الاتحـــــــاد الدولـــــــي للاتصـــــــالات

ITU-T Y.2701

(2007/04)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة Y: البنية التحتية العالمية للمعلومات
وملامح بروتوكول الإنترنت وشبكات الجيل التالي

شبكات الجيل التالي – الأمن

متطلبات الأمن لشبكة الجيل التالي (NGN)، الطبعة 1

التوصيـــة ITU-T Y.2701

الاتحاد الدولي للاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.100 –Y.199
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.200 –Y.299
الجوانب الخاصة بالشبكات	Y.300 –Y.399
السطوح البينية والبروتوكولات	Y.400 –Y.499
الترقيم والعنونة والتسمية	Y.500 –Y.599
الإدارة والتشغيل والصيانة	Y.600 –Y.699
الأمن	Y.700 –Y.799
مستويات الأداء	Y.800 –Y.899
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1000 –Y.1099
الخدمات والتطبيقات	Y.1100 –Y.1199
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1200 –Y.1299
النقل	Y.1300 –Y.1399
التشغيل البيني	Y.1400 –Y.1499
نوعية الخدمة وأداء الشبكة	Y.1500 –Y.1599
التشوير	Y.1600 –Y.1699
الإدارة والتشغيل والصيانة	Y.1700 –Y.1799
الترسيم	Y.1800 –Y.1899
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2000 –Y.2099
نوعية الخدمة والأداء	Y.2100 –Y.2199
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2200 –Y.2249
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2250 –Y.2299
الترقيم والتسمية والعنونة	Y.2300 –Y.2399
إدارة الشبكة	Y.2400 –Y.2499
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2500 –Y.2599
الأمن	**Y.2700 –Y.2799**
التنقلية المعممة	Y.2800 –Y.2899

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

التوصيـــة ITU-T Y.2701

متطلبات الأمن لشبكة الجيل التالي (NGN)، الطبعة 1

ملخص

تعرض التوصية ITU-T Y.2701 متطلبات الأمن لشبكات الجيل التالي (NGNs) وسطوحها البينية (على سبيل المثال، السطوح البينية من المستعمل إلى الشبكة (UNIs)، السطوح البينية من الشبكة إلى الشبكة (NNIs)، السطوح البينية من التطبيق إلى الشبكة (ANIs)) من خلال تطبيق التوصية ITU-T X.805، *معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف* على التوصية ITU-T Y.2201، *متطلبات شبكات الجيل التالي، الطبعة 1* والتوصية Y.2012، *المتطلبات الوظيفية لشبكات الجيل التالي ومعماريتها، الطبعة 1.*

وتتمثل المتطلبات في توفير أمن قائم على الشبكة لاتصالات المستعملين النهائيين عبر مجالات إدارية متعددة للشبكة. ولا يندرج أمن أصول ومعلومات العميل المتضمنة في الميدان الخاص بالعميل (على سبيل المثال شبكة المستعمل)، وكذلك استعمال مقدرات التطبيق من ند إلى ند على تجهيزات العملاء، ضمن مجال تطبيق هذه التوصية.

وتستند هذه التوصية إلى نموذج موثوق يقوم على أساس عناصر الشبكة (صناديق مادية). وسينشر مقدمو شبكات الجيل التالي عناصر الشبكة التي تدعم الكيانات الوظيفية المعرّفة في التوصية ITU-T Y.2012. ويتغير تجمع هذه الكيانات الوظيفية في عنصر شبكة ما تبعاً للبائع. ولذلك لن تحاول هذه التوصية أن تعرض تجمعاً دقيقاً وثابتاً يضم الكيانات الوظيفية المنطقية وعناصر الشبكة المادية.

وينبغي أن تُعتبر المتطلبات الواردة في هذه التوصية بمثابة مجموعة دنيا من متطلبات الأمن، ويشجَّع موردو شبكات الجيل التالي على اتخاذ تدابير إضافية تتجاوز التدابير المحددة في التوصيات المتعلقة بأمن هذه الشبكات.

المصدر

وافقت لجنة الدراسات 13 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 27 أبريل 2007 على التوصية ITU-T Y.2701، بموجب إجراء القرار 1 للجمعية العالمية لتقييس الاتصالات.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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 رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2009

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

المحتـــويات

الصفحة

الصفحة

التوصيـــة ITU-T Y.2701

متطلبات الأمن لشبكة الجيل التالي (NGN)، الطبعة 1

1 مجال التطبيق

تعرض هذه التوصية متطلبات أمن شبكات الجيل التالي (NGNs) من أجل مواجهة التهديدات التي تحدق بأمنها. وتتحقق هذه المواجهة من خلال تطبيق المبادئ الواردة في التوصية [ITU-T X.805]، *معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف* على التوصية [ITU-T Y.2201]، *متطلبات شبكة الجيل التالي، الطبعة 1* والتوصية [ITU-T Y.2012]، *المتطلبات الوظيفية لشبكات الجيل التالي ومعماريتها، الطبعة 1.*

وترمي المتطلبات إلى حماية ما يلي في بيئة متعددة الشبكات:

- البنية التحتية لموردي الشبكات والخدمات وأصولهم (على سبيل المثال أصول وموارد شبكة الجيل التالي NGN مثل عناصر الشبكة والأنظمة والمكونات والسطوح البينية والمعطيات والمعلومات)، والموارد والاتصالات (أي التشوير والإدارة وحركة المعطيات/الحمالة) والخدمات؛
- خدمات ومقدرات الشبكة NGN (على سبيل المثال الخدمات الصوتية والفيديوية وخدمات البيانات)؛
- اتصالات ومعلومات المستعملين النهائيين (على سبيل المثال المعلومات الخاصة).

وتتمثل المتطلبات في توفير أمن قائم على الشبكة لاتصالات المستعملين النهائيين عبر ميادين إدارية متعددة للشبكة. ولا يندرج في نطاق هذه التوصية الأمن الخاص بأصول العملاء ومعلوماتهم في المجال المملوك لهم (على سبيل المثال شبكات المستعمل)، وكذلك استخدام مقدرات تطبيق الند إلى الند على تجهيزات العملاء.

وتنطبق المتطلبات المحددة في هذه التوصية على أي شبكة للجيل التالي، بما في ذلك السطوح البينية من المستعمل إلى الشبكة (UNIs)، والسطوح البينية من الشبكة إلى الشبكة (NNIs) والسطوح البينية من التطبيق إلى الشبكة (ANIs) في بيئة متعددة الشبكات.

وسيضطلع مقدمو خدمات الشبكة NGN بنشر "عناصر الشبكة" التي تدعم الكيانات الوظيفية المعرفة في التوصية [ITU-T Y.2012]. وسيختلف تجمع هذه الكيانات الوظيفية في عناصر شبكة ما تبعاً للبائع. ولذلك لن تحاول هذه التوصية أن تعرض تجمعاً دقيقاً وثابتاً يضم الكيانات الوظيفية المنطقية وعناصر الشبكة المادية.

وينبغي أن تعامَل المتطلبات الواردة في هذه التوصية باعتبارها مجموعة دنيا من المتطلبات اللازمة لأمن شبكات NGN، وينبغي ألا تُعتبر متطلبات شاملة. ولذلك قد يتعين على أي مورد للشبكة NGN اتخاذ تدابير إضافية تتجاوز التدابير المحددة في التوصيات المتعلقة بأمن شبكات NGN.

وبالإضافة إلى ذلك، فإن المتطلبات الواردة في هذه التوصية تغطي بعض الجوانب التقنية لما يعرف بوجه عام باسم (IdM) ("إدارة الهوية"). والتعريف العملي لإدارة الهوية (IdM) هو "إدارة موردي الشبكة NGN لنعوت موثوقة لكيان مثل: مشترك، أو جهاز أو مورد". ولا يُقصد من ذلك بيان الصلاحية الإيجابية المتعلقة بشخص ما.

وقد تطلب الإدارات من الشبكات NGN أن تأخذ في الحسبان المتطلبات التنظيمية الوطنية ومتطلبات السياسة الوطنية لدى تنفيذ هذه التوصية.

1.1 مبادئ التوصية X.805

تحدد التوصية [ITU-T X.805] أبعاد الأمن التالية:

التحكم في النفاذ؛

الاستيقان؛

عدم الإنكار؛

سرية البيانات؛

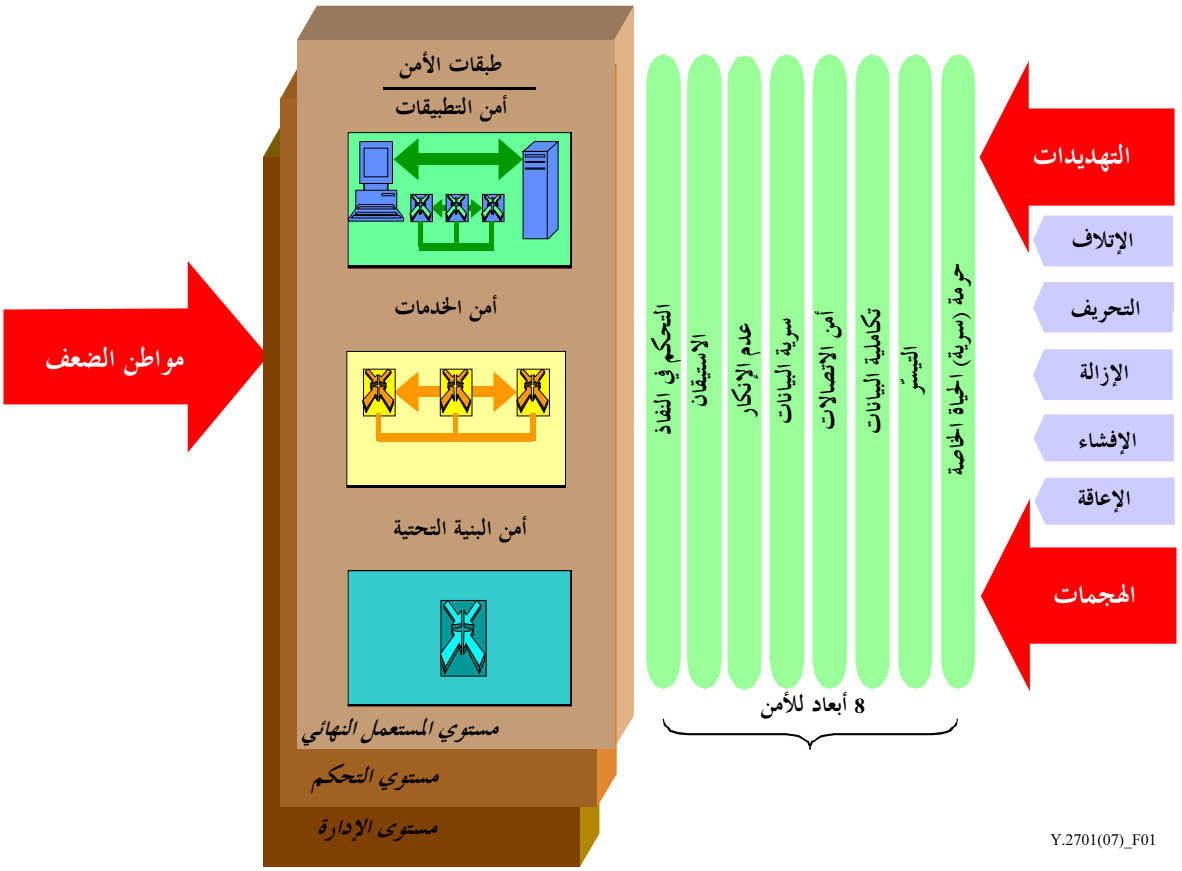
أمن الاتصالات؛

تكاملية المعطيات؛

التيسر؛

احترام حرمة (سرية) الحياة الخاصة.

وتحدِّد أيضاً التهديدات التالية المحدقة بالأمن.



الشكل 1 – معمارية أمن التوصية X.805 (الشكل X.8053/3)

وتُعتبر الأبعاد الخاصة بالأمن والتهديدات المحدقة بالأمن هذه المذكورة أعلاه بمثابة الأساس الذي تستند إليه هذه التوصية.

ولا تحدد هذه التوصية أو تميز استعمال طبقات أمن التوصية X.805 (التطبيقات أو الخدمات أو البنية الأساسية) ولا يحتاج الامتثال لهذا المعيار إلى هذا التمييز. ولا تتناول هذه التوصية التمييز بين الإدارة والتحكم وحركة مستوى المستعمل وإن كانت تنبه القارئ بأن استخدام هذا التصنيف يختلف تبعاً لطبقة كدس البروتوكولات قيد البحث. وبالتالي يلزم الرجوع إلى معايير أخرى لتحديد الامتثال لهذه الاختلافات. ويوفر هذا المعيار توصيات تتعلق بتطبيق أبعاد الأمن وإن كان لا يعني اكتماله بحيث يُستعمل كوسيلة تقييم لأمن الشبكات NGN.

2.1 افتراضات

تستند هذه التوصية إلى الافتراضات التالية:

1) أن تجمُّع كيانات وظيفية على النحو المحدد في التوصية [ITU-T Y.2012]، في عنصر شبكة ما إنما يتغير تبعاً للبائع.

2) لكل مورد لشبكات NGN مسؤوليات خاصة في مجاله المتعلق بالأمن. وعلى سبيل المثال، تنفيذ خدمات وممارسات الأمن الواجبة التطبيق من أجل:

أ) حماية نفسه؛

ب) ضمان ألا يتعرض الأمن من طرف إلى طرف للخطر داخل شبكته؛

ج) ضمان درجة عالية من تيسر اتصالات الشبكة NGN.

3) يضع وينفذ كل ميدان من ميادين الشبكة سياسات عامة فيما يتعلق بالاتفاقات على مستوى الخدمة (SLAs) لضمان أمن الميدان المعني وأمن التوصيلات البينية للشبكة. ويُفترض أن تحدد الاتفاقات SLAs خدمات الأمن وآلياته وممارساته التي يتعين تنفيذها لحماية الشبكات والاتصالات الموصولة بينياً (حركة التشوير/التحكم، حركة الحمالة وحركة الإدارة) عبر السطوح البينية UNIs وANIs وNNIs.

4) وتتناول هذه التوصية الأمن القائم على الشبكة الذي هو عبارة عن معمارية متعددة الطبقات تتكون من أمن خارجي للميادين الموثوقة وأمن مادّي لتجهيزات المورد مع إمكانية استعمال التجفير.

3.1 استعراض عام

نُظِّمت هذه التوصية كما يلي:

- الفقرة 2 (المراجع) – تتضمن هذه الفقرة المراجع المعيارية.
- الفقرة 3 (التعاريف والمختصرات) – تتضمن هذه الفقرة التعاريف والمختصرات المستعملة في هذه التوصية.
- الفقرة 4 (التهديدات والمخاطر المحدقة بالأمن) – تدرس هذه الفقرة التهديدات والمخاطر المحدقة بالأمن المفترضة بالنسبة لبيئة الشبكات NGN. وتُستخدم هذه التهديدات والمخاطر المفترضة على الأمن كإرشادات لإعداد متطلبات الأمن وتعيين المقْدرات والإجراءات الأمنية التي يتعين توفيرها.
- الفقرة 5 (نموذج الأمن الموثوق) – تصف هذه الفقرة نموذجاً موثوقاً لأمن شبكات NGN. ويمكن استخدام النموذج الموثوق في إقامة علاقات موثوقة من أجل توصيلية السطوح البينية UNI وANI وNNI، وتصميم معمارية الأمن.
- الفقرة 6 (معمارية الأمن) – تصف هذه الفقرة العلاقة بين المعمارية الوظيفية لشبكة NGN المحددة في التوصية [ITU-T Y.2012] ومعماريات الأمن المركبة.
- الفقرة 7 (الأهداف والمتطلبات) – تصف هذه الفقرة أهداف الأمن التي يتعين أن تستخدمها شبكة NGN لتحديد متطلبات الأمن بالنسبة لهذه الشبكات.
- الفقرة 8 (متطلبات محددة للأمن) – تتضمن هذه الفقرة متطلبات الأمن المحددة على أساس الفقرة 7.
- التذييل الأول – أهداف ومتطلبات الأمن اللازمة لخدمات اتصالات الطوارئ (ETS).
- (ثبت المراجع).

هذه التوصية محددة لتوفير أساس يستند إليه أمن شبكات الجيل التالي. ويتعين في المستقبل توفير توصيات متممة لهذه التوصية وتتناول مجالات أمنية خاصة، على سبيل المثال، الاستيقان والتخويل وإدارة الشهادات وإدارة الهوية وضمن مجالات أخرى.

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 M.3016.0] التوصية ITU-T M.3016.0 (2005)، *الأمن لمستوى الإدارة: استعراض عام*.

[ITU-T M.3016.1] التوصية ITU-T M.3016.1 (2005)، *الأمن لمستوى الإدارة: متطلبات الأمن*.

[ITU-T X.800] التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف (CCITT)*.

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

[ITU-T Y.2012] التوصية ITU-T Y.2012 (2006)، *المتطلبات والمعمارية الوظيفية لشبكات NGN، الطبعة 1*.

[ITU-T Y.2201] التوصية ITU-T Y.2201 (2007)، *متطلبات شبكات NGN، الطبعة 1*.

3 التعاريف والمختصرات

1.3 مصطلحات معرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في أماكن أخرى:

1.1.3 خدمة اتصالات الطوارئ (ETS): خدمة وطنية توفر اتصالات ذات أولوية مخوَّلة لتيسير عمل القائمين على الطوارئ في أوقات الكوارث. (انظر التوصية ITU-T E.107).

2.1.3 المستعمِل: يشمل المستعمِل المستعمِل النهائي (التوصية ITU-T Y.2091) أو شخص أو مشترك أو نظام أو جهاز أو جهاز طرفي (مثل فاكس أو حاسوب شخصي) أو كيان أو عملية أو تطبيق أو مورِّد أو شبكة مشتركة.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية.

1.2.3 الأصول: أي شيء ذو قيمة للمنظمة وأعمالها وعملياتها ومواصلة عملها.

2.2.3 العنصر الحدّي: عنصر الشبكة الذي يوفر وظائف تتيح توصيل مختلف ميادين الأمن والميادين الإدارية.

3.2.3 الشبكة المشتركة: شبكة خاصة تدعم عدة مستعملين وقد تشغل عدة مواقع (مثل مؤسسة أو مباني جامعة).

4.2.3 العنصر الحدي للميدان: العنصر الحدي الذي يتبع المورِّد فقط ويوفر وظائف الأمن مع ميادين الشبكة الأخرى.

5.2.3 العنصر الحدي للشبكة: عنصر حدي يتبع المورِّد فقط ويوفر وظائف الأمن مع الأجهزة المطرافية.

6.2.3 ميدان الأمن: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر وفقاً للسياسة العامة للأمن. وستدير سلطة الأمن السياسة العامة للأمن. ويمكن لميدان أمن ما أن يغطي عدة مناطق أمن.

7.2.3 منطقة أمن: تعرِّف هذه الوثيقة ثلاث مناطق للأمن:

1) موثوقة؛

2) موثوقة لكن معرَّضة؛

3) غير موثوقة.

وتعرَّف منطقة الأمن من خلال التحكم التشغيلي والموقع والتوصيلية بعناصر الأجهزة/الشبكات الأخرى.

8.2.3 العنصر الحدي للجهاز المطرافي: عنصر حدي يوفر وظائف الأمن بين تجهيزات مقر العميل وشبكة مورِّد الخدمة.

9.2.3 الثقة: يقال إن الكيان X يثق في الكيان Y بالنسبة لمجموعة من الأنشطة إذا وثق الكيان X في أن الكيان Y سيتصرف بطريقة معينة فيما يتعلق بالأنشطة.

10.2.3 المنطقة الموثوقة لكن معرَّضة: من منظور مورِّد شبكات NGN، منطقة أمن يقوم فيها مورد شبكة NGN بتشغيل (تزويد وصيانة) عناصر/أجهزة الشبكة. ويمكن أن تكون التجهيزات تحت سيطرة إما العميل/المشترك أو مورد الشبكة NGN. وبالإضافة إلى ذلك، يمكن أن تقع التجهيزات داخل أو خارج ميدان مورد شبكة NGN. وهي تتصل بعناصر في المنطقة الموثوقة وبعناصر في المنطقة غير الموثوقة على السواء، وهو الذي يفسر لماذا تتسم المنطقة "بالتعرض". وتتمثل وظيفتها الأمنية الرئيسية في حماية عناصر الشبكة في المنطقة الموثوقة بصفة دائمة من الهجمات على الأمن الصادرة عن المنطقة غير الموثوقة.

11.2.3 المنطقة الموثوقة: من منظور مورد شبكات NGN، ميدان أمن يتضمن عناصر الشبكة وأنظمة مورد شبكة NGN لا يتصل أبداً مباشرة بتجهيزات العميل. وتنطوي عناصر شبكة NGN الكائنة في هذا الميدان على خصائص مشتركة تتمثل في أن مورد الشبكة NGN هو الذي يسيطر عليها وأنها تقع في مقر مورد الشبكة NGN (الذي يوفر الأمن المادي)، وهي تتصل فقط بالعناصر الكائنة في الميدان "الموثوق" ومع عناصر كائنة في الميدان "الموثوق لكن المتعرض".

12.2.3 المنطقة غير الموثوقة: من منظور مورد شبكات NGN، منطقة تشمل جميع عناصر شبكات العملاء أو ربما شبكات الأنداد أو مناطق أخرى لموردي شبكات NGN خارج الميدان الأصلي والموصولة بالعناصر الحدية لمورد شبكة NGN.

13.2.3 شبكة المستعمل: شبكة خاصة تتألف من تجهيزات مطرافية قد تنطوي على عدة مستعملين.

3.3 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

3G الجيل الثالث *(3rd Generation)*

AGW بوابة النفاذ *(Access Gateway)*

ANI السطح البيني من التطبيق إلى الشبكة *(Application-to-Network Interface)*

B2BUA وكيل المستعمل ظهراً لظهر *(Back-to-Back User Agent)*

BE العنصر الحدي *(Border Element)*

CSC-FE الكيان الوظيفي للتحكم في دورة الهواء *(Call Session Control Functional Entity)*

DBE العنصر الحدي للميدان *(Domain Border Element)*

DNS نظام أسماء الميادين *(Domain Name System)*

ETS خدمة اتصالات الطوارئ *(Emergency Telecommunications Service)*

FE الكيان الوظيفي *(Functional Entity)*

GW بوابة *(Gateway)*

I-CSC-FE استفهام الكيان الوظيفي للتحكم في دورة النداء *(Interrogating Call Session Control Functional Entity)*

IMS نظام فرعي لتعدد الوسائط في بروتوكول الإنترنت *(IP Multimedia Subsystem)*

IP بروتوكول الإنترنت *(Internet Protocol)*

ISDN الشبكة الرقمية متكاملة الخدمات *(Integrated Services Digital Network)*

LAN شبكة المنطقة المحلية *(Local Area Network)*

MPLS تبديل الوسوم متعددة البروتوكولات *(Multi Protocol Label Switching)*

MRP-FE الكيان الوظيفي لمعالجة موارد وسائط الإعلام *(Media Resource Processing Functional Entity)*

NAC-FE الكيان الوظيفي للتحكم في النفاذ إلى الشبكة *(Network Access Control Functional Entity)*

NAPT	ترجمة عنوان الشبكة ومَنْفَذُها *(Network Address and Port Translation)*
NAT	ترجمة عنوان الشبكة *(Network Address Translation)*
NBE	العنصر الحدي للشبكة *(Network Border Element)*
NE	عنصر الشبكة *(Network Element)*
NGN	شبكة الجيل التالي *(Next Generation Network)*
NNI	السطح البيني من شبكة إلى شبكة *(Network-to-Network Interface)*
OAMP	العمليات، الإدارة، الصيانة، التزويد *(Operations, Administration, Maintenance and Provisioning)*
P-CSC-FE	الكيان الوظيفي البديل للتحكم في دورة النداء *(Proxy Call Session Control Functional Entity)*
POTS	الخدمة الهاتفية العادية *(Plain Old Telephone Service)*
PSTN	الشبكة الهاتفية العمومية التبديلية *(Public Switched Telephone Network)*
QoS	نوعية الخدمة *(Quality of Service)*
RAC-FE	الكيان الوظيفي للتحكم في الموارد والقبول *(Resource and Admission Control Functional Entity)*
RAN	شبكة نفاذ راديوي *(Radio Access Network)*
RTSP	بروتوكول التدفق في الوقت الفعلي *(Real Time Streaming Protocol)*
SAA-FE	الكيان الوظيفي لاستيقان الخدمة وتخويلها *(Service Authentication and Authorization Functional Entity)*
S-CSC-FE	الكيان الوظيفي خادم التحكم في دورة النداء *(Serving Call Session Control Functional Entity)*
SIM	وحدة تعرف المشترك *(Subscriber Identity Module)*
SIP	بروتوكول فتح الدورة *(Session Initiation Protocol)*
SLA	الاتفاق على مستوى الخدمة *(Service Level Agreement)*
SL-FE	الكيان الوظيفي لموقع الاشتراك *(Subscription Locator Functional Entity)*
TAA-FE	الكيان الوظيفي لاستيقان النقل وتخويله *(Transport Authentication and Authorization Functional Entity)*
TE	تجهيزات مطرافية *(Terminal Equipment)*
TE-BE	العنصر الحدي للتجهيزات المطرافية *(Terminal Equipment Border Element)*
TMN	شبكة إدارة الاتصالات *(Telecommunication Management Network)*
UA	وكيل المستعمل *(User Agent)*
UICC	بطاقة دارة متكاملة عامة *(Universal Integrated Circuit Card)*
UNI	السطح البيني من المستعمل إلى الشبكة *(User-to-Network Interface)*
VLAN	شبكة منطقة محلية تقديرية *(Virtual LAN)*
W-CDMA	النفاذ المتعدد بتقسيم شفري عريض النطاق *(Wideband Code Division Multiple Access)*
WLAN	شبكة منطقة محلية لا سلكية *(Wireless LAN)*
xDSL	خط المشترك الرقمي x *(x Digital Subscriber Line)*

4 التهديدات والمخاطر المحدقة بالأمن

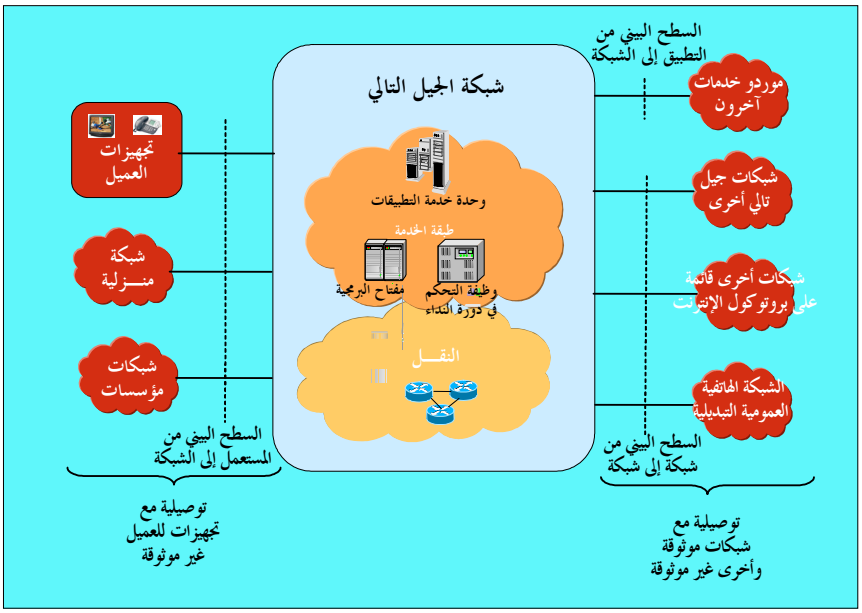
تفترض هذه التوصية أن تتعرض الأنظمة والمكونات والسطوح البينية والمعلومات والموارد والاتصالات (أي التشوير، والإدارة وحركة البيانات/الحمالة) والخدمات التي تشكل شبكات الجيل التالي لطائفة متنوعة من التهديدات والمخاطر المحدقة بالأمن. وتتوقف تلك التهديدات والمخاطر على طائفة متنوعة من العوامل. وبالإضافة إلى ذلك، سيتعرض المستعملون النهائيون أيضاً إلى بعض التهديدات (على سبيل المثال، النفاذ غير المخول إلى المعلومات الخاصة).

وتشمل التهديدات المحدقة بشبكات الجيل التالي:

- الاستكشاف غير المخول مثل تحليل النظام عن بعد لتحديد نقاط ضعفه (قد يتضمن ذلك عمليات مسح وكنس والاستعلام عن المنفذ وجداول التسيير وما إلى ذلك)؛
- عمليات انقطاع/سيطرة على الجهاز بما يؤدي إلى فقدان السيطرة على الجهاز وظهور حالات الشذوذ والأخطاء في مراجعات التشكيل؛
- إتلاف المعلومات و/أو الموارد الأخرى؛
- تحريف المعلومات أو تعديلها؛
- سرقة المعلومات و/أو الموارد الأخرى أو إزالتها أو فقدانها؛
- إفشاء المعلومات؛
- انقطاع الخدمات ورفضها.

ومن الواضح كذلك أن شبكات الجيل التالي ستعمل في بيئة مختلفة عن بيئة الشبكة الهاتفية العمومية التبديلية (PSTN) ويمكن أن تتعرض بالتالي إلى أنماط مختلفة من التهديدات والهجمات من الداخل أو الخارج. وستحقق شبكات الجيل التالي توصيلية مباشرة أو غير مباشرة بشبكات غير موثوقة وبشبكات موثوقة وبتجهيزات المطاريف، ومن ثم فإنها ستتعرض لمخاطر وتهديدات على الأمن مرتبطة بالتوصيلية إلى الشبكات غير المأمونة وتجهيزات مقر العميل. وعلى سبيل المثال، يمكن أن يكون لمورِّد شبكة من شبكات الجيل التالي توصيلية مباشرة أو غير مباشرة (أي من خلال شبكة أخرى) بما يلي على النحو المبين في الشكل 2:

- مقدمي خدمات آخرين وتطبيقاتهم؛
- شبكات جيل تالي أخرى؛
- شبكات أخرى تستند إلى بروتوكول الإنترنت؛
- الشبكة الهاتفية العمومية التبديلية (PSTN)؛
- الشبكات المشتركة؛
- شبكات المستعملين؛
- التجهيزات المطرافية؛
- ميادين النقل الأخرى للشبكات NGN.



الشكل 2 – توصيلية إلى الشبكات والمستعملين

وفي البيئة المتطورة، يعتمد الأمن عبر الميادين المتعددة لمورّد الشبكة على مجمل ما اختاره جميع الموردين من أجل تأمين شبكتهم. وفي النفاذ غير المخول إلى شبكة مورد واحد، يمكن أن يؤدي بسهولة إلى تشغيل شبكة موصولة بينياً والخدمات الملازمة لها. وهذا مثال على استغلال أضعف الحلقات التي يمكن أن تهدد تكاملية شبكة مورد واستمرار خدمتها بالإضافة إلى مجموعة من أنماط الهجمات المختلفة.

وكل مورد لشبكة الجيل التالي (NGN) مسؤول عن الأمن داخل ميدانه. وكل مورد لشبكة الجيل التالي مسؤول عن تصميم وتنفيذ حلول للأمن بتطبيق سياسة ملائمة للشبكة من أجل علاقات موثوقة (الفقرة 5)، وذلك استجابة للاحتياجات الخاصة بشبكته، ودعماً لأهداف الأمن الشاملة من طرف إلى طرف عبر ميادين متعددة لمورد الشبكات.

5 نموذج للثقة في الأمن

تحدد هذه الفقرة نموذج الثقة في أمن شبكة الجيل التالي.

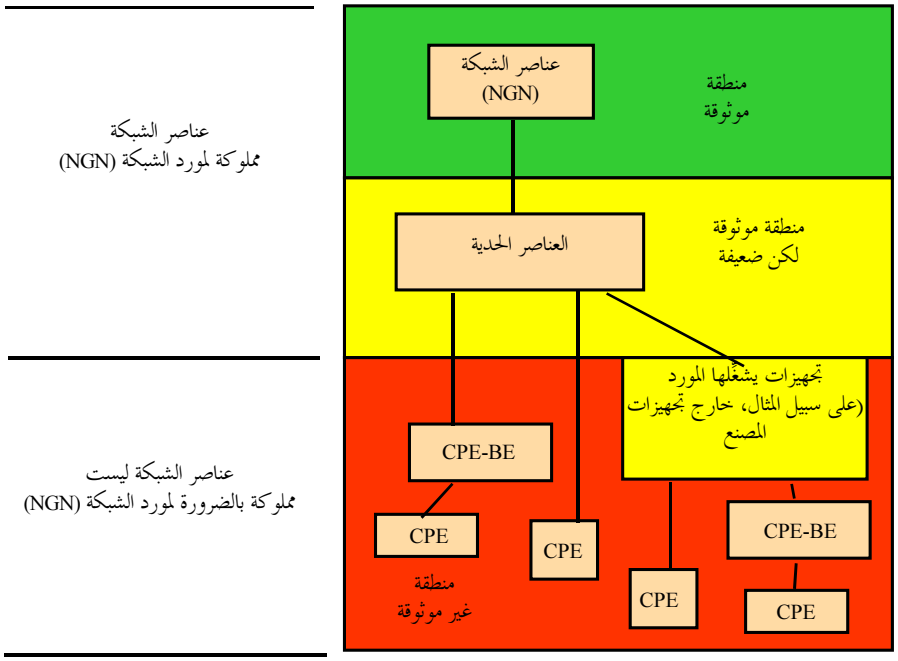
تحدد المعمارية الوظيفية لشبكة الجيل التالي كيانات وظيفية (FEs). إلا أنه نظراً لأن جوانب أمن الشبكات تتوقف بشدة على الطريقة التي تجمع بها الكيانات الوظيفية معاً، فإن معمارية أمن شبكات الجيل التالي تستند إلى عناصر الشبكة المادية (NEs) أي إلى صناديق ملموسة تحتوي على كيان وظيفي واحد أو أكثر. وتختلف الطريقة التي تجمّع بها هذه الكيانات الوظيفية في عنصر الشبكة تبعاً لاختلاف البائعين.

1.5 النموذج موثوق لشبكة منفردة

تحدد هذه الفقرة الفرعية ثلاث مناطق أمن:

1) موثوقة؛
2) موثوقة لكن معرضة؛
3) غير موثوقة،

تعتمد على تحكمات تشغيلها ومكانها وتوصيليتها بالأجهزة/عناصر الشبكة الأخرى. وتظهر هذه المناطق الثلاث في نموذج الثقة في الأمن المبين في الشكل 3.



الشكل 3 – نموذج للثقة في الأمن

وباختصار فإن منطقة الأمن الموثوق لشبكة" أو "المنطقة الموثوقة" هي منطقة تحتوي على عناصر أنظمة شبكة مورِّد شبكة الجيل التالي، ولا تتصل مباشرة على الإطلاق بتجهيزات العميل أو بالميادين الأخرى. وتتمثل الخصائص المشتركة لعناصر شبكة NGN في هذه المنطقة في أنها تحت السيطرة الكاملة لمورد الشبكة NGN، وتقع في ميدان مورد الشبكة NGN، وهي لا تتصل إلا بعناصر في المنطقة "الموثوقة" وبعناصر في المنطقة "الموثوقة لكن المعرضة" ولا ينبغي اعتبار أن العنصر آمن بمجرد وجوده في منطقة موثوقة.

وستُحمى المنطقة "الموثوقة" بمجموعة نهج مختلفة. وتتمثل بعض الأمثلة على ذلك في الأمن المادي لعناصر شبكة الجيل التالي، والتعزيز العام لحماية الأنظمة، واستعمال تشوير مؤمن، الأمن لجميع رسائل العمليات والإدارة والصيانة والتزويد (OAMP) والشبكات التقديرية الخاصة VPN المنفصلة داخل شبكة (تبديل الوسوم متعددة البروتوكولات (MPLS/) شبكة بروتوكول الإنترنت للاتصالات داخل المنطقة "الموثوقة" ومع عناصر شبكة الجيل التالي NGN في المنطقة "الموثوقة لكن المعرضة". انظر الفقرة 8 للاطلاع على مزيد من التفاصيل.

وباختصار فإن "منطقة الأمن الموثوق لكن المعرض لشبكة" أو "المنطقة الموثوقة لكن المعرضة" هي منطقة يقوم مورد شبكة الجيل التالي (NGN) بتشغيل عناصر/أجهزة الشبكة (وتزويدها وصيانتها). ويمكن أن تكون التجهيزات تحت تحكم إما العميل/المشترك أو مورد شبكة الجيل التالي. وبالإضافة إلى ذلك، يمكن أن تقع التجهيزات داخل أو خارج مقر مورد شبكة الجيل التالي. وتتصل التجهيزات بعناصر في المنطقة الموثوقة وبعناصر في المنطقة غير الموثوقة على السواء مما يفسر لماذا هي "معرَّضة". وتتمثل وظيفتها الرئيسية فيما يتعلق بالأمن في توفير الحماية لعناصر الشبكة في المنطقة الموثوقة من الهجمات على الأمن الناشئة في المنطقة غير الموثوقة.

والعناصر الكائنة في ميدان مورد الشبكة NGN والتي يمكن توصيلها بعناصر خارج المنطقة الموثوقة إنما يشار إليها على أنها عناصر حدِّية (NBEs). وفيما يلي أمثلة على هذه العناصر:

- العناصر الحدية للشبكة (NBE) على السطح البيني بين المستعمل والشبكة توفّر الوصل الإلكتروني مع عناصر التحكم في الخدمة أو عناصر نقل مورد الشبكة NGN في المنطقة الموثوقة لكي يتسنى للمستعمل/المشترك النفاذ إلى شبكة مورد الشبكة NGN فيما يتعلق بالخدمات و/أو النقل.

- العناصر الحدية للميادين (DBE) وهي نفس النوع من التجهيزات مثل العناصر الحدية للشبكة فيما عدا أنها تقع على حدود الميادين.
- العناصر NBE لتشكيل وإنهاض الأجهزة (DCB-NBE) التي توفر الوصل الإلكتروني مع نظام تشكيل أجهزة مورد الشبكة NGN في المنطقة الموثوقة من أجل تشكيل أجهزة المستعمل/المشترك وتجهيزات مورد الشبكة NGN الكائنة في المنشآت الخارجية.
- السطوح البينية للعنصر الحدي لأنظمة العمليات، الإدارة، الصيانة، التزويد OAMP الخاصة بمورد الشبكة NGN في المنطقة الموثوقة بغية تزويد وصيانة أجهزة المستعمل/المشترك وتجهيزات مورد الشبكة NGN الكائنة في المنشآت الخارجية.
- العنصر الحدي لوحدة خدمة التطبيق/وحدة خدمة الويب (AS/WS-BE) التي توفر الوصل الإلكتروني مع العنصر الحدي لوحدة خدمة التطبيق/وحدة خدمة الويب في المنطقة الموثوقة من أجل توفير سبل النفاذ للمستعمل/المشترك إلى الخدمات المستندة إلى الويب.

وفيما يلي أمثلة على الأجهزة/العناصر التي يشغلها مورد لشبكة NGN لكنها لا تقع في مقر مورد الشبكة NGN، كما أنها يمكن أو لا يمكن أن تكون تحت تحكم مورد الشبكة NGN.

- تجهيزات المنشآت الخارجية الكائنة في شبكة/تكنولوجيا النفاذ؛
- مفرع محطة القاعدة (BSR)، وهو عنصر شبكة يدمج وظائف المحطة القاعدة ومراقب الشبكة الراديوية، ووظائف المفرع؛
- الوحدات البصرية (ONUs) داخل مسكن المستعمل/المشترك.

وستُحمى المنطقة "الموثوقة لكن المعرضة" التي تتشكل من العناصر الحدية للشبكة بمجموعة من النُّهج المختلفة. على سبيل المثال الأمن المادي لعناصر الشبكة NGN والتعزيز العام للأنظمة واستعمال تشوير مأمون لجميع رسائل التشوير المرسلة إلى عناصر الشبكة NGN في المنطقة "الموثوقة" وأمن الرسائل OAMP ومراشيح وحوائط حماية الرزم حسب الاقتضاء. انظر الفقرة 8 للاطلاع على مزيد من التفاصيل.

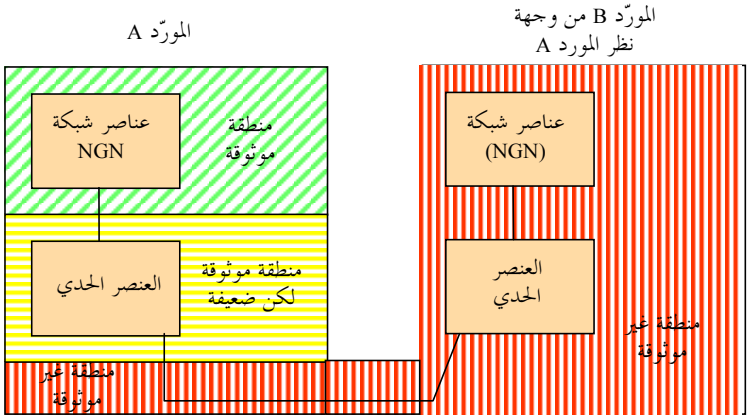
"المنطقة غير الموثوقة" تشمل جميع عناصر شبكات العملاء أو ربما شبكات الند أو الميادين الأخرى لموردي الشبكات NGN الواقعة خارج الميدان الأصلي الموصولة بالعناصر الحدية لشبكة مورد الشبكة NGN. وفي المنطقة "غير الموثوقة" التي تتألف من تجهيزات مطرافية قد لا يكون موردو الشبكات NGN هم المتحكمين في التجهيزات، وقد يكون من المستحيل فرض السياسة الأمنية للمورد على المستعمل. ولا يزال من المستصوب محاولة تطبيق بعض تدابير الأمن، وتحقيقاً لهذا الغرض يوصى بتأمين تشوير وسائط الاتصال وعمليات OAM&P مع تعزيز العناصر الحدية للتجهيزات المطرافية TE-BE. إلا أنه بسبب الافتقار إلى الأمن المادي لا يمكن اعتبار هذه التدابير آمنة بصورة مطلقة. ويرجى الرجوع إلى الفقرة 8 للاطلاع على مزيد من التفاصيل.

2.5 النموذج الموثوق للتوصيل البيني للشبكات الند

عندما يتم توصيل شبكة NGN بشبكة أخرى فإن الموثوقية تعتمد على ما يلي:

- التوصيل البيني المادي، حيث يمكن أن يمتد التوصيل البيني من توصيل مباشر في مبنى مؤمَّن إلى عناصر وظيفية موضع تَشاطُر؛
- نموذج التوصيل البيني، حيث يمكن تبادل الحركة مباشرة بين مورديّ خدمات شبكات NGN أو من خلال مورد أو أكثر لشبكة النقل NGN؛
- العلاقات التجارية، حيث يمكن أن تظهر شروط جزائية في الاتفاقات SLA (الاتفاقات على مستوى الخدمة)، و/أو الثقة في السياسة الأمنية للمورد الآخر للشبكة NGN؛
- بوجه عام، ينبغي أن ينظر موردو الشبكات NGN إلى الموردين الآخرين على أنهم غير موثوقين.

ويُظهر الشكل 4 مثالاً تعتبر فيه شبكة موصولة، شبكة غير موثوقة.



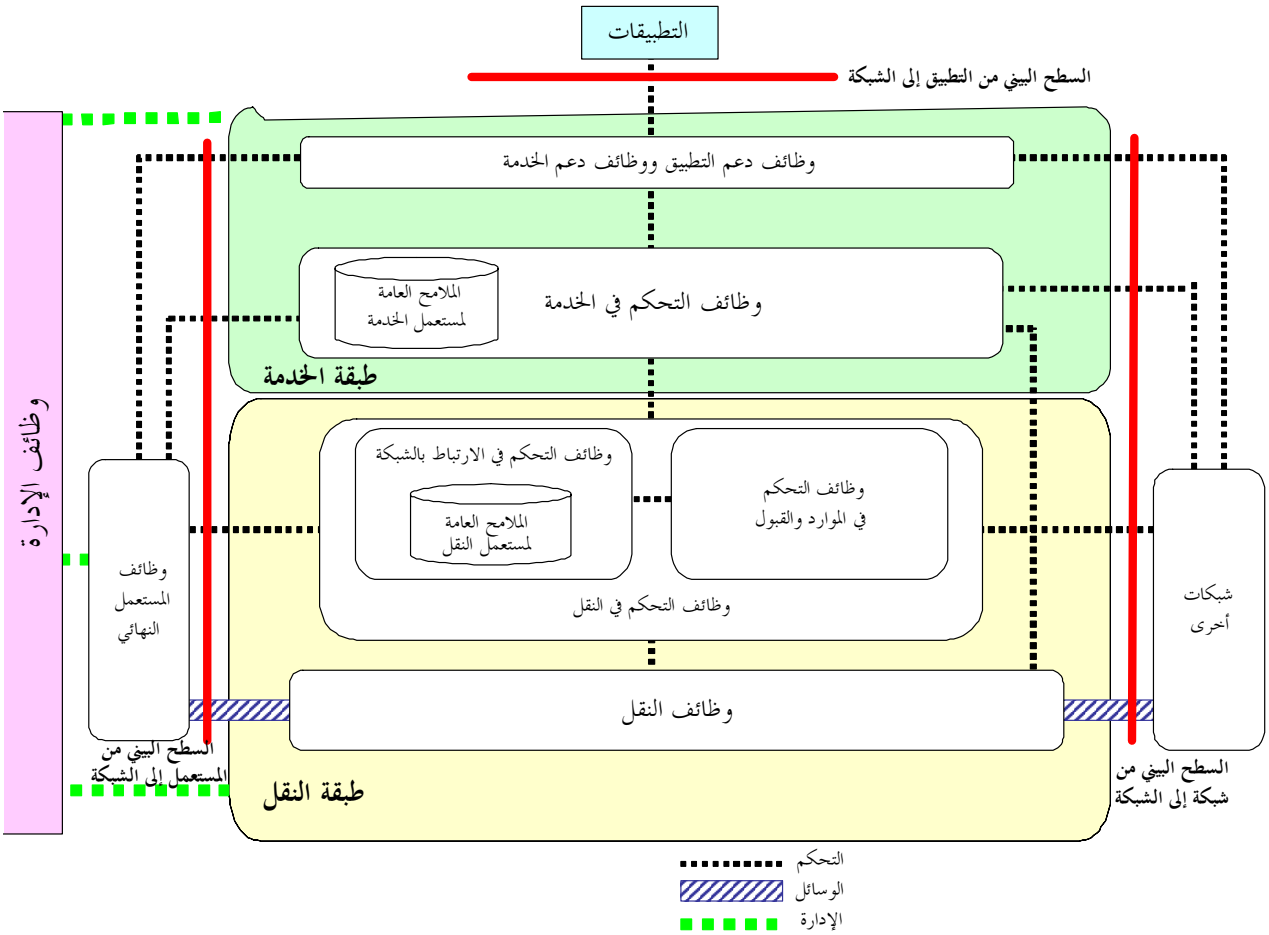
الشكل 4 – نموذج موثوق للتوصيل البيني

6 معمارية الأمن

1.6 المعمارية الوظيفية المرجعية لشبكات NGN

يرد تعريف لمعمارية الشبكة NGN التي تطابق التوصية [ITU-T Y.2201] *ومتطلبات الطبعة 1 من الشبكة NGN*، في التوصية [ITU-T Y.2012]، *المتطلبات الوظيفية ومعمارية الشبكة NGN، الطبعة 1*.

يبين الشكل 5 رؤية وظيفية لمعمارية الشبكات NGN.



الشكل 5 – لمحة معمارية شبكة (NGN) (الشكل Y.2012/1)

وتوفر الشبكة NGN نقطة مرجعية لوظائف المستعمل النهائي8 تسمى السطح البيني من المستعمل إلى الشبكة (UNI) وإلى الشبكات الأخرى تسمى السطح البيني من شبكة إلى شبكة (NNI). وتوفر أيضاً نقطة مرجعية للمجموعة الوظيفية للتطبيقات تسمى السطح البيني من التطبيق إلى الشبكة (ANI)، تمكِّن من استخدام مقدرات الشبكات NGN في إنشاء وتوفير تطبيقات لمستعملي الشبكات NGN.

وتوفر طبقة النقل للطبعة 1 للشبكة NGN خدمات توصيلية بروتوكول الإنترنت إلى مستعملي شبكة NGN تحت رقابة وظائف التحكم في النقل، بما في ذلك وظائف التحكم في الارتباط بالشبكة (NACF)، ووظائف التحكم في الموارد والقبول (RACF).

وتقدم طبقة الخدمة، خدمات وتطبيقات إلى المستعمل النهائي من خلال استعمال وظائف دعم التطبيقات ووظائف دعم الخدمات وما يتصل بها من وظائف تحكم.

أما وظائف المستعمل النهائي فهي وظائف موصولة بشبكات النفاذ إلى شبكة NGN ولم تقدَّم افتراضات بشأن مختلف السطوح البينية للمستعملين النهائيين وشبكات المستعملين النهائيين.

وتوفر وظائف الإدارة المقدِرة على إدارة شبكة الجيل التالي من أجل توفير خدمات هذه الشبكات مع تحقيق النوعية والأمن والموثوقية المتوقعة.

للاطلاع على مزيد من التفاصيل انظر التوصية [ITU-T Y.2012].

2.6 التقابل مع المعمارية الوظيفية لشبكات NGN

تصف هذه التوصية طريقة تحقيق الأمن من خلال استخدام النموذج الموثوق المبين في الفقرة 5، ومؤداه أن أي شبكة NGN تتألف من ميدان موثوق (منطقة خضراء)، وميدان غير موثوق (منطقة حمراء)، وميدان موثوق لكنه معرَّض (منطقة صفراء) يقع بين الميدانين الأولين.

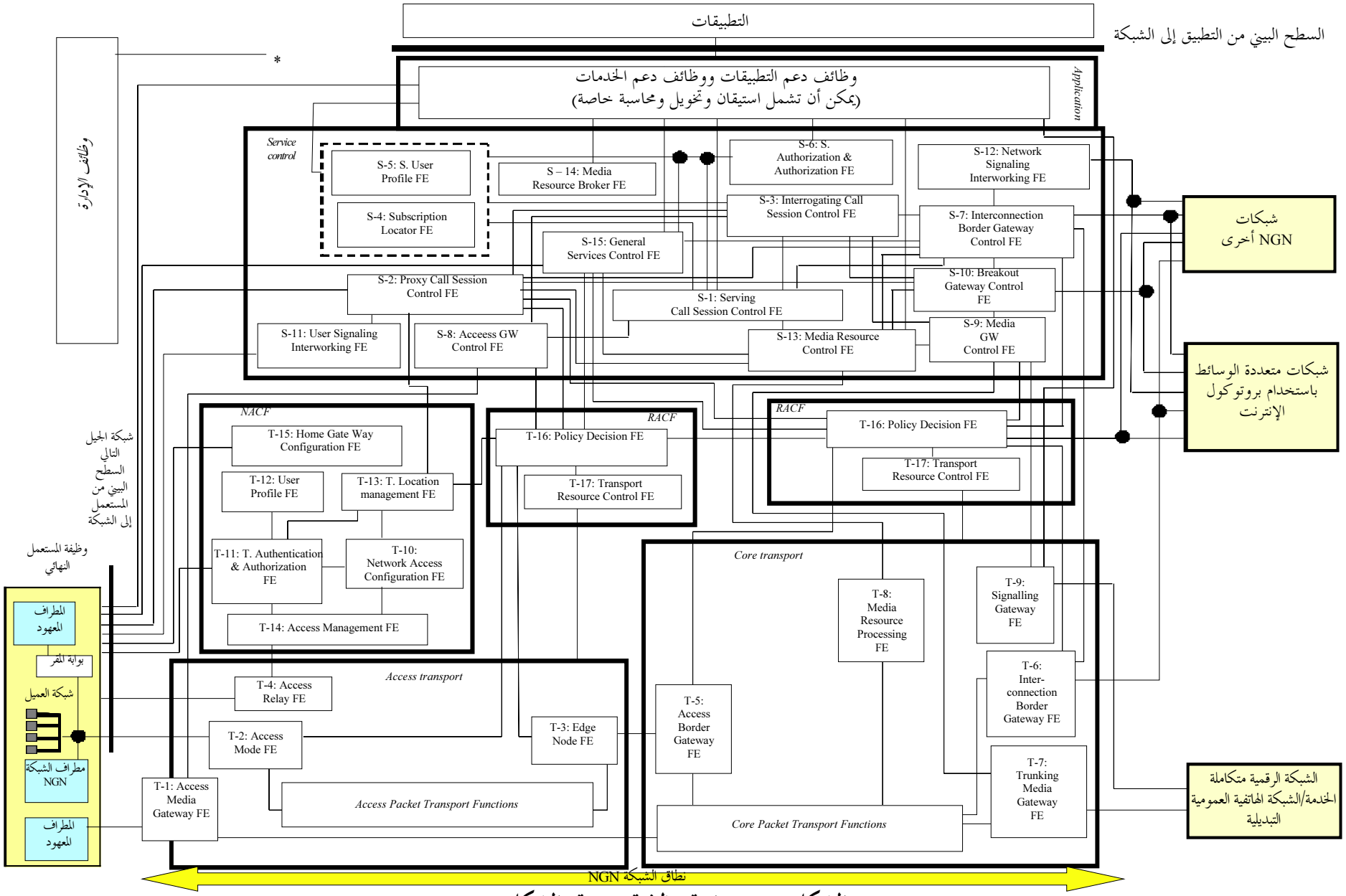
وتتمثل إحدى المسائل الرئيسية لتحقيق الأمن مع هذا النموذج في طريقة إرسال التشوير ووسائط الاتصال وحركة OAMP من الميدان غير الموثوق إلى الميدان الموثوق. وهناك طرق شتى لتحقيق ذلك، ومورد الشبكة NGN هو الذي يقرر الطريقة التي ينتهجها تبعاً لسياسته. وفيما يلي أمثلة على هذه النُّهج.

أ) تركيب عناصر الشبكة لإنهاء الحركة (على سبيل المثال، وكيل المستعمل ظَهراً لظهر (B2BUA) بالنسبة لتشوير بروتوكول فتح الدورة SIP) بين المنطقة الخضراء والمنطقة الحمراء. ويستقبل عنصر الشبكة هذا رزماً من المنطقة الحمراء ويفحصها وينبذها إذا لم تكن ملائمة، وإذا كانت ملائمة ينسخ الجزء اللازم لإعادة بناء حزمة ملائمة للمنطقة الخضراء. وفي هذه الحالة تصبح عناصر الشبكة التي تنهي الحركة عناصر الشبكة للمنطقة الصفراء.

ب) عمليات التحكم في الحركة في طبقة الوسائط (على سبيل المثال من خلال فتح وإغلاق منفذ معين (ثقب صغير) في حائط الحماية، وضمان أن تتمكن عناصر الشبكة (والمستعملون) المخولون فقط من إرسال الحركة إلى التجهيزات الكائنة في المنطقة الخضراء. وفي هذه الحالة، تصبح عناصر الشبكة التي تتحكم في الحركة عناصر شبكة المنطقة الصفراء.

ج) تجفير من طرف إلى طرف بين المرسل والمستقبل.

وفي المعمارية الوظيفية المبينة في المرجع [ITU-T Y.2012] (الشكل 6 في هذه التوصية)، فإن تشوير بروتوكول فتح الدورة SIP الذي تولّده وظيفة المستعمل النهائي (وهي عادة غير موثوقة لأن مورد الشبكة NGN لا يستطيع أن يؤكد أن الوظيفة ليست مزورة) يُرسَل إلى الكيان S-2، P-CSC-FE. ولذلك تُعتبر عناصر الشبكة التي تحتوي على وظائف P-CSC-FE بمثابة عناصر شبكة للمنطقة الصفراء، أو بمثابة عناصر شبكة للمنطقة الخضراء نتيجة لوظائف حائط الحماية. وإذا كانت عناصر الشبكة التي تحتوي على كيان S-1، (S-CSC-FE) منفصلة عن عناصر الشبكة التي تحتوي على كيان P-CSC-FE، فإنها تُعتبر بمثابة عناصر شبكة للمنطقة الخضراء.



الشكل 6 – معمارية وظيفية معممة (الشكل Y.2012/3)

3.6 تحديد موارد الشبكات NGN من أجل الحماية الأمنية

يتعين على كل مورّد شبكة أن يعين الأصول والموارد والمعلومات والسطوح البينية التي يتعين حمايتها داخل شبكته، وكذلك التهديدات التي يتعين التخفيف من مخاطرها. وعلى سبيل المثال عناصر الشبكة والسطوح البينية (UNI وANI وNNI)، وأنظمة الإدارة والتشوير واتصالات الإدارة والوسائط/اتصالات الحمّالة. ولتعيين موارد شبكة NGN لأغراض حماية أمنها من التهديدات، على أن تؤخذ في الاعتبار المعمارية المقسمة نظرياً إلى الطبقات المحددة في المرجع [ITU-T Y.2012] وكذلك التحقيق العملي للكيانات الوظيفية.

وتوفر الجداول التالية أمثلة على أصول وموارد وسطوح بينية الشبكات NGN لأغراض حماية أمنها من التهديدات وهذه الأمثلة منظمة كما يلي:

- الجدول 1 – مثال للأصول والموارد والمعلومات المتصلة بالسطح البيني من المستعمل إلى الشبكة UNI.
- الجدول 2 – مثال للأصول والموارد والمعلومات والسطوح البينية المرتبطة بطبقة النقل.
- الجدول 3 – مثال للأصول والموارد والمعلومات والسطوح البينية المرتبطة بطبقة الخدمة.
- الجدول 4 – مثال للأصول والموارد والمعلومات والسطوح البينية المرتبطة بالإدارة.

والأمثلة الواردة في الجداول 1 إلى 4 ليست شاملة.

الجدول 1 – مثال للأصول والموارد والمعلومات المتصلة بالسطح البيني من المستعمل إلى الشبكة

الأمثلة	الأهداف والمقاصد
موارد المستعمل النهائي: • أجهزة المستعمل • بوابات شبكة المستعمل • بوابات الشبكة المشتركة	أ) حماية تجهيزات المستعمل النهائي الموصولة بالشبكة (على سبيل المثال المطاريف وشبكة المستعمل وبوابات الشبكة المشتركة) من الهجمات الصادرة عن الشبكة (على سبيل المثال، الهجمات الرامية إلى إتلاف تجهيزات المستعمل أو تحريفها أو تعديلها). ب) توفير الحماية من انقطاع الخدمات (على سبيل المثال، الهجمات برفض الخدمة) وتأكيد تيسُّر الخدمة. ج) حماية الشبكة من النفاذ غير المخول (على سبيل المثال، المستعملون غير المخولون وأجهزة المستعملين).
معلومات المستعمل النهائي: • معلومات المشترك • معلومات الهوية • معلومات الموقع	أ) الحماية من تحريف المعلومات أو تعديلها. ب) الحماية من السرقة أو الإزالة أو الفقدان (على سبيل المثال سرقة الهوية). ج) الحماية من الإفشاء (على سبيل المثال النفاذ غير المخول إلى معلومات الموقع).
معلومات مورد الشبكة NGN • معلومات الهوية	أ) الحماية من تحريف المعلومات أو تعديلها. ب) الحماية من السرقة أو الإزالة أو الفقدان (على سبيل المثال سرقة الهوية). ج) الحماية من الإفشاء (على سبيل المثال النفاذ غير المخول إلى معلومات الموقع).
السطوح البينية من المستعمل إلى الشبكة UNI	أ) طبقة النقل – توفير حماية أمنية لحركة الوسائط/الحمالة من خلال السطوح البينية من المستعمل إلى الشبكة. ب) طبقة الخدمة (التحكم في الخدمة) – توفير حماية أمنية للتشوير والإدارة من خلال السطوح البينية من المستعمل إلى الشبكة UNI (على سبيل المثال بروتوكول فتح الدورة SIP، والنص الإلكتروني، والشبكة الرقمية متكاملة الخدمات ISDN، والمرجع H.248). ج) طبقة الخدمة (توفير التطبيقات والخدمات) – توفير حماية أمنية لوظائف التحكم في

	التطبيقات والخدمات عبر السطوح البينية من المستعمل إلى الشبكة (على سبيل المثال التشوير في النطاق).

الجدول 2 – مثال للأصول والموارد والمعلومات والسطوح البينية المرتبطة بطبقة النقل

الأمثلة	الأهداف والمقاصد
تتمثل موارد طبقة النقل فيما يلي: • عناصر شبكة النقل (على سبيل المثال مفرعات بروتوكول الإنترنت، عُقَد تبديل الوسوم متعددة البروتوكولات MPLS) • وصلات الإرسال • معلومات التسيير (على سبيل المثال وحدات خدمة نظام أسماء الميادين DNS) • معلومات الملامح العامة لمستعمل النقل (على سبيل المثال قواعد بيانات النقل ومستودعات البيانات)	أ) حماية جميع عناصر شبكة النقل ومكوناتها ووظائفها من النفاذ غير المخول. ب) حماية تكاملية عناصر شبكة النقل ومكوناتها ووظائفها. ج) حماية تيسُّر عناصر ومكونات ووظائف شبكة النقل. والحماية من انقطاع الخدمات (أي من الهجمات برفض الخدمة). د) الحماية من إفشاء أي معلومات خاصة بالمستعمل أو بالشبكة.
اتصالات طبقة النقل بين الأنظمة (الاتصالات داخل شبكة مورد الشبكة)	أ) توفير حماية أمنية لحركة الوسائط/الحمالة بين الأنظمة داخل شبكة مورد. ب) توفير حماية أمنية للتحكم في النقل (على سبيل المثال أقصر المسيرات المفتوحة أولاً (OSPF)، والتشوير والإدارة داخل شبكة المورد. ج) توفير أمن التشوير بين الأنظمة في طبقة الخدمة (على سبيل المثال مخدّمو التطبيقات) والأنظمة في طبقة النقل (على سبيل المثال، مفرعات بروتوكول الإنترنت).
السطوح البينية والاتصالات الخاصة بالنقل	أ) توفير حماية أمنية لحركة الوسائط/الحمالة عبر نقل السطوح البينية UNI وNNI وANI. ب) توفير حماية أمنية لتشوير وإدارة التحكم في النقل (على سبيل المثال أقصر المسيرات المفتوحة أولاً OSPF) عبر السطوح البينية UNI وNNI وANI للنقل.

الجدول 3 – مثال للأصول والموارد والمعلومات والسطوح البينية لطبقة الخدمة

	الأمثلة	الأهداف والمقاصد
طبقة الخدمة – التحكم في الخدمة	طبقة الخدمة – موارد التحكم في الخدمة • عناصر شبكة التحكم في الخدمة (على سبيل المثال CSC-Fs، والنظام الفرعي للمشترك المنـــزلي HSS، وظيفة موارد الوسائط MRP، والبوابات، مراقب حدود الدورة SBC)	أ) حماية جميع عناصر ومكونات وظائف شبكة التحكم في الخدمة من النفاذ غير المخول. ب) حماية تكاملية عناصر الشبكة ومكونات ووظائف التحكم في الخدمة، بما في ذلك الحماية من إتلاف المعلومات أو تعديلها. ج) حماية تيسر عناصر الشبكة ومكونات ووظائف التحكم في الخدمة. والحماية من انقطاع الخدمات (أي من الهجمات من خلال رفض الخدمة).
	طبقة الخدمة – معلومات التحكم في الخدمة • معلومات المشترك (على سبيل المثال قواعد البيانات ومستودع البيانات الذي يحتوي على الملامح العامة للمستعمل والملامح العامة للخدمة) • معلومات مورد الشبكة NGN (على سبيل المثال قواعد البيانات ومستودع البيانات الذي يحتوي على المعلومات الخاصة بالتسيير والترقيم والعنونة)	أ) الحماية من إتلاف البيانات والمعلومات أو تعديلها. ب) الحماية من السرقة أو الإزالة أو الفقدان (على سبيل المثال سرقة الهوية). ج) الحماية من الإفشاء (على سبيل المثال النفاذ غير المخول إلى المعلومات الخاصة بالمستعمل والشبكة).
	طبقة الخدمة – توصيلات التحكم في الخدمة بين الأنظمة	توفير الحماية الأمنية للتشوير فيما بين الأنظمة (على سبيل المثال بروتوكول فتح الدورة SIP، وخدمة المستعمل المبدلة إلى استيقان عن بعد RADIUS، والقطر) داخل شبكة مورد الشبكات (على سبيل المثال CSCF وظيفة التحكم في دورة النداء إلى تشوير النظام الفرعي للمشترك المنـــزلي HSS).
	السطوح البينية والاتصالات	توفير الحماية الأمنية للتشوير والإدارة عبر السطوح البينية UNI، وNNI، وANI.
طبقة الخدمة – التطبيقات ودعم الخدمات	طبقة الخدمة – موارد التطبيقات ودعم الخدمات: • عناصر الشبكة ومنصات دعم التطبيقات والخدمات (على سبيل المثال مخدّمو التطبيقات، قواعد البيانات، منافذ الويب)	أ) حماية جميع عناصر شبكة دعم الخدمات ومكوناتها ووظائفها من أي نفاذ غير مخول. ب) حماية تكاملية عناصر شبكة دعم الخدمات ومكوناتها ووظائفها، بما في ذلك الحماية من تحريف المعلومات أو تعديلها. ج) حماية تيسر عناصر شبكة دعم الخدمات ومكوناتها ووظائفها. د) الحماية من انقطاع الخدمات (أي الحماية من الهجمات من خلال رفض الخدمة).
	طبقة الخدمة – المعلومات الخاصة بالتطبيقات ودعم الخدمات: • المعلومات المتعلقة بالتطبيقات والخدمات • المعلومات الخاصة بالاشتراك	أ) الحماية من تحريف البيانات والمعلومات أو تعديلها. ب) الحماية من السرقة أو الإزالة أو الفقدان (على سبيل المثال سرقة الهوية). ج) الحماية من الإفشاء (على سبيل المثال النفاذ غير المخول إلى المعلومات الخاصة بالمستعمل والشبكة).
	السطوح البينية	أ) توفير حماية أمنية لعناصر الشبكة والموارد فيما يتعلق بنفاذ موردين آخرين للتطبيقات (بوابات Parlay وOMA). ب) توفير حماية أمنية للسطوح البينية UNI وNNI وANI. ج) توفير حماية أمنية لحركة التشوير والإدارة عبر السطوح البينية ANI.

الجدول 4 – مثال للأصول والموارد والمعلومات والسطوح البينية للإدارة

المثال	الأهداف والمقاصد
موارد الإدارة • أنظمة إدارة طبقة النقل (على سبيل المثال أنظمة إدارة عناصر الشبكة وأنظمة إدارة الشبكة وإدارة الخدمات) • أنظمة إدارة طبقة الخدمة (على سبيل المثال أنظمة إدارة عناصر الشبكة وأنظمة إدارة الشبكة وإدارة الخدمات)	أ) حماية جميع عناصر شبكة الإدارة ومكوناتها ووظائفها وسطوحها البينية من النفاذ غير المخول. ب) حماية تكاملية عناصر شبكة الإدارة ومكوناتها ووظائفها وسطوحها البينية. ويشمل هذا حماية المعلومات من التحريف أو التعديل. ج) حماية تيسر عناصر شبكة الإدارة ومكوناتها ووظائفها وسطوحها البينية. والحماية من انقطاع الخدمات (أي الحماية من الهجمات المتمثلة في رفض الخدمة).
الاتصالات فيما بين الأنظمة داخل شبكة مورد شبكة	أ) توفير حماية أمنية لحركة الإدارة بين أنظمة الإدارة داخل شبكة (على سبيل المثال طبقة الخدمة). ب) توفير حماية أمنية لحركة الإدارة بين شبكة المستعمل وطبقة الخدمة وطبقة نقل خدمة مورد الشبكة.
السطوح البينية والاتصالات فيما بين الأنظمة	أ) توفير أمن السطوح البينية لإدارة الشبكات الداخلية وأي سطوح بينية UNI وNNI وANI للإدارة. ب) توفير حماية أمنية لحركة الإدارة عبر السطوح البينية UNI وANI وNNI.

7 الأهداف والمتطلبات

1.7 الأهداف العامة للأمن

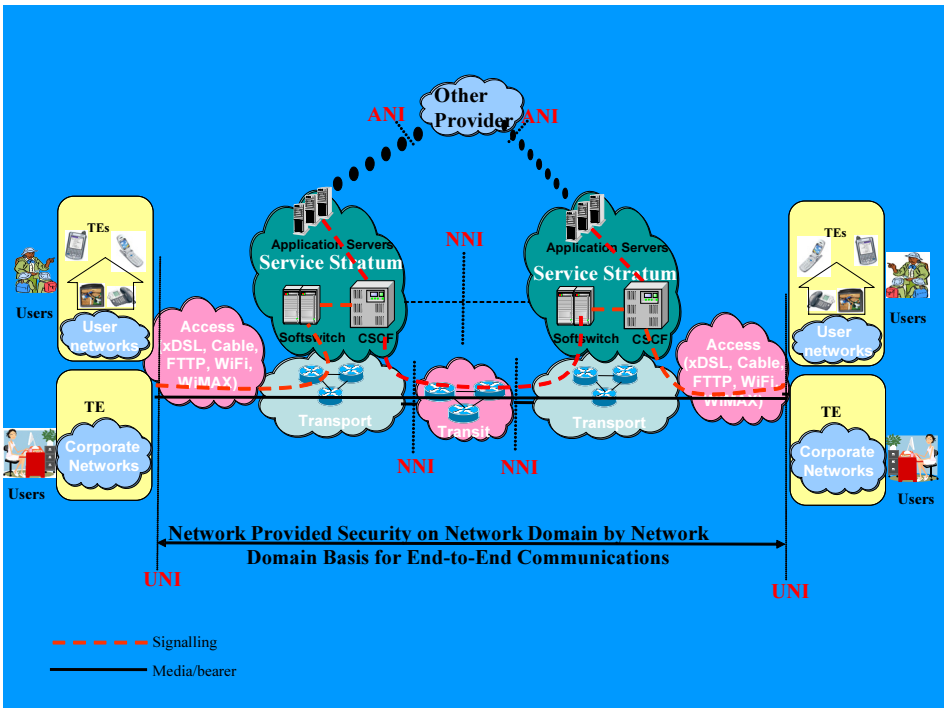
فيما يلي قائمة بالغايات الأمنية العامة التي استُند إليها في تحديد المتطلبات الواردة في هذه التوصية.

- ينبغي أن تكون السمات الأمنية الوظيفية لشبكات الجيل التالي قابلة للتمديد ومرنة بما فيه الكفاية لتلبية مختلف الاحتياجات.
- ينبغي لمتطلبات الأمن أن تأخذ في الاعتبار نوعية أداء شبكة الجيل التالي وقابليتها للاستعمال وللتطور والقيود المتعلقة بتكلفة هذه الشبكات.
- ينبغي أن تستند أساليب الأمن إلى معايير الأمن القائمة والمفهومة جيداً حسب الاقتضاء.
- ينبغي أن تكون معمارية أمن شبكات الجيل التالي تطورية بصورة شاملة (داخل ميادين مورد الشبكة وعبر ميادين موردي شبكات متعددين فيما يتعلق بتوفير الأمن).
- ينبغي لمعمارية أمن شبكة NGN أن تلتزم بالفصل المنطقي أو المادي في حركة التشوير والتحكم وحركة المستعمل وحركة الإدارة.
- ينبغي توفير أمن شبكات NGN على نحو مأمون وإدارة الأمن بطريقة موثوقة.
- ينبغي لشبكة الجيل التالي أن توفر الأمن من جميع المنظورات: الخدمة، مورد الشبكة، المشترك.
- ينبغي لأساليب الأمن ألا تؤثر بوجه عام على نوعية الخدمات المقدمة.
- ينبغي أن يكون باستطاعة المشتركين والموردين توفير الأمن وتشكيله بطريقة بسيطة وموثوقة (وظائف أمنية مهيأة للعمل).

- ينبغي المحافظة على مستويات أمن ملائمة حتى عند استعمال وظائف التوزيع المتعدد.
- ينبغي أن توفر مقدرات كشف الخدمات، طائفة متنوعة من معايير تحديد المجال (على سبيل المثال، الموقع، التكلفة، وما إلى ذلك) لتوفير نتائج ملائمة بآليات ملائمة لضمان أمن واحترام سرية الحياة الخاصة.
- ينبغي أن يكون نظام استبانة العناوين نظاماً خاصاً لا تستعمله سوى هذه الشبكة، ويتعين توفير بعض تدابير الأمن. ويمكن لهذا النظام استخدام قواعد البيانات الداخلية أو الخارجية بالنسبة لميدان.
- ينبغي اتباع المبادئ والغايات الأمنية العامة من أجل تأمين إدارة صيانة الشبكات على النحو المبين في الفقرة 7 من التوصية [ITU-T M.3016.0].

2.7 الأهداف المتعلقة بالأمن عبر ميادين متعددة لمورد الشبكة

ويتمثل الهدف العام في توفير أمن قائم على الشبكة للاتصالات من طرف إلى طرف عبر ميادين متعددة. ويتحقق هذا من خلال توفير أمن الاتصالات من طرف إلى طرف على أساس قفزة قفزة عبر مختلف الميادين المتعددة. ويبين الشكل 7 المفهوم العام لأمن الاتصالات من طرف إلى طرف توفره الشبكة بين المستعملين النهائيين. ولكل قسم من الشبكة مسؤوليات أمنية خاصة داخل منطقة أمنه لتيسير الأمن وتيسير اتصالات الشبكات NGN عبر شبكات متعددة.



الشكل 7 – أمن الاتصالات عبر شبكات متعددة

حسبما وصف في الفقرة الفرعية 2.5، فإن النموذج الموثوق بين شبكات الجيل التالي الموصولة بينياً يتوقف على عدة جوانب مثل التوصيلات البينية المادية، ونماذج التوصيل البيني، والعلاقات التجارية.

3.7 المتطلبات الخاصة بأبعاد الأمن

الأهداف الوارد وصفها هنا خاصة بأبعاد أمن معينة مثل الاستيقان. وهي عامة بالنسبة لجميع السطوح البينية.

1.3.7 التحكم في النفاذ

يتعين على موردي شبكة NGN قصر النفاذ على المشتركين المخولين. ويمكن منح التخويل من جانب المورد الذي يوفر النفاذ أو من جانب موردين آخرين بعد التحقق من الصلاحية من خلال عمليات الاستيقان والتحكم في النفاذ.

يتعين على شبكة الجيل التالي منع النفاذ غير المخول من خلال انتحال المتطفلين هوية المستعملين المخولين، مثلاً.

2.3.7 الاستيقان

يتعين على موردي شبكة الجيل التالي دعم قدرات استيقان المشتركين والتجهيزات، وعناصر الشبكة والموردين الآخرين. وينبغي لهم بوجه خاص أن يدعموا المقدرات التالية (والقائمة ليست شاملة):

1) مقدرات على استيقان المستعملين الذين يأملون في النفاذ إلى شبكات النقل (على سبيل المثال استيقان وتخويل جهاز المستعمل النهائي وبوابة شبكة مستعمل أو بوابة شبكة مشتركة للحصول على النفاذ أو الاتصال بشبكة النقل).

2) مقدرات على استيقان مستعملين يأملون في النفاذ إلى الخدمات في بداية تقديم الخدمات وأثناء تقديمها (على سبيل المثال استيقان مستعمل أو جهاز أو استيقان مشترك لمستعمل/جهاز حيث ينطبق الاستيقان على النفاذ إلى خدمات/تطبيقات الشبكات NGN).

3) مقدرات لمستعمل شبكة NGN على استيقان مورد شبكة NGN في كل طبقة (على سبيل المثال، استيقان المستعمل لهوية مورد شبكة NGN الموصولة أو استيقان مورد الخدمة) إذا استلزمت سياسة الأمن ذلك.

4) مقدرات تتيح إجراء استيقان بين مستعملين أنداد (على سبيل المثال، استيقان المستعمل المطلوب أو الكيان المصدر أو مصدر البيانات) باعتبارها خدمات للشبكة أو عناصر خدمات لها.

5) مقدرات تتيح إجراء استيقان ثنائي بين موردي شبكات NGN على كل طبقة من أجل تبادل حركة التشوير والإدارة وحركة الوسائط/الحمالة (مثال ذلك استيقان الشبكات الموصولة مباشرة، واستيقان الشبكات عن بعد من خلال السطوح البينية NNI).

6) مقدرات تتيح إمكانية استيقان مقدمي خدمات آخرين عبر السطوح البينية ANI. ويتعين توفير نُهُج تستند إلى وحدة تعرف المشترك SIM و/أو نُهج لا تستند إلى هذه الوحدة SIM.

ملاحظة – الاستيقان من الهوية لا ينطوي على كشف الصلاحية الإيجابية لشخص ما.

3.3.7 عدم الإنكار

لا تحدد هذه التوصية أي متطلبات أمن بخصوص عدم الإنكار.

4.3.7 سرية البيانات

يتعين على موردي شبكة NGN حماية سرية حركة المشترك بوسائل التجفير أو بوسائل أخرى.

ويتعين على موردي شبكة NGN حماية سرية رسائل التحكم بوسائل مجفرة أو بوسائل أخرى إذا كانت سياسة الأمن تتطلب ذلك.

ويتعين على موردي شبكة NGN حماية سرية حركة الإدارة بوسائل مجفرة أو بوسائل أخرى.

5.3.7 أمن الاتصالات

يتعين على مورّدي شبكة NGN توفير آليات لضمان ألاّ تُحرَّف المعلومات أو يتم إيقافها على نحو غير قانوني.

6.3.7 تكاملية البيانات

يتعين على موردي شبكة NGN حماية تكاملية حركة المشترك من خلال وسائل مجفرة أو بوسائل أخرى.

ويتعين على موردي شبكة NGN حماية تكاملية رسائل التحكم بوسائل مجفرة أو بوسائل أخرى إذا كانت سياسة الأمن تتطلب ذلك.

ويتعين على موردي شبكة NGN حماية تكاملية حركة الإدارة بوسائل مجفرة أو بوسائل أخرى.

7.3.7 التيسر

يتعين على شبكة NGN توفير قدرات أمن لتمكين موردي شبكات NGN من منع أو إنهاء الاتصالات مع تجهيزات المستعمل النهائي غير الممتثلة للقواعد: مثلاً لتخفيف آثار هجمات رفض الخدمة وانتشار الفيروسات أو الفيروسات المتسللة وغيرها من الهجمات ويجوز تعليق هذه القدرات للسماح بإجراء اتصالات الطوارئ. وقد تكون عناصر الشبكة الداخلية NGN عرضة أيضاً للفيروسات والفيروسات المتسللة وغيرها من الهجمات. وبالتالي يلزم أيضاً وجود تدابير مماثلة لعزل مكونات الشبكة.

ينبغي أن توفر شبكة NGN قدرات أمنية لتمكن مورد الشبكة NGN من ترشيح الرزم والحركة التي تُعتبر ضارة من وجهة نظر السياسة الأمنية ذات الصلة.

ويتعين على شبكات NGN توفير قدرات لدعم وظائف وإجراءات لإعادة الأحوال الطبيعية بعد الكوارث. والمتطلبات الخاصة في هذا الصدد تندرج خارج نطاق هذه التوصية.

8.3.7 الخصوصية

يتعين على شبكات NGN توفير قدرات من أجل حماية المعلومات الخاصة بالمشترك مثل موقع البيانات والهويات وأرقام الهواتف وعناوين الشبكات أو بيانات محاسبة النداء طبقاً للوائح والقوانين الوطنية. وبعض المتطلبات الخاصة بحماية السرية وطنية الطابع وتقع خارج نطاق بحث هذه التوصية.

8 متطلبات الأمن الخاصة

تتناول هذه الفقرة المتطلبات الخاصة بأمن كل عنصر من عناصر الشبكة داخل البنية التحتية للشبكة NGN. إلا أنه نظراً لأن الكثير من احتياجات الأمن سيكون متماثلاً بالنسبة لمختلف أنماط عناصر الشبكة، فإن متطلبات الأمن الإجمالية تحدَّد أولاً في الفقرة الفرعية 1.8.

ويمكن دمج العناصر الحدية أو فصلها تبعاً للتنفيذ.

1.8 متطلبات الأمن المشتركة لعناصر شبكات NGN

تنطبق هذه المتطلبات على عناصر شبكات NGN في المنطقة الموثوقة وفي المنطقة الموثوقة لكن المتعرضة. ومن المستصوب أن تستجيب الأجهزة الكائنة في المنطقة غير الموثوقة لهذه المتطلبات.

وفيما يلي قائمة بمتطلبات الأمن العام:

يتعين على مختلف عناصر الشبكة NGN أن توفر قابلية التشغيل البيني، وبوجه خاص بين مختلف آليات أمن شبكات NGN. ويتعين أن تتيسر على النطاق العالمي وظائف أمنية مقيسة دنيا.

ويتعين أداء الاستيقان والتخويل في طبقتي الخدمة والنقل على السواء (المستعمل إلى الشبكة، الشبكة إلى المستعمل، الشبكة إلى الشبكة). وينبغي أن يكون بالإمكان تحقيق ذلك أيضاً في حالة وجود ترجمة عرضية لعنوان الشبكة ومنفذها NAPT.

ويتعين على عنصر الشبكة NGN توفير تدابير للأمن للحماية من النفاذ غير المخول إلى موارد وأجهزة وخدمات الشبكة وبيانات المشترك (الملامح العامة)، على سبيل المثال وقف الحركة غير المخولة.

ويتعين على البنية التحتية لشبكات NGN أن تتيح للموردين إمكانية الحد من قابلية رؤية الكيانات المخولة لطوبولوجيا الشبكة ومواردها.

ويتعين على البنية التحتية لشبكات NGN أن تدعم مناطق أمنية متعددة. وقد يلزم وجود عزل من الناحية الأمنية بين مختلف مناطق الأمن.

ويتعين على البنية التحتية لشبكات NGN أن تضمن السرية وتكاملية تدفقات التشوير/التحكم وتدفقات الإدارة التي تضطلع بنقلها.

وينبغي للبنية التحتية لشبكات NGN أن تضمن سرية وتكاملية تدفق الوسائط التي تنقلها.

ويتعين أن تضمن الشبكة NGN بعناية أمن عناصر الشبكة المتصلة بموارد الإدارة (نظام دعم العمليات (OSS)، قاعدة البيانات، إلخ) وموارد الخدمات.

وتتبع متطلبات الأمن اللازمة لتأمين إدارة الاتصالات TMN المتطلبات الواردة في الفقرة الفرعية 1.10 من التوصية [ITU-T M.3016.0] وعلى النحو الوارد بالتفصيل أيضاً في الفقرة 6 من التوصية [ITU-T M.3016.1].

ويتعين إنفاذ العناصر الوظيفية للأمن على العناصر الحدية (NBE أو TE-BE، أي عناصر الشبكة في المنطقة الموثوقة لكن المعرضة). ويشمل هذا وظائف مثل التحكم في النفاذ إلى رزم البيانات ومعلومات التشوير وفقاً للسياسات المحددة على سبيل المثال، رفض الحركة من جانب بعض التطبيقات أو المستعملين.

ويمكن لعناصر الشبكة NGN الحساسة، وخصوصاً العناصر الحدية للشبكة أن تؤدي الفصل المنطقي و/أو المادي لمسيرات النقل وفقاً للسياسات الأمنية الموضوعة، على سبيل المثال الفصل بين تدفقات التحكم و/أو الإدارة وتدفقات الوسائط باستعمال سطوح بينية منطقية مختلفة أو خطط عناوين مختلفة، وباستعمال شبكة نقل حقيقية أو تقديرية مختلفة مادياً (تقديرية مثل الشبكات VPNs أو الشبكات VLANs).

ويتعين على الشبكة NGN أن توفر تخزيناً مأموناً للبيانات المتعلقة بالأمن (على سبيل المثال البيانات المتعلقة بالهوية ومستندات الهوية). ويتعين أن يكون هذا التخزين منفصلاً عن مستودع البيانات العامة الذي يحتوي على المعلومات المتصلة بخدمات المشتركين. ويتعين على الشبكة NGN أن توفر سياسة أمنية تشمل مجموعة من القواعد التي تحدد الحركة التي يتعين حمايتها وذلك بالاستناد على سبيل المثال إلى العقود وأي نوع من الحماية يُستعمل ومدى تواتر تغيير مفاتيح الدورات والقواعد التي تحدد امتثال جهاز ما لمتطلبات الأمن.

ويتعين أن تدعم الشبكة NGN إمكانية مراقبة حركة الشبكة ووضع خط أساس لأحداث الشبكة التي ينبغي اعتبارها أحداثاً عادية.

ويتعين أن تكون الشبكة NGN قادرة على كشف أحداث الشبكة غير العادية والإفادة عنها والتخفيف من تواترها.

1.1.8 السياسة الأمنية

والسياسية الأمنية هي مجموعة من القواعد التي تضع سلطة الأمن الناظمة لاستعمال وتوفير خدمات وتسهيلات الأمن. وينبغي لموردي شبكات NGN أن يُعِدُّوا سياسة أمنية ملائمة وأن يضطلعوا بالمسؤولية عن تطبيقها على جميع عناصر الشبكة والأجهزة التي تحت سيطرتهم.

2.1.8 تعزيز حماية الخدمة وتعطيلها

يتعين أن تكون جميع عناصر شبكات NGN قادرة على التشكُّل لتوفير الخدمات الدنيا اللازمة لدعم البنية التحتية لهذه الشبكات التابعة لمورد شبكات NGN. ويتعين تعطيل أي خدمة أو مَنْفَذ طبقة نقل لا يلزم للتشغيل السليم لعناصر الشبكة NGN وذلك في جميع أنظمة الشبكة وعناصرها. وبالإضافة إلى ذلك، يتعين إدارة التطبيقات بأدنى حد من الامتيازات (على سبيل المثال بالنسبة لمنصات "UNIX/Linux" ينبغي ألاّ تدار التطبيقات باعتبارها جذوراً إذا كانت امتيازات الجذور ليست ضرورية). ويتعين أن يكون نظام التشغيل الأساسي الذي يدعم أي عنصر لشبكة NGN قادراً على التشكل على وجه التحديد من أجل الأمن وينبغي دعم حمايته كما ينبغي. لا يُسمح في أي عنصر من عناصر الشبكة NGN بأي "سبل نفاذ سرية" (نفاذ إلى البرمجية من شأنه أن يلتف حول آلية التحكم في النفاذ المعتاد).

وبالإضافة إلى تعزيز الحماية يتعين إجراء عمليات تحكم في النفاذ المادي أو المنطقي بغية الاستجابة لأفضل ممارسات الصناعة.

3.1.8 سجل التدقيق والإيقاع في الشراك والتسجيل

يتعين أن تكون جميع عناصر الشبكة NGN قادرة على إنشاء سجل للتدقيق يحتفظ بتسجيل للأحداث المتعلقة بالأمن وفقاً للسياسة الأمنية لمورد شبكات NGN. ويتعين أن تكون ثمة آليات حاضرة لمنع أي تعديل غير مخوَّل وغير مكتشَف.

ويتعين التمكن من إدارة منفذ التدقيق، ويلزم إتاحة إمكانية نقل البيانات القديمة الواردة في منفذ التدقيق إلى وسائط أخرى، على سبيل المثال، وسائط يمكن نقلها من أجل التخزين الطويل الأجل. ومن الضرورة لهذا السطح البيني أن يتيح للقائمين بالإدارة المخولين نقل البيانات القديمة خارج سجل التدقيق إلى وسائط يمكن نقلها. ويتعين حماية هذه المقدرة من خلال تخويل محدد بإدارة سجل التدقيق.

وتتناول الفقرة الفرعية 3.6.2.1.10 من التوصية [ITU-T M.3016.0] والفقرتان الفرعيتان 6.6 و7.6 من التوصية [ITU-T M.3016.1] بمزيد من التفصيل متطلبات الأمن بالنسبة للتسجيل والتدقيق المتعلقين بالأمن.

4.1.8 تسجيل الوقت ومصدر الوقت

يتعين أن يدعم عنصر الشبكة NGN استعمال مصدر موثوق للوقت بالنسبة لكلا نظامي الميقاتية والتسجيل في سجل التدقيق. ويعني مصدر الوقت الموثوق في هذه الحالة مصدراً للوقت يمكن التحقق من أنه يقاوم أي تعديل غير مخول. والموثوقية المتعدية مقبولة أي أن مصدر الوقت الذي يعوّل على مصدر موثوق للوقت هو في حد ذاته مصدر موثوق مقبول للوقت.

5.1.8 توزيع الموارد ومعالجة الاستثناءات

يتعين على كل عنصر من عناصر الشبكات NGN أن يوفر المقدرة على الحد من كمية موارده الهامة (على سبيل المثال الذاكرة) التي يخصصها للإجابة على الطلبات. ويمكن لهذه الحدود أن تقلل إلى أدنى حد من الآثار السلبية للهجمات المتمثلة في رفض الخدمة. وتتنافس الموارد المستعملة في الاستجابة للطلبات مع الطلبات الأخرى باستعمال موارد النظام. بالإضافة إلى ذلك، يتعين أن تتوافر لكل تطبيق محدد للشبكة NGN القدرة على الحد من استعماله الخاص للموارد الهامة التي يخصصها لتلبية الطلبات.

والغرض من هذا المتطلب هو الحد من أثر دفقات النشاط الشديدة بحيث لا تؤثر على طلبات الخدمة الأخرى. وسيتيح هذا أيضاً للتطبيق (ولنظام التشغيل) المقدرة على تحديد أنظمة المراقبة من أن التطبيق و/أو منصته قد يكونان معرضين لهجوم يتمثل في رفض الخدمة. ويتعين أن يوفر عنصر الشبكة NGN سطحاً بينياً لمراقبة استخدام الموارد.

ويتعين على عنصر الشبكة NGN أن يرفض دون قيد أو شرط أية رزم لا تتطابق مع البروتوكول أو النسق المتوقع، وأن يكون عنصر الشبكة قادراً بالاستناد إلى سياسة الأمن على توليد مدخل لتسجيل خاص بكل هذه الأحداث. ويرمي "الرفض دون قيد أو شرط" إلى إعداد فخ للرزمة المستلمة وتسجيلها، ورفض الرزمة المستلمة مع عدم إرسال رد يدل على الرفض (على سبيل المثال رد خطأ).

ويتمثل الغرض المقصود في هذا الصدد في الحد من الهجمات المحتملة من رزم خبيثة أو خاطئة. ومن الواضح أنه إذا كان استعمال الموارد من قبل عمليات التسجيل كبيراً بحيث يحدث تداخل مع العمليات الأخرى للعنصر، يصبح غنياً عن القول أنه يتعين وقف التسجيل إلى أن يعود استعمال الموارد إلى مستوى مقبول.

ملاحظة – هذا الجزء هو من إدارة الموارد الداخلية حسبما ذكر أعلاه.

6.1.8 تكاملية ومراقبة الشفرة والنظام

يتعين أن يكون عنصر الشبكات قادراً على مراقبة 1) تشكيله وبرمجيته 2) أي تغيرات لكشف التغيرات غير المخولة وذلك باستناد كليهما إلى سياسة الأمن. وبالنسبة لأي تغييرات غير مخولة يلزم أن يسجِّل مُدخل وأن يتولد إنذار. واستناداً إلى سياسة الأمن، يتعين على عنصر الشبكة أن يؤدي ما يلي. يتعين أن يكون العنصر قادراً على أن يقوم بشكل دوري بمسح موارده وبرمجياته بحثاً عن برمجيات خبيثة، على سبيل المثال فيروس. ويتعين على العنصر أن يولد إنذاراً إذا اكتُشفت برمجية خبيثة أثناء عملية فحص.

ويتعين التحكم في المراقبة بحيث لا تؤثر على أداء اتصالات الوقت الفعلي أو الاتصالات الحساسة للتأخير أو تتسبب في انقطاع غير ضروري للتوصيلات.

وتتناول (الفقرة الفرعية 4.6.2.1.10) من التوصية [ITU-T M.3016.0] بمزيد من التفاصيل المتطلب الأمني المتعلق بتكاملية النظام.

7.1.8 برامج التصحيح والتصحيحات المنتظمة والشفرة الإضافية

لضمان موثوقية الإشارات التي تنتجها عناصر شبكات NGN في شبكات غير موثوقة، على سبيل المثال في جهاز مطرافي. ويشترط الحرص على عدم تعريض برمجية النظام للخطر. ويتيح هذا ضمان ألا تكون "أحصنة طروادة"[1] (التي تعمل من الداخل)، "الفيروسات المتسللة" (التي تولد حركة لا فائدة منها أو تحول الأنظمة إلى "zombies")، والفيروسات الأخرى لا يتم تحميلها على عناصر الشبكة NGN أو لا تكمن في نظام التشغيل التحتي. وتعرِّض هذه الفيروسات تكاملية النظام للخطر وكذلك سرية البيانات و/أو تيسرها.

ويتعين على عناصر شبكة وأنظمة مورد شبكات NGN أن توفر المقدرة على التحقق من جميع البرمجيات وتدقيقها. ويجب أن يكون بوسع نظام دعم العمليات OSS النفاذ إلى نتائج التدقيق. فمن شأنه أن يتيح تحليلاً لوضع أمن البنية التحتية لشبكات NGN التابعة لمورد هذه الشبكات وأن يوفر إرشادات إلى القائمين بالإدارة وموردي الشبكات فيما يتعلق بأين تلزم الحلول القائمة على التخفيف.

ويتم الحصول على برامج تصحيح الأمن من بائعي التجهيزات وتركيبها بطريقة مناسبة التوقيت، بمجرد أن يعتمدها مورد شبكات NGN.

وتقدم الفقرة الفرعية 2.5.I من التوصية [ITU-T M.3016.1] مزيداً من الاعتبارات بشأن عملية برامج التصحيح؛ وتقدم الفقرة الفرعية 9.3.5.I من التوصية [ITU-T M.3016.1] اعتبارات بشأن افتراضات أمن نظام التشغيل.

8.1.8 النفاذ إلى وظائف: العمليات، الإدارة، الصيانة، التزويد (OAMP) في الأجهزة

بغية حماية البنية التحتية الوظائف OAMP، يتعين إدارة كل عنصر من شبكات NGN الداخلية من خلال عنوان منفصل على بروتوكول الإنترنت موزع من فدرة عناوين منفصلة. وينبغي أن يكون لكل عنصر من الشبكة NGN الداخلية سطح بيني منفصل متميز على المستوى المادي أو المنطقي مخصص على وجه خاص لاستعمال حركة هذه الوظائف OAMP. وعندما يُستعمل سطح بيني منفصل يتعين على عنصر شبكة NGN أن يرفض دون قيد أو شرط جميع الرزم المتلقاة على السطح البيني OAMP مع عناوين مصدر أخرى غير عنوان الوظائف OAMP. ويتعين على عنصر الشبكة NGN أن يرفض دون قيد أو شرط جميع الرزم المتلقاة على السطح البيني غير OAMP مع عناوين مصدر مخصصة لحركة OAMP.

ويتعين أن يكون في الإمكان التحكم في النفاذ إلى وظائف OAMP بواسطة الاستيقان. وما أن يتم استيقان مستعمل لدى نظام، يتعين على عنصر شبكة NGN الداخلية أن يتتبع جميع التعديلات التي يحملها وأن يوفر إمكانية إلغائها.

ويجب أن يسجَّل في منفذ التدقيق أي استعمال للتخويل ذي صلة بالأمن لأي وقت محدد. ويتعين بوجه خاص أن تسجَّل في منفذ التدقيق جميع محاولات النفاذ سواء أكانت ناجحة أم لا إلى العنصر المعني.

ويتعين حماية حركة الوظائف OAMP على نحو مأمون. وإذا عبرت حركة OAMP (بما في ذلك SNMP وNTP) شبكة غير موثوقة يلزم حمايتها بطريقة موثوقة (على سبيل المثال أمن بروتوكول الإنترنت IPsec أو إجراء تبديل للوسوم متعددة البروتوكولات (MPLS)، إلى آخره).

[1] تعمل أحصنة طروادة بمثابة أجهزة برمجيات يتحكم فيها عند بُعد القرصان الذي يقوم بإرسالها. وعندما تركب بصورة مأمونة على النظام المستهدف فإنها تشرع في إجراء توصيل مع القرصان لإبلاغه أنها جاهزة للاستعمال.

2.8 المتطلبات الخاصة بعناصر الشبكة NGN الكائنة في المنطقة الموثوقة

يخصص لعناصر الشبكة NGN، الطبعة 1 الكائنة في المنطقة "الموثوقة" عنوان بروتوكول إنترنت في الفدرة المحجوزة لعناصر الشبكة NGN الداخلية، وهذا العنوان هو الذي يتعين استعماله بالنسبة لجميع عمليات التشوير. ويتعين أيضاً تخصيص عنوان على بروتوكول الإنترنت لكل عنصر من عناصر الشبكة NGN، الطبعة 1 وذلك في الفدرة المحجوزة لوظائف OAMP، وهذا العنوان هو الذي يتعين استعماله بالنسبة لمجموع حركة الوظائف OAMP.

وبغية المحافظة على سرية وسلامة اتصالات العميل، يجب حماية حركة التشوير والوسائط، سواء باستعمال تجفير النقل أو بالتأكد من عدم عبور الحركة إلاّ من خلال ميادين محمية.

3.8 المتطلبات المتعلقة بالعناصر الحدية لشبكة NGN في الميدان "الموثوق لكن المتعرض"

وتمثل العناصر الحدية الدفاع الرئيسي ضد الهجمات الخارجية، أي الهجمات من أجهزة/عناصر شبكة في المنطقة غير الموثوقة. وترسل جميع الحركات من الأجهزة/عناصر الشبكة في المنطقة "غير الموثوقة" أولاً إلى عنصر حدي يقوم بالتحقق من صلاحيتها قبل أن ينقلها إلى وجهتها في الميدان "الموثوق". وتُستعمل المقدرات على توفير الفصل المادي/المنطقي للشبكات من أجل حظر الحركة من جهاز/عنصر الشبكة في المنطقة غير الموثوقة من الوصول إلى أي عنصر في الميدان "الموثوق".

وتشكل العناصر الحدية للشبكة (NBE) الدفاع الرئيسي ضد الهجمات على التشوير. ويعالَج مجمل حركة التشوير الصادرة عن كيان TE أو TE-BE في المنطقة غير الموثوقة في العنصر الحدي للشبكة المخصص لها الذي يعيد إرسال الإشارات إلى تجهيزات الشبكة الكائنة في المنطقة الموثوقة. وتُستعمل المقدرات على توفير فصل مادي/منطقي للشبكات على مستوى العنصر الحدي للشبكة لمنع الحركة الصادرة عن كيان TE/TE-BE كائن في المنطقة غير الموثوقة من الوصول إلى عنصر شبكة كائن في المنطقة الموثوقة، باستثناء العنصر أو العناصر الحدية للشبكة NBE التي خصصت له.

وكما هو الحال بالنسبة للتشوير، تشكل العناصر الحدية للشبكة أيضاً الدفاع الرئيسي ضد الهجمات التي تستهدف حركة الوسائط. ويعالَج مجمل حركة الوسائط الصادرة عن كيان TE/TE-BE على مستوى عنصر NBE ويُستخدم هذا العنصر كمرحِّل لحركة هذه الوسائط. ويُسيِّر العنصر الحدي للشبكة رزم الوسائط نحو الوجهة المقصودة، ومن خلال الميدان الموثوق فقط، إذا كان بالإمكان ربط رزم الوسائط هذه بدورة مخولة جارية. ورزم الوسائط غير المرتبطة بطلب دورة تكون غير صالحة وليس لها مكان تذهب إليه ويتم رفضها. وبالإضافة إلى ذلك، يتحقق العنصر الحدي للشبكة من مصدر قطار الوسائط ويتحقق من أن معدل الرزم متسق مع الدورة المنشأة. وتُنقَل حركة الوسائط داخل مرافق مورد الشبكة NGN إما إلى بوابة للشبكة الهاتفية العمومية التبديلية (PSTN) (بالنسبة لتوصيلة PSTN) أو إلى عنصر حدي آخر للشبكة NBE. وفي العنصر الحدي الثاني للشبكة تعالَج الوسائط ويعاد إرسالها إلى تجهيزات مقر العميل TE المقصودة.

ملاحظة – يستعمل المصطلح "دورة" ليشير إلى أي نمط من أنماط تدفق الوسائط دون النظر إلى الاتفاقية المستعملة لإقامة الدورة.

ويتعين على العنصر الحدي للشبكة أن يدعم عناوين متعددة لبروتوكول الإنترنت أو سطوح بينية متعددة للشبكة. ويخصَّص عنوان واحد على بروتوكول الإنترنت (العنوان "الداخلي") من الفدرة المحجوزة لعناصر الشبكة NGN، الطبعة 1 الداخلية. ويتعين أن تَستعمل مجمل حركة التشوير والوسائط المتأتية من أو المتجهة إلى عناصر شبكة NGN، الطبعة 1 الداخلية الأخرى، هذا العنوان (أو هذا السطح البيني). ويخصَّص عنوان واحد لبروتوكول الإنترنت (العنوان "الخارجي") يمكن لتجهيزات مقر العميل TE النفاذ إليه. ويتعين أن تَستعمل مجمل حركة التشوير والوسائط المتأتية من أو المتجهة إلى تجهيزات TE هذا العنوان أو (هذا السطح البيني) ويخصَّص عنوان واحد لبروتوكول الإنترنت ("عنوان الوظائف OAMP") من الفدرة المحجوزة للوظائف OAMP التي يمكن النفاذ إليها من وحدات خدمة الوظائف OAMP.

وبغية حماية سرية اتصالات العميل من التنصت الخفي على حركة التشوير، يتعين أن يؤمَّن نقل التشوير الخاص بجميع رسائل التشوير إلى عناصر الشبكة NGN في المنطقة "الموثوقة" أو المنطقة "الموثوقة لكن المعرضة". وبالنسبة لجميع التوصيلات التي يستهلها عنصر حدي للشبكة وتُستعمل لنقل معلومات التشوير إلى عناصر الشبكة NGN يتم إنشاءها باستعمال قنوات مؤمنة

مع الاستيقان. وتُرفض دون قيد أو شرط جميع رسائل التشوير التي يتلقاها عنصر حدي للشبكة في عنوانه "الداخلي" على قنوات غير مؤمنة.

وتُوفَّر الحماية لقطارات الوسائط سواء بتجفير النقل أو بالتأكد من عدم عبور الحركة إلا عبر الشبكات المحمية. وبالإضافة إلى ذلك، فإن ضمان عنوان المصدر عند حد الشبكة سيتيح منع الرزم الآتية من الخارج من الادعاء بأنها آتية من فدرة عنوان الشبكة NGN الداخلية.

وبالنسبة لرزم الوسائط التي يتسلمها العنصر الحدي للشبكة على عنوانه الخارجي، يتم التحقق مما إذا كانت توافق دورة نشطة (تستند إلى تبادل التشوير)، على ضوء عنوان المصدر المتوقع (المستند إلى وصف الدورة المتضمَّن في تبادل التشوير). ويتعين على العنصر الحدي للشبكة رفض أي رزم وسائط مستلَمة لا تقابل دورة نشطة. ويتعين على عنصر الشبكة أيضاً التحقق من أن معدل الرزمة متفق مع معلمات الدورة المتفاوض عليها. ويمكن للعنصر الحدي للشبكة أن يتحقق من أن حجم الرزمة متسق مع الدورة المنشأة. وتُرفض بلا قيد أو شرط رزم الوسائط المستلمة من عنوان مصدر لبروتوكول الإنترنت لا يطابق مرسِل صحيح للوسائط بالنسبة لهذا العنصر الحدي للشبكة.

ويتعين على العنصر الحدي للشبكة أن يستيقن جميع الطلبات إذا لزم ذلك بفعل اتفاق الخدمة مع العميل. وعندما يستلم طلب على توصيل غير مجفر، يتم استيقان كل طلب منفرد. وعندما يُستلَم الطلب على توصيل مجفر أنشئ بدون استيقان الزبون، يتم استيقان أول طلب على ذلك التوصيل. وعندما يُستلَم طلب على توصيل مجفر أنشئ مع الاستيقان، لا يلزم إجراء استيقان آخر. ويلاحَظ أن الطلبات التي ترسَل من خلال العنصر الحدي TE-BE لن تخضع لاستيقان الأجهزة نظراً لأن العنصر الحدي TE-BE سيَستَعْمِل توصيل مجفر إلى العنصر الحدي للشبكة. وإذا أتى الطلب من عنوان مصدر بروتوكول الإنترنت غير صحيح كمصدر للطلبات إلى هذا العنصر الحدي للشبكة فإنه يتم رفضه بلا قيد أو شرط. ويتم أيضاً بلا قيد أو شرط رفض الطلبات المتعلقة بقناة مؤمنة متأتية من عنوان مصدر وبروتوكول الإنترنت لا يطابق مرسِل الطلبات الصحيحة لهذا العنصر NBE.

4.8 المتطلبات الخاصة بالعناصر الحدية لتجهيزات TE في الميدان "غير الموثوق"

يشكل الأمن المادي تحدياً للتجهيزات الموضوعة في مقر العميل. ويجب أن يُقبل في نهاية المطاف أن أمن هذه الأجهزة يتوقف إلى حد كبير على العميل. ويعني ذلك أنه يتعين على كل جهاز أن يوفر الاحتياطات المعقولة للحماية من الهجمات أو التعرض للخطر أو التلاعب بغير ذلك من الأساليب. وبغية حماية سرية اتصالات العميل من التنصت الخفي على حركة التشوير، يتعين أن تستعمل رسائل التشوير توصيلة تشوير مأمونة بين العنصر الحدي TE-BE والعنصر الحدي للشبكة NBE. ويمكن للعنصر الحدي (TE-BE) أن يؤدي وظيفة مرحِّل للوسائط.

1.4.8 وظائف OAMP

يتعين حماية جميع وظائف OAMP بين العنصر TE-BE ومورد شبكات NGN من التنصت الخفي المتعمد. ونظراً لأن الوظائف OAMP يمكن توفيرها داخل النطاق أو خارج النطاق على السواء، فإنه يتم معالجة هاتين الحالتين على نحو منفصل.

5.8 توصيات في مجال الأمن للتجهيزات الطرفية الكائنة في الميدان "غير الموثوق"

تكون التجهيزات الطرفية (TE) غالباً خارج سيطرة مورد الشبكة NGN ولذلك لا يلزم أن يفرض مورد الشبكة NGN متطلبات تتعلق بعناصرها الوظيفية الأمنية أو بسياسة الأمن التي ينبغي لها تطبيقها، غير أنه يتعين على مختلف العناصر الحدية للشبكة أن تتكيف مع السياسات التي يختارها العميل، وأن توفر أفضل خدمة في ظل تلك الظروف.

يخضع موضوع الوظائف الأمنية الحالية للعناصر الحدية لمقدم خدمة شبكات الجيل التالي NGN لمزيد من الدراسة.

وينبغي حماية حركة الوسائط من التنصت الخفي أو التعديل.

التذييـــل I

أهداف الأمن والمبادئ التوجيهية اللازمة للتوصيل البيني لخدمة اتصالات الطوارئ (ETS)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I خلفية

خدمة اتصالات الطوارئ (ETS) هي خدمة وطنية توفر الأولوية في خدمات الاتصالات للمستعملين المخولين باستخدام خدمات اتصالات الطوارئ في أوقات الكوارث وحالات الطوارئ. وتنفيذ خدمات اتصالات الطوارئ هو مسألة وطنية. إلا أن الكوارث/حالات الطوارئ يمكن أن تتجاوز الحدود الجغرافية ومن ثم هناك احتمال لأن تدخل البلدان/الإدارات في اتفاقات ثنائية و/أو متعددة الأطراف لربط أنظمتها الخاصة بخدمات اتصالات الطوارئ. وسيتيح هذا توفير الأولوية لخدمات الاتصالات (على سبيل المثال الاتصالات الصوتية، أو إرسال الرسائل، والرسائل الفيديوية أو البيانات) تحت مظلة خدمات اتصالات الطوارئ أي تلقى الدعم من مختلف الشبكات الوطنية ذات الاتفاقات الثنائية و/أو المتعددة الأطراف في أوقات الكوارث وحالات الطوارئ.

ويتعين حماية خدمات اتصالات الطوارئ بين مختلف الشبكات الوطنية (أي البلدان/الإدارات) من التهديدات المحدقة بالأمن. ولتمكين الشبكات من ضمان أمن خدمات اتصالات الطوارئ من طرف إلى طرف بين مختلف الشبكات الوطنية (أي البلدان/الإدارات) وتنفيذ خدمات اتصالات الطوارئ، يلزم وضع إرشادات وتحديد أهداف ومتطلبات مشتركة للأمن. ويتوقف توافر الأمن وتيسُّر خدمات اتصالات الطوارئ على أمن كل شبكة مشاركة في الاتصالات من طرف إلى طرف.

2.I مجال التطبيق/الغرض

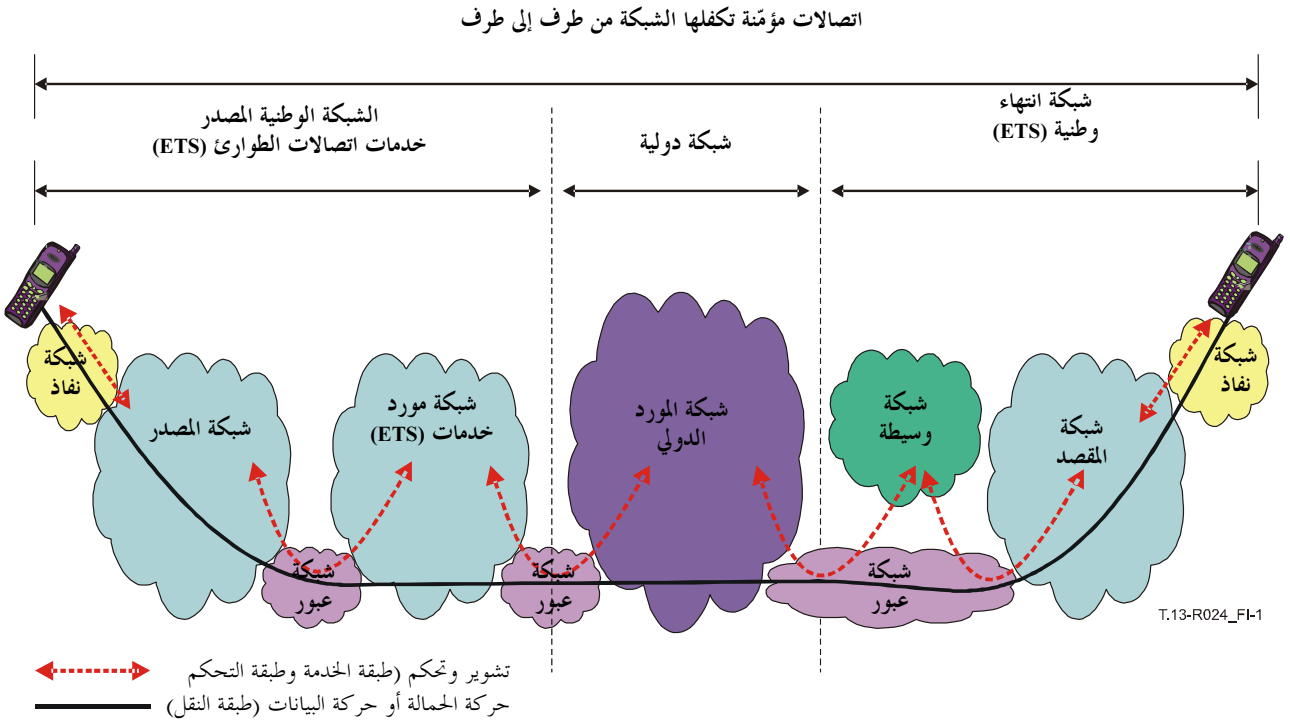
يتضمن هذا التذييل أهداف ومتطلبات الأمن المشتركة، ويوفر إرشادات تتيح للشبكة توفير الأمن لخدمات اتصالات الطوارئ عبر مختلف الشبكات الوطنية (أي البلدان/الإدارات) التي تضطلع بعمليات تنفيذ خدمات اتصالات الطوارئ.

ولا تندرج في نطاق انطباق هذا التذييل وظيفة الأمن بين المستعملين الأنداد الذين يستعملون تجهيزات مستعملين خاصة. ويقتصر انطباق هذا التذييل على الشبكات التي توفر الأمن لخدمات اتصالات الطوارئ عبر شبكات متعددة على أساس قفزة قفزة. إلا أن شبكات NGN ينبغي أن تكون قادرة على أن توفر على نحو شفاف هذه الوظائف بين الأنداد.

ولا يقصد من هذا التذييل فرض شروط على عمليات التنفيذ الوطنية لخدمات اتصالات الطوارئ. فالغرض الأساسي منه هو السماح للشبكات بتوفير الأمن لخدمات اتصالات الطوارئ (أي الاتصالات ذات الأولوية المؤمَّنة للإشارات الصوتية والإشارات الفيديوية والبيانات واتصالات المراسلات).

3.I الأهداف العامة

تتمثل الأهداف العامة في أن تكون الشبكات قادرة على توفير أمن خدمات اتصالات الطوارئ (على سبيل المثال توفير أولوية للاتصالات الصوتية المؤمَّنة وكذلك الفيديوية، وأمن البيانات واتصالات المراسلات) عبر مختلف الشبكات الوطنية (أي البلدان/الإدارات) وحماية تيسر خدمات اتصالات الطوارئ. وينطوي هذا على توفير الأمن للاتصالات من طرف إلى طرف التي يمكن أن تجتاز ميادين مختلفة لشبكات وطنية أو دولية لموردي الشبكات (أي بلدان/إدارات) حيث تكون كل شبكة مسؤولة عن الأمن داخل ميدانها.



ملاحظة: لم يوضح مستوي الإدارة

الشكل I-1 – مثال لاتصال من طرف إلى طرف عبر مختلف عمليات التنفيذ الوطنية لخدمات اتصالات الطوارئ

يوضح الشكل I-1 خدمات اتصالات الطوارئ من طرف إلى طرف (على سبيل المثال الاتصالات ذات الأولوية للإشارات الصوتية أو الإشارات الفيديوية أو البيانات أو المراسلات) بين شبكتين وطنيتين مختلفتين. ويوضح المثل أن الاتصالات ذات الأولوية من طرف إلى طرف والخاصة بخدمات اتصالات الطوارئ يمكن أن تشمل أقسام شبكات متعددة وميادين إدارية متعددة (على سبيل المثال، شبكة النفاذ، شبكة المصدر، شبكة مقدم الخدمات ETS، وشبكة المورد الدولي، والشبكة الوسيطة، وشبكة الانتهاء).

ويكون لكل قسم من أقسام الشبكة مسؤوليات أمنية محددة داخل ميدانه من أجل تيسير الأمن من طرف إلى طرف وتيسير خدمات اتصالات الطوارئ.

وفيما يلي مجموعة دنيا من المبادئ التوجيهية العامة بشأن تخطيط الأمن لحماية التشوير وحركة الحمالة والبيانات والمعلومات المرتبطة بالإدارة (على سبيل المثال المعلومات المتعلقة بالملامح العامة للمستعمل) فيما يخص خدمات اتصالات الطوارئ:

- ينبغي لكل ميدان شبكة أن ينشئ وينفذ سياسات أمنية ويوفر مقدرات للتخفيف بالنسبة لخدمات اتصالات الطوارئ داخل ميدانها. وعلى وجه التحديد يوصى بوجوب تحديد حلول للتخفيف وممارسات أمنية أكثر صرامة من تلك اللازمة للخدمات التطبيقية العامة وتنفيذ هذه الحلول بالنسبة لخدمات اتصالات الطوارئ ذات الأولوية. وعلى سبيل المثال ينبغي صياغة هذه الحلول والممارسات بطريقة تكفل الحيلولة دون استعمال موارد خدمات اتصالات الطوارئ من قبل مستعملين غير مخولين، وكذلك منع الهجمات وبوجه خاص الهجمات المتمثلة في رفض الخدمة من جانب الأنواع الأخرى من الخدمات.
- وينبغي لكل ميدان من ميادين الشبكة أن ينشئ علاقات موثوقة وأساليب وإجراءات لتعيين خدمات اتصالات الطوارئ، ولإدارة الهوية واستيقان المستعملين والشبكات عبر ميادين إدارية متعددة للشبكة. وعلى سبيل المثال،

ينبغي للاتفاقات على مستوى الخدمة (SLAs) أن تضع سياسة أمنية لاستيقان كل ميدان لدى نقل واستلام خدمات اتصالات الطوارئ.

- وينبغي لكل ميدان إداري للشبكة أن يضع وينفذ سياسات أمنية لحماية البيانات والمعلومات المتعلقة بإدارة خدمات اتصالات الطوارئ (على سبيل المثال المعلومات المتعلقة بالملامح العامة للمستعمل).

4.I القدرات العامة للأمن

يوصى بدعم الآتي من أجل خدمات اتصالات الطوارئ:

- مقدرات أمنية لحماية خدمات اتصالات الطوارئ من طرف إلى طرف عبر ميادين متعددة للشبكة.
- مقدرات أمنية لحماية تيسر خدمات اتصالات الطوارئ عبر ميادين متعددة للشبكة.
- مقدرات أمنية لتوفير إدارة واستيقان هويات المستعملين والشبكات عبر ميادين إدارية متعددة للشبكة. ومن المستصوب بدرجة كبيرة أن يتفاعل المستعمل مع خدمة اتصالات الطوارئ مرة واحدة فقط، وأن تضطلع آليات الأمن بنقل مسوغات هوية المستعمل النهائي من ميدان إداري إلى آخر.

5.I الاستيقان والتخويل والتحكم في النفاذ

يوصى بدعم المجموعة الدنيا التالية من مقدرات الاستيقان والتخويل والتحكم في النفاذ من أجل خدمات اتصالات الطوارئ:

- مقدرات أمنية لحماية الآليات المستعملة في استيقان وتخويل مستعملي خدمات اتصالات الطوارئ وأجهزتها.
- مقدرات أمنية لحماية الآليات المستعملة لربط المستعمل النهائي لخدمات اتصالات الطوارئ بالأجهزة الملازمة.
- مقدرات أمنية لحماية الآليات المستعملة لتقاسم معلومات الاستيقان (على سبيل المثال تأكيد أن مستعمل ما قد تم استيقانه) عبر ميادين متعددة للشبكة.
- مقدرات أمنية لحماية الآليات المستعملة في الاستيقان الثنائي للمستعملين والكيانات. وتشمل هذه، آليات يستعملها المستعمل النهائي لخدمات اتصالات الطوارئ لاستيقان الطرف المطلوب أو الكيانات التي يجري معها الاتصال (على سبيل المثال موقع على الويب، وحدة خدمة المحتوى، وما إلى ذلك).
- مقدرات أمنية لحماية الآليات التي تستعملها شبكة واحدة لاستيقان شبكة أخرى. ويشمل هذا الآليات التي تستعمل لاستيقان الشبكة التي تنقل خدمات اتصالات الطوارئ (على سبيل المثال شبكة المصدر) واستيقان الشبكة المستلِمة لخدمات اتصالات الطورائ (على سبيل المثال الشبكات الوسيطة أو شبكات المقصد).
- مقدرات أمنية للحماية من النفاذ غير المخول إلى المعلومات والموارد المتعلقة بخدمات اتصالات الطوارئ (على سبيل المثال معلومات المستعملين المتعلقة باستيقان وحدات الخدمة وأنظمة الإدارة).

6.I السرية والخصوصية

يوصى بدعم المجموعة الدنيا التالية من مقدرات المحافظة على السرية:

- مقدرات أمنية لحماية سرية حركة التشوير والتحكم في خدمات اتصالات الطوارئ.
- مقدرات أمنية لحماية سرية حركة الحمالة وحركة البيانات المتعلقة بخدمة اتصالات الطوارئ (على سبيل المثال الإشارات الصوتية أو الإشارات الفيديوية أو البيانات).
- مقدرات أمنية لحماية سرية هويات المستعملين النهائيين لخدمات اتصالات الطوارئ والكيانات المتصلة وكذلك المعلومات الخاصة بالمشتركين.
- مقدرات أمنية لحماية سرية مكان المستعمل النهائي لخدمات اتصالات الطوارئ.

ويوصى بدعم المجموعة الدنيا التالية من مقدرات الخصوصية:

- مقدرات أمنية لحماية خصوصية المعلومات الخاصة بخدمات اتصالات الطوارئ (على سبيل المثال المعلومات المستمدة من مراقبة أنشطة الشبكة مثل المواقع على الويب التي زارها المستعمل النهائي والموقع الجغرافي للمستعمل، وعناوين بروتوكول الإنترنت، والأسماء الواردة في نظام أسماء الميادين (DNS) في الأجهزة الكائنة في شبكة مورد الخدمات.
- مقدرات أمنية لتوفير الحماية للخصوصية من المراقبة غير المخولة للمعلومات المتعلقة باستعمال خدمة اتصالات الطوارئ (على سبيل المثال مخططات الاستعمال مثل حجم حركة خدمة اتصالات الطوارئ، والمواقع، والأوقات، والتواتر، وما إلى ذلك).

7.I تكاملية البيانات

يوصى بدعم المجموعة الدنيا التالية من المقدرات على تحقيق تكاملية البيانات:

- آليات أمنية لحماية تكاملية خدمات اتصالات الطوارئ (على سبيل المثال الحماية من التعديل غير المخول أو الحذف أو الإنشاء أو إعادة التنفيذ). وتشمل هذه الآليات، الآليات اللازمة للإشارة إلى التبليغ عن التلاعب بالمعلومات أو تعديلها.
- آليات أمنية لحماية تكاملية المعلومات المتعلقة بخدمات اتصالات الطوارئ (على سبيل المثال التوسيم ذو الأولوية، والإشارات الصوتية، والبيانات، والإشارات الفيديوية).
- آليات أمنية لحماية تكاملية بيانات التشكيل الخاصة بخدمات اتصالات الطوارئ (على سبيل المثال المعلومات ذات الأولوية المخزونة في العنصر الوظيفي المتعلق بالقرار السياسي، ومستوى الأولوية الخاص بالمستعمل، وما إلى ذلك).

8.I الاتصال

يوصى بدعم المقدرة الدنيا التالية:

- آليات أمنية لحماية خدمات اتصالات الطوارئ من عمليات الاقتحام الموجهة ضد مستعمل مخول لخدمات اتصالات الطوارئ (على سبيل المثال آليات لمنع الوقف غير القانوني، والقرصنة، أو إعادة تنفيذ حركة التشوير أو حركة الحمالة/البيانات الخاصة بخدمات اتصالات الطوارئ).

9.I التيسُّر

يوصى بدعم المجموعة الدنيا التالية من المقدرات:

- آليات أمنية لحماية تيسر خدمات اتصالات الطوارئ (على سبيل المثال حماية حركة التشوير والتحكم وحركة الحمالة/بيانات خدمات اتصالات الطوارئ من الهجمات وخصوصاً الهجمات المتمثلة في رفض الخدمة).
- آليات أمنية لحماية تيسر الموارد والمعلومات الخاصة بخدمات اتصالات الطوارئ (على سبيل المثال قواعد بيانات الاستيقان/التخويل، والمعلومات ذات الأولوية المخزونة في العنصر الوظيفي المتعلق بالقرار السياسي، وموارد الشبكة المخصصة للحماية من رفض الخدمة (DoS) وأشكال الهجمات الأخرى).

ثبت المراجع

توصيات القطاع ITU-T

[b-ITU-T E.106] ITU-T Recommendation E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[b-ITU-T E.107] ITU-T Recommendation E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[b-ITU-T E.115] ITU-T Recommendation E.115 (2007), *Computerized directory assistance*.

[b-ITU-T M.3016.2] ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.

[b-ITU-T M.3016.3] ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.

[b-ITU-T M.3016.4] ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.

[b-ITU-T M.3060] ITU-T Recommendation M.3060/Y.2401 (2006), *Principles for the management of Next Generation Networks*.

[b-ITU-T X.1121] ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ITU-T X.1122] ITU-T Recommendation X.1122 (2004), *Guideline for implementing secure mobile systems based on PKI*.

[b-ITU-T Y.1271] ITU-T Recommendation Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[b-ITU-T Y.2000-Sup.1] ITU-T Y.2000-series Recommendations – Supplement 1 (2006), *NGN release 1 scope*.

[b-ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks*.

وثائق ETSI TISPAN

[b-ETSI TR 187.002] ETSI TR 187 002 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis*.

[b-ETSI TS 187.001] ETSI TS 187 001 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements*.

[b-ETSI TS 187.003] ETSI TS 187 003 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture*.

[b-3GPP TS 33.102] 3GPP TS 33.102 (2007), *3G security; Security architecture*.

[b-3GPP TS 33.103] 3GPP TS 33.103 (2001), *3G security; Integration guidelines*.

[b-3GPP TS 33.110] 3GPP TS 33.110 (2007), *Key establishment between a UICC and a terminal*.

[b-3GPP TS 33.120] 3GPP TS 33.120 (2001), *Security Objectives and Principles*.

[b-3GPP TS 33.200] 3GPP TS 33.200 (2004), *3G security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *3G security; Access security for IP-based services*.

[b-3GPP TS 33.204] 3GPP TS 33.204 (2007), *3G security; Network Domain Security (NDS); TCAP user security*.

[b-3GPP TS 33.210] 3GPP TS 33.210 (2007), *3G security; Network Domain Security; IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220 (2007), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-3GPP TS 33.310] 3GPP TS 33.310 (2007), *Network Domain Security (DNS; Authentication Framework (AF)*.

[b-3GPP TR 33.901] 3GPP TR 33.901 (2001), *Criteria for cryptographic algorithm design process*.

[b-3GPP TR 33.902] 3GPP TR 33.902 (2001), *Formal Analysis of the 3G Authentication Protocol*.

[b-3GPP TR 33.908] 3GPP TR 33.908 (2001), *3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-3GPP TR 33.909] 3GPP TR 33.909 (2001), *3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-3GPP TR 33.918] 3GPP TR 33.918 (2007), *Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF)*.

[b-3GPP TR 33.919] 3GPP TR 33.919 (2007), *3G Security; Generic Authentication Architecture (GAA); System description*.

[b-3GPP TR 33.920] 3GPP TR 33.920 (2007), *SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature*.

[b-3GPP TR 33.980] 3GPP TR 33.980 (2007), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)*.

[b-ETSI TR 133.901] ETSI TR 133.901 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security – Criteria for cryptographic Algorithm design process*.

[b-ETSI TR 133.902] ETSI TR 133.902 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol*.

[b-ETSI TR 133.908] ETSI TR 133.908 (2001), *Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-ETSI TR 133.909] ETSI TR 133.909 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-ETSI TR 133.919] ETSI TR 133.919 V6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description*.

[b-ETSI TS 133.102] ETSI TS 133 102 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture*.

[b-ETSI TS 133.103] ETSI TS 133 103 V4.2.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines*.

[b-ETSI TS 133.120] ETSI TS 133 120 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives*.

[b-ETSI TS 133.200] ETSI TS 133 200 V6.1.0 (2005), *Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-ETSI TS 133.203] ETSI TS 133 203 V6.10.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services*.

[b-ETSI TS 133.210] ETSI TS 133 210 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS)*.

[b-GPP TS 133.220] ETSI TS 133 220 V7.8.0 (2007), *Digital cellular telecommunications system; (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-ETSI TS 133.310] ETSI TS 133 310 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF)*.

وثائق ATIS/3GPP2

[b-GPP2 S.S0086] 3GPP2 S.S0086 (2004), *IMS Security Framework*.

IPsec related IETF RFCs

[b-IETF RFC 2085] IETF RFC 2085 (1997), *HMAC-MD5 IP Authentication with Replay Prevention*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*.

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2709] IETF RFC 2709 (1999), *Security Model with Tunnel-mode IPsec for NAT Domains*.

[b-IETF RFC 2857] IETF RFC 2857 (2000), *The Use of HMAC-RIPEMD-160-96 within ESP and AH*.

[b-IETF RFC 3526] IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3664] IETF RFC 3664 (2004), *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*.

[b-IETF RFC 4109] IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)*.

[b-IETF RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*.

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*.

[b-IETF RFC 4309] IETF RFC 4309 (2005), *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use With IPsec*.

S/MIME related IETF RFCs

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification*.

[b-IETF RFC 2312] IETF RFC 2312 (1998), *S/MIME Version 2 Certificate Handling*.

[b-IETF RFC 3565] IETF RFC 3565 (2003), *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 3657] IETF RFC 3657 (2004), *Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 3850] IETF RFC 3850 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*.

[b-IETF RFC 3851] IETF RFC 3851 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*.

[b-IETF RFC 3852] IETF RFC 3852 (2004), *Cryptographic Message Syntax*.

[b-IETFB RFC 4134] IETF RFC 4134 (2005), *Examples of S/MIME Messages*.

TLS related IETF RFCs

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2817] IETF RFC 2817 (2000), *Upgrading to TLS Within HTTP/1.1*.

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS*.

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

Miscellaneous IETF security related RFC

[b-IETF i-d.SIPUAP] IETF internet-draft work in progress, draft-ietf-sipping-config-framework-08.txt (March 6, 2006), *A Framework for Session Initiation Protocol User Agent Profile Delivery*.

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3715] IETF RFC 3715 (2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements*.

[b-IETF RFC 3847] IETF RFC 3847 (2004), *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*.

[b-IETF RFC 3948] IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets*.

DNS related IETF RFCs

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

[b-IETF RFC 4034] IETF RFC 4034 (2005), *Resource Records for the DNS Security Extensions*.

[b-IETF RFC 4035] IETF RFC 4035 (2005), *Protocol Modifications for the DNS Security Extensions*.

وثائق TIA

[b-TIA-683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

[b-TIA-1053] TIA Standard TIA-1053 (2005), *Broadcast/Multicast Security Framework*.

[b-TIA-1091] TIA Standard TIA-1091 (2006), *IMS Security Framework*.

وثائق ARIB

[b-ARIB-SS0078] ARIB STD-T64 S.S0078-0 v1.0 (2002), *Common Security Algorithms*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة B	وسائل التعبير: التعاريف والرموز والتصنيف
السلسلة C	الإحصائيات العامة للاتصالات
السلسلة D	المبادئ العامة للتعريفة
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	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) 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
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
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 وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2009