التـوصيــة

ITU-T X.1816 (03/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن شبكات الاتصالات المتنقلة الدولية–2020

مبادئ توجيهية ومتطلبات لتصنيف القدرات الأمنية في شريحة شبكة الاتصالات المتنقلة الدولية–2020

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
القياس الحيوي عن بُعد	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن شبكة الويب (1)	X.1140–X.1149
أمن التطبيقات (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن تكنولوجيا السجلات الموزعة (DLT)	X.1400–X.1429
أمن التطبيقات (2)	X.1450–X.1459
أمن شبكة الويب (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1500–X.1519
تبادل معلومات بشأن مواطن الضعف/الحالة	X.1520–X.1539
تبادل معلومات بشأن الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل معلومات بشأن السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولّد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن شبكات الاتصالات المتنقلة الدولية–2020	**X.1800–X.1819**

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

مبادئ توجيهية ومتطلبات لتصنيف القدرات الأمنية في شريحة شبكة الاتصالات المتنقلة الدولية–2020

ملخص

إن تعريف الوظائف والعمليات الأساسية لتكنولوجيا تقسيم الشبكة إلى شرائح وضع أساساً متيناً للموجة الأولى من نشر الاتصالات المتنقلة الدولية–2020 (IMT-2020) والاستعمال التجاري لخدمات تقسيم الشبكة إلى شرائح. وكشبكة منطقية من طرف إلى طرف مخصصة حسب الطلب، يمكن للتقسيم إلى شرائح أن يوفر تمايز القدرات الأمنية: فأولاً يوفر تقسيم الاتصالات المتنقلة الدولية–2020 (IMT-2020) إلى شرائح تدابير أمنية داعمة لتنفيذ الشبكة المتمايز. ثانياً، تدعم شبكة الاتصالات المتنقلة الدولية–2020 بعض التدابير الأمنية الاختيارية على مستوى الشريحة. ويمكن أن تقدم بعض التدابير الأمنية أيضاً خيارات أمنية متعددة، ويمكن أن يمتلك المشغلون موارد أمنية مختلفة. ويمكن أن تجلب هذه الموارد درجات مختلفة من الضمان الأمني أو الأداء غير ذي الصلة بالأمن. ولعملاء الشريحة أيضاً متطلبات أمنية محددة وقد يطلبون من مشغلي الشرائح شرائح شبكة مخصصة بمستويات حماية أمنية مختلفة. وتظهر بعض التحديات أمام عملاء الشرائح أو مشغلي الشرائح في اختيار القدرات الأمنية لشرائحهم مثل تكلفة الإدارة وعدم اتساق التعاريف، وما إلى ذلك. والهدف من التوصية ITU-R X.1816 هو تقديم وصف للقدرات الأمنية المتمايزة لشرائح شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020) وإرشادات لتصنيف هذه القدرات الأمنية فضلاً عن أمن الشرائح، من أجل مساعدة النظام الإيكولوجي للاتصالات المتنقلة الدولية–2020 على فهم واختيار القدرات الأمنية لشرائح الشبكة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1816	2023-03-03	17	11.1002/1000/15114

مصطلحات أساسية

التصنيف، الاتصالات المتنقلة الدولية–2020، تقسيم الشبكة إلى شرائح، القدرات الأمنية.

* للنفاذ إلى توصية، الرجاء 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 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/حقوق تأليف ونشر برمجيات 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 قواعد البيانات ذات الصلة لقطاع تقييس الاتصالات (ITU-T) في موقع قطاع تقييس الاتصالات http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مبادئ توجيهية ومتطلبات لتصنيف القدرات الأمنية في شريحة شبكة الاتصالات المتنقلة الدولية–2020

1 مجال التطبيق

الهدف من هذه التوصية تقديم مبادئ توجيهية ومتطلبات لتصنيف أمن شريحة شبكة الاتصالات المتنقلة الدولية–2020. وتحدد هذه التوصية ما يلي:

- تعريف القدرات الأمنية المتمايزة لشريحة شبكة الاتصالات المتنقلة الدولية–2020؛
- مبادئ وأساليب تحديد تصنيف القدرات الأمنية لشريحة شبكة الاتصالات المتنقلة الدولية–2020.

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.

[ITU-T X.805] التوصية ITU-T X.805 (2003)، *معمارية الأمن في الأنظمة التي توفر الاتصالات من طرف إلى طرف*.

[ITU-T X.1047] التوصية ITU-T X.1047 (2021)، *متطلبات ومعمارية الأمن لإدارة شرائح الشبكة وتنسيقها*.

[3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.1.0 (2021), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 17)*.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مصادر أخرى:

1.1.3 شريحة شبكة (network slice) [b-ITU-T Y.3100]: شبكة منطقية تقدم قدرات شبكية وخصائص شبكية محددة.

الملاحظة 1 – تمكِّن شرائح الشبكة من إنشاء شبكات مكيّفة حسب الطلب لتقديم حلول مرنة لسيناريوهات السوق المختلفة التي تتسم بمتطلبات متنوعة فيما يتعلق بالوظائف والأداء وتوزيع الموارد.

الملاحظة 2 – يجوز لشريحة الشبكة التمكن من كشف قدراتها.

الملاحظة 3 – يتحقق سلوك شريحة شبكة عبر حالة (حالات) شريحة الشبكة.

2.1.3 حالة شريحة الشبكة (network slice instance) [b-ITU-T Y.3100]: حالة لشريحة الشبكة منشأة على أساس مخطط شريحة الشبكة.

3.1.3 الشبكة الفرعية لشريحة الشبكة (network slice subnet) [b-ETSI TS 128 530]: تمثيل لجوانب إدارة مجموعة من الوظائف المدارة والموارد المطلوبة (مثل موارد الحوسبة والتخزين والتوصيل الشبكي).

2.3 المصطلحات المعرَّفة في هذه التوصية

لا توجد.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والمختزلات التالية:

AAA الاستيقان والتخويل والمحاسبة *(Authentication, Authorization, and Accounting)*

ACL قائمة التحكم في النفاذ *(Access Control List)*

AMF وظيفة إدارة النفاذ والتنقلية *(Access and Mobility Management Function)*

CN الشبكة الأساسية *(Core Network)*

CU الوحدة المركزية *(Central Unit)*

DDoS الحرمان من الخدمة الموزَّع *(Distributed Denial-of-Service)*

DU وحدة موزَّعة *(Distributed Unit)*

EAP بروتوكول الاستيقان القابل للتوسيع *(Extensible Authentication Protocol)*

ENSI معلومات شريحة الشبكة الخارجية *(External Network Slice Information)*

gNB العقدة B للتكنولوجيا الراديوية الجديدة *(NR Node B)*

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

NAT ترجمة عنوان شبكة *(Network Address Translation)*

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

ng-eNB العقدة B المتطورة من الجيل التالي *(Next Generation Evolved Node-B)*

NSSAI معلومات المساعدة في اختيار شرائح شبكة *(Network Slice Selection Assistance Information)*

S-NSSAI معلومات المساعدة في اختيار شريحة شبكة *(Single Network Slice Selection Assistance Information)*

PDU وحدة بيانات البروتوكول *(Protocol Data Unit)*

PNF وظيفة الشبكة المادية *(Physical Network Function)*

RAN شبكة النفاذ الراديوي *(Radio Access Network)*

RB القناة الحاملة الراديوية *(Radio Bearer)*

TLS أمن طبقة النقل *(Transport Layer Security)*

UE معدات المستعمل *(User Equipment)*

URL محدد موقع الموارد الموحد *(Uniform Resource Locator)*

VNF وظيفة الشبكة الافتراضية *(Virtual Network Function)*

WAF جدار حماية تطبيقات الويب *(Web Application Firewall)*

5 الاصطلاحات

يتعين فهم الاصطلاحات 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.

"**من الجائز**" 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 التعريف بتصنيف القدرات الأمنية لشرائح شبكة الاتصالات المتنقلة الدولية-2020

يعد أمن شريحة الشبكة الشرط المسبق للتعريف بتقسيم الشبكة إلى شرائح. وبالنسبة لعملاء الشرائح الذين يستعملون خدمات اتصالات الشرائح، فإنهم يتطلبون ضماناً أمنياً مقابلاً على مقاس تنفيذ شرائحهم ولعل لديهم أيضاً متطلبات أمنية محددة على أساس خدماتهم التي تستعمل الشرائح. لذلك يمكن أن يطلبوا شرائح شبكة مخصصة بحماية أمنية مختلفة من شركات الاتصالات. وبالنسبة لمشغلي الشرائح الذين يصممون الشبكات ويبنونها ويشغلونها ويقدمون شرائح الشبكة، يتضمن التقسيم إلى شرائح العديد من الميادين (من قبيل ميادين اللاسلكي والإرسال والشبكة الأساسية والإدارة) ويمكن أن يقدم قدرات أمنية متمايزة: أولاً، يقدم تقسيم شبكة الاتصالات المتنقلة الدولية-2020 إلى شرائح تدابير أمنية لتنفيذ الشبكة المتمايز. ثانياً، تدعم شبكة الاتصالات المتنقلة الدولية-2020 بعض التدابير الأمنية الاختيارية على مستوى الشريحة. ويمكن لبعض التدابير الأمنية أيضاً أن تقدم خيارات أمنية متعددة، وقد يمتلك المشغلون موارد أمنية مختلفة. وقد يجلب ذلك درجات مختلفة من الضمان الأمني أو الأداء غير ذي الصلة بالأمن. وبالتالي، يتعين تحديد القدرات الأمنية لشريحة واحدة على أساس متطلبات العملاء والقدرات الأمنية التي تستطيع الشبكة تقديمها. وتوجد بعض التحديات لعملاء الشرائح أو مشغلي الشرائح الذين يختارون القدرات الأمنية لشرائحهم:

- قد تكون متطلبات أمن العملاء غامضة وقليلة وغير كافية لربطها مع ما يقابلها من القدرات الأمنية.
- قد يكون لدى العملاء الكثير جداً من المتطلبات الأمنية بما يتجاوز قدرات الشبكة.

يمكن أن تتباين التكلفة المعرفية لأصحاب المصلحة فيما يتعلق بالقدرات الأمنية والاختلافات وقد لا يكون مزيج القدرات التي يختارونها معقولاً. فعلى سبيل المثال، قد لا تتسق الحماية التي تقدمها القدرات المختارة للميادين المتعددة أو أصحاب المصلحة.

- قد يكون عدد توليفات القدرات الأمنية للشرائح هائلاً وقد ترتفع تكلفة إدارة وتنسيق المشغلين نسبياً.

ويوصى بقدرات أمنية متباينة لشرائح شبكة الاتصالات المتنقلة الدولية-2020 (IMT-2020) وبمنهجية لتصنيفها ودمجها إذ يتسم ذلك بالأهمية التالية:

- يساعد دوائر الصناعة على التوصل إلى فهم موحد للقدرات الأمنية للشريحة وللفرق بين القدرات الأمنية للشريحة (كالأداء مثلاً).
- يقدم تصنيفاً أساسياً عاماً للقدرات الأمنية لشرائح شبكات الاتصالات المتنقلة الدولية-2020 لإفهام دوائر الصناعة بوضوح القدرة الأمنية على التقسيم إلى شرائح وتحسين التوافق مع معظم التطبيقات الصناعية.
- يساعد في تحقيق التجوال بين الشرائح المختلفة ويسهل أيضاً إعادة استعمال الشرائح.
- يقدم مرجعاً للمستعملين في دوائر الصناعة لاختيار الشرائح المناسبة التي يمكنها تلبية المتطلبات.
- يقدم مرجعاً لمشرفي الصناعة لصياغة خطط واستراتيجيات تطوير الشرائح.
- يقدم مرجعاً لمقدمي الخدمة لنشر الخدمات في الشرائح المناسبة.
- يقدم مرجعاً للمشغلين لصياغة خطط تطوير الشرائح ولتقييم قيمة وأسعار الشرائح.
- يقدم مرجعاً لبائعي المعدات لتخطيط خارطة طريق التكنولوجيا وخارطة طريق المنتج للشرائح.

وتتضمن المنهجية الجوانب التالية:

- وضع قائمة بالقدرات الأمنية المتمايزة عموماً في شكل مهيكل يشمل الاسم والوصف والبعد الأمني والخيارات. ويرد ذلك في الفقرة 7.
- في كل بُعد أمني، يمكن تشكيل مستويات متعددة لبُعد أمني واحد من خلال إدراج ما يقابلها من توليفات من القدرات الأمنية المقسِّمة إلى شرائح ذات خيارات مختلفة على أساس بعض المبادئ. ويرد ذلك في الفقرة 8.
- علاوةً على ذلك، يمكن تشكيل أنماط الأمن الأساسية للشرائح المكونة للأبعاد الأمنية باختيار مستوى واحد لكل بُعد أمني على أساس بعض المبادئ. ويرد ذلك في الفقرة 9.
- يمكن لأصحاب المصلحة استعمال مبدأ وأساليب ونتائج التصنيف لتحديد القدرات الأمنية لشريحة واحدة. ويرد ذلك في القسم 10.

7 القدرات الأمنية لشرائح شبكة الاتصالات المتنقلة الدولية–2020

1.7 الصيغة النموذجية لوصف القدرات الأمنية لشريحة الشبكة

تقدم الفقرة 7 قائمة القدرات العامة لأمن شبكة الاتصالات المتنقلة الدولية–2020 التي يمكن أن تختلف بين شرائح الشبكة. وينبغي أن تكون أوصاف القدرات الأمنية واضحة وموجزة لا لبس فيها. ويتضمن كل وصف ما يلي:

- وصف القدرة: وصف مفصّل لتمايز قدرة أمن شريحة شبكة الاتصالات المتنقلة الدولية–2020.
- اسم القدرة: اسم متفرد ومختصَر مخصص لكل قدرة أمنية.
- بُعد القدرة الأمني: جانب معين من جوانب الأمن صُممت القدرة الأمنية لمعالجته. وهناك ثمانية (8) أبعاد أمنية تشمل التحكم في النفاذ والاستيقان وعدم التنصل وسرية البيانات وأمن الاتصالات وسلامة البيانات والتيسر والخصوصية [ITU-T X.805].
- خيارات القدرة: خيارات متعددة لكل قدرة أمنية يمكن أن تختلف بين الشرائح. ويشار إلى كل خيار في هذه التوصية "بالرقم التسلسلي المختصَر للقدرة". ملاحظة: الخيارات عامة وغير مرتبطة بعمليات تنفيذ محددة للشبكة. ويمكن الاسترسال في تقسيمها فرعياً لكي تتسق مع تنفيذ محدد.

2.7 القدرات الأمنية لشرائح الاتصالات المتنقلة الدولية–2020 المتمايزة

1.2.7 قدرة الاستيقان والتخويل الخاصة بشريحة في الشبكة

- وصف القدرة: يقدم نظام الاتصالات المتنقلة الدولية–2020 (IMT-2020) خيار استعمال الاستيقان والتخويل الخاص بشريحة في الشبكة [3GPP TS 33.501] بين جهاز المستعمل (UE) ومخدِّم الاستيقان والتخويل والمحاسبة (AAA-S) الذي قد تملكه مؤسسة طرف ثالث خارجية. ويمكن إطلاق الاستيقان والتخويل الخاصين بشريحة في الشبكة على أساس معلومات المساعدة في اختيار شريحة شبكة (S-NSSAI) بعد الاستيقان الأولي. ويمكن لمخدم AAA أيضاً أن يطلق إلغاء التخويل الخاص بشريحة وإعادة الاستيقان وإعادة التخويل.
- اسم القدرة: الاستيقان والتخويل الخاصين بشريحة في الشبكة (NSSAA)
- البعد الأمني للقدرة: الاستيقان، التحكم في النفاذ
- خيار القدرة:
  - NSSAA.0: إيقاف
  - NSSAA.1: تشغيل

2.2.7 قدرة موارد الشبكة على عزل شريحة في الشبكة

- وصف القدرة: تعمل شرائح شبكة الاتصالات المتنقلة الدولية–2020 على موارد البنية التحتية الموحدة للمشغلين. وهناك مجموعة متنوعة من حلول العزل لمنع عناصر شبكة الشريحة من النفاذ إلى الشبكات في الشرائح المختلفة أو التأثير عليها من خلال موارد البنية التحتية المشتركة: من جانب ميادين الشبكة الفرعية للشريحة:

  – في شبكة النفاذ (AN): بالنسبة للسطح البيني الهوائي، يتاح التشارك الدينامي في الموارد بين القنوات الحاملة الراديوية (RB) والحجز السكوني لهذه الموارد من أجل توزيعها. ويتميز التشارك الدينامي بتأثير أفضل وأكثر مرونة في التغطية واستعمال الموارد بينما يتسم الحجز السكوني بقدر أعلى من الموثوقية والتكلفة. وفي حالة محطة القاعدة، يمكن أن تتماثل الوحدة المركزية (CU) والوحدة الموزعة (DU) للشرائح المختلفة. ولإعلاء مستويات العزل، يمكن عزلهما مادياً بتوزيع عتاد مخصص أو عزلهما منطقياً باستعمال التمثيل الافتراضي لوظائف الشبكة (NFV) (أي الآلة/الحاوية الافتراضية) للتشارك في العتاد.

  – في شبكة النقل (TN): يمكن أن يكون العزل على شبكات النقل معدوماً بلا أي عزل، أو عزلاً مادياً (مثل عزل وظيفة الشبكة المادية، وعزل وصلة الشبكة المادية، وما إلى ذلك)، أو عزلاً منطقياً (مثل عزل وظيفة الشبكة المنطقي، وعزل وصلة الشبكة المنطقي/الافتراضي، وما إلى ذلك) [ITU-T X.1047].

  – في الشبكة الأساسية (CN): يتألف العزل المادي لموارد الشبكة الأساسية من عزل مخصص واحد أو أكثر لوظيفة الشبكة المادية (PNF)، وعزل مخصص لوصلة الشبكة المادية، وعزل الموقع الجغرافي، وعزل الحوسبة، وعزل الذاكرة، وعزل التخزين، ووظيفة الشبكة المادية، وعزل قائم على الأمن وهلم جرا. ويتألف العزل المنطقي لموارد الشبكة الأساسية من عزل واحد أو أكثر لوظيفة الشبكة الافتراضية (VNF)، وعزل الوصلة الافتراضية، وعزل تكنولوجيا التمثيل الافتراضي، وعزل الحوسبة الافتراضية، وعزل الذاكرة الافتراضية، وعزل التخزين الافتراضي، وعزل الموقع الجغرافي للعتاد (HW) الممثَّل افتراضياً لتقديم موارد افتراضية، والعزل القائم على أمن وظيفة الشبكة الافتراضية، وهلم جرا [ITU-T X.1047].

  ومن جانب أنماط الموارد وتقنيات العزل:

  - في مورد السطح البيني الهوائي: التشارك في القناة الحاملة الراديوية (RB) أو حجز RB
  - في مورد وظيفة شبكة AN/TN/CN: العزل المادي أو العزل المنطقي أو انعدام العزل

- اسم القدرة: عزل موارد الشبكة عن شريحة (SIR)
- البعد الأمني للقدرة: التحكم في النفاذ، التيسر، الخصوصية
- خيارات القدرة والأداء المقابل:
  – SIR.0: انعدام العزل
  – SIR.1: عزل منطقي + التشارك في القناة الحاملة الراديوية (RB)
  – SIR.2: عزل منطقي + مادي + التشارك في RB
  – SIR.3: عزل مادي + التشارك في RB
  – SIR.4: عزل منطقي + حجز RB
  – SIR.5: عزل منطقي + مادي + حجز RB
  – SIR.6: عزل مادي + حجز RB

3.2.7 قدرة حماية بيانات مستوي المستعمل

- وصف القدرة: يمكن لنظام الاتصالات المتنقلة الدولية–2020 (IMT-2020) أن يقدم قدرات متمايزة لحماية بيانات مستوي المستعمل على مستوى الشريحة. ويمكن للعقدة B المتطورة من الجيل التالي (ng-eNB)/العقدة B للتكنولوجيا الراديوية الجديدة (gNB) أن تبت في تفعيل سرية مستوي المستعمل و/أو حماية سلامة مستوي المستعمل لكل دورة لوحدة بيانات البروتوكول (PDU)، وفقاً لسياسة أمن مستوي المستعمل المستلَمة. ويمكن تشكيل سياسة أمن مستوي المستعمل للإشارة إلى كونها "مطلوبة" أو "غير مطلوبة". وتوجد خوارزميات تجفير اختيارية [3GPP TS 33.501].
- اسم القدرة: حماية بيانات مستوي المستعمل (UPDP)
- البعد الأمني للقدرة: سرية البيانات، سلامة البيانات
- خيار القدرة:
  - UPDP.0: عدم تفعيل سرية مستوي المستعمل و/أو حماية سلامة مستوي المستعمل
  - UPDP.1: تفعيل سرية مستوي المستعمل و/أو حماية سلامة مستوي المستعمل بخوارزميات التجفير الاختيارية

4.2.7 قدرة حماية الحدود

- وصف القدرة: من المهم حماية شريحة شبكة من هجمات على الشبكة بنشر وظائف/ميزات التحكم الأمني عند الحدود، خاصة عند حدود الشبكة المركزية (مثل تشكيلة حماية العقدة 6 (N6Protection) عند السطح البيني للعقدة 6 (N6)) [b-3GPP TS 28.541]. وبالنسبة لمختلف مستهلكي شرائح الشبكة، قد تختلف وظائف/ميزات التحكم الأمني وقد تتغير دينامياً وفقاً للمتطلبات. ويمكن أن تتجلى وظائف التحكم الأمني في جدار حماية، وترجمة عنوان الشبكة (NAT)، ومكافحة البرمجيات الضارة، ورقابة أولياء الأمور، ووظيفة الحماية ضد الحرمان من الخدمة الموزَّع (DDoS)، وما إلى ذلك، [b-3GPP TS 28.541]. وتحتكم الميزات إلى قواعد إعادة التسيير وقواعد الاصطفاء وتشكيلة المعلمات وما إلى ذلك. ويمكن أن تقتضي المتطلبات التحكم في النفاذ إلى شبكة البيانات وآلية تمرير في أنفاق.
- اسم القدرة: حماية الحدود (BP)
- البعد الأمني للقدرة: التحكم في النفاذ، التيسر، أمن الاتصالات
- خيار القدرة:
  - BP.0: بدون وظائف تحكم أمني
  - BP.1: بنشر وظائف/ميزات التحكم الأمني

5.2.7 قدرات حماية خدمة التطبيق

- وصف القدرة: يمكن للمشغلين نشر أجهزة أمنية أو وحدات أمنية على جانب الشبكة لتقديم حماية أمنية مختلفة لخدمات التطبيق باستعمال الشرائح والمستعملين الذين يستعملون خدمات التطبيق. فعلى سبيل المثال، يمكن لشبكة المشغل أن تقدم كشف مطراف شاذ، وتنظيف حركة الشبكة، وكشف محدد موقع الموارد الموحد الضار (URL)، وجدار حماية تطبيقات الويب (WAF)، وهجمات الحرمان من الخدمة الموزَّع (DDoS)، وما إلى ذلك.
- اسم القدرة: حماية خدمة التطبيق (ASP)
- البعد الأمني للقدرة: أمن الاتصالات، التحكم في النفاذ، التيسر
- خيار القدرة:
  - ASP.0: بدون حماية لخدمة التطبيق
  - ASP.1: بنشر حمايات لخدمة التطبيق

6.2.7 قدرة حماية خصوصية هوية بروتوكول الاستيقان القابل للتوسيع (EAP) خلال الاستيقان والتخويل الخاصين بشريحة في الشبكة (NSSAA)

- وصف القدرة: تتعدد أساليب بروتوكول الاستيقان القابل للتوسيع (EAP) [b-IETF RFC 3748] الممكنة للاستيقان الخاص بشريحة. ويمكن اختيار أسلوب لبروتوكول EAP قادر على حماية الخصوصية مثل أمن طبقة النقل (TLS) لبروتوكول EAP [b-IETF RFC 5216] وأمن طبقة النقل الممرَر في نفق (TTLS) لبروتوكول EAP [b-IETF RFC 5281] للاستعمال في حماية خصوصية هوية بروتوكول EAP المستعملة في الاستيقان والتخويل الخاصين بشريحة في الشبكة (NSSAA) على أساس بروتوكول EAP [3GPP TS 33.501].
- اسم القدرة: حماية خصوصية هوية بروتوكول الاستيقان القابل للتوسيع (EAP) خلال الاستيقان والتخويل الخاصين بشريحة في الشبكة (PPEAP)
- البعد الأمني للقدرة: الخصوصية
- خيار القدرة:
  - PPEAP.0: عدم استعمال أساليب لبروتوكول EAP قادرة على حماية الخصوصية
  - PPEAP.1: استعمال أساليب لبروتوكول EAP قادرة على حماية الخصوصية

7.2.7 قدرة حماية خصوصية معلومات المساعدة في اختيار شرائح (شريحة) شبكة (NSSAI(-S))

- وصف القدرة: تُستعمل معلومات المساعدة في اختيار شرائح شبكة (NSSAI) لتعرف هوية شريحة/نمط خدمة شبكة. ويمكن الحصول على بعض المعلومات عن شبكة المشغل والعملاء من معلومات NSSAI ومن استعمالها. وتقدم شبكة الاتصالات المتنقلة الدولية–2020 (IMT-2020) القدرات اللازمة لحماية خصوصية معلومات المساعدة في اختيار شريحة شبكة (NASSAI(-S)) من خلال السماح بعدم استعمال معلومات المساعدة في اختيار شرائح شبكة أو استعمال معلومات بديلة خارج ميدان المشغِّل. وأثناء إجراء التسجيل، يمكن لوظيفة إدارة النفاذ والتنقلية أن تقدم لمعدات المستعمل في رسالة قبول التسجيل معلمة أسلوب إدراج معلومات NASSAI عند إقامة توصيل في طبقة النفاذ لتبين متى وما إذا كانت معدات المستعمل يجب أن تتضمن معلومات NASSAI في إقامة توصيل طبقة النفاذ طبقاً لمختلف الأساليب. ويجب مبدئياً ألا تقدم معدات المستعمل معلومات NASSAI في طبقة النفاذ في النفاذ الخاصة بمشروع الشراكة 3GPP إلا إذا كانت قد زُوِّدت بإيعاز للعمل بأساليب أخرى [b-3GPP TS 23.502]. وأثناء الاستيقان والتخويل الخاصين بشريحة في الشبكة (NSSAA)، إذا كان مخدِّم الاستيقان والتخويل والمحاسبة (AAA) المستعمَل ينتمي إلى طرف ثالث، يمكن إجراء تقابل اختياري بين معلومات S-NSSAI المتداولَة داخلياً في صلب الاتصالات المتنقلة الدولية–2020 في شبكة المشغِّل وبين معلومات شريحة الشبكة الخارجية (ENSI) المرسَلة والمستعمَلة خارج ميدان المشغِّل [3GPP TS 33.501].
- اسم القدرة: حماية خصوصية معلومات المساعدة في اختيار شريحة شبكة (PPSI)
- البعد الأمني للقدرة: الخصوصية
- خيار القدرة:
  - PPSI.0: استعمال معلومات المساعدة في اختيار شريحة شبكة NASSAI خارج ميدان المشغِّل
  - PPSI.1: عدم استعمال معلومات المساعدة في اختيار شريحة شبكة NASSAI أو استعمال معلومات بديلة خارج ميدان المشغِّل

3.7 تصنيف القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية–2020

يمكن تصنيف القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية–2020 على أساس بُعدها الأمني على النحو المبين في الجدول 7-1.

الجدول 7-1 – تصنيف القدرات الأمنية لشرائح الاتصالات المتنقلة الدولية–2020 على أساس البعد الأمني

البعد الأمني قدرة أمن الشريحة	الاستيقان والتخويل الخاصان بشريحة في الشبكة (NSSAA)	عزل موارد الشبكة عن شريحة (SIR)	حماية بيانات مستوي المستعمل (UPDP)	حماية الحدود (BP)	حماية خدمة التطبيق (ASP)	حماية خصوصية هوية بروتوكول الاستيقان القابل للتوسيع خلال الاستيقان والتخويل الخاصين بشريحة في الشبكة (PPEAP)	حماية خصوصية معلومات المساعدة في اختيار شريحة شبكة (PPSI)
التحكم في النفاذ	√	√		√	√		
الاستيقان	√						
عدم التنصل							
سرية البيانات			√				
أمن الاتصالات				√	√		
سلامة البيانات			√				
التيسر		√		√	√		
الخصوصية		√				√	√

8 تصنيف الأبعاد الأمنية المحقَقة بالقدرات الأمنية لشريحة

1.8 أسلوب ومبدأ تصنيف الأبعاد الأمنية القائم على القدرات الأمنية لشريحة

فيما يلي أسلوب لتصنيف كل بُعد أمني:

1) يوصى بإدراج القدرات الأمنية والخيارات ذات الصلة التي تنتمي إلى البعد الأمني. وإذا كانت هناك إمكانية ضئيلة لقدرة أمنية واحدة تؤثر على بعض الأبعاد الأمنية، لا يمكن إدراج هذه القدرة الأمنية اختيارياً في البُعد الأمني بل تُدرج حصراً في أبعاد أمنية أخرى تتأثر بشكل أساسي.

2) يوصى بإدراج توليفة من الخيارات المختلفة للقدرات وتشكيل المستويات المختلفة للبعد الأمني. وفي حال تحقيق بُعد أمني بقدرات أمنية متعددة، ينبغي أن يبقى كل مستوى من مستويات مؤثر الحماية متسقاً مع تعدد الميادين أو أصحاب المصلحة عند الجمع بين خيارات القدرات الأمنية. وتشير الصيغة xx.nn (من قبيل AC.1، ...، DI.0) إلى اسم مستوى البعد الأمني xx.

وتقدم الفقرة 2.8 القائمة العامة للأبعاد الأمنية الثمانية بمستويات تستند إلى القدرات الأمنية والخيارات الواردة في الفقرة 7.

2.8 الأبعاد الأمنية ذات المستويات القائمة على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية–2020

1.2.8 التحكم في النفاذ استناداً إلى القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية–2020

يمكن تحقيق التحكم في النفاذ بقدرات ذات خيارات تشمل، على سبيل المثال لا الحصر، الاستيقان والتخويل الخاصين بشريحة في الشبكة وعزل موارد الشبكة عن شريحة وحماية الحدود وحماية خدمة التطبيق. وهناك مجموعة متنوعة من توليفات القدرات ذات الخيارات المختلفة لتحقيق مستويات مختلفة من التحكم في النفاذ. ويرد عرضها على النحو التالي استناداً إلى الفقرة 7.

الجدول 8-1 – مستويات التحكم في النفاذ

البعد الأمني: التحكم في النفاذ (AC)													
القدرة	الاستيقان والتخويل الخاصان بشريحة في الشبكة (NSSAA)		حماية خدمة التطبيق (ASP)		عزل موارد الشبكة عن شريحة (SIR)							حماية الحدود (BP)		اسم المستوى
الخيارات	NSSAA.1	NSSAA.0	ASP.1	ASP.0	SIR.6	SIR.5	SIR.4	SIR.3	SIR.2	SIR.1	SIR.0	BP 1	BP.0	
التوليفة	NSSAA.0		ASP.0		SIR.0							BP.0		AC.0000
					SIR.0							BP.1		AC.0001
					SIR.1 SIR.4							BP.0		AC.0010 AC.0040
					SIR.1 SIR.4							BP.1		AC.0011 AC.0041
					SIR.2 SIR.5							BP.0		AC.0020 AC.0050
					SIR.2 SIR.5							BP.1		AC.0021 AC.0051
					SIR.3 SIR.6							BP.1		AC.0031 AC.0061
			ASP.1		SIR.0							BP.0		AC.0100
					SIR.0							BP.1		AC.0101
					SIR.1 SIR.4							BP.0		AC.0110 AC.0140
					SIR.1 SIR.4							BP.1		AC.0111 AC.0141
					SIR.2 SIR.5							BP.0		AC.0120 AC.0150
					SIR.2 SIR.5							BP.1		AC.0121 AC.0151
					SIR.3 SIR.6							BP.1		AC.0131 AC.0161
	NSSAA.1		ASP.0		SIR.0							BP.0		AC.1000
					SIR.0							BP.1		AC.1001
					SIR.1 SIR.4							BP.0		AC.1010 AC.1040
					SIR.1 SIR.4							BP.1		AC.1011 AC.1041
					SIR.2 SIR.5							BP.0		AC.1020 AC.1050
					SIR.2 SIR.5							BP.1		AC.1021 AC.1051
					SIR.3 SIR.6							BP.1		AC.1031 AC.1061
			ASP.1		SIR.0							BP.0		AC.1100

الجدول 8-1 – مستويات التحكم في النفاذ

البعد الأمني: التحكم في النفاذ (AC)													
القدرة	الاستيقان والتخويل الخاصان بشريحة في الشبكة (NSSAA)		حماية خدمة التطبيق (ASP)		عزل موارد الشبكة عن شريحة (SIR)							حماية الحدود (BP)		اسم المستوى
الخيارات	NSSAA.0	NSSAA.1	ASP.0	ASP.1	SIR.0	SIR.1	SIR.2	SIR.3	SIR.4	SIR.5	SIR.6	BP.0	BP 1	
					SIR.0							BP.1		AC.1101
						SIR.1 SIR.4						BP.0		AC.1110 AC.1140
						SIR.1 SIR.4						BP.1		AC.1111 AC.1141
							SIR.2 SIR.5					BP.0		AC.1120 AC.1150
							SIR.2 SIR.5					BP.1		AC.1121 AC.1151
								SIR.3 SIR.6				BP.1		AC.1131 AC.1161

2.2.8 الاستيقان القائم على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية–2020

يمكن تحقيق الاستيقان من خلال القدرات بما في ذلك الاستيقان والتخويل الخاصين بشريحة في الشبكة. وهناك مستويان من الاستيقان. ويرد عرضهما على النحو التالي:

الجدول 8-2 – مستويا الاستيقان

البعد الأمني: الاستيقان (Au)			
القدرة	الاستيقان والتخويل الخاصان بشريحة في الشبكة (NSSAA)		اسم المستوى
الخيارات	NSSAA.0	NSSAA.1	
التوليفة	NSSAA.0		Au.0
	NSSAA.1		Au.1

3.2.8 عدم التنصل القائم على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية–2020

لا توجد قدرة في الفقرة 7 تحقق عدم التنصل.

4.2.8 سرية البيانات القائمة على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية-2020

يمكن تحقيق سرية البيانات بقدرات من بينها حماية بيانات مستوي المستعمل. وهناك مستوَيان من الاستيقان. ويرد عرضهما على النحو التالي:

الجدول 8-3 – مستويا سرية البيانات

البعد الأمني: سرية البيانات (DC)			
القدرة	حماية بيانات مستوي المستعمل (UPDP)		اسم المستوى
الخيارات	UPDP.0	UPDP.1	
التوليفة	UPDP.0		DC.0
	UPDP.1		DC.1

5.2.8 أمن الاتصالات القائم على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية-2020

يمكن تحقيق أمن الاتصالات بقدرات من بينها حماية الحدود وحماية خدمة التطبيق. هناك مجموعات متنوعة من القدرات ذات الخيارات المختلفة تحقق مستويات مختلفة من أمن الاتصالات. ويرد عرضها على النحو التالي:

الجدول 8-4 – مستويات أمن الاتصالات

البعد الأمني: أمن الاتصالات (CS)					
القدرة	حماية الحدود (BP)		حماية خدمة التطبيق (ASP)		اسم المستوى
الخيارات	BP.0	BP.1	ASP.0	ASP.1	
التوليفة	BP.0		ASP.0		CS.00
	BP.0		ASP.1		CS.01
	BP.1		ASP.0		CS.10
	BP.1		ASP.1		CS.11

6.2.8 سلامة البيانات القائمة على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية-2020

يمكن تحقيق سلامة البيانات بقدرات من بينها قدرة حماية بيانات مستوي المستعمل. وهناك مستويان من سلامة البيانات. ويرد عرضهما على النحو التالي:

الجدول 8-5 – مستويا سلامة البيانات

البعد الأمني: سلامة البيانات (DI)			
القدرة	حماية بيانات مستوي المستعمل (UPDP)		اسم المستوى
الخيارات	UPDP.0	UPDP.1	
التوليفة	UPDP.0		DI.0
	UPDP.1		DI.1

7.2.8 التيسر القائم على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية-2020

يمكن تحقيق التيسر بقدرات من بينها عزل موارد الشبكة عن شريحة وحماية الحدود وحماية خدمة التطبيق. وهناك توليفات متنوعة من القدرات ذات خيارات مختلفة تحقق مستويات مختلفة من التيسر. ويرد عرضها على النحو التالي:

الجدول 8-6 – مستويات التيسر

البعد الأمني: التيسر (Av)						
القدرة	حماية خدمة التطبيق (ASP)		عزل موارد الشبكة عن شريحة (SIR)		حماية الحدود (BP)		اسم المستوى
الخيارات التوليفة	ASP.0	ASP.1	SIR.1/SIR.2/SIR.3	SIR.4/SIR.5/SIR.6	BP.0	BP.1	
	ASP.0		SIR.1/SIR.2/SIR.3		BP.0		Av.000
					BP.1		Av.001
				SIR.4/SIR.5/SIR.6	BP.0		Av.010
					BP.1		Av.011
	ASP.1		SIR.1/SIR.2/SIR.3		BP.0		Av.100
					BP.1		Av.101
				SIR.4/SIR.5/SIR.6	BP.0		Av.110
					BP.1		Av.111

8.2.8 الخصوصية القائمة على القدرات الأمنية لشريحة الاتصالات المتنقلة الدولية-2020

يمكن صون الخصوصية بقدرات تشمل حماية خصوصية هوية بروتوكول الاستيقان القابل للتوسيع (EAP) خلال الاستيقان والتخويل الخاصين بشريحة في الشبكة، وحماية خصوصية معلومات المساعدة في اختيار شريحة شبكة. وهناك توليفات متنوعة من القدرات ذات الخيارات المختلفة تحفظ مستويات مختلفة من الخصوصية. ويرد عرضها على النحو التالي:

الجدول 8-7 – مستويات الخصوصية

البعد الأمني: الخصوصية (Pr)				
القدرة	حماية خصوصية هوية بروتوكول الاستيقان القابل للتوسيع (EAP) خلال الاستيقان والتخويل الخاصين بشريحة في الشبكة (PPEAP)		حماية خصوصية معلومات المساعدة في اختيار شريحة شبكة (PPSI)		اسم المستوى
الخيارات	PPEAP.0	PPEAP.1	PPSI.0	PPSI.1	
التوليفة	PPEAP.0		PPSI.0		Pr.00
	PPEAP.0		PPSI.1		Pr.01
	PPEAP.1		PPSI.0		Pr.10
	PPEAP.1		PPSI.1		Pr.11

9 مبادئ توجيهية ومتطلبات لأنماط أمن الشرائح

يمكن لمجموعة الأبعاد الأمنية أن تميز نمط أمن أي شريحة في شبكة ويمكن التمييز بين الأنماط بواسطة فئة الخدمة. وستكثر أنماط أمن الشرائح بالجمع بين الأبعاد الأمنية والمستويات المختلفة. ولكن التوليفات ليست جميعها معقولة.

أما أسلوب ومبدأ تشكيل أنماط أمن الشرائح فهما كالتالي:

1) يوصى بتحديد مستويات الأبعاد الأمنية ذات الأولوية الأعلى أولاً وفقاً لمتطلبات الخدمة وأداء المستويات.

2) يوصى بتحديد سائر مستويات الأبعاد الأمنية وفقاً لمتطلبات الخدمة وأداء المستويات.

3) يوصى بالتحقق من وجود تضارب بين كل بُعد أمني وآخر لأغراض التنسيق. وفي شريحة معينة، ينبغي أن تتسق خيارات القدرات الأمنية للأبعاد الأمنية المختلفة التي تحتوي على القدرات الأمنية نفسها.

4) عند تحديث خيار بعض القدرات أو مستوى بعض الأبعاد الأمنية لنمط أمن الشريحة، يوصى بتغيير القدرات والأبعاد الأمنية ذات الصلة لإدامة الاتساق.

10 مبادئ توجيهية ومتطلبات لأصحاب المصلحة مع تصنيف القدرات الأمنية لشريحة الشبكة

يوصى بأن يعد مشغلو الشريحة قائمة بالقدرات الأمنية لشريحتهم على أساس قائمة القدرات الأمنية العامة لشريحة في الفقرة 7 وقدراتهم الأمنية الخاصة.

يوصى بأن يقوم مشغلو الشرائح بإعداد قائمتهم الخاصة بالأبعاد الأمنية ذات المستويات على أساس القائمة العامة للأبعاد الأمنية ذات المستويات والقدرات الأمنية الخاصة بهم أو غير ذلك من الأبعاد وفقاً للأسلوب الوارد في الفقرة 8.

يوصى بأن يعد مشغلو الشرائح قائمتهم الخاصة بأنماط أمن الشرائح وفقاً للأسلوب الوارد في الفقرة.

يوصى مشغلو الشرائح بالبت في القدرات والخيارات الأمنية لحالة شريحة معينة (خلال التهيئة مثلاً [b-ETSI TS 128 531]) على أساس قائمة قدرات أمن شرائحهم أو قائمة الأبعاد الأمنية ذات المستويات أو قوائم أنماط أمن الشرائح لديهم من خلال إقامة التقابل بين مستويات الأبعاد الأمنية أو الأنماط الأمنية للشرائح.

يوصى بأن يختار عملاء الشرائح توليفات من القدرات الأمنية والخيارات من قائمة القدرات الأمنية لشريحة عامة أو قائمة القدرات الأمنية لشريحة المشغِّل إذا كان العملاء على علم واضح بمتطلباتهم الأمنية وما يقابلها من القدرات الأمنية.

يوصى بأن يختار عملاء الشرائح مستويات الأبعاد الأمنية ذات الصلة وفقاً لأداء المستويات استناداً إلى القائمة العامة للأبعاد الأمنية ذات المستويات أو إلى قائمة المشغِّل بالأبعاد الأمنية ذات المستويات، إذا كان العملاء على علم بتأثير بعض الأبعاد الأمنية التي يرغبون في تحقيقها.

يوصى بأن يختار عملاء الشرائح نمطاً واحداً من قائمة المشغلين الخاصة بأنماط أمن الشرائح، إذا كانت معرفة العملاء بالمحتوى الأمني التفصيلي سطحية.

التذييل I

الأداء في خيارات القدرات الأمنية لشريحة شبكة الاتصالات المتنقلة الدولية–2020

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

ملاحظة – يعتمد الأداء على تفاصيل تنفيذ محددة وقد يتغير مع تطور التكنولوجيا.

- أداء خيارات NSSAA:
  - NSSAA.0: بالمستوى الأساسي
  - NSSAA.1: مزيد من الاستقلالية (لصناعة تخصصية)
- أداء خيارات SIR:
  - SIR.0: انعدام العزل: بالمستوى الأساسي
  - SIR.1: عزل منطقي + التشارك في القناة الحاملة الراديوية (RB): الخيار SIR.1 أكثر مرونة وقد تقل تكاليفه عن تكاليف الخيارين SIR.2 وSIR.3.
  - SIR.2: عزل منطقي + مادي + التشارك في RB: الخيار SIR.2 أكثر مرونة وأقل تكلفة من الخيار SIR.3. ولهذا الخيار SIR.2 موثوقية أعلى من الخيار SIR.1.
  - SIR.3: عزل مادي + التشارك في RB: موثوقية الخيار SIR.3 أعلى وتكلفة موارده أعلى مقارنةً بالخيارين SIR.1 وSIR.2.
  - SIR.4: عزل منطقي + حجز RB: الخيار SIR.4 أكثر مرونة وقد تقل تكاليفه عن تكاليف الخيارين SIR.5 وSIR.6.
  - SIR.5: عزل منطقي + مادي + حجز RB: الخيار SIR.5 أكثر مرونة وقد تقل تكاليفه عن تكاليف الخيار SIR.6. وللخيار SIR.2 موثوقية أعلى من الخيار SIR.4.
  - SIR.6: عزل مادي + حجز RB: للخيار SIR.6 كمون أخفض وموثوقية وتكاليف أعلى من الخيارات الأخرى.

وقد يكون للخيارات العزل المنطقي تكاليف أقل بشأن موارد المخدِّم مقارنة بخيارات العزل المادي، في حين قد تحتاج خيارات العزل المنطقي إلى تكاليف أكثر فيما يتعلق بالتدابير الأمنية المضادة من أجل تحقيق أثر حماية مماثل.

وتتيح الخيارات المزودة بالعزل المادي مستوى أعلى من التحكم في النفاذ مقارنة بالخيارات المزودة بالعزل المنطقي.

ولخيارات التشارك في القناة الحاملة الراديوية (RB) تأثير أفضل وأكثر مرونة في التغطية واستعمال الموارد من الخيارات التي تحجز القناة الحاملة الراديوية.

- أداء خيارات حماية بيانات مستوي المستعمل (UPDP):
  - UPDP.0: لا توجد حماية للبيانات في السطح البيني الهوائي وكُمونها أقل منه في الخيار UPDP.1
  - UPDP.1: توجد حماية للبيانات في السطح البيني الهوائي وتختلف مؤثرات الحماية تبعاً لخوارزميات التجفير الاختيارية.
- أداء خيارات حماية الحدود (BP):
  - BP.0: بالمستوى الأساسي
  - BP.1: توجد حماية حدودية وتختلف مؤثرات الحماية تبعاً لما ينفَّذ من وظائف/ميزات التحكم الأمني الاختيارية.
- أداء خيارات حماية خدمة تطبيق (ASP):
  - ASP.0: بالمستوى الأساسي
  - ASP.1: توجد حماية لخدمة تطبيق وتختلف مؤثرات الحماية حسب حمايات خدمة التطبيق الاختيارية

- أداء خيارات PPEAP:
  - PPEAP.0: هوية معدات المستعمل مكشوفة
  - PPEAP.1: هوية معدات المستعمل مغفَلة
- أداء خيارات PPSI:
  - PPSI.0: معلومات (S-)NSSAI مكشوفة
  - PPSI.1: معلومات (S-)NSSAI مغفَلة

التذييل II

مثال أنماط الأمن الأساسية لشريحة الاتصالات المتنقلة الدولية–2020

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

يتشكل الجدول التالي من أنماط الأمن الأساسية للشرائح على أساس الأسلوب الوارد في الفقرة 9 ويمكن لأصحاب المصلحة استعماله مباشرة أو تعديله لتشكيل أنماط الأمن الأساسية للشرائح الخاصة بهم.

الجدول 1.II – أمثلة أنماط الأمن الأساسية للشرائح

أنماط أمن الشريحة	التحكم في النفاذ	الاستيقان	التيسر	أمن الاتصالات	سرية البيانات	سلامة البيانات	عدم التنصل	الخصوصية	الحُكم	الخدمات المناسبة
0	AC.0	Au.0	Av.0	CS.0	DC.0	DI.0	-	Pr.0	أمن أساسي	شبكة عمومية
1	AC.1161	Au.1	Av.111	CS.11	DC.1	DI.1	-	Pr.11	أمن عالي المستوى، أعلى التكاليف	أنماط الأمن العالي المستوى مثل الخطوط الخاصة للحكومة والخدمات المالية والأوراق المالية وشبكات الكهرباء
2	AC.0000	Autor.0	Av.0	CS.0	–	–	-	–	تكلفة منخفضة	نمط التكلفة المنخفضة والنفاذ إلى الإنترنت وفيديو OTT
3	AC.xx61	–	Av.x11	–	–	–	–	Pr.xx4 Pr.xx6	عزل عال وتكلفة عالية	نمط العزل العالي
4	–	–	Av.x1x	–	DC.0	DI.0	–	–	كمون منخفض	نمط كمون منخفض، كألعاب المنصات السحابية

ملاحظة – يشير الحرف x في الرقم التسلسلي لاسم المستوى إلى أي قيمة.

بيبليوغرافيا

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

[b-3GPP TS 23.502] 3GPP TS 23.502, *Procedures for the 5G System (5GS)*.
<https://www.3gpp.org/ftp/Specs/archive/23_series/23.502>

[b-3GPP TS 28.541] 3GPP TS 28.541, *Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3*.
<https://www.3gpp.org/ftp/Specs/archive/28_series/28.541>

[b-IETF RFC 3748] IETF RFC 3748, *Extensible Authentication Protocol (EAP).*
<https://tools.ietf.org/html/rfc3748>

[b-IETF RFC 5216] IETF RFC 5216, *The EAP-TLS Authentication Protocol*.
<https://www.rfc-editor.org/rfc/rfc5216.html>

[b-IETF RFC 5281] IETF RFC 5281, *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*.
<https://datatracker.ietf.org/doc/html/rfc5281>

[b-ETSI TS 128 530] Technical Specification ETSI TS 128 530 V17.1.0 (2022), *5G; Management and orchestration; Concepts, use cases and requirements* (3GPP TS 28.530 version 17.2.0 Release 17). <
https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf>

[b-ETSI TS 128 531] Technical Specification ETSI TS 128 531 V16.9.0 (2021), *5G; Management and orchestration; Provisioning;* (3GPP TS 28.531 version 16.6.0 Release 16).
<https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/16.06.00_60/ts_128531v160600p.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، 2023