة التخصصية ومصنعو مطاريف الاتصالات ومقدِّمو بطاقة الدارة المتكاملة الشاملة (UICC)، ومصنِّعو المطاريف الصناعية، وباعة عناصر الشبكة، ومقدِّمو مخدمات التطبيقات أو مقدمو خدمات المنصات السحابية، ومقدمو التطبيقات ومشغلو الشبكة.



الشكل 8 – أصحاب المصلحة الرئيسيون في سيناريو انفتاح قدرات الشبكة

2.5.8 أدوار أصحاب المصلحة في هذا السيناريو

يقوم أصحاب المصلحة الرئيسيون بالأدوار التالية في هذا السيناريو:

- مستعمل صناعة تخصصية: يقوم مستعمل الصناعة التخصصية بالتحكم في مطراف صناعي عن بُعد عبر شبكة الاتصالات باستعمال تطبيقات مخصصة تعمل على مخدمات التطبيق أو منصات سحابية عامة أو خاصة.
- مصنّع المطراف المتنقل: يقدم هذا الكيان مطاريف يمكن أن يستعملها مشتركون على اتصال مع الشبكة.
- مقدِّم بطاقة الدارة المتكاملة الشاملة (UICC): يقدم هذا الكيان بطاقات الدارة المتكاملة الشاملة التي يمكن استعمالها لتمثيل هويات المشتركين.
- مصنّع الجهاز المطرافي الصناعي: الكيان الذي يقدم آلة صناعية أو شبكة صناعية أو نظام صناعي لمصنع أو شركات.
- بائع عناصر الشبكة: يقدم هذا الكيان أجهزة أو مكونات في الأجهزة التي يمكن تكوينها لإنشاء نظام اتصالات أو منصة أو نظام خدمة.
- مقدِّم مخدِّم التطبيق أو مقدِّم خدمة منصة سحابية: يملك هذا الكيان البنية التحتية والمنصة التي تقدم خدمات موارد التخزين والحوسبة لتطبيقات الطبقة العليا.
- مقدِّم التطبيق: يجمع المصنّع أو المؤسسات المعلومات، أو يقدم المصنّع أو المؤسسات تشوير التحكم إلى المطاريف الصناعية.
- مشغِّل الشبكة: يملك هذا الكيان أو يتحكم في جميع العناصر اللازمة لبيع خدمات الاتصالات وتقديمها للمشتركين ولمقدمي الخدمات.

6.8 السيناريو 5: سلاسل التوريد

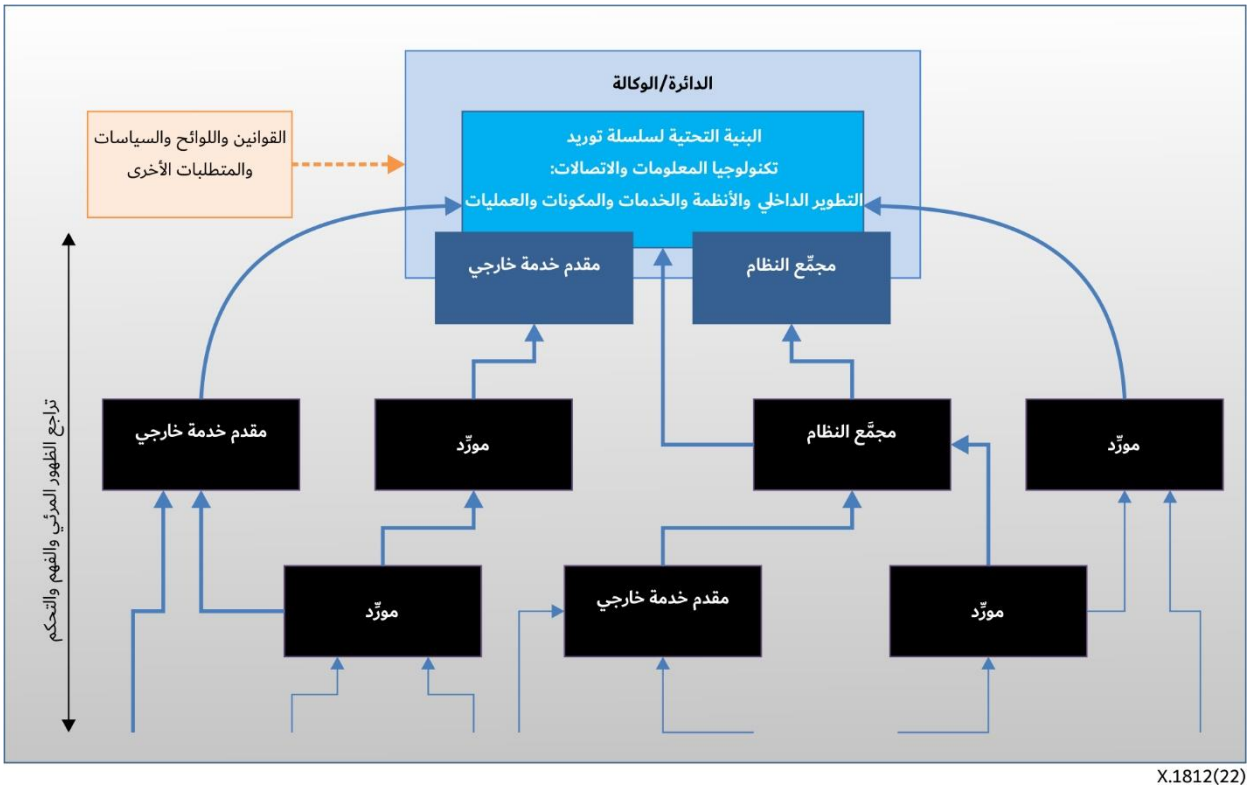
1.6.8 اعتبارات عامة

يشير النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 إلى مجتمع يضم العديد من المنظمات التي تساهم بكميات كبيرة من التكنولوجيات والخبرات لإنجاح خدمات الاتصالات المتنقلة الدولية–2020 وتطبيقاتها.

وسلسلة التوريد هي نظام للمنظمات والأفراد والأنشطة والمعلومات والموارد المشاركة في نقل منتج أو خدمة من المورِّد إلى العميل. وإدارة مخاطر سلسلة التوريد هي الجهود المنسقة التي تبذلها منظمة لتحديد التهديدات لاستمرارية سلسلة التوريد والربحية ومراقبتها واكتشافها والتخفيف منها. وهناك أربع دعائم أمنية لإدارة مخاطر سلسلة التوريد للنظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 كما يلي:

- جانب الأمن: وهو يتعامل مع كتمان المعلومات وسلامتها وتوفرها وهو أ) يصف سلسلة التوريد (من قبيل معلومات عن المسارات المستعرضة لمنتجات وخدمات الاتصالات المتنقلة الدولية –2020، المنطقية والمادية على حد سواء)؛ أو ب) يجتاز سلسلة التوريد (مثل الملكية الفكرية المتضمنة في منتجات وخدمات الاتصالات المتنقلة الدولية–2020)، إلى جانب معلومات عن أصحاب المصلحة المشاركين في سلسلة التوريد (أي شخص يمس منتج أو خدمة الاتصالات المتنقلة الدولية–2020 طوال دورة حياته)؛
- جانب السلامة: وهو يضمن أن تكون منتجات أو خدمات الاتصالات المتنقلة الدولية–2020 في سلسلة التوريد أصلية وغير معدلة وأن تعمل المنتجات والخدمات وفقاً لمواصفات الحائز وبدون خاصية وظيفية إضافية غير مطلوبة؛
- جانب الصمود: وهو يضمن أن تقدم سلسلة التوريد المنتجات والخدمات المطلوبة في حالة الضغط والعطل؛
- جانب الجودة: وهو يقلل من نقاط الضعف التي يمكن أن تحد من الوظيفة المقصودة لمكون ما، وتؤدي إلى عطل المكون، أو تتيح فرصاً للاستغلال.

ويركز هذا السيناريو أساساً على سلاسل التوريد والعلاقات. ويوضح الشكل 9 الجهات الفاعلة الرئيسية في سيناريوهات سلسلة التوريد.



ICT: تكنولوجيا المعلومات والاتصالات

الشكل 9 – أصحاب المصلحة الرئيسيون في سيناريوهات سلسلة التوريد

2.6.8 أدوار أصحاب المصلحة في هذا السيناريو

يتعدد أصحاب المصلحة في سلسلة التوريد فهم: المطور أو المصنّع، ومجمّع النظام، والبائع، وموزع المنتجات، والمورِّد، ومقدم الخدمة الخارجي: ويشير المطوّر أو المصنّع إلى: '1' مطوري أو مصنعي أنظمة المعلومات أو مكونات الأنظمة أو خدمات أنظمة المعلومات؛ '2' مجمعي الأنظمة؛ '3' الباعة؛ أو '4' موزعي المنتجات.

ومجمِّع النظام هو شخص أو شركة تتعامل مع تجميع مكونات الأنظمة الفرعية معاً والتأكد من أن هذه الأنظمة الفرعية تعمل معاً، في ممارسة تُعرف باسم تجميع النظام.

والبائع هو أي شخص يقدم سلعاً أو خدمات إلى شركة أو أفراد. وكثيراً ما يقوم البائع بتصنيع المواد ثم يبيعها إلى العميل. والمؤسسة كيان قانوني منفصل عن الشركة المتعاقدة تقدم خدمات مثل الاستشارات أو تطوير البرمجيات.

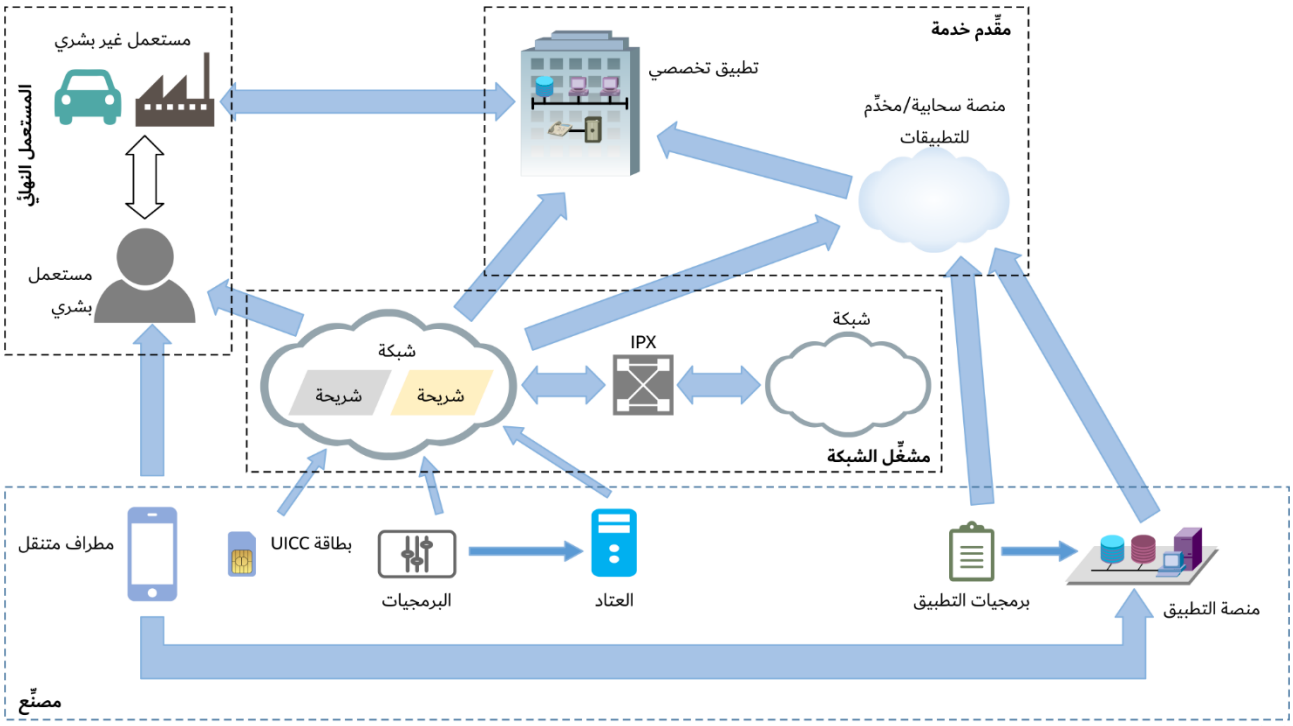
وموزع المنتَج هو شركة أو فرد يشتري سلعاً أو خدمات بغرض بيعها بدلاً من استهلاكها أو استعمالها.

والمورّد هو كيان يقدم سلعاً وخدمات إلى طرف آخر.

ويشير مقدم الخدمة الخارجي إلى '1' كيانات داخل المنظمة ولكن خارج حدود التخويل الأمني الموضوعة لأنظمة معلومات المنظمة؛ أو '2' كيانات خارج المنظمة إما في القطاع العام (مثل الوكالات الفيدرالية) أو القطاع الخاص (مثل مقدمي الخدمات التجارية)؛ أو '3' مزيج ما من خيارات القطاعين العام والخاص.

7.8 أصحاب المصلحة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

يمكن تصنيف النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 ضمن أربعة أنواع من أصحاب المصلحة في الشكل 10 هي: المصنّع ومشغل الشبكة ومقدم الخدمة والمستعمل النهائي، وذلك استناداً إلى حالات استعمال يرد وصفها في الفقرات من 2.8 إلى 6.8.



الشكل 10 – أصحاب المصلحة ضمن النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020

وقد يكون لأحد أصحاب المصلحة علاقة مباشرة مع صاحب مصلحة آخر، وقد يكون له علاقات غير مباشرة مع أصحاب المصلحة في الميادين الفرعية الأخرى من خلال صاحب مصلحة يتصرف مثلاً كجزء من سلسلة التوريد.

وبالنسبة للنظام الإيكولوجي للاتصالات المتنقلة الدولية–2020، يمكن اعتبار المصنّع مجموعة من المطورين أو المصنعين، ومجمِّعي الأنظمة والباعة. ويمكن اعتبار مشغلي الشبكة بمثابة موزعين للمنتجات وموردي خدمات الشبكة. ويمكن اعتبار مقدمي الخدمة بمثابة جهات خارجية.

ويقدم مصنعو المكونات اللبنات التكنولوجية لمصنعي الأجهزة اللاسلكية ومصنعي معدات الشبكات. ويمكن أيضاً لمصنعي هذه المكونات تقديم هذه اللبنات الأساسية مباشرة لمشغلي الشبكات. ويقدم مصنعو الأجهزة اللاسلكية معدات للمستعملين النهائيين أو كمكون من الآلات الصناعية، بينما يقوم مصنعو معدات الشبكات بإنتاج المعدات لدعم البنية التحتية للشبكة (بما في ذلك البنية التحتية اللاسلكية والسلكية). ويجمع مشغلو الشبكات بين هذه الأجهزة ومكونات الشبكات ومعدات الشبكات والشبكات من مشغلين آخرين من خلال تبادل الرزم بين الشبكات (IPX) في شبكة تشغيلية في جميع أنحاء العالم لخدمة المستعملين النهائيين. ويقوم المستعملون النهائيون بإجراء المكالمات الصوتية وإرسال الرسائل النصية وتشغيل التطبيقات عبر الشبكة. ويقدم مشغلو الشبكات الاتصالات والخدمات ذات الصلة لمقدمي الخدمات الخارجيين من خلال خدمة الانفتاح على قدرات شبكاتهم أو خدمات محددة أخرى.

9 مستوى الثقة ومعايير الثقة ونموذج الثقة

1.9 اعتبارات عامة

على النحو المعرَّف في الفقرة 11.1.3، الثقة هي الدرجة التي يثق بها المستعمل أو أي صاحب مصلحة آخر بأن المنتج أو النظام سيتصرف على النحو المنشود. وتؤدي الثقة أيضاً دوراً هاماً في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020. وتوصِّف هذه التوصية نموذجاً للثقة في النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 لتمكين أصحاب المصلحة من اتخاذ قرارات منطقية بشأن القرارات المتعلقة بالثقة والأمن.

وينقسم نموذج ثقة النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 إلى ثلاثة مستويات:

- المستوى الأول من الثقة هو تغطية متطلبات الثقة من الحكومات والهيئات التنظيمية. ومن العوامل الرئيسية الناظمة للثقة اعتماد المعايير الدولية، وإصدار الشهادات العلني والشفاف.
- أما المستوى الثاني فيتمثل في معالجة متطلبات الثقة من المنظمات الصناعية. ومن العوامل الرئيسية لهذه الهيئات، تعريف أصحاب المصلحة، ومالك الحل من طرف إلى طرف (E2E)، والمستعمل النهائي للسوق، ونموذج الأعمال، ومستويات الثقة، وعلاقات الثقة.
- أما المستوى الثالث فيتمثل في تأمين الثقة من خلال تقديم حلول تقنية تستند إلى العوامل الرئيسية من المستويين الأول والثاني.

وتركز هذه التوصية على المستويين الثاني والثالث، أي المنظمات الصناعية والحلول التقنية.

ويحتاج مشغل شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020) إلى الاعتماد على الأجهزة و/أو المعدات المقدمة من المصنعين لإنشاء نظام شبكته. وبالتالي، فإنه يحتاج إلى الثقة في أن المصنعين يقدمون أجهزة يمكنها تلبية متطلبات مشغل الشبكة.

ويعتمد مقدم الخدمة على الشبكة لإرسال المعلومات، لذلك عليه أن يثق في مشغل الشبكة لضمان نقل البيانات بشكل صحيح وفي الوقت المناسب. ويحتاج مقدم الخدمة أيضاً إلى الاعتماد على الأجهزة المقدمة من المصنعين لإنشاء خدماته، وبالتالي عليه أيضاً أن يثق في المصنعين في تقديم أجهزة يمكن أن تفي بمتطلبات مقدم الخدمة.

ويحتاج أن يعتمد المستعملون النهائيون على إرسال الشبكة وتطبيقات الخدمة، لذلك عليهم أن يثقوا في أن النفاذ إلى الشبكة الذي يقدمه مشغل الشبكة قانوني وفعال. ومتطلبات ثقتهم فيما يتعلق بمقدم الخدمة هي متطلبات مماثلة.

2.9 مستويات الثقة

يصعب بطبيعة الحال قياس الثقة كمياً بطريقة مجدية. وفي نموذج الثقة المحدد في هذه التوصية، يُطرح مفهوم نوعي لمستوى الثقة للتمكن من تفسير الآثار المترتبة على درجات مختلفة من الثقة.

وتعمل الخدمات الممكَّنة بالاتصالات المتنقلة الدولية–2020 في مجموعة من السياقات وبالتالي فهي تتطلب متطلبات مختلفة بشأن الثقة. فعلى سبيل المثال، تحمل القطاعات التخصصية المختلفة خدمات مختلفة وتعمل في سيناريوهات مختلفة، وبالتالي فإن لها مواضع مختلفة للثقة. وعلاوة على ذلك، تصنَّف بعض الصناعات بوصفها جزءاً من البنية التحتية الوطنية الحرجة، مثل الشبكة الكهربائية الذكية، في حين ينحصر عمل صناعات أخرى في سيناريوهات يومية أقل حراجة مثل تأجير السيارات.

وإذا اعتُبر قطاع تخصصي معين جزءاً من البنية التحتية الحرجة، فمن الواضح أن هذه الصناعة ستحتاج إلى مستوى أعلى من الثقة بأن نظام الاتصالات المتنقلة الدولية–2020 سيتصرف على النحو المنشود. وبعبارة أخرى، يتعين تحديد مستوى أعلى من الثقة لهذه الصناعة لأن أي ضرر بها سيؤثر على الاستقرار الوطني. ومن ناحية أخرى، سيلزم مستوى أدنى من الثقة بالنسبة لتلك الصناعات التي يكون فيها لمؤثرات العطل ذيول طفيفة نسبياً.

فعلى سبيل المثال، تختلف مستويات الثقة لكل من خدمات إنترنت الأشياء (IoT) ضيقة النطاق مثل إنترنت المركبات (IoV) والإنترنت الصناعية والشبكة الكهربائية الذكية وسقاية الزهور، لأن للأضرار التي تلحق بهذه الصناعات عواقب مختلفة على المجتمع أو المستعملين.

ويعتمد مستوى الثقة لحالة استعمال محددة أساساً على مستوى وطأة الضرر الذي يلحق بقطاع تخصصي معين على المجتمع والأمة. ولعل المنظمة التخصصية هي أفضل من يحدد ذلك حيث سيكون لها ممثلون من مجالات متعددة وخبراء مهنيون لإجراء التحليل اللازم؛ وذلك أيضاً جزء من الاحتياط الواجب لتوصيف مستوى الثقة. وبالتالي، في حالات الاستعمال المستلزِمة لمستوى أعلى من الثقة، يجب أن تكون المسؤولية التي تقع على عاتق أصحاب المصلحة المعنيين أعلى؛ وبعبارة أخرى، يتعين أيضاً إسناد مستوى أعلى من الثقة لأصحاب المصلحة هؤلاء.

ولأغراض نموذج الثقة المحدد هنا، تُفترض إمكانية ضبط مستوى الثقة لمختلف الأطراف بواحد من ثلاثة مستويات نوعية: عال أو متوسط أو منخفض. ويُفترض هذا الافتراض لسببين رئيسيين:

- أولاً، يرجَّح أن يشكل إسناد قيم كمية إلى مستويات الثقة مشكلة كبيرة نظراً لغياب مقياس واضح للثقة (على غرار تحليل المخاطر مثلاً، حيث يمكن أن يستند المقياس إلى توليفة من احتمال الحدوث وتقييم تكلفة التأثير السنوي)؛
- ثانياً، هذا المقياس ثلاثي المستويات غني بما يكفي لتغطية العديد من حالات الاستعمال القائمة، وهو معتمَد أيضاً في مواضع أخرى، من قبيل خطة ضمان أمن معدات الشبكة في المراجع [b-GSMA FS.13] (NESAS) و[b-GSMA FS.14] و[b-GSMA FS.15] و[b-GSMA FS.16] لقياس متطلبات الثقة.

وتظل المشكلة تتمثل في تحديد معنى مستويات الثقة الثلاثة هذه، بحيث يمكن استعمال النموذج المحدد في هذه التوصية بشكل متسق. وترد في الفقرة 3.9 معايير الثقة المصممة لتمكين تحديد مستويات الثقة.

ونظراً لتنوع الأصول والطائفة الواسعة من سيناريوهات النشر في قطاعات تخصصية محددة، فمن الناحية العملية، تتعين مواصلة صقل مستوى الثقة العام وفقاً للسياق. فعلى سبيل المثال، يختلف مستوى الثقة المطلوب للقيادة الذاتية بوضوح حسب شبكة إنترنت المركبات (IoV) أو الشبكة المحلية أو الشبكة الكلية.

ويوضح المثال التالي أيضاً الحاجة إلى تعريف معقد ومستوى ثقة خاص بالسياق. لنفترض أن مشغلاً يختار مصنعي معدات الشبكة وفقاً لمستوى الثقة الموصَّف. وفي حال توصيف مستوى واحد حصراً، ينبغي اختيار جميع مصنعي معدات الشبكة طبقاً لمستوى ثقة واحد. بيد أن الشبكة الأساسية أكثر حساسية وقيمة ونفوذاً مما هي عليه الهوائيات مثلاً، لذا سيلزم في سيناريو نمطي أن يعلو مستوى الثقة لمصنّع الشبكة الأساسية على مستوى ثقة مُصنّع الهوائي.

وكتحسين آخر، يوصَّف مستوى الثقة بشكل منفصل لوحدة الأعمال وسيناريو الأعمال. وهذا يعني في صناعة تخصصية، مواصفات منفصلة لمستوى الثقة في الصناعة التخصصية بأكملها، وسيناريو الصناعة التخصصية المعيَّن. ويبين الجدول 1 توليفات ممكنة من مستويات الثقة للحالتين.

الجدول 1 – مستوى الثقة لوحدة الأعمال وسيناريوهات وعلاقة الأعمال

مستوى الثقة لوحدة الأعمال	مستوى الثقة لسيناريوهات الأعمال
مرتفع	مرتفع
	متوسط
	منخفض
متوسط	متوسط
	منخفض
منخفض	منخفض

ولجعل توصيف المستوى أكثر عملية وأكثر شمولاً، يوصى بتعريف مستوى ثقة للمكون بطريقة مرنة. فعلى سبيل المثال، يمكن تحديد مستوى الثقة للمكون طبقاً لقيمة الأصول أو مجال النشر.

وللنظر في مثال محدد، يكون مستوى الثقة للشبكة الكهربائية الذكية بأكملها مرتفعاً، ولكن داخل الشبكة الكهربائية، لا تكون قيمة الكبلات والأعمدة الكهربائية بنفس قيمة أجهزة الاستشعار والبنية التحتية لإرسال الإشارة في شبكة الاتصالات المتنقلة الدولية–2020. وحتى بالنسبة لأجهزة الاستشعار والبنية التحتية لإرسال الإشارة، فإن الشبكة الكهربائية الذكية المنشورة في مدينة صغيرة ليست حساسة كشبكة كهربائية منشورة في مدينة حضرية.

ويرد في الجدول 2 وصف لمستويات الثقة الممكنة للعلاقات بين الصناعة التخصصية وصاحب مصلحة.

الجدول 2 – مستويات الثقة الممكنة بين صناعة تخصصية وصاحب مصلحة

مستوى الثقة للنظام	مستوى ثقة للمكون	مستوى ثقة لصاحب مصلحة
مرتفع	مرتفع	مرتفع
	متوسط	متوسط
	منخفض	منخفض
متوسط	متوسط	متوسط
	منخفض	منخفض
منخفض	منخفض	منخفض

3.9 معايير الثقة

يتطلب تقييم مستوى الثقة، على أنه مرتفع أو متوسط أو منخفض، تقييم علاقات الثقة بين أصحاب المصلحة. وتتأثر علاقة الثقة بين أي اثنين من أصحاب المصلحة بعوامل عديدة، وستختلف أيضاً درجة الثقة بين مختلف أصحاب المصلحة في فئة ما ومختلف أصحاب المصلحة في فئة أخرى. ولذلك يتعين توصيف معايير التقييم كل على حدة.

ونظراً لاختيار مستوى الثقة لتقليل الضرر الناجم عن التهديدات المحتملة والمخاطر التي تسببها، يمكن أن تتضمن المعايير قيمة الأصول، ونطاق التأثير، وشدة التأثير، وأرجحية وقوع المخاطر، استناداً إلى معايير لإدارة المخاطر مثل [b-NIST SP800-30] و[b-ISO 31000] و[b-ISO/IEC 27005] .

- الأصول: أهمية هذا العامل واضحة. وكلما زادت أهمية الأصل، زادت الحاجة إلى إبقاء الأصل تحت السيطرة الكاملة لأصحاب المصلحة، وارتفع مستوى الثقة اللازم.
- نطاق التأثير: بالنسبة لصاحب المصلحة ذي النطاق الواسع، كلما اتسع النطاق، اشتد تأثير أي عطل. لذلك، يلزم مستوى عال من الثقة إذا كان نطاق التأثير واسعاً. فعلى سبيل المثال، يحتاج المشغّل إلى مستوى أدنى من الثقة في بائع يبيع خلايا صغيرة تغطي مناطق صغيرة مقارنةً ببائع يبيع عناصر الشبكة الأساسية التي تغطي منطقة شاسعة.

- شدة التأثير: بالنسبة لصاحب مصلحة يعمل كجزء من بنية تحتية رئيسية، تشتد خطورة عواقب الضرر، وبالتالي يُتطلب بذل جهود أكبر لمنع مثل هذا الضرر. ويؤدي ذلك إلى زيادة الحاجة إلى تقييمات دقيقة عند التفاعل مع الأطراف الأخرى. ومن ثم، كلما زادت خطورة تأثير العطل في علاقة، ارتفع مستوى الثقة اللازم.
- أرجحية وقوع المخاطر: إذا كانت أرجحية الحدوث أعلى، يرجح أن تقع المخاطر.

والنظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 معقد للغاية. وفي الفئات المختلفة من أصحاب المصلحة، مثل المستعملين النهائيين ومصنعي المعدات ومشغلي الشبكات ومقدمي الخدمات، تحتوي كل فئة على مجموعة متنوعة من الأمثلة المحددة. وبما أن الثقة مفهوم شخصاني، يصعب قياس الثقة وتقييسها، ويتمايز مستوى الثقة بين حالتين أيضاً. ولكن تقتضي الضرورة تحديد مجموعة من مستويات الثقة العامة التي تغطي معظم الحالات، لتقديم التوجيه لكل كيان في نظام إيكولوجي للاتصالات المتنقلة الدولية–2020، وهي مستويات الثقة المنخفضة والمتوسطة والمرتفعة.

ويقدم الجدول 3 مثالاً على كيفية تحديد مستوى الثقة الإجمالي بناءً على معايير الثقة المختلفة.

الجدول 3 – معايير مستوى الثقة

مستوى الثقة الإجمالي	معايير مستوى الثقة			
	قيمة الأصول	نطاق التأثير	شدة التأثير	أرجحية وقوع المخاطر
مرتفع	مرتفع	مرتفع	مرتفع	مرتفع
متوسط	متوسط	متوسط	متوسط	متوسط
منخفض	منخفض	منخفض	منخفض	منخفض

وعند استعمال التقابل الوارد في الجدول 3، من المهم أن يأخذ مستوى مخاطر معايير الثقة في الاعتبار تخفيف المخاطر سواء القائمة بالفعل أو التي سيصار إلى تنفيذها. فعلى سبيل المثال، عند استعمال الإنترنت الحالية للتجارة الإلكترونية عالية القيمة، يمكن تقييم قيمة الأصول، ونطاق التأثير وشدة التأثير كلها على أنها عالية جداً؛ وعلاوة على ذلك، يبدو ظاهرياً أن أرجحية وقوع هجوم كبيرة جداً، لأن بروتوكولات الاتصالات عبر الإنترنت لا تتضمن ميزات أمنية متينة. وباستعمال الجدول 3، يُستنتج أن مستوى الثقة في الإنترنت يجب أن يكون مرتفعاً لتلبية احتياجات التجارة الإلكترونية. ولكن رغم أن مستوى الثقة الحقيقي في الإنترنت منخفض فعلياً، بالنظر إلى أن الإنترنت لا تقدم ضمانات بشأن كتمان قنوات الاتصالات أو سلامتها أو توفرها، فإن التجارة الإلكترونية تستعمل على نطاق واسع وناجح جداً في كميات هائلة من المعاملات.

وفي الواقع، يعود سبب نجاح هذا السيناريو إلى التصدي للمخاطر التي تهدد كتمان وسلامة نقل البيانات من خلال الاستعمال الروتيني لأمن طبقة النقل [b-IETF RFC 5246] لحماية الاتصالات بين نقاط الاتصالات الطرفية، وهو ما يمكن اعتبارها جزءاً من متطلبات الأمن المحددة في الفقرة 2.10.

وختاماً، يُتطلب أن يراعي حساب مستوى الثقة المطلوب المستوى الفعلي للتهديدات بعد تطبيق تدابير التخفيف من المخاطر الخاصة بالتطبيقات. وبخلاف ذلك، يمكن تطلُّب متطلبات غير واقعية بشأن مستوى الثقة اللازم من مقدمي المعدات والخدمات، مما يؤدي إلى زيادة كبيرة في التكاليف.

4.9 نموذج الثقة القائم على خارطة ارتباطات علاقة الثقة

لوضع حدود أمنية وتدابير أمنية للاتصالات المتنقلة الدولية–2020 بطريقة مقيَّسة قابلة للتشغيل البيني، تقتضي الضرورة وضع نموذج ثقة واستعماله على نحو مناسب. ولكي يكون نموذج الثقة فعالاً، يلزم تحليل علاقات الثقة.

وبالنظر إلى العوامل المحددة في الفقرة 2.9، فإن علاقة الثقة الإجمالية بين طرفين هي أيضاً أحادية الاتجاه وليست ثنائية الاتجاه. ويعرض الجدول 4 أدناه مثالاً لتحليل علاقات الثقة بين مختلف فئات أصحاب المصلحة.

الجدول 4 – علاقات الثقة بين أصحاب المصلحة

الجهة الفاعلة	الجهة التي يقع عليها الفعل			
	المستعمل النهائي	المصنّع	مشغل الشبكة	مقدم الخدمة
المستعمل النهائي		متوسط/منخفض	مرتفع/متوسط/منخفض	مرتفع/متوسط/منخفض
المصنّع	–		مرتفع	مرتفع
مشغل الشبكة	منخفض	مرتفع/متوسط/منخفض		مرتفع/متوسط/منخفض
مقدم الخدمة	مرتفع/متوسط/منخفض	مرتفع/متوسط/منخفض	مرتفع/متوسط/منخفض	

وعادة ما تكون علاقات الثقة بين مختلف الشركاء في نظام إيكولوجي للاتصالات المتنقلة الدولية–2020 معقدة للغاية. لذلك، من الضروري إنشاء نموذج ثقة يمكن أن يبين هذا التعقيد. أي يمكن تحسين علاقة الثقة الإجمالية لإعطاء قيم ثقة على مستوى النظام الفرعي. ويرد مثال لتحليل علاقات الثقة على مستوى النظام الفرعي في الجدول 5.

الجدول 5 – علاقة الثقة على مستوى النظام الفرعي داخل الميدان الفرعي للمصنّع

الجهة الفاعلة	الجهة التي يقع عليها الفعل			
	مجموعة الرقاقات الإلكترونية/المودم	وحدة نمطية	مقدم الجهاز	مقدم البرمجيات
مجموعة الرقاقات الإلكترونية/المودم		–	–	–
وحدة نمطية	مرتفع/متوسط		–	–
مقدم الجهاز	مرتفع/متوسط	مرتفع/متوسط		–
مقدم البرمجيات	مرتفع/متوسط	مرتفع/متوسط	مرتفع/متوسط	

وباستعمال النموذج الوارد في الجدول 6، يرد سيناريو استئجار سيارة كمثال من طرف إلى طرف.

الجدول 6 – نموذج ثقة قائم على علاقات الثقة في سيناريو استئجار سيارة

الجهة الفاعلة		الجهة التي يقع عليها الفعل						
		مقدم الخدمة (مركبة)	المستأجر	المصنّع			مشغل الشبكة	مقدم الخدمة
				مطراف/UICC	سيارة (باستثناء المطراف وUICC)	معدات الشبكة		
مركبة			متوسط/ منخفض	متوسط	مرتفع/متوسط	–	مرتفع/ متوسط/ منخفض	مرتفع
المستأجر		مرتفع/ متوسط		متوسط/منخفض	متوسط/منخفض	–	مرتفع/ متوسط/ منخفض	مرتفع/ متوسط/ منخفض
المصنّع	مطراف/ UICC	–	–		–	–	مرتفع	مرتفع
	سيارة	–	–	–		–	–	مرتفع
	معدات الشبكة	–	–	–	–		مرتفع	–
مشغل الشبكة		منخفض	منخفض	مرتفع/متوسط/ منخفض	–	مرتفع/ متوسط/ منخفض		مرتفع/ متوسط/ منخفض
مقدم الخدمة		مرتفع	متوسط/ منخفض	مرتفع/متوسط/ منخفض	مرتفع/متوسط	–	مرتفع/ متوسط/ منخفض	

10 متطلبات الأمن المدعوم بنموذج الثقة القائم على علاقات الثقة

1.10 اعتبارات عامة

في سيناريو محدد، تنشئ مجموعة من أصحاب المصلحة الذين يقدمون خدمات ووظائف مختلفة نظاماً لضمان سلوكه وعمله على النحو المنشود وجلب الفوائد لأصحاب المصلحة. ويشكل أصحاب المصلحة هؤلاء معاً النظام الإيكولوجي.

وأثناء تشغيل النظام الإيكولوجي، قد تنشأ تهديدات وأخطار محتملة لمنع تشغيل الأعمال. ولمنع التهديدات من إلحاق الضرر، يحتاج جميع أصحاب المصلحة إلى المساعدة في ضمان استمرار التزام النظام الإيكولوجي من خلال الامتثال القانوني ومن خلال تقديم منتجات وخدمات وحلول آمنة تستعمل إجراء تطوير آمن.

ويمكن استعمال نموذج الثقة المحدد في الفقرة 9 للمساعدة في تحديد متطلبات الأمن القائمة على الثقة لأصحاب المصلحة.

2.10 متطلبات الأمن من مستوى الثقة

1.2.10 لمحة عامة

يمكن استعمال مستوى الثقة في أحد أصحاب المصلحة لتقييم ما إذا كان صاحب المصلحة قادر على تقديم القدرة المناسبة لدرء الأضرار. ويمكن وضع المتطلبات الأمنية للتخفيف من هذه الأضرار. ونتيجة لذلك، يمكن أن تستند المتطلبات الأمنية إلى قدرات المنظمة التي تشمل المستوى المهني للموظفين، واستعمال عمليات التطوير الآمنة مثل دورة حياة تطوير الأمن، أو قدرات إجراءات التشغيل الأمني، وقدرات التكنولوجيا ذات الصلة بالحل الجدير بالثقة. وللاطلاع على تفاصيل أوفى، انظر المعايير والممارسات الواردة في مراجع مثل [b-NIST FICIC] و[b-BSIMM] . انظر الجدول 7.

الجدول 7 – مستوى الثقة وفئات المتطلبات الأمنية

مستوى الثقة	فئات المتطلبات الأمنية		
	الجهة التي يقع عليها الفعل		
الجهة الفاعلة	قدرات المنظمة (ائتمان جيد)	أمن تطوير النظام ودورة حياة المنتجات أو قدرة تشغيل أمني (إجراء جيد)	قدرات التكنولوجيا ذات الصلة بالحل الجدير بالثقة (حل جيد)
مرتفع	✓	✓	✓
متوسط	✓	✓	–
منخفض	✓	–	–

2.2.10 متطلبات المنظمة

1.2.2.10 مقدمة

يمكن فرز القدرات الأمنية المتعلقة بالثقة لدى منظمة ما وفق: سمعتها، وقدرتها على تنفيذ العقود، واتساق القيم، وإمكانية التعويض عن انتهاك العقد، واستقلاليتها.

2.2.2.10 السمعة

تعبِّر السمعة عن درجة التمسك التاريخي بالأهداف المحددة لمنتج أو نظام. والسمعة هي مقياس يمكن اشتقاقه من المعرفة المباشرة أو غير المباشرة بالتعاملات السابقة مع أصحاب المصلحة وتُستعمل لتقييم مستوى الثقة في أحد أصحاب المصلحة. وكتمثيل للوثوق، تعتمد الثقة عادة على معلومات تاريخية لاستنتاج احتمال الجدارة بالثقة في المستقبل. لذلك، عندما يحْسن صاحب مصلحة معين أداءه في السابق وفقاً لاتفاق ما، ستتحسن سمعته في أوساط الصناعة أيضاً، وبالتالي يمكنه اكتساب ثقة أكبر من الطرف الآخر. ويمكن الحصول على البيانات الخاصة بإدارة السمعة من مختلف الموارد الموثوقة والمقبولة على نطاق واسع استناداً إلى أدلة، مثل الشهادات أو التقارير السنوية والمالية الرسمية، وما إلى ذلك. بيد أن سمعة صاحب مصلحة معين قد تختلف في مجالات مختلفة. فعلى سبيل المثال، العلاقة بين مصنّع جهاز ومشغل شبكة أو مقدم خدمة هي بين بائع وعميل، فيما يمكن أن تكون تنافسية بين مصنِّعين مختلفين. لذلك، يمكن أن يتمتع مصنِّع الأجهزة بسمعة جيدة مع مشغل شبكة أو مقدم خدمة، ولكن يمكن أن تسوء لدى منافس له. ونتيجة لذلك، عند استعراض معلومات السمعة المقدمة من الخارج، لا يمكن لمشغلي الشبكات أو مقدمي الخدمات الأخذ بمعلومات عن السمعة واردة من مصنّع منافس كمصدر رئيسي.

3.2.2.10 تنفيذ العقد

في حالة التنفيذ التعاوني المستمر أو المتعدد المتقطع، ستؤثر جودة تنفيذ العقد على ثقة كلا الطرفين. وستؤثر أيضاً على علاقة الثقة بين الطرفين. وعند تنفيذ العقد بشكل سليم، ستنشأ الثقة المتبادلة وستتوطد علاقة الثقة. وعلى العكس من ذلك، عند تنفيذ العقد بشكل غير سليم، تتراجع الثقة المتبادلة وتتراجع علاقة الثقة بالإضافة إلى ذلك. وبشأن التعاون المتعدد المستمر، من قبيل زيارة مقدم خدمة عدة مرات، ستؤثر تجربة المستعمل التاريخية تأثيراً مباشراً على ثقته في نظام الخدمة. وفي هذه الحالة، يوصى بتصنيف المعلومات عن تجربة المستعمل التاريخية كقضية تخص تنفيذ عقد المستعمل بدلاً من كونها قضية سمعة.

4.2.2.10 اتساق القيمة

عندما يشترك أصحاب المصلحة في القيم نفسها، تصبح العلاقة بينهم أقرب وتزيد توقعاتهم للمستقبل طويل الأجل اتساقاً. ونتيجة لذلك، تتحقق درجة أعلى من الثقة المتبادلة، وتنشأ علاقة ثقة أفضل بينهم.

5.2.2.10 التعويض

تتعلق القدرة على التعويض بتوقع التعويض في حال عدم الإيفاء بالتزام. ويمكن اعتبار توقع التعويض ضماناً آخر بأن صاحب المصلحة سيسعى إلى تنفيذ العقد حتى في ظروف غير طبيعية. وبصورة عامة، كلما زاد سخاء التعويض، قلت خسارة النظير ضمناً.

ومن شأن هذه القدرة أن تعزز الثقة والاطمئنان بشأن الطرف الآخر. فعلى سبيل المثال، يمكن أن تملي القوانين السيبرانية الإقليمية مستوى وشدة العقوبة/التعويض على مختلف أصحاب المصلحة لتعزيز الجدارة بالثقة.

6.2.2.10 الاستقلالية

تعبر استقلالية صاحب المصلحة عن استقلاله الذاتي في تنفيذ العقد. وتشمل الاستقلالية قدرة الشركة الأم على التحكم في شركة فرعية، وتتضمن أيضاً تأثير السلطات على كيان الأعمال. وكلما زاد عدد أصحاب المصلحة المعنيين، زاد التأثير الذي ستتلقاه منهم وزادت علاقة الثقة لديها تأثراً.

7.2.2.10 ملخص

ويرد في الجدول 8 مثال على الطرق التي يمكن أن ترتبط بها مستويات الثقة بقدرات مؤسسة ما. ومن الناحية العملية، تختلف الخيارات الدقيقة للجوانب المطلوبة لمستويي الثقة المتوسط والمنخفض تبعاً لميدان التطبيق. فعلى سبيل المثال، قد تظل سمعة المورِّد المناسبة مطلوبة في بعض الحالات، لتحقيق مستوى ثقة منخفض، في حين أن هذا الجانب قد لا يكون مهماً في حالات أخرى حتى عندما تدعو الحاجة إلى مستوى ثقة متوسط.

الجدول 8 – مستويات الثقة والمتطلبات الأمنية المتعلقة بقدرات المنظمة

مستوى الثقة	المتطلبات الأمنية لجانب قدرة المنظمة				
	السمعة	تنفيذ العقد	اتساق القيمة	القدرة على التعويض	الاستقلالية
مرتفع	✓	✓	✓	✓	✓
متوسط	(✓)	✓	–	✓	(✓)
منخفض	–	✓	–	(✓)	–

3.2.10 المتطلبات الإجرائية

1.3.2.10 مقدمة

تمكن تلبية قدرة التشغيل الأمني من خلال استعمال القدرات التالية: أمن التطوير ودورة حياة المنتَج وقدرة التشغيل الأمني.

2.3.2.10 أمن التطوير ودورة حياة المنتَج

ضمن خطة ضمان أمن معدات الشبكة (NESAS)، يغطي التطوير ودورة حياة المنتَج جميع الجوانب التي يحتمل أن تؤثر على عمر منتَج الشبكة، بما في ذلك تخطيطه وتصميمه وتنفيذه وتسليمه وتحديثه، وانحساره في نهاية المطاف. وفي الوقت الحالي، بالنسبة لشبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020)، فإن خطة ضمان أمن معدات الشبكة (NESAS)، التي اشتركت في وضعها رابطة النظام العالمي للاتصالات المتنقلة (GSMA) ومشروع شراكة الجيل الثالث (3GPP)، حددت أمن التطوير ودورة حياة المنتَج لمعدات شبكة الاتصالات المتنقلة الدولية–2020؛ التي تغطي المراحل التي تمر بها منتجات الشبكة طوال مسيرة تطويرها، (بما في ذلك مراحل التخطيط والتصميم والتنفيذ والاختبار والإصدار والتسليم؛ التي تغطي المراحل التي تعبرها منتجات الشبكة المطوَرة حتى نهاية عمرها، بما في ذلك إصدارات الصيانة والتحديث). ويوصى بالرجوع إلى تقييم البائع لتطوير ودورة حياة المنتجات.

3.3.2.10 قدرة التشغيل الأمني

إن قدرة التشغيل الأمني تعني حاجة المنتجات أو الشبكة إلى إدارة سليمة عند استعمالها تجارياً، بما في ذلك النشر الأمني والتحصين والتحكم في النفاذ المقيَّد.

4.3.2.10 ملخص

وهكذا، يوصى بإدراج المتطلبات الأمنية، فيما يتعلق بقدرة التشغيل الأمني، في الجدول 9.

الجدول 9 – مستويات الثقة والمتطلبات الأمنية لقدرة التشغيل الأمني

مستوى الثقة	المتطلبات الأمنية لجانب قدرة التشغيل الأمني	
	أمن التطوير ودورة حياة المنتَج	التشغيل الأمني
مرتفع	✓	✓
متوسط	(✓)	✓
منخفض	=	✓

4.2.10 المتطلبات التكنولوجية

تمكن تلبية قدرة الجدارة بالثقة من خلال تلبية المستويات المناسبة في النواحي التالية: الإجراءات الأمنية والخصوصيات والصمود، والسلامة والموثوقية والتوفر. ومن منظور الجدارة بالثقة، هذه النعوت هي النعوت الرئيسية التي يوصى بأن تتمتع بها المنتجات والحلول الأمنية التي يقدمها أصحاب المصلحة، على النحو المبين في مجموعة من الوثائق مثل [b-BSI 10754-1] و[b-NIST SP800-160v1]، وما إلى ذلك.

ويرد في الجدول 10 مثال عن الطرق التي يمكن من خلالها أن ترتبط بها مستويات الثقة بجدارة منظمة ما بالثقة. وكما ذُكر من قبل، تختلف من الناحية العملية الخيارات الدقيقة للجوانب المطلوبة لمستويي الثقة المتوسط والمنخفض تبعاً لميدان التطبيق. فعلى سبيل المثال، قد تظل الحماية المناسبة لحرمة البيانات مطلوبة في بعض الحالات لتحقيق مستوى ثقة منخفض، في حين أن هذا الجانب قد لا يكون مهماً في حالات أخرى حتى عندما تدعو الحاجة إلى مستوى ثقة متوسط.

الجدول 10 – مستويات الثقة والمتطلبات الأمنية لقدرة الجدارة بالثقة

مستوى الثقة	المتطلبات الأمنية لقدرة الجدارة بالثقة					
	الإجراءات الأمنية	الخصوصيات	الصمود	السلامة	الموثوقية	التوفر
مرتفع	✓	✓	✓	✓	✓	✓
متوسط	✓	(✓)	(✓)	(✓)	(✓)	✓
منخفض	✓	–	–	(✓)	(✓)	–

وفي عمليات التنفيذ على أرض الواقع، ستعتمد المتطلبات الدقيقة على سيناريوهات الخدمة ويتعين السماح بالمرونة. وكما ذُكر سابقاً، في حالة انخفاض مستوى الثقة، رغم قلة المتطلبات الأمنية نسبياً، قد تدعو الحاجة إلى متطلبات محددة أقوى بشأن الخصوصيات مثلاً.

3.10 تفسير الثقة بمتطلبات ضمان تفصيلية

بمجرد تحديد مستوى الثقة المطلوب لحالة استعمال معينة، من الضروري تفسير مستوى الثقة هذا لاتخاذ قرارات التنفيذ والتشغيل في ضوئه.

ويمكن تحقيق ذلك من خلال برسم خارطة ارتباطات مستوى الثقة المطلوب مع متطلبات محددة مدرجة في الفقرة 2.10، ويمكن الإيفاء بهذه المتطلبات من خلال ضمان المنتَج والنظام. وهناك مجموعة من التقنيات المقيّسة الراسخة منذ وقت طويل لضمان المنتجات والأنظمة بالثقة من خلال الاختبارات والتقييمات، المنفَّذة على يد أطراف ثالثة متخصصة مثلاً. ويمكن استعمالها كأساس لرسم خارطة ارتباطات مستوى الثقة المطلوب، نتيجة لتحليل النمط الموضح في الفقرة 4.9، مع متطلبات الضمان الدقيقة بشأن المعدات وحيازة الخدمات واستعمالها.

ويهدف المثال في الجدول 11 إلى تمكين رسم خارطة ارتباطات مستويات متطلبات الثقة مع القرارات التجارية والتشغيلية القائمة على الثقة استناداً إلى تقييمات المنتجات والأنظمة.

الجدول 11 – مثال رسم خارطة ارتباطات متطلبات ضمان مستوى الثقة المطلوب

مستوى الثقة المطلوب	نمط كيان الضمان	أمثلة على خطة ضمان الأمن
مرتفع	تقييم من هيئة عامة معترف بها	معايير شائعة [b-ISO/IEC 15408 (جميع الأجزاء)] هيئة تنظيمية وطنية [b-ISO/IEC 27001] NESAS توصيف ضمان الأمن (SCAS) [b-3GPP TS33.511] و[b-3GPP TS33.512] و[b-3GPP TS33.513] و[b-3GPP TS33.514] و[b-3GPP TS33.515] و[b-3GPP TS33.516] و[b-3GPP TS33.517] و[b-3GPP TS33.518] و[b-3GPP TS33.519]
متوسط	تقييم من هيئة معتمدة لتقييم المطابقة (CAB)	معايير شائعة [b-ISA/IEC 62443 (جميع الأجزاء)] [b-ISO/IEC 27001] NESAS/SCAS
منخفض	تقييم من هيئة معتمدة لتقييم المطابقة أو تقييم ذاتي	معايير شائعة NESAS/SCAS

وحتى ضمن خطة ضمان معينة، قد تكون درجات أو أنواع مختلفة من كفالات الضمان مناسبة لمستويات الثقة المختلفة.

- وتتيح بعض التقنيات، على النحو المحدد في المرجع [b-ISO/IEC 15408 (جميع الأجزاء)]، توصيف مستويات متعددة من الضمان، بحيث يمكن اختيارياً أن تتطلب مستويات مختلفة من الثقة مستويات مختلفة من التقييم حسب المرجع [b-ISO/IEC 15408 (جميع الأجزاء)]، ولكن لا تسمح خطط أخرى، مثل المرجع [b-ISO/IEC 27001] إلا بمستوى واحد من التقييم.
- وقد تختلف اختيارياً درجة الضمان التي يمكن الحصول عليها من تقييم تبعاً للهيئة التي تؤديه (كما يبين ذلك العمود الأوسط في الجدول 11). فعلى سبيل المثال، قد يكون التقييم الذاتي قياساً بمتطلبات المرجع [b-ISO/IEC 27001] مناسباً لمستوى الثقة المنخفض.

وعلاوة على ذلك، يمكن تعزيز الترجيح المسنَد للتقييم بعوامل أخرى، مثل:

- ما إذا كانت المعدات أو الخدمة حرجة لإنجاز المهام أو هي مجرد وسيلة من وسائل متعددة يمكن أن تقدَّم فيها وظيفة معينة (من خلال الإطناب الرديف مثلاً)؛
- ما إذا كان هناك تقييمات ضمان متعددة ترتبط بالجوانب المختلفة لمنتَج أو نظام أو خدمة على وجه التحديد.

بيبليوغرافيا

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ISO 10393] ISO 10393:2013, *Consumer product recall – Guidelines for suppliers*.

[b-ISO 28598-1] ISO 28598-1:2017, *Acceptance sampling procedures based on the allocation of priorities principle (APP) – Part 1: Guidelines for the APP approach*.

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*. Available [viewed 2022-07-18] at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en .

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*.

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

[b-ISO/IEC/IEEE 15288] ISO/IEC/IEEE 15288:2015, *Systems and software engineering – System life cycle processes*.

[b-ISO/IEC 15408(all parts)] ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security*

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*.

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*.

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

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

[b-ISO/IEC 27005] ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management*.

[b-ISO/PAS 19450] Publicly Available Specification ISO/PAS 19450:2015, *Automation systems and integration – Object-process methodology*.

[b-ISO/TS 21089] Technical Specification ISO/TS 21089:2018, *Health informatics – Trusted end-to-end information flows.*

[b-ISO/TS 21719-2] Technical Specification ISO/TS 21719-2:2018, *Electronic fee collection – Personalization of on-board equipment (OBE) Part 2: Using dedicated short-range communication.*

[b-ISO/TS 22318] Technical Specification ISO/TS 22318:2021, *Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management*.

[b-ISA/IEC 62443] ISA/IEC 62443 (all parts) [series of automation and control systems cybersecurity standards].

[b-GSMA FS.13] GSM Association (2022). *Network equipment security assurance scheme – Overview*, Official Document FS.13, version 2.1. London: GSM Association. 29 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf

[b-GSMA FS.14] GSM Association (2022). *Network equipment security assurance scheme – Security test laboratory accreditation*, Official Document FS.14, version 2.1. London: GSM Association. 15 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.14-v2.1.pdf .

[b-GSMA FS.15] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle assessment methodology*, Official Document FS.15, version 2.1. London: GSM Association. 33 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.15-v2.1.pdf .

[b-GSMA FS.16] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle security requirements*, Official Document FS.16, version 2.1. London: GSM Association. 22 pp. Available [viewed 2022-07-17] at: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf .

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2*.

[b-IETF RFC 6733] IETF RFC 6733 (2012), *Diameter base protocol*.

[b-3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.6.0 (2022), *Security architecture and procedures for 5G system*.

[b-3GPP TS 33.511] Technical Specification 3GPP TS 33.511 V17.1.0 (2022), *Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class*.

[b-3GPP TS 33.512] Technical Specification 3GPP TS 33.512 V17.3.0 (2022), *5G security assurance specification (SCAS); Access and mobility management function (AMF)*.

[b-3GPP TS 33.513] Technical Specification 3GPP TS 33.513 V17.0.0 (2022), *5G security assurance specification (SCAS); User plane function (UPF)*.

[b-3GPP TS 33.514] Technical Specification 3GPP TS 33.514 V17.0.0 (2022), *5G security assurance specification (SCAS) for the unified data management (UDM) network product class*.

[b-3GPP TS 33.515] Technical Specification 3GPP TS33.515 V17.0.0 (2022), *5G security assurance specification (SCAS) for the session management function (SMF) network product class*.

[b-3GPP TS 33.516] Technical Specification 3PGP TS33.516 V17.0.0 (2022), *5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*.

[b-3GPP TS 33.517] Technical Specification 3GPP TS33.517 V17.0.0 (2022), *5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class*.

[b-3GPP TS 33.518] Technical Specification 3GPP TS33.518 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network repository function (NRF) network product class*.

[b-3GPP TS 33.519] Technical Specification 3GPP TS33.519 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network exposure function (NEF) network product class*.

[b-BSI 10754-1] BS 10754-1:2018, *Information technology. Systems trustworthiness – Governance and management specification*.

[b-BSIMM] British Standards Institution (2021). *Building security in maturity model*, BSIMM 12. London: British Standards Institution.

[b-NIST FICIC] NIST (2018). *Framework for improving critical infrastructure cybersecurity*, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. 48 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[b-NIST SP800-30] Joint Task Force Transformation Initiative (2012). *Guide for conducting risk assessments*, NIST Special Publication, NIST SP800-30 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology. 95 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf .

[b-NIST SP 800-53] NIST SP 800-53 Rev 5 2020, *Security and privacy controls for information systems and organizations*.

[b-NIST SP800-160v1] Ross, R., McEvilley, M., Carrier Oren, J. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems – Volume 1*, NIST Special Publication, NIST SP800-160v1. Gaithersburg, MD: National Institute of Standards and Technology. 243 pp. Available [viewed 2022-07-18] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf .

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، 2022