الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2704

(2010/01)

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

شبكات الجيل التالي – الأمـــن

آليات وإجراءات الأمن لشبكات الجيل التالي (NGN)

التوصيـــة ITU-T Y.2704

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
نوعية الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الأمن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900

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

التوصيـــة ITU-T Y.2704

آليات وإجراءات الأمن لشبكات الجيل التالي (NGN)

ملخص

تقدم التوصية ITU-T Y.2701، *متطلبات الأمن لشبكات الجيل التالي (NGN) الإصدار 1*، متطلبات الأمن لشبكات الجيل التالي (NGN) وسطوحها البينية (مثل السطوح البينية من المستعمل-إلى-الشبكة (UNI)، السطوح البينية من الشبكة-إلى-الشبكة (NNI)، السطوح البينية من التطبيق إلى الشبكة (ANI)). أما التوصية ITU-T Y.2704 فتعرض بعض آليات الأمن الممكن استعمالها للوفاء باشتراطات التوصية ITU-T Y.2701، وتبيِّن مجموعة الخيارات لكل آلية منتقاة. وعلى وجه التحديد، تعرض هذه التوصية آليات تعرُّف الهوية، والاستيقان، والتخويل؛ ثم تبحث موضوع أمن النقل بخصوص التشوير، ووظائف التشغيل–الإدارة–الصيانة–التزويد (OAMP)، وأمن الوسائط. وبعدئذ تصف الآليات المتعلقة بتسجيل التدقيق، وأخيراً تصف عملية التزويد. وتستند آليات الأمن الموصوفة في هذه التوصية إلى استعمال نموذج الثقة في الأمن المعرَّف في التوصية ITU-T Y.2701.

وقائمة آليات الأمن الموصوفة في هذه التوصية ليست كاملة. فلذا يُشجَّع مزوِّدو شبكات الجيل التالي على توفير أكثر مما تصفه هذه التوصية من الأدوات والمقْدِرات الأمنية وإجراءات التشغيل، حسبما تقتضي الحاجة لحماية أمن شبكات الجيل التالي (NGN).

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2704	2010.01.29	13

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 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 المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

المحتويات

الصفحة

الصفحة

التوصيـــة ITU-T Y.2704

آليات وإجراءات الأمن لشبكات الجيل التالي (NGN)

1 مجال التطبيق

تقدم التوصية ITU-T Y.2701، *متطلبات الأمن لشبكات الجيل التالي (NGN) الإصدار 1*، متطلبات الأمن لشبكات الجيل التالي (NGN) وسطوحها البينية (مثل السطوح البينية من المستعمل-إلى-الشبكة (UNI)، والسطوح البينية من الشبكة-إلى-الشبكة (NNI)، والسطوح البينية من التطبيق-إلى-الشبكة (ANI))، بما في ذلك نموذج للثقة. وتشتمل آليات الأمن المنتقاة لإنفاذ تلك الاشتراطات على خيارات، لكن الخيارات غير الموائمة ليست مرغوباً فيها، لأنها تنطوي على مطاعن أمنية، وتجعل من الصعب تحقيق التشغيل البيني.

وعليه فإن هذه التوصية تسلط الضوء على بعض الآليات الأمنية الهامة الممكن استعمالها للوفاء بمتطلبات التوصية ITU-T Y.2701، وتحدد مجموعة الخيارات اللازمة استعمالها بخصوص كل آلية منتقاة، من أجل تقليل مشكلات التشغيل البيني وعدم التواؤم. وليست قائمة الآليات الموصوفة في هذه التوصية بكاملة. فلذا يُشجَّع مزوِّدو شبكات الجيل التالي على توفير أكثر مما تصفه هذه التوصية من الأدوات والمقْدِرات الأمنية وإجراءات التشغيل، حسبما تقتضي الحاجة لحماية أمن شبكات الجيل التالي (NGN).

أريدَ لهذه التوصية أن تُستعمَل مع التوصية ITU-T Y.2701 لتوفير أساس لأمن شبكات الجيل التالي (NGN). وينبغي استعمالها مع توصيات أخرى متعلقة بالأمن ومع مواصفات أخرى، حسبما يناسب، بخصوص مجالات أمنية محددة.

ملاحظة – إن الآليات الموصوفة في هذه التوصية من أجل تعرّف الهوية والاستيقان تشكل جزءاً من موضوع أوسع معروف عموماً بتسمية IdM ("إدارة شؤون الهوية").

1.1 افتراضات

تستند هذه التوصية إلى الافتراضات التالية:

1) أن ضم الكيانات الوظيفية، كما هو معرَّف في التوصية ITU-T Y.2012، إلى عنصر شبكي معيّن يتغيّر، تبعاً للصانع.

2) يتحمّل كل مزود شبكة NGN مسؤوليات أمنية محددة ضمن ميدانه. مثلاً، تأدية الخدمات والممارسات الأمنية المنطبقة، من أجل: أ) حماية نفسه، ب) ضمان عدم المساس داخل شبكته بالأمن من طرف–إلى–طرف، وج) ضمان سوية عالية من التيسّر والسلامة للاتصالات في إطار شبكات الجيل التالي (NGN).

3) يضع كل ميدان شبكي وينفِّذ سياسات اتفاق على مستوى الخدمة (SLA) تضمن أمن الميدان وأمن التوصيلات البينية للشبكة. ويُفترَض أن يبيّن اتفاق سوية الخدمة (SLA) الخدمات والآليات والممارسات الأمنية اللازم تأديتها من أجل حماية الشبكات والاتصالات المترابطة بتوصيلات بينية (حركة التشوير/التحكم، وحركة الحمالة، وحركة الإدارة) عبر السطوح البينية: من المستعمل إلى الشبكة (UNI)، ومن الشبكة إلى الشبكة (NNI)، ومن التطبيق إلى الشبكة (ANI).

4) تعالج هذه التوصية موضوع الأمن الشبكي، وهو معمارية ذات طبقات، تتكون من أمن المحيط الخارجي للميادين الموثوقة، وأمن مادّي لتجهيزات المورّد، مع إمكانية استعمال التجفير.

2.1 استعراض عام

نُظِّمت هذه التوصية كما يلي:

- الجزء 2 (المراجع) – يتضمن هذا الجزء المراجع المعيارية.
- الجزء 3 (التعاريف) – يتضمن هذا الجزء التعاريف المستعملة في هذه التوصية.

- الجزء 4 (المختصرات والأسماء المختصرة) – يتضمن هذا الجزء المختصرات والأسماء المختصرة المستعملة في هذه التوصية.
- الجزء 5 (الاصطلاحات) – هذا الجزء لا يتضمن أيّ شيء.
- الجزء 6 (التهديدات والمخاطر المحدقة بالأمن) – يوفر هذا الجزء مرجعاً بشأن التهديدات والمخاطر المحدقة بالأمن المفترضة بالنسبة لبيئة الشبكات NGN.
- الجزء 7 (نموذج الأمن الموثوق) – يقدم هذا الجزء ملخَّصاً لنموذج الثقة في الأمن المعرَّف في [ITU-T Y.2701].
- الجزء 8 (تعرُّف الهوية، والاستيقان، والتخويل) – يعرض هذا الجزء آليات وتدابير أمنية بخصوص تعرف الهوية والاستيقان والتخويل.
- الجزء 9 (أمن النقل بخصوص التشوير والوظائف OAMP) – يصف هذا الجزء آليات لتجفير التشوير ووظائف التشغيل–الإدارة–الصيانة–التزويد (OAMP)، وحماية السلامة.
- الجزء 10 (أمن الوسائط) – يعرض هذا الجزء آليات لحماية الوسائط (كحركة الحمالة، مثلاً).
- الجزء 11 (الوظائف OAMP) – يقدم هذا الجزء معلومات ومراجع عن تسجيل التدقيق، وحصر، وتسجيل الأحداث الأمنية.
- الجزء 12 (تزويد التجهيزات في منطقة غير موثوقة) – يقدم هذا الجزء معلومات عن تزويد تجهيزات المستعمِلين في منطقة غير مأمونة.
- التذييل I – أمثلة على ضمان عنوان المصدر، وتطبيقها على آلية تعرّف هوية المشترك واستيقانه.
- التذييل II – أمن التوصيل البيني لخدمة اتصالات الطوارئ (ETS).
- التذييل III – أفضل الممارسات الأمنية.
- ثبت المراجع.

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 توصية.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional Requirements and Architecture of the NGN release 1.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*

[ITU-T Y.2703] Recommendation ITU-T Y.2703 (2009), *The application of AAA service in NGN.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

[ITU-T X.509] Recommendation ITU-T X.509 (2008) |ISO/IEC 9594-8:2008, Information technology – *Open systems interconnection – The Directory: Public-Key and attibute certificate frameworks.*

[ITU-T X.660] Recommendation ITU-T X.660 (2008) | ISO/IEC 9834-1:2008)|ISO/IEC 9834-1:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of*

OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree.

[ITU-T X.1035] Recommendation ITU-T X.1035 (2007), *Password-authenticated key exchange (PAK) protocol.*

[IETF RFC4302] IETF RFC 4302 (2005), *IP Authentication Header.*

[IETF RFC4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

[IETF RFC5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2.*

3 التعاريف

1.3 مصطلحات معرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في أماكن أخرى.

1.1.3 الأصول (asset) [ITU-T Y.2701]: أي شيء ذو قيمة للمنظمة وأعمالها وتشغيلها واستمرارها.

2.1.3 العنصر الحدّي (border element) [ITU-T Y.2701]: عنصر شبكي يؤدّي وظائف تتيح توصيل مختلف ميادين الأمن والميادين الإدارية.

3.1.3 الشبكة المشتركة (corporate network) [ITU-T Y.2701]: شبكة خاصة تستطيع تأدية الخدمة لعدة مستعملين وقد تشغل عدة مواقع (مثل مؤسسة أو مباني جامعة).

4.1.3 العنصر الحدي للميدان (domain border element) [ITU-T Y.2701]: العنصر الحدي الذي يؤدّي وظائف أمنية مع ميادين أخرى للشبكة بتحكم من المورّد فقط.

5.1.3 خدمة اتصالات الطوارئ (ETS, emergency telecommunications service) [b-ITU-T E.107]: خدمة وطنية تزوِّد باتصالات ذات أولوية لمستعمل خدمة اتصالات المخوّلين في أوقات الكوارث.

6.1.3 العنصر الحدي للشبكة (network border element) [ITU-T Y.2701]: عنصر حدي يتحكم به المورِّد فقط ويؤدّي وظائف الأمن مع الأجهزة المطرافية.

7.1.3 ميدان الأمن (Security domain) [ITU-T Y.2701]: مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة ذات صلة بالأمن تدار فيها العناصر وفقاً للسياسة الأمنية. وتدير سلطة الأمن السياسة الأمنية. ويمكن لميدان أمن ما أن يشمل عدة مناطق أمن.

8.1.3 إذنة الأمن (security token) [ITU-T X.810]: مجموعة معطيات تحميها خدمة أمنية أو عدة خدمات أمنية، مع المعلومات الأمنية المستعملة في التزويد بتلك الخدمات الأمنية، وتُنقل أثناء الاتصال من كيان اتصال إلى آخر.

9.1.3 منطقة أمن (security zone) [ITU-T Y.2701]: تعرِّف التوصية ITU-T Y.2701 ثلاث مناطق للأمن: (1) موثوقة، (2) موثوقة لكنها معرَّضة، (3) غير موثوقة. وتعرَّف منطقة الأمن من خلال التحكم التشغيلي، والموقع، والتوصيلية بعناصر الأجهزة/الشبكات الأخرى.

10.1.3 العنصر الحدّي للتجهيز المطرافي (terminal equipment border element) [ITU-T Y.2701]: عنصر حدي يؤدي وظائف أمنية بين تجهيزات مقر الزبون وشبكة مورِّد الخدمة.

11.1.3 الثقة (trust) [ITU-T Y.2701]: يقال على الكيان X أنه يثق بالكيان Y بخصوص مجموعة من الأنشطة، إذا كان وفقط إذا كان الكيان X يعتمد على الكيان Y في تصرفه بأسلوب معيّن من حيث الأنشطة المقصودة.

12.1.3 المنطقة الموثوقة لكنها معرَّضة (trusted but vulnerable zone) [ITU-T Y.2701]: هي، من منظور مورِّد شبكة NGN، منطقة أمن يقوم فيها هذا المورد بتشغيل (تزويد وصيانة) عناصر/أجهزة الشبكة. ويتحكم بالتجهيزات إما الزبون/المشترك وإما مورد الشبكة NGN. وبالإضافة إلى ذلك، يمكن أن تقع التجهيزات داخل أو خارج ميدان مورد الشبكة NGN. وتتصل هذه التجهيزات بعناصر في المنطقة الموثوقة وبعناصر في المنطقة غير الموثوقة على السواء، مما يفسر لماذا تتسم المنطقة "بالتعرض". وتتمثل وظيفتها الأمنية الرئيسية في حماية عناصر الشبكة في المنطقة الموثوقة بصفة دائمة من الاعتداءات الأمنية الصادرة عن المنطقة غير الموثوقة.

13.1.3 المنطقة الموثوقة (trusted zone) [ITU-T Y.2701]: هي، من منظور مورد شبكة NGN، ميدان أمن فيه عناصر ومنظومات هذه الشبكة قائمة ولا يتصل أبداً اتصالاً مباشراً بتجهيزات الزبون. والخصائص المشتركة لعناصر الشبكة NGN الكائنة في هذا الميدان هي أن مورد الشبكة NGN هو وحده الذي يتحكم بها، وأنها تقع في مقر هذا المورد (موقع يوفر لها الأمن المادي)، وأنها تتصل فقط بالعناصر الكائنة في الميدان "الموثوق" وبالعناصر الكائنة في الميدان "الموثوق لكنه معرَّض".

14.1.3 المنطقة غير الموثوقة (un-trusted zone) [ITU-T Y.2701]: هي، من منظور مورد شبكة NGN، منطقة تشمل جميع عناصر شبكات الزبائن أو ربما شبكات الأنداد أو مناطق أخرى لموردي شبكات NGN واقعة خارج الميدان الأصلي وموصولة بالعناصر الحدية لمورد شبكة NGN.

15.1.3 المستعمِل (user) [ITU-T Y.2091]: يشمل مصطلح المستعمِل ما يلي: المستعمِل النهائي، والشخص، والمشترك والمنظومة أو الجهاز أو الجهاز الطرفي (مثل فاكس أو حاسوب شخصي)، والكيان (الوظيفي)، والعملية، والتطبيق، والمورِّد، والشبكة المشتركة.

16.1.3 شبكة المستعمل (user network) [ITU-T Y.2701]: شبكة خاصة تتألف من تجهيزات مطرافية قد يكون لها عدة مستعملين.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلح التالي:

1.2.3 المستَيْقِن (authenticator): هو عنصر شبكي يسهِّل تعرف الهوية مع الاستيقان لكل من المشتركين والأجهزة والمستعملين النهائيين. مثلاً: العناصر الحدية المزوَّدة بوظيفة "وكيل المستعمل ظهراً لظهر" (B2BUA) أو وظيفة "الكيان الوظيفي المفوَّض للتحكم في دورة النداء" (P-CSCF) يمكن أن تكون مستيْقِنات للمشتركين في الخدمات المعتمدة على بروتوكول استهلال الدورة (SIP).

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

3G الجيل الثالث *(3rd Generation)*

AGW بوابة النفاذ *(Access Gateway)*

AH رأسية الاستيقان (*Authentication Header*)

AKA الاستيقان واتفاق المفاتيح (*Authentication and Key Agreement*)

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

AS/WS مخدم التطبيقات/مخدم ويب (*Application Server/Web Server*)

AuC مركز الاستيقان (*Authentication Centre*)

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

BE العنصر الحدي *(Border Element)*

BSR مسيِّر المحطة القاعدة *(Base Station Router)*

CA سلطة إصدار الشهادة *(Certification Authority)*

COPS خدمة مشتركة في سياسة مفتوحة *(Common Open Policy Service)*

CRL قائمة إبطال الشهادات *(Certificate Revocation List)*

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

DBE العنصر الحدي للميدان *(Domain Border Element)*

DNS نظام أسماء الميادين *(Domain Name System)*

DoS منع الخدمة *(Denial of Service)*

DTMF تردد متعدد بنغمة مزدوجة *(Dual-Tone Multi-Frequency)*

ECC تجفير بمنحنٍ إهليلجي *(Elliptic Curve Cryptography)*

ESP بروتوكول أمني تغليفي *(Encapsulating Security Protocol)*

ETS خدمة اتصالات الطوارئ *(Emergency Telecommunications Service)*

FE الكيان الوظيفي *(Functional Entity)*

GBA معمارية التمهيد التنوعية (*Generic Bootstrapping Architecture*)

GW وصلة بوابية *(Gateway)*

HMAC شِفرة استيقان الرسالة مع التظليل *(Hash Message Authentication Code)*

HTTP بروتوكول نقل النصوص المترابطة *(Hypertext Transfer Protocol)*

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

ID هوية *(Identity)*

IdM إدارة شؤون الهوية *(Identity Management)*

IDPS أنظمة كشف ومنع الاقتحام *(Intrusion Detection and Prevention Systems)*

IDS أنظمة كشف الاقتحام *(Intrusion Detection Systems)*

IKE تبادل مفاتيح إنترنت *(Internet Key Exchange)*

IMS نظام فرعي متعدد الوسائط لبروتوكول الإنترنت *(IP Multimedia Subsystem)*

IP بروتوكول الإنترنت *(Internet Protocol)*

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

LAN شبكة المنطقة المحلية *(Local Area Network)*

MD5 خوارزمية 5 لخلاصة رسالة *(Message Digest 5)*

MIB قاعدة معلومات الإدارة *(Management Information Base)*

MPLS تبديل بالوسم متعدد البروتوكولات *(MultiProtocol Label Switching)*

MRP-FE الكيان الوظيفي لمعالجة الموارد الوسائطية *(Media Resource Processing Functional Entity)*

MS محطة متنقلة *(Mobile Station)*

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

NAPT ترجمة عنوان الشبكة ومنفذها *(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 التشغيل، الإدارة، الصيانة، التزويد *(Operations, Administration, Maintenance and Provisioning)*

OID معرِّف هوية الشيء *(Object Identifier)*

ONU وحدة (وحدات) شبكية بصرية *(Optical Network Units)*

PAK مفتاح مستَيْقَن لكلمة السر *(Password Authenticated Key)*

P-CSC-FE الكيان الوظيفي المفوَّض للتحكم في دورة النداء *(Proxy Call Session Control Functional Entity)*

POTS الخدمة الهاتفية العادية *(Plain Old Telephone Service)*

PSTN الشبكة الهاتفية التبديلية العمومية *(Public Switched Telephone Network)*

QoS جودة الخدمة *(Quality of Service)*

RAC-FE الكيان الوظيفي للتحكم في الموارد والقبول *(Resource and Admission Control Functional Entity)*

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

RAN شبكة نفاذ راديوي *(Radio Access Network)*

RTSP بروتوكول التدفق المتصل في الوقت الفعلي *(Real Time Streaming Protocol)*

SAA-FE الكيان الوظيفي لاستيقان الخدمة وتخويلها *(Service Authentication and Authorization Functional Entity)*

SASL الطبقة البسيطة للاستيقان والأمن *(Simple Authentication and Security Layer)*

S-CSC-FE الكيان الوظيفي القائم بخدمة التحكم في دورة النداء *(Serving Call Session Control Functional Entity)*

SDP بروتوكول وصف الدورة *(Session Description Protocol)*

SIM وحدة هوية المشترك *(Subscriber Identity Module)*

SIP بروتوكول فتح الدورة *(Session Initiation Protocol)*

SLA اتفاق سوية الخدمة *(Service Level Agreement)*

SL-FE الكيان الوظيفي المحدِّد لموْقِع الاشتراك *(Subscription Locator Functional Entity)*

SNMP بروتوكول إدارة الشبكات البسيط *(Simple Network Management Protocol)*

SRTP البروتوكول المأمون للوقت الفعلي *(Secure Real Time Protocol)*

TAA-FE الكيان الوظيفي لاستيقان النقل وتخويله *(Transport Authentication and Authorization Functional Entity)*

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

TE تجهيز/تجهيزات مطرافية *(Terminal Equipment)*

TE-BE العنصر الحدي للتجهيزات المطرافية *(Terminal Equipment Border Element)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TMN شبكة إدارة الاتصالات *(Telecommunications Management Network)*

TRIP تسيير المهاتفة بواسطة بروتوكول الإنترنت *(Telephony Routing over IP)*

UA وكيل المستعمل *(User Agent)*

UDP بروتوكول وحدات بيانات المستعمل *(User Datagram Protocol)*

UE تجهيز/تجهيزات المستعمل *(User Equipment)*

UICC بطاقة دارة متكاملة عامة *(Universal Integrated Circuit Card)*

UMTS شبكة الاتصالات العالمية المتنقلة (*Universal Mobile Telecommunications System*)

UNI السطح البيني من المستعمل إلى الشبكة *(User-to-Network Interface)*

URL موقع الموارد الموحَّد *(Uniform Resource Locator)*

USIM وحدة هوية عامة للمشترك *(Universal Subscriber Identity Module)*

VLAN شبكة منطقة محلية تقديرية *(Virtual LAN)*

VPN شبكة خاصة تقديرية *(Virtual Private Network)*

WLAN شبكة منطقة محلية لا سلكية *(Wireless LAN)*

xDSL خط المشترك الرقمي x *(x Digital Subscriber Line)*

5 الاصطلاحات

لا يوجد.

6 التهديدات والمخاطر المحدقة بالأمن

بخصوص التهديدات والمخاطر الأمنية المفترض أن تتعرض لها بيئة شبكات الجيل التالي (NGN)، انظر الجزء 4 من التوصية [ITU-T Y.2701].

7 نموذج للثقة في الأمن

يُعتمد اختيار أي مورّد لشبكات الجيل التالي لآليات على نموذج الثقة المطبّق. وهذه التوصية تفترض استعمال نموذج الثقة المعرَّف في [ITU-T Y.2701]. ويقدّم هذا الجزء خلاصة لنموذج الثقة في الأمن الخاص بشبكات الجيل التالي المعرَّف في [ITU-T Y.2701].

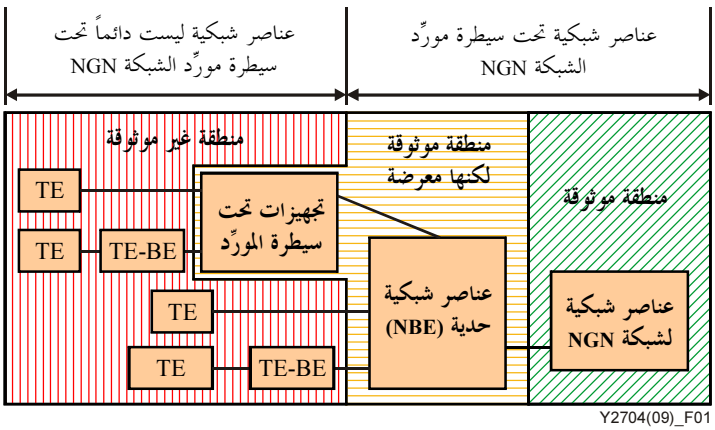
تحدد المعمارية الوظيفية لشبكات الجيل التالي كيانات وظيفية (FE). ولكن، في حين تتوقف جوانب أمن الشبكات بقدر كبير على الطريقة التي تُحزِّم بها الكيانات الوظيفية مادياً معاً، تستند معمارية أمن شبكات الجيل التالي إلى العناصر المادية للشبكة (NE) أي إلى صناديق ملموسة تحتوي على كيان وظيفي واحد أو أكثر. وتختلف الطريقة التي تُحزِّم بها هذه الكيانات الوظيفية في العناصر المادية للشبكة تبعاً لاختلاف الصانعين وموردّي الشبكات NGN.

1.7 النموذج الموثوق لشبكة منفردة

يحدد هذا الجزء الفرعي ثلاث مناطق أمن؛

1) موثوقة،
2) موثوقة لكنها معرضة،
3) غير موثوقة،

تبعاً لضبط تشغيلها ومكانها وتوصيليتها بالأجهزة/العناصر الشبكية الأخرى. وتظهر هذه المناطق الثلاث في نموذج الثقة في الأمن المبين في الشكل 1.



الشكل 1 – نموذج الثقة في الأمن/[ITU-T Y.2701]

وباختصار فإن "منطقة الأمن الموثوق لشبكة" أو "المنطقة الموثوقة" هي منطقة تقيم فيها العناصر والمنظومات الشبكية لمورِّد شبكة الجيل التالي، ولا تتصل مباشرة على الإطلاق بتجهيزات الزبون ولا بالميادين الأخرى. وتتمثل الخصائص المشتركة لعناصر شبكة NGN في هذه المنطقة في الآتي:

1) أنها تحت السيطرة الكاملة لمورّد الشبكة NGN (من منظور التزويد والصيانة والتحكم التشغيلي)؛

2) وتقع في ميدان مورد الشبكة NGN؛

3) ولا تتصل إلا بعناصر في المنطقة "الموثوقة" وبعناصر في المنطقة "الموثوقة لكن المعرضة".

ولا ينبغي اعتبار أن عنصر الشبكة آمن بحكم وجوده في منطقة موثوقة.

وتتم حماية عناصر الشبكة الموجودة في المنطقة "الموثوقة" بتوليفة من الطرائق المتنوعة. ومن الأمثلة على ذلك: الأمن المادي لعناصر شبكة الجيل التالي، وتشديد مناعة الأنظمة عموماً، واستعمال تشوير مؤمَّن، وتوفير الأمن لرسائل الإدارة، واستعمال شبكة تقديرية منفصلة (تبديل متعدد البروتوكولات بالوسم داخل شبكة بروتوكول الإنترنت(MPLS/IP)). ويُتوقع تطبيق نفس توليفة الطرائق لتأمين الاتصالات داخل المنطقة "الموثوقة" وبين عناصر شبكة الجيل التالي NGN في المنطقة "الموثوقة" والمنطقة "الموثوقة لكن المعرّضة".

وباختصار فإن "المنطقة الأمنية الموثوقة لكن المعرضة لشبكة" أو "المنطقة الموثوقة لكن المعرضة" هي منطقة تتصل فيها عناصر/أجهزة الشبكة بعناصر في منطقة "غير موثوقة" وهو ما يجعلها "معرضة". وتتصل هذه العناصر/الأجهزة، علاوةً على ذلك، بعناصر في منطقة "موثوقة". وكما هو الحال في عناصر الشبكة الموجودة في منطقة "موثوقة" يتولّى مورد شبكة الجيل التالي (NGN) التحكم في تجهيزات الشبكة، على الرغم من أن هذه التجهيزات قد تكون داخل أو خارج مقر مورد شبكة الجيل التالي. وتتمثل وظيفتها الرئيسية فيما يتعلق بالأمن في توفير الحماية لعناصر الشبكة في المنطقة الموثوقة من الهجمات الأمنية المنطلقة من المنطقة غير الموثوقة. وتوليفة الطرائق المستعملة في تأمين الاتصال بين عناصر الشبكة NGN في منطقة "موثوقة لكن معرّضة" وفي منطقة "غير موثوقة" قد تختلف عن تلك المستعملة في تأمين الاتصالات داخل منطقة "موثوقة".

والعناصر الكائنة في ميدان مورّد الشبكة NGN والممكن توصيلها بعناصر خارج المنطقة الموثوقة إنما يشار إليها على أنها عناصر حدِّية شبكية (NBE). وفيما يلي أمثلة على هذه العناصر:

- "العناصر الحديّة الشبكية (NBE)" التي على السطح البيني من المستعمل إلى الشبكة (UNI) التي توفر سطحاً بينياً مع عناصر التحكم في الخدمة أو عناصر النقل الخاصة بمورد الشبكة NGN في المنطقة الموثوقة لكي يتسنى للمستعمل/المشترك النفاذ إلى شبكة NGN للمورد والانتفاع بالخدمات و/أو النقل.
- "العناصر الحديّة للميادين (DBE)" وهي مثل العناصر الحدية للشبكة، وتختلف عنها فقط بأنها موجودة على الحدود بين الميادين.
- "العناصر الحدية الشبكية (NBE) الخاصة بتشكيل وتدميث الأجهزة (DCB-NBE)" التي تؤدي وظيفة سطح بيني مع نظام تشكيل أجهزة مورد الشبكة NGN في المنطقة الموثوقة، من أجل تشكيل أجهزة المستعمل/المشترك وتجهيزات مورد الشبكة NGN الكائنة في المنشآت الخارجية.
- "العناصر الحديّة الشبكية لوظائف التشغيل–الإدارة–الصيانة–التزويد (OAMP)" التي تعمل كسطح بيني مع الأنظمة OAMP لمورّد الشبكة NGN في المنطقة الموثوقة، من أجل تزويد وصيانة أجهزة المستعمل/المشترك وبعض تجهيزات مورد الشبكة NGN الكائنة في المنشآت الخارجية.
- "العناصر الحدية الشبكية لمخدّم التطبيق/الويب (AS/WS-NBE)" التي تؤدي وظيفة سطح بيني مع نظيره لدى مورِّد شبكة NGN في المنطقة الموثوقة، من أجل توفير النفاذ للمستعمل/المشترك إلى الخدمات القائمة على الويب.

ويبيِّن الشكل 1 العلاقة بين هذه العناصر الحدية الشبكية والعناصر الشبكية المطلوب حمايتها.

وفيما يلي أمثلة على الأجهزة/العناصر التي يشغّلها مورد لشبكة NGN لكنها لا تقع في مقر مورّد الشبكة NGN، كما أنها قد تكون أو لا تكون تحت سيطرة مورد الشبكة NGN:

- تجهيزات المنشآت الخارجية الكائنة في شبكة النفاذ/تكنولوجيا النفاذ؛
- مسيِّر محطة القاعدة (BSR)، وهو عنصر شبكي يدمج وظائف المحطة القاعدة ومراقب الشبكة الراديوية والمسيّر من أجل النفاذ اللاسلكي؛
- الوحدات الشبكية البصرية (ONU) داخل مسكن المستعمل/المشترك.

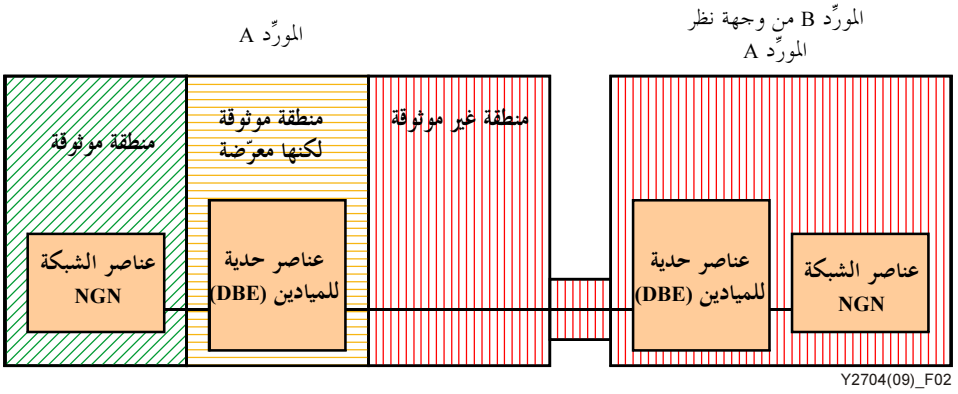
وتُوفَّر الحماية للمنطقة "الموثوقة لكن المعرضة" المشتملة على عناصر حدية شبكية، بتوليفة من الطرائق المختلفة. ومن الأمثلة على ذلك الأمن المادي لعناصر الشبكة NGN، والتعزيز العام للأنظمة، واستعمال تشوير مأمون لجميع رسائل التشوير المرسلة إلى عناصر الشبكة NGN في المنطقة "الموثوقة"، وأمن رسائل الوظائف OAMP، والمراشيح، والجدران الحامية للرزم. "المنطقة غير الموثوقة" التي تشتمل على جميع العناصر الشبكية لشبكات الزبائن أو ربما الشبكات النظيرة أو الميادين الأخرى لمورِّد الشبكة NGN، الموصولة بالعناصر الشبكية الحدية لمورِّد الشبكة NGN. وفي المنطقة "غير الموثوقة" التي تتألف من تجهيزات مطرافية قد لا يكون مورّدو الشبكات NGN هم المتحكمون في التجهيزات، وقد يكون من المستحيل فرض تنفيذ سياسة المورِّد الأمنية على المستعمل. ولا يزال من المستصوب محاولة تطبيق بعض تدابير الأمن، وتحقيقاً لهذا الغرض يوصى بتأمين التشوير، والوسائط، وعمليات التشغيل، الإدارة، الصيانة، التزويد (OAM&P)، وتعزيز العناصر الحدية للتجهيزات المطرافية TE-BE الواقعة في "المنطقة غير الموثوقة". إلا أنه بسبب الاتصال بعناصر شبكية في منطقة "غير موثوقة"، يكون الأمن أقل مما هو الحال في المنطقة "الموثوقة".

2.7 النموذج الموثوق للتوصيل بين الشبكات الأنداد

عندما يتم توصيل شبكة NGN بشبكة أخرى فإن وجود الموثوقية أو غيابها يعتمد على ما يلي:

- التوصيل البيني المادي، وهذا يمكن أن يتنوّع متمادياً من توصيل بيني مباشر في مبنى مؤمَّن إلى توصيل بين مبان منفصلة يُحتمل أن تكون غير مؤمّنة وذلك عبر مرافق مشتركة؛
- نموذج التوصيل بين الأنداد، حيث يمكن تبادل الحركة مباشرة بين مورّدي خدمات شبكات NGN أو عن طريق مورّد أو أكثر للنقل في شبكة NGN؛
- العلاقات التجارية بين الشبكات، حيث يمكن أن تظهر شروط جزائية في اتفاقات SLA (اتفاقات سوية الخدمة)، و/أو الثقة في السياسات الأمنية للمورّد الآخر للشبكة NGN؛ بوجه عام، ينبغي أن ينظر مورّدو الشبكات NGN إلى الموردين الآخرين على أنهم غير موثوقين.

ويعرض الشكل 2 مثالاً فيه شبكة موصولة تعتبر غير موثوقة.



الشكل 2 – النموذج الموثوق للتوصيل بين الشبكات الأنداد/[ITU-T Y.2701]

8 تعرف الهوية والاستيقان والتخويل

يُرجَع إلى التوصيات: [ITU-T Y.2701] و[ITU-T Y.2702] و[ITU-T Y.2703] و[ITU-T Y.2720] من أجل المعلومات عن آليات وإجراءات تعرف الهوية والاستيقان والتخويل وإدارة شؤون الهوية (IdM).

أما هذا الجزء فيصف آليات تعرف الهوية والاستيقان والتخويل المتعلقة على وجه الخصوص بالخدمات المعتمِدة على بروتوكول فتح الدورة (SIP). وتبقى الآليات المتعلقة بخدمات أخرى لدراسة لاحقة.

1.8 المشتركون

يكون طلب خدمة في إطار شبكة من الجيل التالي (NGN) متصاحباً مع المشترك. وهذا التصاحب يحدَّد خلال تعرف هوية الطلب مع المشترك. وقد يلزم تعرف هوية (تعرّفاً مصحوباً بالاستيقان)، تبعاً لاتفاق سوية الخدمة (يعني التعاقد على الخدمة) المبرم بين مورِّد شبكة الجيل التالي (NGN) والمشترك.

وهذا الإجراء يمكن تنفيذه باستعمال عنصر وظيفي يسهِّل تعرف الهوية والاستيقان بخصوص المشتركين والأجهزة والمستعملين النهائيين (يُعرف بالمستيقن). مثلاً: العناصر الحدية الشبكية (NBE) المزوَّدة بوظيفة وكيل المستعمل ظهراً لظهر (B2BUA) أو بكيان وظيفي مفوَّض للتحكم في دورة النداء (P-CSC-FE) يمكن أن تكون مستَيقِنات للمشتركين من أجل الخدمات المعتمدة على بروتوكول فتح الدورة (SIP). ويتم تعرف الهوية والاستيقان بتبادل إثباتات التفويض بين المستيقن والتجهيز الطرفي (TE) والتحقق منها.

2.8 العنصر الشبكي

توصي الوثيقة [ITU-T Y.2701] بتعرف هوية العناصر الشبكية واستيقانها من أجل الاتصالات.

إذا استلم العنصر الحدي طلباً من عنصر شبكي لشبكة من الجيل التالي (NGN) داخل المنطقة الموثوقة، أمكن اعتبار تعرّف الهوية الذي يتضمنه الطلب دقيقاً، والعدول عن التدقيق، مع التقيد بالسياسة الأمنية التي ينتهجها مورِّد الشبكة NGN.

إذا استلم العنصر الحدي طلباً من عناصر شبكية داخل المنطقة غير الموثوقة أو داخل المنطقة الموثوقة لكنها معرَّضة، يوصى بتعرّف هوية هذه العناصر الشبكية واستيقانها والتحقق من امتيازات الاتصال الخاصة بهم. وتتحقق عمليتا تعرّف الهوية والاستيقان من خلال تبادل الإثباتات والتحقق منها بين المستيقن وعنصر الشبكة.

3.8 استعمال الثبوتيات في النهج الأمني لشبكات الجيل التالي (NGN)

في النهج الأمني لشبكات NGN تُستعمَل الثبوتيات لتعرف الهوية والاستيقان بخصوص جهاز أو مشترك أو مستعمل نهائي. ويأتي وصف الثبوتيات المستخدمة في تعرّف هوية واستيقان جهاز و/أو مشترك و/أو مستعمل نهائي في الجزء 1.3.8. ويجوز أن تتخذ الثبوتيات أحد شكلين مختلفين: إما شكل الشهادات الخاصة بالمفاتيح العمومية المذكورة في التوصية X.509 (الموصوفة في الجزء 2.3.8 منها) وإما شكل مفتاح مشترك (يأتي وصفه في الجزء 3.3.8). فشهادة المفتاح العمومي المذكورة في التوصية X.509 تُستعمل لإقامة نقل مأمون بين التجهيز الطرفي والمستَيقِن (يأتي وصفه في الجزء 1.3.8) بناء على سياسة مورِّد الشبكة NGN المعيَّنة. والمفتاح المشترك يُستعمَل إما لإقامة نقل مأمون، وإما لتوليد إجابة لمستيقن/التحقق منها – أي الرد على التحدي المبتَدَر (الموصوف في الجزء 1.3.8)، وذلك بناء على سياسة مورِّد الشبكة NGN.

1.3.8 ثبوتيات الجهاز والمشترك والمستعمل النهائي

يُستعمَل في شبكات الجيل التالي (NGN) ثلاثة أنماط متميِّزة من الثبوتيات وهي:

1) ثبوتيات الجهاز؛
2) ثبوتيات المشترك؛
3) ثبوتيات المستعمل النهائي.

يجوز في إثباتات الجهاز أن يزوّده بها الصانع. مثلاً: أثناء صنع الجهاز، يدمغ فيه الصانع الثبوتيات، وهذه تتضمن معلومات مثل الرقم التسلسلي للجهاز أو معلومات الصانع. وتُعرَف هوية الجهاز من ثبوتياته. ويجوز لمورِّد شبكة NGN أن يقيم تصاحباً بين إثباتات الجهاز وخدمة مشترك معيّن تخفيفاً للحاجة إلى إثباتات مشترك. وفي مثل هذه الحالة يقام تصاحب بين الطلبات الصادرة عن الجهاز وحساب معيّن، بناء على سياسة مورِّد الشبكة NGN.

تُستعمَل إثباتات المشترك لإقامة تصاحب بين مرسل طلب في إطار شبكة NGN وحساب معيَّن. وثبوتيات المشترك هذه تُدخَل في أجهزة مهيّأة لقبولها (عن طريق التنـــزيل، مثلاً، أو بواسطة وحدة هوية المشترك (SIM)، وغير ذلك). ومتى رُكِّبت إثباتات المشترك في جهاز أقامت تصاحباً بين الجهاز والمشترك. ويتسنّى تركيب مجموعات متعددة من الثبوتيات في جهاز واحد، ففي هذه الحالة يوفّر الجهاز الوسائل لتمييز الطلبات المصاحبة لكل من المشتركين.

ملاحظة – ويُسترعى هنا الانتباه إلى أن زبون الشبكة NGN يجوز أن يكون له اشتراك واحد أو أكثر في الشبكة NGN، متصاحب مع عدد من الأجهزة يساوي صفراً أو أكثر. كما أن الاشتراك في الشبكة قد يكون مرتبطاً بمستعمل نهائي واحد أو أكثر (يعني ليس بحكم الضرورة أن يكون المستعمل النهائي هو المشترك)، قد يستعملون أجهزة مختلفة أو يتقاسمون نفس الجهاز، تبعاً لسياسة مورِّد شبكة NGN.

تُستعمَل إثباتات المستعمل النهائي لتعرّف واستيقان مستعملين طرفيين في الشبكة. مثلاً: تستطيع بطاقة SIM تعريف هوية مستعمل نهائي لخدمة ما؛ حين يُدخِل المستعمل النهائي بطاقة تعريفه (SIM) في جهاز الهاتف، يصير هذا الجهاز مصاحباً لهذا المستعمل النهائي (وتُعرَف جميع النداءات أنها صادرة عن هذا المستعمل النهائي). ولنا مثال آخر في إذنة الأمن، ويجوز في هذه أن تكون إذنة عَتادية (أي جهازاً مادياً) أو إذنة برمجية (إي برنامجاً مركّباً في جهاز متنوع الأغراض كالحاسوب الشخصي). ويزوَّد بها مستعمل مخوَّل لتعزيز عملية الاستيقان. ومن شأن إذنة الأمن أن تخزن مفاتيح تجفير، مثل التوقيع الرقمي أو معطيات القياس الحيوي كبصمة الإصبع، مثلاً. فإذا صدر طلب من جهاز داخل في شبكة NGN، يتم تعرّفه واستيقانه طلباً من المستعمل النهائي المصاحب لإذنة الأمن المعيّنة. وفي بعض الخيارات (كما هو الحال في البطاقة SIM أعلاه، مثلاً) يمكن لعدد من المستعملين النهائيين استعمال الخدمة المصاحبة لمشترك واحد (أي لحساب مشترك واحد)، فتقيَّد رسوم النداءات الصادرة عن هؤلاء المستعملين النهائيين في حساب هذا المشترك المعيّن. ومن الجائز أن يكون المشترك والمستعمل النهائي واحدا، كما يجوز أن يكون مستعملون نهائيون كثيرون تابعين لمشترك واحد. ويستطيع المستعملون النهائيون تعريف هويتهم واستيقانها لدى الشبكة لكي ينتفعوا بخدمات شخصية. فتقام لهم تصاحبات أمنية فرادية في طبقة النقل، بين التجهيزات المطرافية (TE) والشبكة NGN (أي مستَيْقِنات الشبكة)، وذلك باستعمال إثباتات المستعملين النهائيين. ولأغراض الفوترة، يقيم مورِّد الشبكة NGN تصاحباً بين إثباتات المستعملين النهائيين وخدمة مشترك معيّن.

2.3.8 اعتبار شهادات المفاتيح العمومية الموصَّفة في التوصية X.509 ثبوتيات

شهادة المفاتيح العمومية للتوصية X.509 عبارة عن وثيقة رقمية تحتوي معرِّف هوية، ونعوته، ومفتاحاً عمومياً يمتلكه الكيان، ومعلومات استيقان أخرى (كالمعلومات عن مُصدِر الشهادة، وقائمة إبطال الشهادات (CRL)، وتاريخ وساعة بدء وانتهاء صلاحية الشهادة، وغير ذلك). ويرد في الجدول 1 وصف لبعض الحقول الأساسية وبعض التحديدات في شهادة مفاتيح عمومية الشهادات الموصَّفة في التوصية [ITU-T X.509]. راجع التوصية ITU-T X.509 من أجل الوصف التفصيلي لحقول شهادات المفاتيح العمومية للتوصية X.509. وتحمل شهادة المفاتيح العمومية التوقيع الرقمي لطرف ثالث موثوق، يشار إليه عادة بصفة سلطة إصدار الشهادة (CA, Certification Authority) بالنسبة لشهادات المفاتيح العمومية. تحتسب السلطة CA دالة الفرم لجميع الحقول باستثناء *حقل قيمة التوقيع* (بأن تستعمل، مثلاً، خوارزمية تظليل مأمون، بصيغة تعديلها رقم 1 (SHA-1))، والتي يتم تشفيرها بمفتاحها الخاص، ثم تضيف التوقيع مع خوارزمية التوقيع المطبّقة إلى الشهادة (في *حقل قيمة التوقيع*).

الجدول 1 – بعض الحقول الأساسية والتمديدات لشهادة مفاتيح عمومية موصّفة في التوصية X.509

اسم الحقل	الوصف
الموضوع	يعرف هوية الكيان المصاحب لشهادة المفاتيح العمومية (لاسم المميّز في الدليل لموضوع الشهادة)
الرقم التسلسلي	معرِّف وحيد لهوية الشهادة
مُصدِر الشهادة	يعرف هوية الكيان الذي وقع وأصدر الشهادة (اسم سلطة إصدار الشهادة (CA) المميز في الدليل)
صالحة ابتداء من	تاريخ وساعة بدء صلاحية الشهادة
صالحة حتى	تاريخ وساعة انتهاء صلاحية الشهادة
المفتاح العمومي	المفتاح العمومي الذي يستعمله حامل الشهادة
الصيغة	صيغة شهادة المفاتيح العمومية المشفّرة حسب التوصية X.509
الاسم البديل للموضوع	معرِّف هوية آخر لحامل الشهادة
نقاط توزيع قائمة إبطال الشهادات (CRL)	اسم أو عنوان (URL) لقائمة إبطال الشهادات (CRL) التي وضعتها سلطة إصدار الشهادة
المنفذ إلى معلومات السلطة	موقع الموارد الموحَّد (URL) للنفاذ إلى المعلومات عن سلطة إصدار الشهادة (CA)
الاستعمال المحسَّن للمفتاح	وصف الأغراض الممكن استعمال الشهادة من أجلها (قائمة معرِّفات هوية الأشياء (OIDs) التي حددها قطاع تقييس الاتصالات أو المنظمة ISO/IEC (في التوصية [ITU-T X.660]
السياسات التطبيقية	التطبيقات والخدمات التي تُستعمل فيها الشهادة (كما تبيّنه معرِّفات هوية الأشياء (OIDs))
سياسات الشهادة	السياسات والآليات التي تستعملها سلطة إصدار الشهادة (CA) لتلقّي طلبات الشهادات، ومعالجتها، وتخويلها، وإصدارها، وإدارتها.
خوارزمية التوقيع	معرّف هوية الخوارزمية ودالة الفرم التي تستعملها سلطة إصدار الشهادة (CA) لتوقيع الشهادة (مثل SHA-1 باستعمال RSA)
قيمة التوقيع	التوقيع الفعلي للشهادة

شهادات المفاتيح العمومية الموصَّفة في التوصية [ITU-T X.509] يمكن للعناصر الشبكية في شبكات الجيل التالي (NGN) أن تستعملها لإقامة تصاحبات أمنية مع عناصر شبكية أخرى، ولتوفير أساس لتبادل تعرُّف الهوية والاستيقان. وتُستعمَل أيضاً للإغراض نفسها بين التجهيزات الطرفية والمستيْقِن.

في صدد شهادة مشترك أو شهادة مستعمل نهائي، يستعمل المستيقن *معرِّف هوية حساب المشترك* (انظر الفقرة 2.4.8)، وهو معرِّف يبحث بواسطته عن معلومات حساب المشترك، من أجل الحصول على معلومات إضافية عن الثبوتيات بواسطة الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). وفي صدد شهادة جهاز، يستعمل المستيقن اسم الصانع والرقم التسلسلي للجهاز لتحديد مصاحبه *معرِّف هوية حساب المشترك* (وهذا يكون صالحاً إذا كان أقيم تصاحب بين الجهاز والمشترك)، وعندئذ يُستعمَل *معرِّف هوية حساب المشترك* للحصول على مزيد من المعلومات عن الإثباتات خلال الكيانات الوظيفية SAA/TAA-FEs.

ويجوز أن تُستعمَل شهادات كل من المستعمل النهائي والخدمة والجهاز لإنشاء توصيلات لأمن طبقة النقل (TLS) بين الجهاز والمستيقن (انظر الفقرة 2.1.9)، أو لإنشاء توصيلات لأمن بروتوكول الإنترنت (IPsec)، من خلال استيقان تبادل مفاتيح إنترنت (IKE) (انظر الفقرة 3.4.2.9).

3.3.8 اعتبار المفاتيح المشتركة ثبوتيات

تُستعمَل المفاتيح المشتركة لتعزيز أمن النفاذ إلى شبكات الجيل التالي (NGN). وفي هذه الحالة يُعطى المشترك أو المستعمل النهائي نسخة من المفتاح المشترك، وتُخزن منه نسخة في الكيانات الوظيفية ذات الصلة، مثل الكيانات الوظيفية لخصائص

مستعملي الخدمة (SUP-FEs) أو الكيانات الوظيفية لخصائص مستعملي النقل (TUP-FEs). ويُشترط في كل مفتاح أن يكون له اسم فريد، يستعمله المستيقن للحصول على معلومات إضافية عن الثبوتيات.

في حالة استعمال مفاتيح مسبق التشارك فيها، تكون متانة النظام مرهونة بمتانة السر المشترك. والمنشود هو جعل السر المشترك في منأى عن أن يكون الحلقة الضعيفة في السلسلة الأمنية. وهذا يفترض أن السر المشترك يلزمه أن يحتوي من الإنتروبية (العشوائية) مقدار ما تحتوي منها الشفرة المستعملة. أي بعبارة أخرى، يوصى بأن يتصف السر المشترك بإنتروبية لا تقل عن 128–160 بتة.

وتجدر الإشارة إلى أن نهج المفاتيح المتناظر تختلف بعض الاختلافات مقارنة بنهج المفاتيح غير المتناظرة الموصوفة في الفقرة 2.3.8 ومن ثم ينبغي مراعاة ما يلي:

- يتعيّن أن يكون لدى أي كيان مجموعة منفصلة من المفاتيح المتناظرة مع كل شريك في الاتصالات؛
- يجب أن يتم التزويد بالمفاتيح وأن تستنبط وتخزن بطريقة مؤمّنة؛
- يجب أن يعتمد الكيان على شريكه للحفاظ على سرية المفاتيح المشتركة.

4.3.8 تزويد الكيانات الوظيفية لخصائص مستعملي الخدمة/النقل (SUP/TUP-FEs) بالمعلومات اللازمة عن كل مجموعة من الثبوتيات

الكيانات الوظيفية لخصائص مستعملي الخدمة/النقل (SUP/TUP-FEs) هي مستودعات تحتوي جميع الثبوتيات التي يلزم أن يستعملها كل من الأجهزة والمشتركين والمستعملين النهائيين للنفاذ إلى البنية التحتية لشبكة NGN. وهي تُنفَّذ نمطياً كجزء لا يتجزّأ من المستيقِن، توخياً لاستمثال معالجة طلبات الاستيقان. ولكن المستيقن قد يحتاج، حفاظاً على التنقلية، إلى استشارة مخدم بعيد للكيانات الوظيفية لاستيقان وتخويل الخدمة/النقل (SAA/TAA-FEs) من أجل الحصول على معلومات إضافية عن الثبوتيات. فيستعمل معرِّف هوية حساب المشترِك، أو اسم المفتاح من أجل الحصول على هذه المعلومات عن طريق مخدم الكيانات الوظيفية SAA/TAA-FEs.

فالمعلومات التالي ذكرها، المتعلقة بالأمن، المصاحبة لكل مجموعة من الثبوتيات، مطلوب تزويد الكيانات الوظيفية بها، مثل الكيانات الوظيفية لخصائص مستعمل الخدمة/خصائص مستعمل النقل (SUP/TUP-FEs) الخازنة للثبوتيات؛ وهذه المعلومات هي:

1) معرّف هوية حساب المشترك أو اسم المفتاح؛
2) ما إذا كان تعرّف هوية المستعمل النهائي واستيقانه مطلوبين بخصوص هذا المشترك؛
3) ما إذا كانت هذه الثبوتيات تصف مشتركاً أو مستعملاً نهائياً؛
4) القيم المسموح بها لرأسية "المرسِل" في الطلبات.

وفيما يلي عدة أمثلة على المعلومات المخزّنة في مستودعات الثبوتيات مثل الكيانات الوظيفية لخصائص مستعملي الخدمة/خصائص مستعملي النقل (SUP/TUP-FEs).

في حالة شهادة تجهيز مطرافي لشبكة NGN يعالج أربعة من خطوط الخدمة الهاتفية العادية، بواسطة الأرقام 212–555–1111–1113 و1151:

حساب المشترِك:	123-456789
رأسيات المرسِل:	sip:212-555-111[1-3]@NGN.ngn.com | sip:212-555-1151@NGN .ngn.com
سلسلة الهوية:	sip:212-555-1111@NGN .ngn.com
نمط الثبوتيات:	مشترِك
اشتراط هوية المستعمل النهائي:	لا

في حالة شهادة مشترك مخصصة للأسرة John Doe:

حساب المشترك: الأسرة Doe

رأسية المرسِل: sip:*Doe@NGN .ngn.com

سلسلة الهوية: sip:Doe@NGN.ngn.com

نمط الثبوتيات: مشترِك

اشتراط هوية المستعمل النهائي: لا

في حالة مفتاح مشترَك مخصص لأسرة John Doe:

اسم المفتاح: JohnDoe

المفتاح: dfe56131d1958046689d83306477ecc

رأسية المرسِل: sip:*Doe@NGN.ngn.com

سلسلة الهوية: sip:Doe@NGN.ngn.com

نمط الثبوتيات: مشترِك

اشتراط هوية المستعمل النهائي: لا

في حالة عنصر حدي لتجهيزات مطرافية (TE-BE) قائمة بخدمة شركة Acme Widget Company:

حساب المشترِك: Acme Widget Company

رأسية المرسِل: sip:*@acme.com

سلسلة الهوية: sip:acme.com

نمط الثبوتيات: مشترِك

اشتراط هوية المستعمل النهائي: لا

في حالة مستعمل نهائي داخل الشركة Acme Widget Company:

حساب المشترِك: Acme Widget Company

رأسية المرسِل: sip:bob@acme.com

سلسلة الهوية: sip:bob@acme.com

نمط الثبوتيات: مستعمل نهائي

4.8 تعرُّف واستيقان المشتركين

1.4.8 الاستراتيجية العامة

في بروتوكول فتح الدورة (SIP) تكون هوية المرسل محتواة في رأسية "المرسل". لكنّ تعرف هوية المشترك باستعمال رأسية "المرسل" في طلب ضمن إطار بروتوكول فتح الدورة (SIP) يتعرَّض لهجمات خداعية، ولذا فإنه لا يعوَّل عليه حين يقتضي الأمر سويّة عالية من الضمان لتعرّف هوية المشترك. فيجري، بدلاً من ذلك، مقارنة قيمة رأسية "المرسل" بهوية المشترك المحصَّلة بوسائل أخرى.

فتوخّياً لتقليل الأثر على مهلة إقامة النداء إلى أدنى حد ممكن، يُعمد، كلما أمكن، إلى اشتقاق تعرّف هوية المشترك واستيقانه من العنوان الأصلي الشبكي (العنوان الأصلي في رأسية الرزم في بروتوكول الإنترنت (IP)) أو من التصاحب الأمني للنقل (تصاحب يقيمه مثلاً أمن بروتوكول الإنترنت (IPsec) أو أمن طبقة النقل (TLS) بين الجهاز المصدر والمستيقِن). وإذا

لم تُسفِر هذه التقنيات عن تعرُّف هوية متسق مع رأسية "المرسل" في طلب بروتوكول فتح الدورة (SIP)، يوجَّه تحدٍّ إلى المرسِل؛ فإذا احتوى الرد على الثبوتيات الصحيحة، يأخذ الطلب مجراه. ويأتي في الفقرات التالية وصف هذه الإجراءات بمزيد من التفصيل.

فالإجراءات الموصوفة في الفقرة 2.4.8 تبيّن كيف يبتّ المستيقِن، بناءً على العنوان الأصلي الشبكي، في أحد الأمور التالية:

1) إما أنه لا يمكن تعرّف المشترك بهذه الطريقة،
2) وإما أن المشترك تم تعرّفه وهو متوائم مع رأسية "المرسل" الواردة في الطلب،
3) وإما أن المشترك تم تعرّفه لكنه مختلف عما تتضمنه رأسية "المرسل" الواردة في الطلب.

والإجراءات الموصوفة في الفقرة 3.4.8 تبيّن كيف يبتّ المستيقِن، بناءً على تصاحب أمن طبقة النقل (TLS) في أحد الأمور التالية:

1) إما أنه لا يمكن تعرّف المشترك بهذه الطريقة،
2) وإما أن المشترك تم تعرّفه وهو متوائم مع رأسية "المرسل" الواردة في الطلب،
3) وإما أن المشترك تم تعرّفه لكنه مختلف عما تتضمنه رأسية "المرسل" الواردة في الطلب.

وعندئذ يتخذ المستيقِن التدابير المبيّنة في الجدول 2:

الجدول 2 – تدابير المستيقِن في صدد كل نتيجة استيقان

تعرّف المشترك بناءً على العنوان الأصلي	تعرّف المشترك بناءً على تصاحب أمن طبقة النقل	تدابير المستيقن
لا ينطبق	لا ينطبق	إصدار التحدي/وانتظار الإجابة
لا ينطبق	موائم	موافقة
لا ينطبق	مختلف	إصدار التحدي/وانتظار الإجابة
موائم	لا ينطبق	موافقة
موائم	موائم	موافقة
موائم	مختلف	استعمال هوية المشترك الواردة في العنوان الأصلي الشبكي
مختلف	لا ينطبق	إصدار التحدي/وانتظار الإجابة
مختلف	موائم	استعمال هوية المشترك الواردة في تصاحب أمن طبقة النقل
مختلف	مختلف	إصدار التحدي/وانتظار الإجابة

إذا كان التدبير الحاصل هو إصدار التحدي/وانتظار الإجابة، تُتّبع الإجراءات المبيّنة في الجزء 4.4.8.

عدا الاستراتيجية الموصوفة في الفقرات من 2.4.8 إلى 4.4.8، يمكن أيضاً استعمال معمارية التمهيد التنوعية (GBA, Generic Bootstrapping Architecture) من أجل تعرف هوية المشتركين واستيقاهم. ويأتي وصفها في الفقرة 5.4.8.

إن استراتيجيات الاستيقان الموصوفة في هذه التوصية أمثلة نمطية، ويجوز لكل مورِّد شبكة NGN أن ينتقي أياً منها ومن غيرها لاستعماله (كأن يستعمل إجراءً واحداً مما يأتي وصفه في المقاطع التالية).

2.4.8 تعرف هوية المشترك من العنوان الأصلي الشبكي

أبسط أشكال تعرف هوية المشترك يستند فقط إلى العنوان الأصلي الشبكي الموفَّر في رُزم البروتوكول IP. ويقوم ذلك على أن يراجع المستيقن تقابلاً مسبقاً تزويده بين سلاسل العنوان في IP وسلاسل *معرِّف هوية حساب المشترك*، فإذا وجد المستيقن العنوان الأصلي في إحدى هذه السلاسل، اعتبر الطلب صادراً عن المشترك. وعندئذ يُستعمَل *معرِّف هوية حساب المشترك* للحصول على إثباتات المشترك عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE)، ثم تدقيق التوافق مع قيمة رأسية "المرسل".

فإذا توافقت قيمة رأسية "المرسل" مع المشترك، اعتُبرت الحالة "موائمة"؛ وإذا لم تتوافق قيمة رأسية "المرسل" مع المشترك، اعتُبرت الحالة "مختلفة"؛ وإذا كان العنوان الأصلي في البروتوكول IP غير موجود في أي من سلاسل العنوان المسبق تزويدها، اعتُبرت الحالة "غير منطبقة" (N/A).

قوة هذه الطريقة لتعرف المشترك مرهونة بتزويد ضمانة العنوان الأصلي مسبقاً. وتزويد ضمانة العنوان الأصلي يعني أن العنوان المودع في البروتوكول IP لا يستطيع أحد أن يستعمله غير المشترك الشرعي الذي خُصص له هذا العنوان. ولا بد لتحقيق ذلك من استعمال الآليتَيْن التالي بيانهما في معالجة النقل أو في الكيان الوظيفي للتحكم بالنقل، ويجب فيهما أن تكونا متناسقتين حق التناسق: 1) الإدارة الصارمة للتقابل بين المشترك والعنوان المخصص له، و2) منع الخديعة في العنوان على أساس تحصيل هذه المعلومات. انظر الأمثلة الواردة في التذييل I، على الآليتين المتقدم ذكرهما وعلى التنسيق بينهما.

3.4.8 تعرف هوية المشترك من التصاحب الأمني لطبقة النقل/أمن البروتوكول IP

إذا كان أقيم نقل مأمون في أمن طبقة النقل (TLS) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل شهادة العنصر الحدي للتجهيزات المطرافية (TE-BE) كما هي موصَّفة في التوصية X.509 (انظر الفقرة 2.3.8)، فعندئذ يدقق المستيقن ما إذا كانت رأسية "المرسل" متسقة مع القيم المسموح بها للمشترك المعرَّفة هويته في *معرِّف حساب المشترك* (<Subscriber Account Identifier>).

وإذا كان أُقيم نقل مأمون (إما في أمن بروتوكول الإنترنت (IPsec) وإما في أمن طبقة النقل (TLS)) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل شهادة التجهيز المطرافي لشبكة الجيل التالي (TE NGN) كما هي موصَّفة في التوصية X.509 (انظر الفقرتين 1.3.8 و2.3.8)، فعندئذ يستعمل المستيقن رقم الصانع والرقم التسلسلي للجهاز للتحقق من *معرِّف هوية حساب المشترك* المصاحب لهما (ولا تصلح هذه الطريقة إلا إذا كان أقيم تصاحب بين الجهاز والمشترك). ثم يُستعمل *معرِّف هوية حساب المشترك* (<Subscriber Account Identifier>) للحصول على إثباتات المشترك، ويُدقق في اتساق هذه الثبوتيات مع قيمة رأسية "المرسل".

وإذا كان أقيم نقل مأمون (إما في أمن بروتوكول الإنترنت (IPsec) وإما في أمن طبقة النقل (TLS)) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل شهادة المشترك في الجهاز المطرافي لشبكة الجيل التالي (TE NGN) كما هي موصَّفة في التوصية X.509 (انظر الفقرتين 1.3.8 و2.3.8)، فعندئذ يستعمل المستيقن *معرِّف هوية حساب المشترك* للحصول على إثباتات المشترك عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). ثم يُدقق المستيقن في اتساق هذه الثبوتيات مع قيمة رأسية "المرسل".

وإذا كان أقيم نقل مأمون (إما في أمن بروتوكول الإنترنت (IPsec) وإما في أمن طبقة النقل (TLS)) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل شهادة المستعمل النهائي للتجهيز المطرافي لشبكة الجيل التالي (TE NGN) كما هي موصَّفة في التوصية X.509 (انظر الفقرتين 1.3.8 و2.3.8)، فعندئذ يستعمل المستيقن *معرِّف هوية حساب المشترك* (<Subscriber Account Identifier>) للحصول على إثباتات المشترك عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). ثم يُدقق المستيقن في اتساق هذه الثبوتيات مع قيمة رأسية "المرسل".

وإذا كان أقيم نقل مأمون (إما في أمن بروتوكول الإنترنت (IPsec) وإما في أمن طبقة النقل (TLS)) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل مفتاح مشترك مسبق (انظر الفقرة 1.3.4.2.9)، فعندئذ يستعمل المستيقن اسم المفتاح للحصول على إثباتات المشترك عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). ثم يُدقق المستيقن في اتساق هذه الثبوتيات مع قيمة رأسية "المرسل".

أما إذا لم يكن قائماً نقل مأمون بين الجهاز المُصدِر والمستيْقِن، أو كان توصيل "زبون غُفْل" هو المستعمَل في التوصيل بأمن طبقة النقل (TLS)، فعندئذ "لا تنطبق" هذه الطريقة.

4.4.8 تعرف هوية المشترك بطريقة التحدي والرد

طريقة التحدي والرد هي صيغة أوفر أمناً من الخطة القديمة القائمة على هوية المستعمل/كلمة السر (يعني إرسال تعريف هوية المستعمل وكلمة السر كجزء من طلب الخدمة، طريقة لازمتها مشكلة سهولة استعمالها للحصول على الخدمة احتيالاً). أما في طريقة التحدي والرد فإن المخدم يرسل تحدياً إلى الزبون، طالباً منه تأدية مهمة ما تجفيرية، باستعمال مفتاح مشترك. ويكون الرد متضمناً نتيجة الحساب، ويتحقق المخدم من صحة النتيجة. وفيما لو التقط آخرون اعتراضياً هذا التبادل، لا يمكن إعادة تنفيذه، لأن المخدم لا يكرر أبداً استعمال تحدٍّ سابق.

وهناك نمط هام من أنماط طريقة التحدي والرد، يجمع بين يُسْر طرائق الاستيقان المبنية على كلمة السر وأمن الطرائق المبنية على خطة التحدي والرد. وهذا النمط الهام يتمثل في بروتوكول تبادل المفتاح المستَيْقَن لكلمة السر (PAK, Password Authenticated Key). فبروتوكول تبادل PAK هذا يضمن الاستيقان المتبادل لكلا الطرفين في فعل إقامة مفتاح تجفيري تناظري عبر ما يُعرف بتبادل Diffie-Hellman. إن استعمال تبادل Diffie-Hellman يضمن *تمام السرية في الاتجاه الأمامي* – وهذه خاصة بروتوكول إقامة مفتاح يضمن أن افتضاح مفتاح دورة ما أو الافتضاح على أثر دورة ما لمفتاح خاص طال استعماله لن يسبب افتضاح أي دورة سابقة. ثم إن طريقة الاستيقان بتبادل PAK تحمي التبادل من هجمات مَنْ يكون بين الطرفين. ففي هذه الحالة يعتمد الاستيقان على سر مشترك ومحميّ (يعني يُستبقى غير مباح) من التنصّت الخفي بحيث يدرأ الهجوم القاموسي من خارج الخط. وهكذا فإن البروتوكول المذكور يمكن استعماله في تطبيقات شتى كلما وُجد سر مشترك مبني على كلمة سر قد تكون ضعيفة. وتوصيف البروتوكول PAK وارد في الوثيقتين [ITU-T X.1035] و[b-TIA 683-D].

وينطوي تبادل التحدي والرد على تبادل رسالة أخرى بين المستيقِن والنقطة الطرفية المُصدِرة، وعلى عملية حساب تنفّذها النقطة الطرفية المُصدِرة. ومن ثَمّ فهو يؤثر على المهلة التي يحسّ بها المستعمل. ولذا فمن أهداف أمن شبكات الجيل التالي (NGN) قَصْر استعمال طريقة التحدي والرد على حالات الضرورة المطلقة، التي تستلزم تحقيق السوية الضرورية من حيث تعرف الهوية والاستيقان.

فإذا كان أقيم نقلٌ مأمون (إما في أمن بروتوكول الإنترنت (IPsec) وإما في أمن طبقة النقل (TLS)) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم بنجاح على يد المستيقِن استيقان طلب سابق في غضون الفترة الزمنية التشكيلية، بالمقارنة مع نفس محتوى رأسية "المرسل"، فعندئذ يُعتبَر الاستيقان حاصلاً ويُقبَل الطلب. وفي حالة تشوير إقامة النداء، على اعتبار أن الطلب الأول النمطي عبر توصيل جديد هو "سجل"، تُجرى عملية التحدي/الرد هذه في وقت لا يؤثر على مهلة إقامة النداء.

وبما أن طلبات الاستيقان حوسبتها كثيفة جداً، فمن الأمور الأساسية أن يقلل المستيقن تواتر الطلبات الموجَّهة إلى الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو إلى الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). والحدود الموضوعة لذلك في هذه الفقرة يصلح اتّباعها، سواء كان كل من هذين الكيانين جزءاً لا يتجزّأ من المستيقِن أو عنصراً منفصلاً عنه. ويتمثل شكل بسيط للعدوان برفض الخدمة من جانب وحدة طرفية في إغراق المستيقن بطلبات غير صالحة يتطلب كل منها حساباً تجفيرياً في الكيان SAA-FE أو الكيان TAA-FE – بحيث يُعاق المستيقن عن الاهتمام بكل الطلبات (الصالحة وغير الصالحة). ولصدّ هذه الهجمات، يستطيع المستيقِن محلياً أن يرفض طلباً إذا كان يشتمل على طلب تخويل معلق صادر عن نفس النقطة الطرفية. ولإجراء الصدّ هذا صيغة أخرى أكثر تعقيداً بقليل، تقوم على أن يرفض المستيقن محلياً الطلب بعدما يتسلم ما لا يقل مجموعه عن XXX طلب في غضون الثواني الـ YYY الأخيرة (وتشكّل قيم XXX وYYY في المستيقِن). ويجوز بالإضافة إلى ذلك أن يتلكّأ المستيقن عن عمد فترةً من الزمن، يمكن تشكيلها فيه، قبل أن يستجيب لطلب تخويل فاشل. وهذا الإجراء يمنع أيضاً أنواعاً شتى من الهجمات بـ "كسر كلمة السر".

1.4.4.8 طريقة التحدي والرد في حالة استعمال الجهاز المُصدِر بروتوكول فتح الدورة (SIP)

إذا كان الجهاز المُصدِر قائماً باستعمال بروتوكول تشوير فتح الدورة (SIP)، يمكن أن تُستعمَل اختيارياً آليات الاستيقان بالتفويض المعرَّفة في المعيار [b-IETF RFC 3261]، من أجل تنفيذ طريقة التحدي والرد. انظر الجزء 2.22 من المعيار [b-IETF RFC 3261] والجزء 3 من المعيار [b-IETR RFC 2617] والجزء 3 من المعيار [b-IETF RFC 3310].

يستجيب المستيقن لطلب بروتوكول SIP بالرد رقم 407 (مطلوب الاستيقان بالتفويض). ويضمِّن ردَّه هذا رأسيةَ استيقان بالتفويض تحتوي ما يلي: خطة استيقان "Digest"، وميدان "NGN.ngn.net"، وجودة الحماية (qop) لـ "auth"، وقيمة ظرفية، عشوائية التجفير، طولها 16 أثمونا (بنسق ستة عشري)، واختيارياً قيمة معلمة "Opaque"، وخوارزمية 5 لخلاصة رسالة ("MD5") أو خوارزمية "AKAv1-MD5"، تبعاً لاتفاق الخدمة المبرم مع الزبون.

ومن الأمثلة على رأسية الاستيقان بالتفويض في الرد رقم 407 ما يلي:

استيقان بالتفويض (**Proxy-Authenticate**): **Digest realm="NGN.ngn.com", qop="auth", nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5**

ويرد الجهاز المُصدِر على الاستجابة 407 بطلب معاد توليده، يحتوي رأسية استيقان بالتفويض. ويتحقق المستيقن من أن هذه الرأسية تحتوي المعلومات التالية: خطة استيقان "Digest"، وميداناً (Realm) هو نفس ميدان الاستجابة 407، وقيمة ظرفية هي نفس القيمة الظرفية في الاستجابة 407، وقيمة معلمة "Opaque" هي نفس قيمة معلمة "Opaque" التي في الاستجابة 407. وبالإضافة إلى ذلك تتضمن رأسية الاستيقان بالتفويض معلمة "Username" (اسم المستعمِل) التي تعطي الاسم المفتاحي، ومعلمة "Uri" موائمة لمعلمة Request-URI التي في الطلب، وأخيراً معلمة "Response" وهي دالة التظليل الموصَّفة في المعيار [b-IETF RFC 2617] أو المعيار [b-IETF RFC 3310].

ومن الأمثلة على رأسية التخويل بالتفويض في طلب معاد إصداره ما يلي:

تخويل بالتفويض (**Proxy-Authorization**): **Proxy-Authorization: Digest username="bob", realm="NGN.ngn.com", nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:5551212@ngn.com", response="dfe56131d1958046689d83306477ecc"**

ويمكن أن تُستعمَل أيضاً آليات الاستيقان من مستعمل إلى مستعمل، المعرَّفة في المعيار [b-IETF RFC 3261]، من أجل تنفيذ طريقة التحدي والرد. انظر التفاصيل في الجزء 2.22 من المعيار [b-IETF RFC 3261] والجزء 3 من المعيار [b-IETF RFC 2617] والجزء 3 من المعيار [b-IETF RFC 3310].

وفي حالة تشعب الطلب، قد يرغب عناصر شبكية مختلفة لشبكة الجيل التالي (NGN NEs) (مثل الكيان الوظيفي–مراقب البوابة الوسائطية) و/أو تجهيزات مطرافية (TEs) في ممارسة طريقة التحدي تجاه الجهاز المُصدِر. وعندئذ يجمّع الكيان الوظيفي (NE) المتشعب (مثل S-CSC-FE: الكيان الوظيفي القائم بخدمة التحكم في دورة النداء) هذه التحديات ويضعها في استجابة واحدة ويرسلها إلى الجهاز المُصدِر. ومتى استلم الجهاز المُصدِر الرد المتضمن تحديات متعددة، يولّد طلباً جديداً يضمّنه إثباتات متعددة ويقدمه.

2.4.4.8 طريقة التحدي والرد في حالة استعمال الجهاز المُصدِر بروتوكولاً غير SIP

إذا كان الجهاز المُصدِر يتوقَّع منه استعمال البروتوكول SIP، لكنه يصدر طلبه باستعمال بروتوكول تشوير غير SIP، فعندئذ يُعتبَر أن طريقة التحدي والرد أخفقت. فيُرفَض الطلب.

5.4.8 معمارية التمهيد التنوعية (GBA, *Generic Bootstrapping Architecture*)

تحدد معمارية التمهيد التنوعية (GBA) إجراءً مستقلاً عن النفاذ. إنها توفر إطاراً لاستيقان متبادل بين المستعملين النهائيين، ووظيفة تطبيقية شبكية (NAF, *Network Application Function*) يمكن استعمالها لتعرف هوية المشتركين في شبكات NGN واستيقانهم. راجع المعيار [b-ETSI TS 133220] للوقوف على مزيد من المعلومات عن المعمارية GBA.

5.8 تعرُّف واستيقان المستعملين النهائيين

1.5.8 الاستراتيجية العامة

في حين يلزم تعرف هوية المشترك لزوماً حتمياً للبنية التحتية لشبكات الجيل التالي (NGN)، يبقى تعرف هوية المستعمل النهائي خدمة اختيارية يجوز للمشترك أن يطلبها. ويكون هذا الطلب عادة من أجل توفير خدمات إضافية، مثل التنقلية

الشخصية والحضور الشخصي، حيث تكون هوية المستعمل الطالب ضرورية لتأدية الخدمة. فإذا كان المشترك يرغب في هذه السوية الإضافية من تعرف الهوية، يلزمه أن تكون جميع أجهزة النقاط الطرفية ذات مقدرة لإدخال إثباتات إضافية للمستعملين النهائيين أو أن تستعمل شهادة المستعمل النهائي بدلاً من شهادة المشترك.

وأمام المستيقن طريقتان لتعرف هوية المستعمل النهائي واستيقانه. الأولى عن طريق التصاحب الأمني لسوية النقل المستعمَل لتبادل التشوير. فإذا كان هذا التصاحب الأمني قائماً مع شهادة المستعمل النهائي (أو كان مفتاح مشترك متصاحباً مع مستعمل نهائي واحد)، فعندئذ يكون تعرف هوية المستعمل النهائي كاملاً. والطريقة الأخرى هي تبادل التحدي والرد، حيث يكون اسم المفتاح المعطى في الرد متصاحباً مع مستعمل نهائي واحد. ويأتي وصف هاتين الطريقتين بإسهاب في الفقرات التالية.

يجوز في الأجهزة المتطورة لشبكات NGN تعدد الهويات، أي شهادة مشترك وشهادة أو شهادات لمستعملين نهائيين، من أجل الأشخاص الذين يستعملون الجهاز. ومن شأن هذه الأجهزة إنشاء توصيلات لأمن طبقة النقل (TLS) متعددة مع المستيقن، توصيلاً مستقلاً من أجل كل شهادة. ثم يوجه الجهاز طلبات إلى المستيقن عبر التوصيل التشويري المناسب، بناءً على الهوية المرغوبة للنداء.

ومما يثير الاهتمام إثباتات المستعمل الواحد التي تظل صالحة بعد "مغادرة" هذا المستعمِل. إذا كان التصاحب الأمني للنقل مبنياً على شهادة مستعمل نهائي، يجوز للمشترك أن يطلب استمرار النشاط لاستبقاء صلاحية الاستيقان. وإذا لم يستمر هذا النشاط يُغلق المستيقن التوصيل الخاص بالنقل المأمون، ويتطلب من الجهاز المُصدِر أن يقيمه من جديد بخصوص شهادة المستعمل النهائي الحالي (أو شهادة المشترك أو شهادة الجهاز في حالة عدم تيسّر شهادة مستعمل نهائي). ويأتي بيان مفصّل عن المتطلبات المتعلقة بهذا التصرف من المستيقن في المقطعين 2.1.9 و1.3.4.2.9، وهي تعتمد على مؤقِّتَيْن: أحدهما يحدد مقدار الوقت الذي يمكن أن تبقى فيه إثباتات المستعمل النهائي صالحة لتصاحب أمني، والآخر يحدد مدة الشغور بين طلبين متتاليين. أما قيم انقضاء المهلة فيجوز أن يضعها المشترك أو المستعمل النهائي، ولكن يجب أن تظل محدودة بالقيم القصوى التي يضعها مورِّد خدمة الشبكة NGN.

2.5.8 تعرّف هوية المستعمل النهائي من التصاحب الأمني TLS/IPsec

إذا كان أقيم نقل مأمون في أمن طبقة النقل (TLS) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل شهادة العنصر الحدي للتجهيزات المطرافية (TE-BE) كما هي موصَّفة في التوصية X.509 (انظر الفقرة 6.8)، فعندئذ يدقق المستيقن ما إذا كانت رأسية "المرسل" متسقة مع القيم المسموح بها للمشترك المعرَّفة هويته في *معرِّف حساب المشترك* (<Subscriber Account Identifier>) الذي تتضمنه الشهادة.

وإذا كان أقيم نقل مأمون (إما في أمن بروتوكول الإنترنت (IPsec) وإما في أمن طبقة النقل (TLS)) لحركة التشوير بين الجهاز المُصدِر والمستيْقِن، وتم استيقان النقل المأمون بفضل شهادة المستعمل النهائي للتجهيز المطرافي لشبكة الجيل التالي (TE NGN) كما هي موصَّفة في التوصية X.509 (انظر الفقرة 6.8)، فعندئذ يستعمل المستيقن *معرِّف هوية حساب المشترك* للحصول على إثباتات المشترك عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). ثم يُدقق المستيقن في اتساق هذه الثبوتيات مع قيمة رأسية "المرسل". وإذا كان أقيم في أمن بروتوكول الإنترنت (IPsec) نقل مأمون لحركة التشوير بين الجهاز المُصدِر والمستيْقِن (انظر الفقرة 4.4.8)، وتم استيقان النقل المأمون بفضل مفتاح مسبق التشارك فيه (انظر الفقرة 1.3.4.2.9)، فعندئذ يستعمل المستيقن اسم المفتاح للحصول على إثباتات المشترك عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). ثم يُدقق المستيقن في اتساق هذه الثبوتيات مع قيمة رأسية "المرسل". وهذا هو تعرف هوية المستعمل النهائي بطريقة التحدي والرد.

3.5.8 التعرّف على هوية المستعمِل النهائي من خلال التحدي والردّ

وإجراءات طريقة التحدي والرد بخصوص تعرف هوية المستعمل النهائي مماثلة لإجراءات تعرف هوية المشترك المذكورة في الفقرة 4.4.8.

والتمديد الوحيد هو أن المستيقن يدقق المعلومات المسترَدَّة عن طريق الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو طريق الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE)، بخصوص اسم المفتاح ولا سيما الدلالة على تصاحب المفتاح مع هوية المستعمل النهائي. فإذا تطابقت يكون تعرف هوية المستعمل النهائي قد تم بنجاح.

وإذا سبق للمستيقن أن نفّذ إجراء تحدّ ورد لتعرف هوية المشترك، و لم يمكن تعرّف هوية مستعمل نهائي من المفتاح المسمّى المعاد في الرد، فعندئذ يكون تعرف هوية المستعمل النهائي قد فشل. أما إذا كان إجراء التحدي والرد غير لازم لتعرف هوية المشترك، فعندئذ يُصدَر تحدٍّ.

6.8 التعرُّف والاستيقان بواسطة العنصر الحدي للتجهيزات المطرافية (TE-BE)

إن إجراءات التعرف والاستيقان بواسطة العنصر الحدي للتجهيزات المطرافية (TE-BE) مماثلة للإجراءات التي ينفِّذها المستيقن، ولا تختلف عنها إلا بأمرين:

1) يجوز في العنصر الحدي للتجهيزات المطرافية (TE-BE) تزويده بجميع الثبوتيات اللازمة لتعرف هوية واستيقان من يخدمهم من مشترك (مشتركين) ومستعملين نهائيين، على اعتبار أن ليس له نفاذ إلى الوظيفة الموزعة على الكيانين الوظيفيين SAA/TAA-FEs المتيسِّرة للمستيقن.
2) الطلب المعاد إصداره رداً على التحدي من جانب المستيقن، طلب يحتوي رأسية "التخويل بالتفويض"، يُمرر إلى المستيقن ولا يعالَج في العنصر TE-BE.

1.6.8 استعمال الشهادات الموصَّفة في التوصية X.509

يوجد تصاحب أمني بين كل عنصر حدي لتجهيزات مطرافية (TE-BE) وواحد على الأقل من العناصر الشبكية الحدية، تمّت إقامته بموجب شهادة X.509 سبق إصدارها إلى العنصر TE-BE. والطلبات التي يتلقاها العنصر NBE تخضع لإجراءات التعرف والاستيقان المعروضة في الفقرة 3.4.8 التي تقتصر على حد أدنى من التحقق والتعرف يضطلع به العنصر TE-BE. وفي حال لزم تنفيذ إجراء التحدي والرد (كما في حالة مستعمل "متجوِّل"، مثلاً)، يجري التبادل بين النقطة الطرفية المصدر والعنصر NBE، ويمرَّر مروراً شفافاً بالعنصر TE-BE.

أما النقل المأمون بين النقطة الطرفية والعنصر TE-BE فهو شيء اختياري. ومن المعلوم سلفاً أن العنوان الأصلي الشبكي سيعرّف بصورة وافية هوية معظم الطلبات.

والنقاط الطرفية تسجل لدى العنصر الحدي الشبكي (NBE) عن طريق العنصر الحدي للتجهيزات المطرافية (TE-BE).

7.8 السطح البيني للمستيقن والكيانين الوظيفيين SAA/TAA

1.7.8 استعمال بروتوكول RADIUS (بروتوكول خدمة الاستيقان عن بعد للمستعملين الداخلين) وتمديداته

في البنية التحتية لشبكات الجيل التالي (NGN) تحتوي الكيانات الوظيفية لاستيقان وتخويل الخدمة/النقل (SAA/TAA-FE) نقطة القرار، والكيانات الوظيفية لخصائص مستعمل الخدمة/مستعمل النقل (SUP/TUP-FE) هي مستودعات تخزين جميع إثباتات المستعمل النهائي والجهاز. ومن الجائز توزيع بعض وظائف الكيانات SAA/TAA-FE، كوظيفة الاستيقان مثلاً، من أجل استمثال الأداء في استيقان الطلبات.

وقد شاع استعمال خيارين متنافسين بخصوص بروتوكول الاتصال بين المستيقن والكيانات الوظيفية لاستيقان وتخويل الخدمة/النقل (SAA/TAA-FE)، وهما البروتوكول RADIUS المعرَّف في المعيار [b-IETF RFC 2865] (المعروف جيداً وتأديته مستطاعة جيداً)، والبروتوكول Diameter المعرَّف في المعيار [b-IETF RFC 3588] (من أجل تعويض عدد من أوجه القصور في RADIUS). ومن الأهداف المحتملة للبنية التحتية للشبكات NGN الانتقال إلى البروتوكول Diameter. ولكن من المعترف به أن الصيغ الحالية لتنفيذ الخواديم مبنية على RADIUS، ثم إنه تم وضع تمديدات مخصصة كثيرة للبروتوكول الأساسي RADIUS من أجل تلبية احتياجات وظيفة الاستيقان هذه. ولكن، على الرغم من كون الإصدار الحالي لهذه

التوصية مبنياً على RADIUS مع تمديده المعرَّف في المعيار [b-IETF RFC 5090]، فمن الراجح في الصيغة التي تُصدر مستقبلاً لهذه التوصية أن يُغيَّر هذا السطح البيني ويُبنى على البروتوكول Diameter مع تمديده المعرَّف في المعيار [b-IETF RFC 4740].

في حالة استعمال بروتوكول RADIUS يصير المستيقن زبوناً لـ RADIUS، ويصير مخدم الكيانات الوظيفية SAA/TAA-FE مخدماً لـ RADIUS كما هو معرَّف في الوثيقة [b-RFC 2865]. ويجوز في كلا الزبونين تنفيذ التمديدات الخاصة باستيقان SIP Digest، كما هو معرَّف في الوثيقة [b-RFC 5090]. ومن الجائز أيضاً في التوصيل بين المستيقِن ومخدم الكيانات الوظيفية SAA/TAA-FE تأمينه بفضل أمن بروتوكول الإنترنت (IPsec) بالاستيقان المتبادل.

في حالة تنفيذ التمديدات المعرَّفة في [b-RFC 4590]، يوجّه المستيقن بموجب البروتوكول RADIUS طلباً يضمِّنه المعلومات التي تحتويها رأسية الاستيقان بالتفويض؛ فيحسب مخدم RADIUS الجواب المنتظر ويرسله جواباً إلى المستيقن. وعندئذ يقارن المستيقن الجواب الفعلي الواصل من النقطة الطرفية بالجواب المنتظر، ويُقِرّ صلاحية الطلب.

وها هو مثال على الرسالة الموجَّهة من المستيقن إلى مخدم الكيانات SAA/TAA-FE:

```
Code = 1 (Access-Request)
      Identifier = 1
      Length = 164
      Authenticator = 56 7b e6 9a 8e 43 cf b6 fb a6 c0 f0 9a 92 6f 0e
      Attributes:
      NAS-IP-Address = d5 89 45 26 (213.137.69.38)
      NAS-Port-Type = 5 (Virtual)
      User-Name = "bob"
      Digest-Response (206) = "2ae133421cda65d67dc50d13ba0eb9bc"
      Digest-Attributes (207) = [Realm (1) = "NGN .ngn.com"]
      Digest-Attributes (207) = [Nonce (2) = " ea9c8e88df84f1cec4341ae6cbe5a359
"]
      Digest-Attributes (207) = [Method (3) = "INVITE"]
      Digest-Attributes (207) = [URI (4) = " sip:5551212@ngn.com "]
      Digest-Attributes (207) = [Algorithm (5) = "md5"]
      Digest-Attributes (207) = [User-Name (10) = "bob"]
```

ومثال على الجواب المرسَل من مخدم الكيانات **SAA/TAA-FE** إلى المستيقن:

```
Code = 2 (Access-Accept)
      Identifier = 1
      Length = 20
      Authenticator = 6d 76 53 ce aa 07 9a f7 ac b4 b0 e2 96 2f c4 0d
      Attributes:
      Digest-Response (206) = "dfe56131d1958046689d83306477ecc"
```

2.7.8 التصاحب الأمني لتشوير النقل

في حالة استعمال شهادة طبقاً لتوصيف التوصية X.509، في إقامة تصاحب أمني لتشوير النقل، تقوم الكيانات الوظيفية لخصائص مستعمل الخدمة/ مستعمل النقل (SUP/TUP-FEs) بتخزين مجموعة من رأسيات "المرسل" المقبولة (مفهرسة بحسب *معرِّف هوية حساب المشترك*) الجائز ورودها في طلبات من ذلك المصدر، ثم تقابَل هذه الرأسيات مع رأسية "المرسل" الواردة في الطلب المعيّن.

وإذا استُعمل مفتاح مسبق التشارك فيه لإقامة تصاحب أمني لتشوير النقل (مثل مزوِّد خدمة تبادل بين أنداد)، تقوم الكيانات الوظيفية لخصائص مستعمل الخدمة/مستعمل النقل (SUP/TUP-FEs) بتخزين مجموعة من رأسيات "المرسل" المقبولة (مفهرسة بحسب اسم المفتاح) الجائز ورودها في طلبات من ذلك المصدر، ثم تقابَل هذه الرأسيات مع رأسية "المرسل" الواردة في الطلب المعيّن.

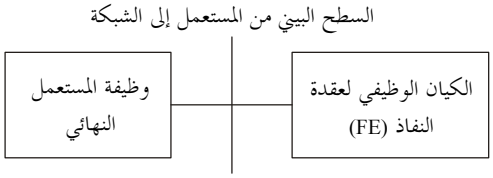
8.8 تعرف واستيقان حركة الحمالة

تحصل ظروف يُستحسَن فيها تعرف تدفق حركة الحمالة فردياً من أجل تعزيز الأمن، كما في العمل على صد هجمات احتيالية، مثل الخداع أو حُقَن RTP (بروتوكول الوقت الفعلي). وفي شبكات الجيل التالي (NGN)، يمكن تعرّف حركة الحمالة بخماسيّ يحتوي:

- العنوان IP للمصدر؛
- العنوان IP للمقصد؛
- مَنْفذ المصدر؛
- مَنْفذ المقصد؛
- رقم البروتوكول.

وآلية التعرف الموصوفة في هذا الجزء تستعمل معرِّف الهوية هذا، لاستيقان كل رُزمة. وتعتمد الآلية على تقاسم سر واستعمال دالة التظليل التجفيرية، وشفرة ذات مفتاح لاستيقان الرسالة مع التظليل (HMAC, *keyed-Hash Message Authentication Code*). اطلب المعلومات في المعيار [b-NIST FIPS 198-1].

ويرد في التوصية [ITU-T Y.2701] وصف الكيانين – وظيفة المستعمل النهائي، والكيان الوظيفي لعقدة النفاذ – الداخلين في عملية الاستيقان، ويأتي بيانهما في الشكل 3 باتّخاذ السطح البيني من المستعمل إلى الشبكة (UNI) مثالاً.



الشكل 3 – كيانا شبكة NGN الضالعان في إجراء الاستيقان – السطح البيني UNI مثالاً

تُستعمَل في وصف الآلية الاصطلاحات التالية:

- *F* يدل على معرِّف حركة الحمالة (معرِّف خماسي).
- *K* يدل على السر المتقاسم الذي يمتلكه كل من وظيفة المستعمل النهائي والكيان الوظيفي لعقدة النفاذ.
- *P* يدل على الرزمة التي تعتزم وظيفة المستعمل النهائي إرسالها إلى الكيان الوظيفي لعقدة النفاذ.
- *i* يدل على الرقم التتابعي للرزمة الجاري استكماله على يد طرفي الاتصال. قيمته 64 بتة.
- *t* يدل على دمغة الوقت – قيمتها 64 بتة تبين الوقت بالثواني. ويمكن، بدلاً من ذلك، أن يكون قيمة ظرفية.
- *(P', Q)* يدل على رزمة استلمها الكيان الوظيفي لعقدة النفاذ.

عندما تعتزم وظيفة المستعمل النهائي إرسال رزمة *P* إلى الكيان الوظيفي لعقدة النفاذ، تعمَد أولاً إلى حساب كمية ما، تتمثل في *H(F, t+i, K)* وهي دالة تظليل لتسلسل *F* و*t+i* و*K*، ثم تُلحِق هذه الكمية بالرزمة *P*. وعليه تكون الرزمة الكاملة المرسلة من وظيفة المستعمل النهائي إلى الكيان الوظيفي لعقدة النفاذ هي *[P, H(F, t+i, K)]*. ومتى تسلّم الكيان الوظيفي لعقدة النفاذ الرزمة *(P', Q)*، يحسب الكمية *H(F, t+i, K)*. وإذا كانت دمغة وقت مستعمَلة، يحسب الكيان الوظيفي لعقدة النفاذ المظلّلات مستعملاً جميع قيم الوقت *t* التي توجد داخل المدى المتفق عليه للفرق بين وقت وظيفة المستعمل النهائي ووقت الكيان الوظيفي لعقدة النفاذ (ولا حاجة لإجراء هذه العملية إلا مرة واحدة، في بدء الدورة). وفي هذه العملية يبحث الكيان الوظيفي لعقدة النفاذ عن التواؤم بين *Q* وأي من القيم المحسوبة للمظلّلات. فإذا حصل تواؤم تم استيقان الرزمة. ثم تُستعمَل قيمة *t* المطابقة، بخصوص سائر رزم التدفق.

وإذا استُعمِلت قيمة ظرفية، يكتفي الكيان الوظيفي لعقدة النفاذ بالتحقق مما إذا كانت القيمة المحسوبة للمظلَّل تساوي Q. فإن تساوتا تم استيقان الرزمة.

وفي بيئة تعرِّض الرزم لاحتمال الخسارة، قد لا يكفي مجرد استكمال العدد i من رزمة إلى رزمة. ففي هذه الحالة يحاول الكيان الوظيفي لعقدة النفاذ إعادة مزامنة i باحثاً من i إلى نهاية $i+d$ (حيث d عدد صغير).

إن استعمال آلية الاستيقان هذه يسهم في صد الهجمات الاحتيالية مثل الخداع أو حُقَن RTP (بروتوكول الوقت الفعلي).

وفي الآلية روعيت أيضاً حالة استيقان حركة، متولّدة عن المستعمل، بدون الكشف عن هوية المستعمل.

ولصالح التنفيذ، يُرتأى أن يقوم، بين وظيفة المستعمل النهائي والكيان الوظيفي لعقدة النفاذ، توافق على نسق المعرِّف F، والسر المشترك K، ودالة التظليل H، والتوقيت المزامَن لبدء دمغة الوقت t، وأين وكيف يمكن إضافة الكمية المظلَّلة إلى الرزمة P، وقيمة d، وأي جهة تبدأ إعادة تزامن i.

إن استعمال هذه الآلية خاضع للسياسة الأمنية لمشغِّل الشبكة. وهناك آليات أخرى يمكن استعمالها لاستيقان التدفقات، كأمن بروتوكول الإنترنت (IPsec)، مثلاً. لكن هذه الآلية تَفضُل IPsec بأنها تستلزم فقط حساب التظليل $H(F, t+i, K)$، وحسابه يمكن أن يؤدّى تأدية أسرع، وباستعمال موارد حسابية أقل مما في حالة IPsec الذي يتطلب تجفير رزمة IP بكاملها (في أسلوب النفق)، أو كامل الحمولة النافعة (في أسلوب النقل).

9 أمن النقل بخصوص التشوير والوظائف OAMP

في البنية التحتية لشبكات الجيل التالي (NGN)، يُستعمَل أمن النقل لضمان السرية والسلامة لمعطيات التشوير ورسائل التشغيل والإدارة والصيانة والتزويد (OAMP). وهذا الجزء يتضمن توصيف المظهر الجانبي لأمن طبقة النقل (TLS) وأمن بروتوكول الإنترنت (IPsec)، المتوجّب استعماله على العناصر الشبكية في البنية التحتية لشبكة NGN، على اعتبار TLS وIPsec آليّـــتَيْ أمن هامتين. وليست قوائم آليات الأمن بحاصرة، بل يجوز اعتماد أشكال تنفيذ أخرى، تبعاً لسياسات مورِّدي شبكات NGN.

يكون مطلوباً لأمن رسائل الوظائف OAMP، داخل المنطقة الموثوقة والمنطقة الموثوقة لكنها معرضة، نفق في الشبكة الخاصة التقديرية (VPN) (بواسطة IPsec أو TLS). وتعرض الفقرة 1.9 المظهر الجانبي لحالات استعمال الآلية TLS، والفقرة 2.9 ملامح لحالات استعمال الآلية IPsec. وتُستعمَل الآلية IPsec بين العنصر الحدي للتجهيزات المطرافية (TE-BE) والعنصر الحدي الشبكي لوظائف التشغيل والإدارة والصيانة والتزويد (OAMP-NBE) (يعني بين المنطقة الموثوقة والمنطقة الموثوقة لكنها معرّضة)، من أجل استحداث نفق VPN. وتعرض الفقرة 3.9 المظهر الجانبي المنطبق من البروتوكول IPsec.

وعلى الرغم من أنه غير مطلوب في البنية التحتية لشبكات NGN توفير أمن للوسائط، يتولّى بعض العناصر الحدية تحقيق أمن الوسائط بخصوص خدمة نقاط طرفية معينة. فبخصوص هذه العناصر الحدية، يحتوي الجزء 10 مظهراً جانبياً لبروتوكولات أمن الوسائط.

1.9 أمن طبقة النقل (TLS)

في البنية التحتية لشبكات NGN، كثيراً ما تُستعمَل الآلية TLS لتوفير الأمن لأنماط مختلفة من حركة التشوير (كبروتوكول فتح الدورة (SIP)، مثلاً، والخدمة المشتركة في سياسة مفتوحة (COPS))، وتسيير المهاتفة بواسطة بروتوكول الإنترنت (TRIP)، وبروتوكول نقل النصوص المترابطة (HTTP))، بين العناصر الشبكية داخل المنطقة الموثوقة. والآلية TLS موفَّرة أيضاً في العناصر الحدية المحتمل أن تستقبل تشويراً مجفراً من نقاط طرفية زبونة، وكذلك في العنصر الحدي للتجهيزات المطرافية (TE-BE) من أجل الاتصال بعنصر حدّي شبكي (NBE).وتحتوي التوصية [ITU-T Y.2701] متطلبات نوعية بخصوص كل نمط من أنماط العناصر الشبكية.

بروتوكول أمن طبقة النقل (TLS) معرَّف في المعيار [b-IETF RFC 5246]. إنه يوفّر السرية والسلامة للمعطيات بواسطة بروتوكول طبقة نقل موثوق مثل بروتوكول التحكم في الإرسال (TCP) أو بروتوكول إرسال أوامر التحكم في التدفق (SCTP).

ما لم يرد في هذا الجزء نص مخالف، يُستحسن في العناصر الشبكية التي من البنية التحتية لشبكات NGN وتتطلب الآلية TLS أن تكون وافية بمواصفة TLS الموضوعة في المعيار [b-IETF RFC 5246] وبأي اشتراطات مذكورة في المعيار [b-IETF RFC 3261] بشأن استعمالها في البروتوكول SIP. وعلى الرغم من أن الآلية TLS تستطيع تأدية التفاوض واستعمال طرائق ضغط المعلومات، قد لا يصلح استعمال طرائق الضغط هذه في البنية التحتية لشبكات NGN، بسبب انحطاط الأداء في إطارها.

1.1.9 متواليات التجفير

تتضمن متوالية التجفير طريقة الاتفاق على مفتاح الاستيقان المستعملة في تنظيم الاتصال في إطار بروتوكول أمن طبقة النقل (TLS)، وتتضمن كذلك جَفْرَتَيْ التجفير والاستيقان المستعملتين لتأمين طبقة التسجيل. وتخضع متواليات التجفير للتفاوض مع زبون TLS الذي يعرض قائمة بمتواليات التجفير الموفَّرة في رسالة نداء الزبون، ومع المخدم المجيب مستعملاً متوالية التجفير التي تتضمنها رسالة نداء المخدم.

ويخضع اختيار خوارزمية التجفير لتأثير عوامل كثيرة. وفيما يلي أمثلة للعوامل الشائعة التي تؤثر في اختيار خوارزمية التجفير:

1) الأمن المطلوب
   - قيمة المعطيات (الخاصة بمنظمة و/أو كيانات أخرى – كلما عظمت قيمة المعطيات، عظم التشدد في التجفير).
   - القيمة الزمنية للمعطيات (إذا كانت المعطيات صالحة لمدة قصيرة فقط (لأيام، مثلاً، لا لسنين)، أمكن استعمال خوارزمية تجفير أضعف).
   - التهديد المحدق بالمعطيات (كلما ارتفعت سوية التهديد، ازداد التشدد في التجفير).
   - تدابير الحماية الأخرى المعمول بها، التي من شأنها تقليل الحاجة إلى تجفير أقوى – مثلاً: استعمال طرائق اتصال محمية، كالدارات المكرّسة بدلاً من الإنترنت العمومية.
2) الأداء المطلوب (تطلّب أداء عالٍ قد يستلزم تزويد النظام بموارد إضافية، مثل قطعة عتاد مسرِّعة للتجفير، أو يستلزم تجفيراً أضعف).
3) موارد النظام (الموارد القليلة (مثل قدرة المعالجة، والذاكرة) قد توجب تجفيراً أضعف).
4) أنواع التقييد المفروضة على الاستيراد والتصدير والاستعمال.
5) خطط التجفير التي تستطيع العناصر الشبكية تأديتها.
6) خطط التجفير التي تستطيع أجهزة المستعملين تأديتها.

ويعرض الجدول 3 التالي قائمة بمتواليات التجفير المرشحة لاستعمالها في شبكات NGN، لكنه ليس كاملاً.

الجدول 3 – متواليات التجفير المرشحة لاستعمالها في شبكات NGN

اسم متوالية التجفير	المرجع	تبادل المفتاح	الجَفْرَة	الفرم
TLS_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	RSA	AES-128 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with RSA signatures	AES-128 in CBC mode	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 2246	RSA	3DES in CBC mode	SHA-1
TLS_DHE_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman Ephemeral mode with RSA signatures	3DES in CBC mode	SHA-1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	RSA	Camellia-128 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman Ephemeral mode with RSA signatures	Camellia-128 in CBC mode	SHA-1

متواليات التجفير المُدرجة في الجدول 4 مأخوذة من المعايير: [b-IETF RFC 5246] و[b-IETF RFC 4132] و[b-IETF RFC 4492]، ويمكن أيضاً لأي عنصر شبكي استعمالها اختيارياً.

الجدول 4 – متواليات تجفير تُستعمَل (اختياريا) في شبكات NGN

اسم متوالية التجفير	المرجع	تبادل المفتاح	الجَفْرَة	الفرم
Cipher suite name	Reference	Key Exchange	Cipher	Hash
TLS_DH_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman with DSS signature	AES-128 in CBC mode	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman with RSA signature	AES-128 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman Ephemeral mode with DSS signature	AES-128 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman Ephemeral mode with RSA signatures	AES-128 in CBC mode	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	RSA	AES-256 in CBC mode	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman with DSS signature	AES-256 in CBC mode	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman with RSA signature	AES-256 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	Diffie-Hellman Ephemeral mode with DSS signature	AES-256 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman Ephemeral mode with RSA signatures	AES-256 in CBC mode	SHA-1

الجدول 4 – متواليات تجفير تُستعمَل (اختياريا) في شبكات NGN

اسم متوالية التجفير	المرجع	تبادل المفتاح	الجَفْرَة	الفرم
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman with DSS signature	Camellia-128 in CBC mode	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman with RSA signature	Camellia-128 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman Ephemeral mode with DSS signature	Camellia-128 in CBC mode	SHA-1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	RSA	Camellia-256 in CBC mode	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman with DSS signature	Camellia-256 in CBC mode	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman with RSA signature	Camellia-256 in CBC mode	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman Ephemeral mode with DSS signature	Camellia-256 in CBC mode	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	Diffie-Hellman Ephemeral mode with with RSA signatures	Camellia-256 in CBC mode	SHA-1
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman with ECDSA signature	3DES in CBC mode	SHA-1
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman with ECDSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman with ECDSA signature	AES-256 in CBC mode	SHA-1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman Ephemeral mode with ECDSA signature	3DES in CBC mode	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman Ephemeral mode with ECDSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman Ephemeral mode with ECDSA signature	AES-256 in CBC mode	SHA-1
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman with RSA signature	3DES in CBC mode	SHA-1
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman with RSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman with RSA signature	AES-256 in CBC mode	SHA-1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman Ephemeral mode with RSA signature	3DES in CBC mode	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman Ephemeral mode with RSA signature	AES-128 in CBC mode	SHA-1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	EC-Diffie-Hellman Ephemeral mode with RSA signature	AES-256 in CBC mode	SHA-1

الملاحظة 1 – RC-4 هي جفرة معروفة على نطاق واسع ومستعملة جدا. لكنها لم تُدرَج في القائمة أعلاه، لأنها ليست معياراً مفتوحاً.

الملاحظة 2 – الكتابة التجفيرية بمنحنى إهليلجي (ECC, *Elliptic Curve Cryptography*) هي نظام تجفير ذو مفتاح عمومي قد يُستحسَن العمل به في بعض تطبيقات الشبكات NGN. وعلى وجه التحديد، تُستحسَن الكتابة ECC لبعض التطبيقات نظراً لبساطتها وفعاليتها. فهي، مقارنةً بنظام التجفير RSA، توفر مستوى أمن مكافئ، وقدود مفاتيحها أصغر بكثير. ثم إن الكتابة ECC، إضافة إلى ذلك، تَفضُل بفعاليتها ومحاسنها الحسابية بعض التقنيات الأخرى ذات المفاتيح العمومية التي تحقق نفس السوية من الحماية.

2.1.9 استعمال الشهادات في أمن طبقة النقل (TLS)

أمن طبقة النقل (TLS) هو بروتوكول يعتمد على مخدم زبون، وفيه يكون استيقان الزبائن اختياريا. ولكن من الجائز، داخل المنطقة الموثوقة من البنية التحتية للشبكات NGN، وبين المنطقة الموثوقة والمنطقة الموثوقة لكنها معرَّضة، أن يُجرى استيقان متبادل باستعمال البروتوكول TLS. في مثل هذه الحالة، يرسل مخدم TLS طلب شهادة إلى الزبون. فإذا لم يقدم الزبون شهادة، وهو في المنطقة الموثوقة والمنطقة الموثوقة لكنها معرضة، يجوز للمخدم رفض طلب التوصيل. وينبغي أن تكون كلتا شهادتي زبون ومخدم TLS وافية بمواصفات إصدار الشهادات في إطار البنية التحتية للشبكات NGN، مواصفات معروضة في الفقرة 3.8. ويجرى التحقق من الشهادات طبقاً للتوصيف الوارد في الفقرة 3.8. وقبل المضي في التوصيل TLS، يقوم مخدم أو زبون TLS بإقرار الصلاحية أن النظام البعيد موائم لشهادته.

بين المنطقة الموثوقة لكنها معرّضة والمنطقة غير الموثوقة، يرسل مخدم TLS طلب شهادة إلى الزبون. فإذا لم يكن لدى الزبون شهادة، يرد على المخدم برسالة شهادة زبون فارغة، وعندئذ تجرى الدورة مع زبون غُفْل.

حين يقبل عنصر حدي شبكي (NBE) توصيلاً مستيقَناً مع نقطة طرفية، بناءً على شهادة مستعمل نهائي في شبكة NGN (انظر الفقرة 2.5.8)، يجوز للعنصر NBE تشغيل مؤقّتين على التوصيل. المؤقّت الأول، T1، يُطلَق اشتغاله حين إقامة التوصيل. والمؤقّت الثاني، T2، يُطلَق اشتغاله حين إقامة التوصيل ويعاد تدميثه من الصفر كلما ورد إلى العنصر طلب عبر التوصيل. ومتى بلغ أي من المؤقّتين قيمته الحدّية (وهذه تابعة للقيم التي تحتويها الشهادة)، يعاد تدميث الاتصال على يد العنصر NBE، وتعاد إقامة الاتصال على يد النقطة الطرفية من أجل تحديد شهادة المستعمل النهائي للشبكة NGN.

3.1.9 إدارة مفاتيح الدورات

يُنتظَر من دورات البروتوكول TLS بين العناصر الشبكية في البنية التحتية للشبكات NGN أن تكون مستديمة. ولذا فمن الأهمية بمكان أن تُغيَّر مفاتيح الدورات على فترات منتظمة. ويجوز في مفاتيح دورات البروتوكول TLS تغييرها بعد مدة معيَّنة ممكن إدخالها في التشكيلة.

2.9 أمن بروتوكول الإنترنت (IPsec) في المنطقة الموثوقة والمنطقة الموثوقة لكنها معرَّضة

يُستعمَل أمن بروتوكول الإنترنت (IPsec) في إطار البنية التحتية للشبكات NGN من أجل تأمين أنواع مختلفة من الحركة (مثل بروتوكول إدارة الشبكات البسيط (SNMP)، وخدمة الاستيقان عن بعد للمستعملين الداخلين (RADIUS))، بين العناصر الشبكية داخل المنطقة الموثوقة. وتحتوي التوصية [ITU-T Y.2701] اشتراطات نوعية بشأن كل نوع من العناصر الشبكية.

يتكون IPsec، كما وُصِف بوجه عام في الوثيقة [b-IETF RFC 4301]، من عدد من القطع المختلفة. وهذه القطع يمكن استعمالها لتوفير حماية السرية والسلامة والحماية من إعادة التنفيذ. وبعض هذه القطع يمكن إدخالها في التشكيلة يدوياً، ولكن على العموم تُستعمَل لهذا الغرض إحدى مكوِّنات إدارة المفاتيح. يضاف إلى ذلك أن قرار استعمال IPsec تتحكم به عادة قاعدة معطيات السياسة. وتصف هذه الفقرة المجموعة الفرعية من مكوِّنات IPsec الواجب تنفيذها.

بخصوص العناصر الشبكية التي تستعمل IPsec، يوصى بضمان أن التوصيلات المؤمَّنة بواسطة TLS لا يجرى تشغيلها عبر IPsec.

ملاحظة – يجب في العناصر الشبكية التي تستعمل IPsec التأكد من أن تدفقات الوسائط المؤمَّنة بواسطة SRTP أو RC4 لا يجري تشغيلها عبر IPsec، وذلك تحاشياً لازدواج التجفير، لأنه يهدر موارد الشبكات NGN. وينبغي الملاحظة أيضاً أنه قد يحصل تسريب التجفير من جانب المستعمل النهائي.

1.2.9 رأسية الاستيقان (AH) والبروتوكول الأمني التغليفي (ESP)

رأسية الاستيقان (AH) الموصوفة في المعيارين [IETF RFC 4302] و[b-IETF RFC 4835] والبروتوكول الأمني التغليفي (ESP) الموصوف في المعيار [IETF RFC 4303] هما الخياران المفضلان بين بروتوكولات الأمن الفعلي على الخط. كلاهما يوفّر اختيارياً الحماية من إعادة التنفيذ. والبروتوكول ESP يستعمَل عادة لتحقيق سرية الحركة وسلامتها واستيقاظها. ويمكن أن يحقق ESP أيضاً السلامة والاستيقان بدون السرية. ومن شأنه كذلك تحقيق السرية وحدها. أما رأسية الاستيقان (AH) فتحمي أجزاءً من رأسية IP السابقة، بما في ذلك عنوان كل من المصدر والمقصد. وفي استطاعة الرأسية AH أن تحمي أيضاً خيارات IP التي تحتاج إلى أن تراها المسيِّرات الوسيطة، ولكن يُشترط أن تكون خيارات IP هذه سليمة كل السلامة وأصيلة، عند تسليمها إلى النظام المتلقّي، وإن يكن استعمالها نادراً غاية الندرة.

وتستطيع العناصر الشبكية للبنية التحتية لشبكة NGN الاشتغال بالبروتوكول الأمني التغليفي (ESP) المعرَّف في المعيار [IETF RFC 4303]. وتستطيع العناصر المذكورة أيضاً أن تشغِّل بأسلوب تسلسل فِدَر التجفير (CBC, *Cipher Block Chaining*) البروتوكولات التالية: ESP_DES (بكلا الصيغتين 40 و56 بتة)، وESP_3DES وESP_AES المعرَّفة في المعيار [b-IETF RFC 3602] وESP_CAMELLIA المعرَّف في [b-IETF RFC 4312]. والعناصر الشبكية التي تستطيع تأدية البروتوكول ESP_NULL قد لا تستعمل ESP_NULL حين تتصل بعنصر شبكي آخر للبنية التحتية لشبكة NGN. ثم إن خوارزمية التجفير الفعلية التي تستعمَل في البروتوكول الأمني التغليفي (ESP) يُتفاوَض عليها أثناء عملية إدارة المفاتيح.

يقضي المعيار [b-IETF RFC 4301] بأن تكون جميع الصيغ التنفيذية للبروتوكول الأمني التغليفي (ESP) قادرة على تأدية التصاحبات الأمنية (SAs)، ويوفر المعيار [b-IETE RFC 4301] نموذجاً عاماً لمعالجة حركة IP ذات الصلة بالتصاحبات الأمنية (SAs). وعلى الرغم من أن الصيغ التنفيذية المعيّنة للبروتوكول IPsec لا تتقيد بتفاصيل هذا النموذج العام، فقد يوائم السلوكُ الخارجي لأي تنفيذ للبروتوكول IPsec السلوكَ الخارجي للنموذج العام. وهذا يضمن أن المكوِّنات لا تقبل حركة من عناوين مجهولة ولا ترسل أو تستقبل حركة بدون أمن (حيثما كان الأمن مطلوباً). ويجوز في العناصر الشبكية للبنية التحتية للشبكات NGN، التي تنفذ البروتوكول IPsec، أن توفر سلوكاً يوائم سلوك النموذج العام الموضوع تعريفه في المعيار [b-IETF RFC4301].

2.2.9 أسلوب النقل وأسلوب النفق

يمكن استعمال رأسية الاستيقان (AH) والبروتوكول الأمني التغليفي (ESP) كليهما بأسلوب النقل أو بأسلوب النفق. ففي حالة استعمال رأسية IPsec بأسلوب النفق، تعقبها رأسية IP داخلية. وهذا هو الاستعمال العادي في الشبكات الخاصة التقديرية (VPNs)، ويكون على العموم مطلوباً حين لا يكون أي من طرفي المسير المحمي بالبروتوكول IPsec هو المقصد الأخير؛ مثلاً: حين ينفَّذ IPsec في مِصَدّ (firewall) أو في مسيِّر. وأسلوب النقل مفضَّل في حالات الاتصال من نقطة إلى نقطة.

والعناصر الشبكية للبنية التحتية لشبكات NGN تستطيع تأدية IPsec بأسلوب النقل.

3.2.9 الحماية من إعادة التنفيذ

تستعمل العناصر الشبكية للبنية التحتية لشبكات NGN خدمة IPsec الاختيارية للحماية من إعادة التنفيذ (الخدمة الصادّة لإعادة التنفيذ). وهذه الخدمة يمكن تشغيلها في أي وقت داخل العناصر الشبكية للبنية التحتية لشبكات NGN. ففي سياق IPsec، متى وُجد عدد تتابعي خارج النافذة الحالية للخدمة الصادة لإعادة التنفيذ، يُميَّز بعلم على أنه إعادة تنفيذ، وتُرفَض الرزمة. وحين تُشغَّل الخدمة الصادة لإعادة التنفيذ، لا يمكن لرقم تتابعي عائد لـ IPse أن يفيض ويعود بالعداد إلى 0. فتفادياً لحدوث ذلك ينبغي إقامة تصاحب أمني جديد كما هو موصَّف في المعيار [IETF RFC 4303].

4.2.9 إدارة المفاتيح

تقتضي جميع أنظمة التجفير إدارة مفاتيح. وقد روعي في البروتوكول IPsec كلا مخططَيْ إدارة المفاتيح، اليدوي والأوتوماتي، لكن المخططات اليدوية ليست مرنة ودقيقة مثل المخططات الأوتوماتية، فلا تحمي من إعادة التنفيذ. جميع مخططات إدارة المفاتيح توفر الاستيقان. ويُفترَض في العناصر الشبكية للبنية التحتية لشبكات NGN إعمال واحدة من الآليات الأوتوماتية الموصوفة في هذه الفقرة لتبادل المفاتيح.

حيث لا يكون تبادل مفاتيح إنترنت (IKE) مستعمَلاً لإدارة المفاتيح، يحتاج البروتوكول البديل لإدارة المفاتيح إلى سطح بيني مع طبقة البروتوكول IPsec من أجل استحداث تصاحبات أمنية IPsec أو تحيينها أو شطبها. والتصاحبات الأمنية IPsec يمكن أن تقام أو تعاد إقامتها أوتوماتياً حسب الاقتضاء. وذلك يعني ضمناً أن طبقة IPsec أيضا تحتاج إلى وسيلة لتشوير تطبيق إدارة مفاتيح حين يلزم إقامة تصاحب أمني جديد (كأن يكون التصاحب الأمني القديم على وشك انقضاء صلاحيته، أو أن يخلو سطح بيني معيّن من تصاحب أمني). وبالإضافة إلى ذلك، قد يكون مطلوباً من بعض العناصر الحدية تشغيل بروتوكولات متعددة لإدارة المفاتيح (مثلاً: تشغيل البروتوكول IKE (تبادل مفاتيح إنترنت) لتأمين التوصيلات الخاصة بالوظائف OAMP، والبروتوكول PKINIT (الاستيقان البدئي بتجفير ذات مفتاح عمومي) من أجل تأمين التوصيلات). وفي مثل هذه الحالات يوصى باستعمال السطح البيني PF_KEY المعرَّف في المعيار [b-IETF RFC 2367].

1.4.2.9 معرِّفات هوية المحوَّلات

معرِّف هوية محوَّلة IPsec تستعمله إجراءات إدارة المفاتيح للتفاوض على خوارزمية تجفير يستعملها البروتوكول الأمني التغليفي (ESP) في إطار IPsec. ومعرِّف هوية المحوَّلة يستعمله أيضاً برتوكول تبادل مفاتيح إنترنت (IKE) لتأمين رسائله في المرحلة الأولى والثانية. وفي المعيار [b-IETF RFC 5282] قائمة بمعرِّفات متيسِّرة لهوية محوَّلات IPsec. وداخل البنية التحتية لشبكات NGN، يمكن توفير معرِّفَيْ هوية المحوَّلات التاليين: IDs ESP_3DES (بقيمة 0x03، ومفتاح قدّه 192 بتة، وأسلوب تسلسل فِدَر التجفير (CBC)، وESP_CAMELLIA (بقيمة 0x16، ومفتاح قدّه 128 بتة، وأسلوب CBC)، المعيار [b-IETF RFC 4312]. ويوصى بتوفير معرِّف هوية المحوَّلات ESP_AES (بقيمة 0x0C، ومفتاح قدّه 128 بتة، وأسلوب CBC). وينطوي برتوكول تبادل مفاتيح إنترنت (IKE) على وظيفة تمكّن من التفاوض على قدّ مفتاح التجفير؛ فإذا وُجدت في المستقبل رغبة لزيادة قدّ المفتاح لأي من الخوارزميات المذكورة أعلاه، فسيستعمل البروتوكول IKE هذه الوظيفة المدمَجَة.

ومن أجل كل واحدة من هذه المحوَّلات، يكون متَّجه التدميث (IV) لتسلسل فِدَر التجفير (CBC) محمولاً بصيغة واضحة داخل كل حمولة نافعة لكل رزمة من رزم البروتوكول ESP طبقاً لما هو معرَّف في المعيار [b-IETF RFC 2451]. والخوارزمية AES-128 (معيار التجفير المتقدم) المعرَّفة في المعيارين [b-NIST FIPS 197] و[b-IETF RFC 3602] قابلة للاستعمال في الأسلوب CBC بفِدرة قدّها 128 بتة، ومتَّجه تدميث توليده عشوائي. وتستلزم الخوارزمية AES-128 10 جولات من عمليات التجفير حسب توصيف المعيار [b-IETF RFC 3602]. والخوارزمية Camellia-128، المعرَّفة في المعيارين [b-IETF RFC 3713] و[b-IETF RFC 4312]، هي أيضاً قابلة للاستعمال في الأسلوب CBC بفِدرة قدّها 128 بتة، ومتَّجه تدميث توليده عشوائي. إنها تستلزم 18 جولة من عمليات التجفير، المعيار [b-IETF RFC 3713].

2.4.2.9 خوارزميات الاستيقان

خوارزمية الاستيقان التابعة للبروتوكول IPsec تستعملها إجراءات إدارة المفاتيح للتفاوض على الخوارزمية التي تُستعمل لاستيقان الرزمة. ويحتوي المعيار [b-IETF RFC 5282] على قائمة بخوارزميات الاستيقان التابعة للبروتوكول IPsec المتيسِّرة. وداخل البنية التحتية لشبكات NGN، يمكن توفير خوارزميتَيْ الاستيقان التاليتين: HMAC-MD5-96 (بقيمة 0x01، ومفتاح قدّه 128 بتة، وتعريفها في المعيار [b-IETF RFC 2403])، وHMAC-SHA-1-96 (بقيمة 0x02، ومفتاح قدّه 160 بتة، وتعريفها في المعيار [b-IETF RFC 4835]).

3.4.2.9 تبادل مفاتيح إنترنت (IKE)

يتضمن المعيار [b-IETF RFC 2409] وصف آلية أوتوماتية واحدة لتبادل المفاتيح، معروفة بالتسمية المختصرة IKE. وتتصف إدارة IKE للمفاتيح بلا تزامن كلي مع رسائل المعطيات، فلا تسهم في أي تأخير مما يحصل أثناء إقامة الاتصالات. وربما كان الاستثناء الوحيد من هذه القاعدة هو حصول خطأ غير متوقَّع، وهو فقدان التصاحب الأمني بصورة غير متوقعة في إحدى النقاط الطرفية.

وIKE هو بروتوكول إدارة مفاتيح ند إلى ند، قوامه مرحلتان. في المرحلة الأولى، يجري التفاوض على سر مشترك بواسطة تبادل المفاتيح المسمّى Diffie-Hellman. ثم يُستعمل لاستيقان المرحلة الثانية من IKE. في المرحلة الثانية يجري التفاوض على سر آخر، يستعمل لاشتقاق مفاتيح من أجل البروتوكول الأمني التغليفي (ESP) التابع للبروتوكول IPsec.

1.3.4.2.9 المرحلة الأولى من IKE

هناك ثلاثة أساليب معرَّفة من أجل الاستيقان خلال المرحلة الأولى من IKE. لا يجوز استعمال التجفير بمفتاح عمومي في الاستيقان الذي يخص التبادل IKE داخل البنية التحتية لشبكات NGN، لأن ذلك يقتضي أن يكون المبادر على علم بالمفتاح العمومي الذي يستعمله المستجيب. والجائز في الاستيقان الخاص بـ IKE هو استعمال إما التواقيع وإما المفاتيح المسبق التشارك فيها.

يعرِّف IKE مجموعتين نوعيتين من معلمات Diffie-Hellman (أي مجموعة أولية ومجموعة توليد) يجوز استعمالهما في المرحلة الأولى من التبادل IKE. يجوز في الزمرة الأولى أن تؤدّى داخل البنية التحتية لشبكات NGN، أما الزمرة الثانية فيوصى بتوفيرها.

إذا استُعمِل استيقان IKE بواسطة التواقيع، يجوز لكلا الزبون والمخدم تبادل الشهادات الموصَّفة في X.509 (انظر الفقرة 2.3.8). ويُتحقق من هذه الشهادات كما هو مبيّن في الفقرة 3.8.

حين يقبل العنصر الحدي للشبكة (NBE) توصيلا مستيقَنا مع نقطة طرفية، بناء على شهادة مستعمل نهائي لشبكة NGN (انظر الجزء xx)، يكون للعنصر NBE هذا إعمال مؤقِّتَين على التوصيل. المؤقِّت الأول، T1، يُطلَق اشتغاله حين إقامة التوصيل. والمؤقِّت الثاني، T2، يُطلَق اشتغاله حين إقامة التوصيل، ويعاد تدميثه من الصفر كلما ورد إلى العنصر طلب عبر التوصيل. ومتى بلغ أي من المؤقِّتين قيمته الحدّية (وهذه تابعة للقيم التي تحتويها الشهادة)، يعاد تدميث الاتصال على يد العنصر NBE، وتعاد إقامته على يد النقطة الطرفية من أجل تحديد شهادة المستعمل النهائي للشبكة NGN.

إذا جرى استيقان الخاص بـ IKE بواسطة المفاتيح المسبق التشارك فيها، يُستعمَل مفتاح مشتق بآلية ما من خارج النطاق (يدوية، مثلاً) لاستيقان التبادل. وقد يسمح التنفيذ باستعمال مفتاح مسبق التشارك فيه لا يقل قدّه عن 128 أثمونا. وليس مشترطا في العناصر الشبكية التحقق من اشتراطات المفاتيح المسبق التشارك فيها. ويجوز في أوجه التنفيذ إعمال الأسلوب الهجومي، المعرَّف في الجزء 4.5 من الوثيقة [b-RFC2409]، فيُستعمَل اسم المفتاح بمثابة هوية المبادر/المستجيب.

من المعروف أن الأسلوب الهجومي للإصدار 1 لعملية تبادل مفاتيح الإنترنت [المعيار IETF RFC 2409] بالاشتراك مع المفتاح المتقاسم سلفاً غير مأمون. ومن خلال هذا الأسلوب يرسل فرم للسر بوضوح عبر الشبكة؛ فإذا حدث اعتراض لحركة بروتوكول الإنترنت من مهاجم، يمكن استعادة المفتاح عن طريق محاولة عشوائية من خارج الخط. ويُوصى باستعمال مفتاح PSK طوله 128 bit على الأقل لتفادي الحساب العشوائي للمفتاح استناداً إلى عملية الفرم الخاصة به.

وفي حالة استعمال مفاتيح مسبق التشارك فيها، تكون متانة النظام مرهونة بمتانة السر المشترك. والمنشود هو جعل السر المشترك في منأى عن أن يكون الحلقة الضعيفة في السلسلة الأمنية. وهذا يفترض أن السر المشترك يلزمه أن يحتوي من الإنتروبية (العشوائية) مقدار ما تحتوي منها الشفرة المستعملة. أي بعبارة أخرى، يوصى بأن يتصف السر المشترك بإنتروبية لا تقل عن 128–160 بتة.

2.3.4.2.9 المرحلة الثانية من IKE

في المرحلة الثانية من IKE يقام تصاحب أمني IPsec ESP، يشتمل على مفاتيح ESP ومتواليات تجفيرية. أولاً، يقام سر للمرحلة الثانية، وتُشتقّ منه جميع المواد المفتاحية لـ IPsec باستعمال الوظيفة الأحادية الاتجاه الموضوع توصيفها في الوثيقة [b-IETF RFC2409]. ويتكون سر المرحلة الثانية من قيم ظرفية مجفَّرة يتبادلها الطرفان. والوثيقة [b-IETF RFC2409] تجيز استعمال تبادل آخر لمعلمات Diffie-Hellman بالإضافة إلى القيم الظرفية المجفَّرة، ولكن لا يجوز استعماله في العناصر الشبكية للبنية التحتية لشبكات NGN، تجنباً لما يصاحبه من مساوئ أدائية.

3.9 بروتوكول اتفاق المفاتيح (AKA) بين منطقة غير موثوقة ومنطقة موثوقة لكنها معرضة

يمكن استعمال بروتوكول اتفاق المفاتيح الموصّف لشبكات النظام ImS في حالتنا هذه أيضاً حسبما يتناسب. واستيقان النظام العالمي للاتصالات المتنقلة (UMTS) وبروتوكول اتفاق المفاتيح الخاص به يدعمان الاستيقان المتبادل بين المحطة المتنقلة (MS) والشبكة. وبروتوكول اتفاق المفاتيح الخاص بالنظام UMTS عبارة عن بروتوكول قائم على التحدي والسرد حيث يستعمل مفتاح طويل الأمد، *K*، يجري تقاسمه بين وحدة الهوية العامة للمشترك (USIM) ومركز الاستيقان (AuC). ويوجد هذان الكيانان في بطاقة الدارة المتكاملة العامة (UICC) للمحطة MS وفي الشبكة الأصلية للمحطة المتنقلة، على التوالي. ويرد وصف للبروتوكول AKA في المعيار [b-3GPP TS 33.102]، معمارية الأمن.

وعلى الرغم من أن آلية البروتوكول AKA تستعمل نمطياً لاستيقان الأجهزة اللاسلكية المجهّزة ببطاقات ذكية (مثل البطاقة UICC)، لا يوجد أي شيء في مواصفات البروتوكول AKA يحول دون استعمال هذه الآلية في استيقان الأجهزة الثابتة القادرة على تشغيل تطبيق للنظام UMTS.

4.9 أمن بروتوكول الإنترنت (IPsec) بين المنطقة غير الموثوقة والمنطقة الموثوقة لكنها معرَّضة

العنصر الحدي للتجهيزات المطرافية (TE-BE) هو عنصر شبكي من عناصر شبكات الجيل التالي (NGN)، ويُجعل موضع إقامته في المنطقة غير الموثوقة. لكنه يظل مع ذلك تحت إدارة حمالة الشبكة NGN، ويحتاج إلى النفاذ إلى وظائف التشغيل والإدارة والصيانة والتزويد (OAMP) الواقعة داخل المنطقة الموثوقة. وعليه فإنه يوجد عنصر خدمة لهذه الوظائف (OAMP-SE) مقيم في المنطقة الموثوقة لكنها معرَّضة، يؤدي عمل نقطة ترحيل لرسائل الوظائف OAMP.

يستطيع العنصر TE-BE أن يكفل عدم تشغيل التوصيلات المأمونة الخاصة بأمن طبقة النقل (TLS) في نفق شبكة خاصة تقديرية (VPN) للبروتوكول IPsec. ويستطيع العنصر TE-BE أن يكفل عدم تشغيل التدفقات الوسائطية المؤمَّنة بفضل أمن وسائط البروتوكول المأمون للوقت الفعلي (SRTP) في نفق شبكة خاصة تقديرية (VPN) للبروتوكول IPsec.

يستطيع نفق الشبكة VPN لـ IPsec استعمال البروتوكول الأمني التغليفي (ESP) التابع لـ IPsec المعرَّف في المعيار [IETF RFC 4303] بأسلوب النفق كما هو معرَّف في الوثيقة [b-IETF RFC 4301].

الخدمة الصادَّة لإعادة التنفيذ قابلة للتفعيل في أي وقت.

يستطيع نفق الشبكة VPN لـ IPsec تشغيل معرِّفَيْ هوية المحوَّلات التاليين: IDs ESP_3DES (بمفتاح قدّه 192 بتة، وأسلوب تسلسل فِدَر التجفير (CBC)، وESP_CAMELLIA (بمفتاح قدّه 128 بتة، وأسلوب CBC) طبقاً لتوصيف الوثيقة [b-IETF RFC 4312]. ويوصى بأن يستطيع نفق الشبكة VPN لـ IPsec تشغيل معرِّف هوية المحوَّلات ESP_AES (بمفتاح قدّه 128 بتة، وأسلوب CBC).

يستطيع نفق الشبكة VPN لـ IPsec تشغيل الخوارزميتين HMAC-MD5-96 (بمفتاح قدّه 128 بتة) وHMAC-SHA-1-96 (بمفتاح قدّه 160 بتة).

يمكن أن يتم توليد المفاتيح وإدارتها من أجل نفق الشبكة VPN لـ IPsec بواسطة التبادل IKE [b-IETF RFC2409]، باستعمال استيقان IKE مع توقيعات رقمية، أو استيقان IKE مع مفتاح مسبق التشارك فيه. وفي حالة استعمال استيقان IKE مع توقيعات رقمية، يتبادل كلا الزبون والمخدم شهادات X.509، ويتحققان منها.

10 أمن الوسائط

ليس تجفير الوسائط مطلوباً داخل البنية التحتية لشبكات NGN، ولكن قد يكون مطلوباً توفيره من أجل الزبائن الراغبين في استعماله. وتوفيره يستتبع توفير بروتوكولات تجفير الوسائط، ولا سيما البروتوكول المأمون للوقت الفعلي (SRTP) المعرَّف في المعيار [b-IETF RFC 3711]. وفي باقي هذا الجزء يُفترض أن العناصر الحدية للشبكة (أي حافة ميدان مورِّد الشبكة) تنفذ التجفير/فك التجفير، وإن يكن من الممكن أن تؤدّى نفس الوظيفة في منصة منفصلة مشتركة بين العناصر الحدية للشبكة. وفي كلا الحالين يكون مطلوباً تواجد التجفير وفك التجفير مع مقدرات أخرى لمعالجة الوسائط، مثل الكشف وتحويل الشفرة بواسطة التردد المتعدد بنغمة مزدوجة (DTMF).

وإزاء متطلبات توصيل مشتركين راغبين في تجفير الوسائط على وصلة نفاذهم مع المشتركين غير الراغبين (أو غير المتيسر لهم ذلك)، تتهيأ خمس حالات منفصلة تستلزم النظر، كما هو مبيّن في الشكل 4.

الحالة الأولى والأبسط هي عدم الرغبة في التجفير عند كلتا النقطتين الطرفيتين. وفي هذه الحالة تتدفق الوسائط من المصدر إلى المقصد، عبر العناصر الحدية، بدون أي تجفير في أي وصلة. فلا العناصر الحدية الشبكية التي تخدم المصدر (NBE(#1)) ولا العناصر الحدية الشبكية التي تخدم المقصد (NBE (#2)) تنفذ التجفير أو فك التجفير.

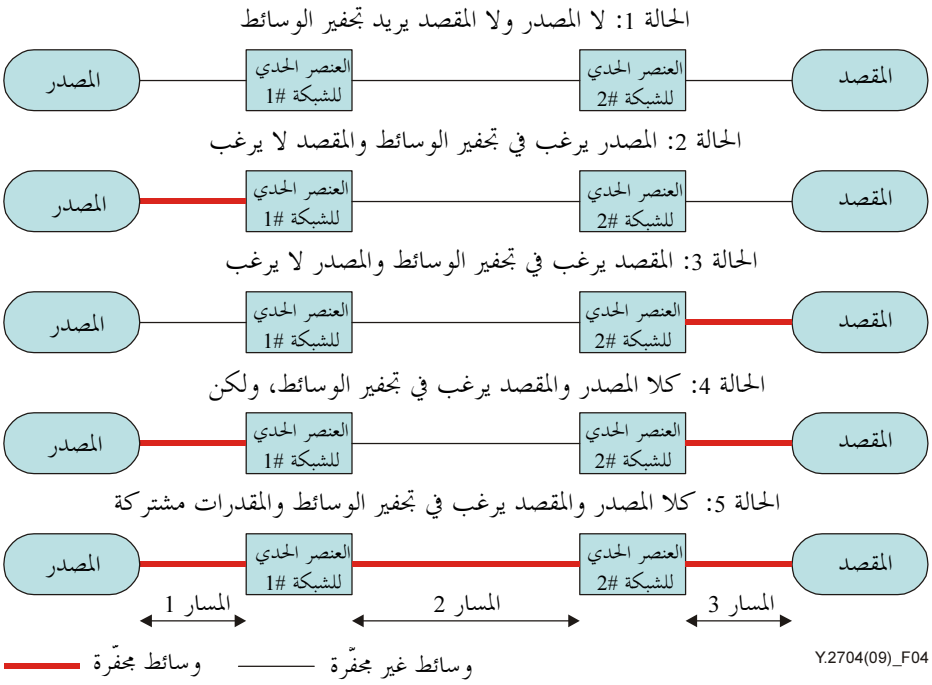
تحصل الحالة الثانية عندما يرغب المصدر في تجفير تدفق الوسائط، لكن المقصد لا يرغب. في هذه الحالة يقوم العنصر الحدي NBE #1 بمثابة نقطة ترحيل للتجفير/فك التجفير. يستقبل العنصر NBE #1 التدفق المجفَّر من المصدر، فيفك تجفيره ويمرره عبر البنية التحتية لشبكة NGN إلى العنصر الحدي NBE #2، وهذا يمرره بدوره (مفكوكَ التجفير) إلى المقصد. في الاتجاه المعاكس يستقبل العنصر NBE #1 تدفق الوسائط غير المجفَّر عبر البنية التحتية لشبكة NGN، فيجفِّره قبل أن يرسله إلى المصدر. وهكذا فإن تدفق الوسائط يكون مجفَّرا في المسار #1 (من المصدر إلى NBE #1)، وغير مجفَّر في المسار #2 (بين العنصر NBE #1 والعنصر NBE #2)، وغير مجفَّر في المسار #3 (بين العنصر NBE #2 والمقصد).

وتحصل الحالة الثالثة إذا كان المقصد يرغب في أن يكون تدفق الوسائط مجفَّراً ولا يرغب المصدر. في هذه الحالة يقوم العنصر NBE #2 بمثابة نقطة ترحيل للتجفير/فك التجفير. يستقبل العنصر NBE#1 تدفق الوسائط غير مجفَّر من المصدر ويمرره (وهو غير مجفَّر) عبر البنية التحتية لشبكة NGN إلى العنصر NBE #2. ينفذ العنصر NBE #2 التجفير ويمرر تدفق الوسائط إلى المقصد. في الاتجاه المعاكس يستقبل العنصر NBE #2 تدفق الوسائط مجفَّراً من النقطة الطرفية للمقصد فيفك تجفيره قبل أن يعيد تسييره عبر البنية التحتية لشبكة NGN. العنصر NBE #1 يمرر تدفق الوسائط غير مجفَّر إلى المصدر. وهكذا يكون تدفق الوسائط غير مجفَّر في المسارين #1 و#2، ومجفَّراً في المسار #3.

وتحصل الحالة الرابعة إذا كان كلا المصدر والمقصد يرغبان في أن تكون الوسائط مجفَّرة، ولكن يكونان إما غير قادرين على تأدية مخططي تجفير متوائمين، وإما منتفعين بخدمة ما معززة بفضل البنية التحتية لشبكة NGN (مثل الكشف بواسطة التردد المتعدد بنغمة مزدوجة (DTMF) من أجل تطبيقات بطاقات المناداة). في هذه الحالة يؤدي كلا العنصرين الحديين NBE #1 وNBE #2 وظيفة نقطة ترحيل للتجفير/فك التجفير. يستقبل العنصر NBE #1 التدفق المجفَّر من المصدر، فيفك تجفيره ويمرره عبر البنية التحتية لشبكة NGN إلى العنصر NBE #2. فيجفّره العنصر NBE #2 ويمرره إلى المقصد. في الاتجاه المعاكس يستقبل العنصر NBE #2 تدفق الوسائط المجفَّرة من النقطة الطرفية للمقصد، فيفك التجفير قبل إعادة إرسالها عبر البنية التحتية لشبكة NGN. ويستقبل العنصر NBE #1 تدفق الوسائط غير مجفَّر فيجفّره قبل إرساله إلى المصدر. وهكذا تكون الوسائط في المسارين #1 و#3 مجفَّرة، وفي مسارها عبر البنية التحتية لشبكة NGN (المسار #2) غير مجفَّرة.

وتقع الحالة الخامسة إذا كان كلا المصدر والمقصد يرغب في أن تكون الوسائط مجفَّرة، ويستطيع تنفيذ مخططات تجفير متوائمة، ولا يوجد خدمة معززة توفِّرها البنية التحتية لشبكة NGN. في هذه الحالة يستقبل العنصر NBE #1 الوسائط من المصدر مجفَّرة ويمررها بدون تغيير عبر البنية التحتية لشبكة NGN إلى العنصر NBE #2 فيمررها هذا بدون تغيير إلى المقصد. وفي الاتجاه المعاكس يستقبل العنصر NBE #2 الوسائط من المقصد مجفَّرةً ويمررها بدون تغيير عبر البنية التحتية لشبكة NGN إلى العنصر NBE #1 فيمررها هذا بدون تغيير إلى المصدر. وهكذا تكون الوسائط مجفّرة في المسارات الثلاثة. أما التشوير اللازم لتطبيق هذه الحالة فلا يدخل في مجال هذه التوصية.

إن تجفير الوسائط الموصوف في هذا الجزء يوفّر الاستيقان والسرية وسلامة الرسائل.



الشكل 4 – العلاقات بين تجفير الوسائط، ومقدرات العناصر الحدية للشبكة، ورغبة كل من المصدر والمقصد

1.10 البروتوكول SRTP

البروتوكول المأمون للوقت الفعلي (SRTP) موصوف في المعيار [b-IETF RFC 3711]، وهو معرَّف كمظهر جانبي لبروتوكول الوقت الفعلي (RTP) [b-IETF RFC 3550]. وقد أُعِد من أجل تنفيذه بين تطبيق البروتوكول RTP وطبقة النقل في بطارية البروتوكول – يعترض رزمة RTP ويعيد إرسال رزمة SRTP مكافئة في جانب الإرسال، ويعترض رزمة SRTP ويمرر رزمة RTP مكافئة داخل البطارية في جانب الاستقبال. فهو أساساً يجفّر الحمولة النافعة لرزمة RTP ويضيف وسم استيقان على نهاية الرزمة في جانب الإرسال، ويتحقق من وسم الاستيقان، ويفك تجفير الحمولة النافعة في جانب الاستقبال.

1.1.10 خوارزميات التجفير والاستيقان

من الجائز في عنصر حدي لشبكة (NBE) يستطيع تأدية البروتوكول SRTP أن يستطيع تأدية خوارزمية التجفير المتقدمة (AES) بأسلوب السحب من الشبّاك طبقاً للمعيار [b-IETF RFC 3711]. انظر أيضاً المعيار [b-NIST FIPS SP 800-38a] للوقوف على مزيد من المعلومات. ويستطيع العنصر NBE تأدية الخوارزمية HMAC-SHA1 من أجل تدقيق سلامة رسالة ما، بوسم طوله 80 بتة.

2.1.10 توليد المفتاح والتفاوض على متوالية التجفير

يمكن أن يتم توليد مفتاح للبروتوكول SRTP بعدة وسائل:

1) بالتزويد (عن طريق عنصر تزويد التجهيزات المطرافية)؛
2) باستعمال مواد مفتاح، ولّده جهاز النقطة الطرفية وأُدرِج في بروتوكول وصف الدورة (SDP) طبقاً للمعيار [b-IETF RFC 4566]، وذلك في طلبات التمهيد؛
3) تبادل مواد مفتاح باستعمال بروتوكول إدارة مستقل يعقبه البروتوكول SDP.

بخصوص كل مشترك، يستطيع العنصر الحدي للشبكة (NBE) أن يحصل من الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA -FE) أو الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) على المفتاح الرئيسي للبروتوكول SRTP، ثم يشتق منه المفتاحين الأوليين لدورتي التجفير والاستيقان. ويمكن توفير مفتاح رئيسي للبروتوكول SRTP بطول 128 بتة. ويستطاع توفير خوارزمية اشتقاق المفتاح الموصوفة في الوثيقة [b-IETF RFC 3711]. قد يكون طول المفتاح الأولي للتجفير 128 بتة، ومفتاح salt الأولي للدورة قد يكون طوله 112 بتة، وقد يكون طول المفتاح الأولي للاستيقان 160 بتة. ومتى أُصدِر مفتاح SRTP رئيسي إلى مشترك، يكون في استطاعة العنصر الحدي للشبكة (NBE) أن يستعمله فوراً.

إذا كان بروتوكول وصف الدورة (SDP) الذي يحتويه طلب التمهيد له قيمة "RTP/SAVP" كقيمة بروتوكول وسائط في السطر (line) "m="، ولم يكن أي قيمة مفتاح في السطر "k="، ولا يوجد نعت "a=crypto"، فعندئذ يستطيع العنصر الحدي للشبكة (NBE) استعمال المفاتيح الأولية، التي ولّدها نظام التزويد، مفاتيحَ فعلية للدورة. وفي هذه الحالة تكون متوالية التجفير غير خاضعة للتفاوض.

إذا كان البروتوكول SDP الذي يحتويه طلب التمهيد له قيمة "RTP/SAVP" كقيمة بروتوكول وسائط في السطر "m="، ولا يوجد نعت "a=crypto"، وكانت قيمة مفتاح في السطر "k="، فعندئذ يستطيع العنصر NBE أن يستعمل المفتاح الذي يحتويه السطر "k=" مفتاحاً رئيسياً للبروتوكول SRTP، وأن يولّد منه مفتاح الدورة ومفتاح الاستيقان. وفي هذه الحالة تكون متوالية التجفير غير خاضعة للتفاوض.

إذا كان البروتوكول SDP الذي يحتويه طلب التمهيد له قيمة "RTP/SAVP" كقيمة بروتوكول وسائط في السطر "m=" line، ويوجد نعت "a=crypto"، فعندئذ يستطيع العنصر NBE أن يعمل بمتطلّبات الوثيقة [b-RFC 4568] من أجل توليد مفتاح الدورة ومفتاح الاستيقان. مثلاً: مدخل البروتوكول SDP وهو: "a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4" يدل على أن متوالية التجفير هي: AES_CM_128_HMAC_SHA1_80، وأن المعلمة المفتاحية (key_param) يعرّفها النص البادئ بكلمة "inline:". وداخل المعلمة المفتاحية، المجال الأول هو المفتاح الرئيسي مذيَّل بالمفتاح salt الرئيسي، متسلسلاً ثم مشفَّرا على أساس base64. وقائمة متواليات التجفير الصالحة معطاة في الجزء 2.5 من المعيار [b-IETF RFC 4568] ومن هذه القائمة تختار متوالية تكون بمثابة جزء من تبادل العرض/الاستجابة في إطار البروتوكول SDP.

إذا كان البروتوكول SDP الذي يحتويه طلب التمهيد له قيمة "RTP/SAVP" كقيمة بروتوكول وسائط في السطر "m="، وله نعت "a=key-mgmt"، فعندئذ يستطيع العنصر NBE أن يعمل بمتطلّبات المعيار [b-IETF RFC 4567] فيولّد مفاتيح ومعلمات أمن. مثلاً: يدل النص "a=key-mgmt:mikey AQAFgM0XflABAAAAAAAAAAAAA..." على أن بروتوكول إدارة المفاتيح هو mikey المعرَّف في الوثيقة [b-IETF RFC 3830]، وأن باقي النص هو معطيات إدارة المفاتيح مشفَّرة على أساس base64 طبقاً للمعيار [b-IETF RFC 4648].

3.1.10 السطح البيني للاستيقان بين عنصر لشبكة NGN ومخدم الإذنات المأمونة

تستطيع عناصر شبكة NGN إنفاذ الطبقة البسيطة للاستيقان والأمن (SASL) المعرَّفة في [b-IETF RFC 4422] التي تحمي وظائف OAMP لهذه العناصر. وتستطيع الطبقة SASL هذه أن تتضمّن تحقق استيقان مبنيا على إذنة مأمونة، طبقاً للتعريف الموضوع في المعيار [b-IETF RFC 2808]. وتتطابق هذه مع "الإذنة المأمونة" لمفتاح الطبقة SASL. فالمستعمل الراغب في النفاذ إلى الوظائف OAMP يقدم ما يلي:

1) هوية تخويل (تمكّن مدراء النظام من فتح الدورة بواسطة هوية مستعمل مختلفة؛ وفي حالة الخلو، تتخذ القيمة الفرضية أي هوية الاستيقان)؛
2) هوية استيقان (هوية يُستعمَل معها الرمز السري)؛
3) قيمة رقم تعريف الهوية الشخصي للمستعمل مع رمز سري سداسي الأرقام على الإذنة المأمونة.

يستطيع العنصر الشبكي لشبكة NGN إعمال زبون ممتثِل للكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA -FE) أو الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE) كجزء من مناولة الطبقة SASL للإذنة المأمونة. يجمع عنصر الشبكة NGN ما قدّم المستعمل من إثباتات ويرسلها إلى مخدم الإذنات المأمونة. والمجالات التي يشملها جمع الثبوتيات هي مجال كل من اسم المستعمِل، ورقم تعريف الهوية الشخصي له، والقيمة المعروضة حاليا للإذنة المأمونة. ويستقبل العنصر الشبكي رداً بالقبول/الرفض/تكرار المحاولة. فإذا نجحت المحاولة، تُمكّن الطبقةُ SASL المستعملَ من النفاذ إلى وظائف التشغيل والإدارة والصيانة والتزويد (OAMP)، بناءً على سوية النفاذ المصاحبة لاسم المستعمل.

11 الوظائف OAMP

ينبغي أن يؤخذ تسجيلُ تدقيق لجميع محاولات النفاذ إلى وظائف التشغيل والإدارة والصيانة والتزويد (OAMP)، ولجميع التغييرات التي تُدخَل على الوظائف OAMP، ولجميع إعلانات مغادرة الوظائف OAMP. وبالإضافة إلى ذلك، تُسجَّل أيضاً الأحداث التي تُعتَبر هامة من حيث نهج مورِّد شبكة NGN.

في هذا الجزء توصف بعض الآليات المتعلقة بالخصائص الهامة. وليس ذلك على سبيل الحصر، بل من الجائز اعتماد أشكال أخرى من التنفيذ، تبعاً لسياسة مورِّد شبكة NGN.

ملاحظة – من الضروري مراعاة الأمن في تسجيل الحدث. وبشأن المزيد من المعلومات يُرجَع إلى التوصيتين [ITU-T Y.2701] و[b-ITU-T M.3016.0].

1.11 السطح البيني للعناصر الشبكية وأنظمة التسجيل

يُوصى بأن ترسل العناصر الشبكية معلوماتها التسجيلية إلى مخدم تسجيل بعيد. تستطيع العمل بمتطلبات هذا الجزء العناصر التي تستعمل بروتوكول التسجيل النظامي (Syslog) المعرَّف في [b-IETF RFC 5424] لتأدية هذه الوظيفة.

والعناصر التي تستعمل بروتوكول التسجيل النظامي (Syslog) تستطيع أن تُدرِج دمغة وقت، بناء على قيمة الوقت المستلمة عن طريق بروتوكول وقت الشبكة البسيطة/بروتوكول وقت الشبكة (SNTP/NTP) من مصدر توقيت موثوق، وتستطيع العناصر المشار إليها أن تعطي دمغة الوقت بالتوقيت العالمي المنسَّق (UTC). وتستطيع هذه العناصر إدراج اسم مخدمها (إذا سبق تزويدها به) أو عنوانها حسب بروتوكول IP في رأسية الرسالة المعتمِدة على البروتوكول syslog.

2.11 استعمال العناصر الشبكية بروتوكول إدارة الشبكات البسيط (SNMP)

من الأمور الأساسية أن تكون العناصر الشبكية لشبكات الجيل التالي (NGN) قابلة أن تُدار من منصّة نائية. وبروتوكول إدارة الشبكات البسيط (SNMP) هو الآلية المعيارية صناعياً لعمل ذلك. ولما كانت الصيغة 3 لهذا البروتوكول (SNMPv3) المعرَّفة في [b-IETF RFC 3413] و[b-IETF RFC 3414] و[b-IETF RFC 3415] تحل كثيراً من الأعطاب الأمنية الحاضرة في الصيغة SNMPv2، فقد أصبحت متيسّرة على نطاق يتزايد اتساعاً.

يوصى بأن ترسل العناصر الشبكية معلوماتها التسجيلية إلى مخدم تسجيل بعيد. وتستطيع هذه العناصر استعمال بروتوكول إدارة الشبكات البسيط (SNMP) لتأدية هذه الوظيفة، مع مراعاة التحذيرات الواردة في مواضع أخرى من هذه التوصية بشأن الصيغة 3 من هذا البروتوكول (SNMP v3).

والبروتوكول SNMP معرَّف بمعمارية إجمالية في المعيار [b-IETF RFC 3411]، وبآلية تسمية الأشياء والأحداث (قاعدة معلومات الإدارة = MIB, *management information base*) (انظر المعايير التالية: [b-IETT RFC 1155] و[b-IETF RFC 1212] و[b-IETF RFC 1215] و[b-IETF RFC 2578] و[b-IETF RFC 2579] و[b-IETF RFC 2580])، وبالعمليات البروتوكولية، (المعياران [b-IETF RFC 3416] و[b-IETF RFC 3417]). وفي الجزء 7 من المعيار [b-IETF RFC 3410] عرضٌ شامل أكثر تفصيلاً عن الوثائق التي تصف إطار الإدارة الحالي حسب معيار الإنترنت.

يستطيع كل عنصر من عناصر الشبكات NGN إعمال زبون لبروتوكول إدارة الشبكات البسيط (SNMP). وإذا استعملت هذه العناصر الصيغة 1 أو الصيغة 2 للبروتوكول SNMP، يتوجّب عليها استعمال بروتوكول وحدات بيانات المستعمل (UDP) كوسيلة نقل في إطار أمن الإنترنت (IPSec)، إذا كانت تقتضي ذلك السياسة الأمنية التي ينتهجها مورِّد الشبكةNGN . ويُشفَّر كل مِثْل من أمثال رسالة ما باستعمال قواعد التشفير الأساسية الموضوعة في ASN.1 (قواعد التركيب المجردة رقم 1)، الوثيقة [ITU-T X.690]، وذلك في وحدة بيانات من وحدات البروتوكول UDP. ويستطيع الزبون الاستماع على المنفذ 161 إلى تطبيقات مستجيب الأوامر، ويستطيع الاستماع على المنفذ 162 إلى تطبيقات مستقبِل التبليغات.

ويتوجب على عناصر الشبكات NGN إعمال كل قواعد معلومات الإدارة (MIB) الضرورية للإخبار عن الأحداث الأمنية وتسجيلات التدقيق.

3.11 إدارة التصويبات الأمنية

إن تركيب تصويبات صيانة وتصويبات أمن بصورة منتظمة على العناصر الشبكية والخوادم لشبكات NGN يقلل مطاعنها أمام الهجمات والأعطال غير المقصودة. فمن المطلوب وضع وإنفاذ استراتيجية شاملة لإدارة التصويبات، بما في ذلك تركيب إجراءات ومنصّات تحقق.

4.11 إدارة الصيغ

يتوجب حفظ تشكيلات العناصر الشبكية وتغييراتها. والهدف الرئيسي لاحتياطيّ النظام هو التمكين من استعادة النظام إذا وقعت أعطال عَتادية أو برمجية تسفر عن تلف حمولة برمجيات و/أو معطيات النظام المصاحبة لها. يمكن تضمين حمولة احتياطي النظام الأنواع التالية من المعلومات:

- معطيات الزبون ومنطقه.
- توصيلية حركة الشبكة مثل المرافق والخطوط الرئيسية.
- الموجة الحاملة لشبكة NGN والبرمجيات التطبيقية التي زوّد بها الصانع النظام.
- نظام التشغيل.
- تشكيلة العتاد.

ومطلوب عمل تسجيل مستمر لنشاط التزويد لكي يمكن تحيين أي عنصر شبكي مع أعمال التزويد التي حصلت منذ أُخذت صورة الاحتياطي.

وتستطيع منصة التزويد الإمداد بالمقْدِرات التالية:

- ملف رصد لأنشطة التزويد لكل من العناصر الشبكية التي زوّدتها مباشرة.
- ما يعادل على الأقل أسبوعاً من أنشطة التزويد لكل عنصر شبكي.

وتستطيع منصة التزويد تمكين المستعملين من القيام يدوياً باستعراض أنشطة التزويد المخزَّنة لكل عنصر شبكي. ويجب في وصف النشاط المتاح للمستعمل أن يوفر خلاصة لقدِّ المعاملات التي جرت في فاصل زمني معيّن، وقدّ كل منها، وعددها، وأنواعها.

كما تستطيع منصة التزويد توفير مرفق يمكّن من إعادة تزويد عنصر شبكي معيّن عن طريق إعادة إدخال معطيات في عنصر شبكي محدد. ويُفترض في هذا المرفق أن يمكّن من اختيار يوم/ساعة البدء والنهاية للمعطيات التي يلزم إعادة التزويد بها. وينبغي أن تستطيع منصة التزويد، بناءً على التاريخ والتوقيت المحددَيْن، أن تُدخِل من جديد أوتوماتياً جميع المعطيات الحادثة في العنصر الشبكي المحدد.

5.11 تسجيل التدقيق، والتفخيخ، وتسجيل الأداء والوقائع في العنصر TE-BE

ينطبق على العنصر الحدي للتجهيزات المطرافية (TE-BE) جميع الاشتراطات المطلوب أن تفي بها العناصر الشبكية لشبكات NGN من تسجيل التدقيق والتفخيخ وتسجيل الأداء والوقائع.

العنصر الحدي للتجهيزات المطرافية (TE-BE) موصول بأنظمة الوظائف OAMP عن طريق نفق شبكة خاصة تقديرية (VPN). فهو يرسل إذاً رسائله المتعلقة بتسجيل الأداء والوقائع، ويستقبل طلبات البروتوكول SNMP ويستقبل استجابات SNMP عن طريق الشبكة VPN هذه. ولا يوصى بأن يقبل العنصر TE-BE طلبات من الوظائف OAMP على أي سطح بيني آخر.

والاشتراطات بخصوص نفق الشبكة VPN مبيَّنة في الفقرة 4.9.

12 تزويد التجهيزات في المنطقة غير الموثوقة

جميع تجهيزات مقر الزبون تتلقى تشكيلتها من عنصر تزويد التجهيزات المطرافية. ويكون عنصر تزويد التجهيزات المطرافية مقيما في المنطقة المأمونة، ولا يستطيع الاتصال بهذه التجهيزات إلا عن طريق العنصر الحدي للشبكة (NBE) كما هو مبيّن في الشكل 2. يستطيع تجهيز مطرافي أو العنصر الحدي للتجهيزات المطرافية إجراء الاستيقان وإقامة تصاحب أمني مع العنصرNBE قبل أن يتمكن من الحصول على ملف التشكيلة من عنصر تزويد التجهيزات المطرافية. ويستطيع العنصر NBE الاشتغال بالبروتوكول TLS وبالبروتوكول IPsec من أجل إقامة تصاحب أمني مع التجهيزات المطرافية (بما فيها العنصر الحدي لهذه التجهيزات (TE-BE). راجع التفاصيل في الفقرتين 1.9 و2.9.

وفي هذا السياق تعامل التجهيزات التي يتحكم فيها المورِّد معاملة جزء من العنصر الحدي للشبكة (NBE).

يُدرج عنصر التزويد عنوان العنصر NBE في معطيات التشكيلة التي تُنزَّل في الجهاز الذي تم استيقانه. ويستطيع عنصر تزويد التجهيزات المطرافية أيضا أن يدرج شهادة استعملت لاستيقان المشترك في NBE كما هو موصوف في الفقرة 4.8.

يطلب الجهاز TE تزويده لدى مورِّد خدمة شبكات NGN. ويستقبل العنصر الحدي للشبكة (NBE) هذا الطلب، فيستيقن التجهيز المطرافي بواسطة الكيان الوظيفي لاستيقان الخدمة وتخويلها (SAA-FE) أو الكيان الوظيفي لاستيقان النقل وتخويله (TAA-FE). ومتى تم استيقان الجهاز، يعيد العنصر الحدي تسيير طلب التزويد إلى عنصر تزويد التجهيزات المطرافية. ويقوم عنصر تزويد التجهيزات المطرافية بعد ذلك بتحميل التشكيلة و/أو البرامج الثابتة في التجهيز المطرافي. وإذا تعذّر استيقان التجهيز المطرافي، تُسجَّل واقعة الإخفاق هذه.

التذييل I

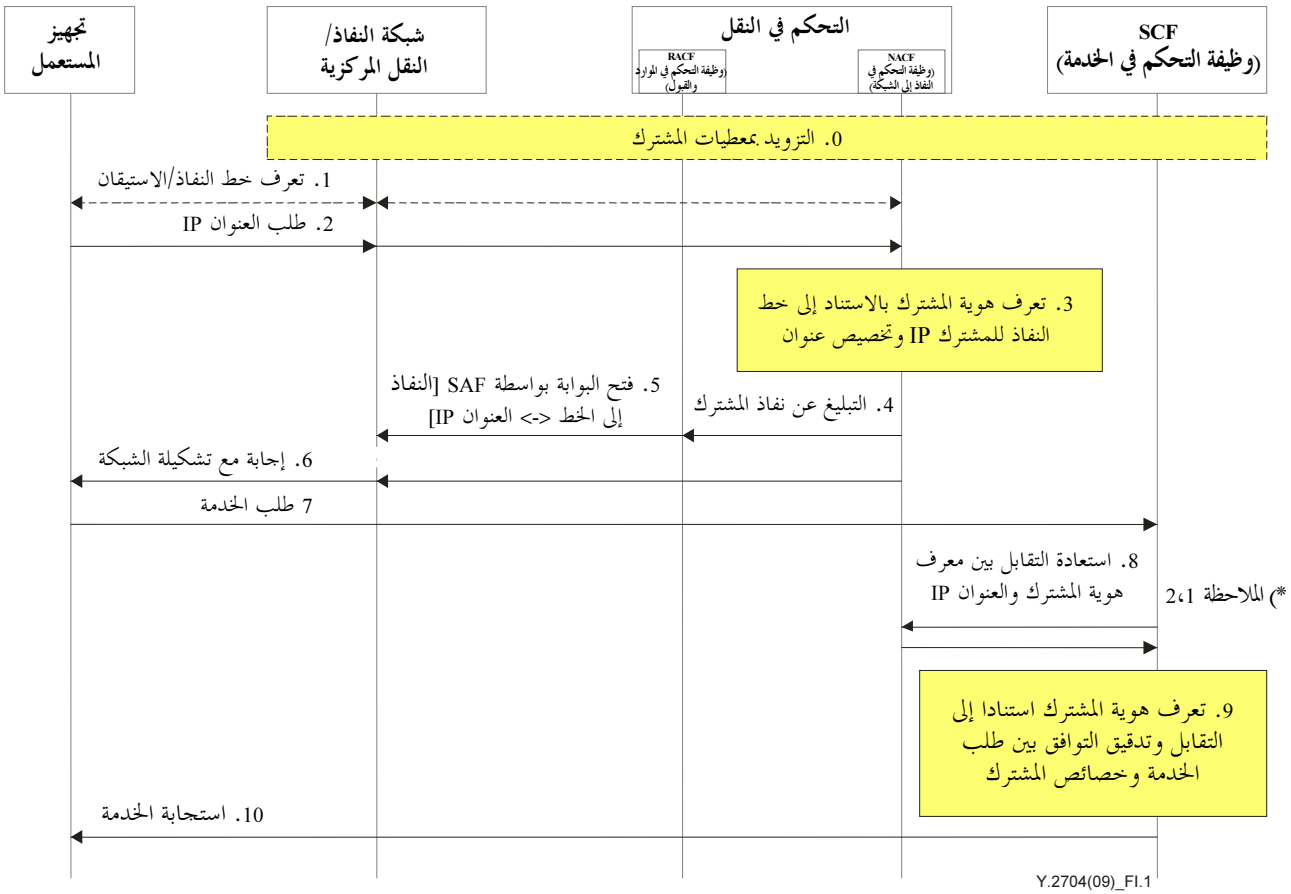
أمثلة على آليات ضمانة العنوان الأصلي
وتطبيقها على آلية تعرّف هوية المشترك واستيقانه

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل أمثلة محسوسة على آليات ضمانة العنوان الأصلي وتطبيقها على تعرف هوية المشترك واستيقانه، من خلال العنوان الأصلي الشبكي الموصوف في الجزء 2.4.8.

1.I تعرّف هوية المشترك واستيقانه مقروناً باستيقان خط النفاذ

يقدم هذا الجزء مثالاً على تعرف هوية المشترك واستيقانه، وفيه يُخصص له عنوان IP نتيجة لاستيقان خط النفاذ. وفي هذا النفاذ يقام تصاحب سكوني بين المشترك وخط نفاذه. وعليه فإن الآلية الموصوفة في هذا المثال لا تنطبق إلا على الخدمات غير الرحالة (أي الثابتة).



الملاحظة 1 – معلومات التقابل بين العنوان IP ومعرّف هوية المشترك تستطيع وظيفة التحكم في النفاذ إلى الشبكة (NACF) أن تزوّد بها وظيفة التحكم في الخدمة (SCF) عند تخصيص الوظيفة NACF العنوان IP.

الملاحظة 2 – تستطيع الوظيفة NACF، بدلاً من معلومات التقابل بين العنوان IP ومعرّف هوية المشترك، أن تزوِّد بمعلومات التقابل بين العنوان IP ومعلومات تحديد الموقع (معرّف هوية خط النفاذ، مثلاً). وفي هذه الحالة، يتوجّب على وظيفة التحكم في الخدمة (SCF) استبقاء التقابلات بين معرّفاً حسابات المشتركين (subscriber IDs) ومعلومات تحديد الموقع، واشتقاق هوية المشترك من المعلومات عن الموقع التي أرسلتها وظيفة التحكم في النفاذ إلى الشبكة (NACF).

الشكل 1.I – تدفقات الرسائل رفيعة المستوى للمثال 1

شروح

0 خصائص المشترك تكون تشكيلتها مرسلة سلفاً إلى الكيانات الوظيفية ذات الصلة (مثل الكيان الوظيفي لخصائص مستعمل النقل (TUP-FE)، والكيان الوظيفي لخصائص مستعمل الخدمة (SUP-FE)) القائمة في وظيفة التحكم بالنفاذ إلى الشبكة (NACF) أو في وظيفة التحكم بالخدمة (SCF).

1) أهم المسائل التشكيلية في هذا السيناريو اثنتان: (1) أن الوظيفة NACF (أي عادة الكيان الوظيفي TUP-FE) تستبقي التقابلات بين معرِّفات حسابات المشتركين (subscriber IDs) ومعرّفات خطوط النفاذ المنطقية/المادية (مثل معرِّف هوية شبكة منطقة محلية تقديرية (VLAN ID) أو نقطة النفاذ)؛

2) أن الوظيفة SCF (أي عادة الكيان الوظيفي SUP-FE) تستبقي التقابلات بين معرِّفات حسابات المشتركين (subscriber IDs) ونعوت أو خصائص المشتركين المناظرين (أي قيم رأسية "المرسل " في الخدمات المبنية على بروتوكول فتح الدورة (SIP)). وفي حالة اختلاف اسم حيِّز معرِّفات حسابات المشتركين (subscriber IDs) في SCF عنه في NACF، توصَى SCF أيضاً باستبقاء التقابلات بين هذه المعرِّفات.

بالمقابل، لا يتوجب على NACF استبقاء التقابلات بين معرِّفات حسابات المشتركين (subscriber IDs) ومعرِّفات خطوط النفاذ. وفي مثل هذه السيناريوهات، توصَى SCF باستبقاء التقابلات بين معرِّفات حسابات المشتركين (subscriber IDs) ومعرِّفات خطوط النفاذ، بحيث تكون الوظيفة SCF قادرة على استعادة معرِّف هوية مشترك من معرِّف خط نفاذ.

على جميع الوصلات البوابية (gateways) لشبكة النفاذ/شبكة النقل المركزية، تكون جميع بوابات (gates) خطوط النفاذ للمشتركين مشكَّلة في البدء تشكيل إغلاق، بحيث تُسقَط أي رُزَم IP واصلة، باستثناء الرزم الضرورية لربط تجهيز المستعمل بالشبكة (مثل إرسال طلبات عناوين أو طلبات استيقان).

1 يرتبط تجهيز المستعمل بشبكة النفاذ عن طريق خط النفاذ لكي يحصل على توصيلية IP لشبكة NGN. هذا المثال يفترض أن استيقان NACF جارٍ ضمنياً ويتم تنفيذه في المرحلة 3. لكنّ NACF تستطيع بدلاً من ذلك استعمال طريقة استيقان للنفاذ صريحة (كما هو موصَّف في IEEE 802.1X). وعندئذ يُنفَّذ استيقان النفاذ إلى الشبكة في هذه المرحلة، أي قبل تخصيص العنوان IP.

2 يطلب تجهيز المستعمل تخصيص عنوان IP له. ويتم عادة تخصيص هذا العنوان بإرسال رسالتي استكشاف وطلب بواسطة بروتوكول التشكيلة لمخدم دينامي (DHCP)، وتُرحَّل هاتان الرسالتان عن طريق الوصلات البوابية إلى الوظيفة NACF.

3 في هذا المثال تستيقن شبكة النفاذ خط النفاذ، وتزوِّد الوظيفة NACF بمعرِّف هوية خط النفاذ الذي تم استيقانه (مثل معرِّف هوية شبكة منطقة محلية تقديرية (VLAN ID) أو نقطة نفاذ). وانطلاقاً من ذلك تتمكن وظيفة التحكم في النفاذ إلى الشبكة (NACF) من تعرُّف هوية المشترك الخاصة بتجهيز المستعمل، استناداً إلى معرِّف هوية خط النفاذ الذي أُرسِل عبره طلب العنوان IP. وعندئذ تخصص الوظيفة NACF عنواناً IP لتجهيز المستعمل، مقدِّم الطلب، وتخزّن التقابل بين معرِّف هوية المشترك والعنوان IP الذي تم تخصيصه.

ومن الجائز أن تُدفَع معلومات التقابل هذه من NACF إلى SCF فتُخزَّن (تحفظ منها نسخة خفية) في SCF. وفي هذه الحالة، يمكن تخطّي المرحلة الثامنة أدناه.

4 تبلِّغ NACF الوظيفة RACF (وظيفة التحكم في الموارد والقبول) أن المشترك تم توصيله. وهذا التبليغ يتضمن معرِّف هوية المشترِك، ومعرِّف هوية خط النفاذ (المادي/المنطقي)، والعنوان IP الذي تم تخصيصه، وملفات QoS (جودة الخدمة).

5 تتخذ RACF قراراً سياسياً بتخصيص موارد شبكية للمشترك، وتأمر الوصلات البوابية بفتح البوابة أمام خط النفاذ مع قواعد ترشيح الرزم، قواعد موضوعة من أجل قبول وإعادة تسيير الرزم IP الواصلة التي عنوانها الأصلي هو العنوان IP الذي خُصِّص للمشترك، وإسقاط سائر الرزم الواصلة.

إن إنفاذ ترشيح العنوان IP الأصلي بالاتساق مع استيقان الوظيفة NACF لخط النفاذ، ما تقدم وصفه، يضمن أن العنوان IP لا يمكن أن يستعمله إلا المشترك الذي خُصَّ بهذا العنوان.

6 تعيد الوظيفة NACF العنوان IP المخصص إلى تجهيز المستعمل مع معلمات أخرى لتشكيلة الشبكة (مثل عناوين خواديم نظام أسماء الميادين (DNS)، والوظيفة المفوَّضة للتحكم في دورة النداء (P-CSC-FE)). وهذا يتم عادة بإرسال رسالتي عرض وإجابة بواسطة بروتوكول التشكيلة لمخدم دينامي (DHCP).

7 بعدما يحصل تجهيز المستعمل على توصيلية IP، يرسل طلب خدمة (مثلاً: إشارة تسجيل، في حالة الخدمات المبنية على SIP (بروتوكول فتح الدورة)) إلى الوظيفة SCF. لكن طلب الخدمة لا تمرره الوصلات البوابية (مصدّات ترشّح العنوان الأصلي) إلى الوظيفة SCF إلا إذا كان العنوان الأصلي الذي يحمله الطلب عنواناً خصصته الوظيفة NACF.

8 تسترد الوظيفة SCF معلومات التقابل (أي معرِّف هوية المشترك والعنوان IP المخصص له) المطابقة للعنوان الأصلي الذي يحمله طلب الخدمة وخصصته NACF.

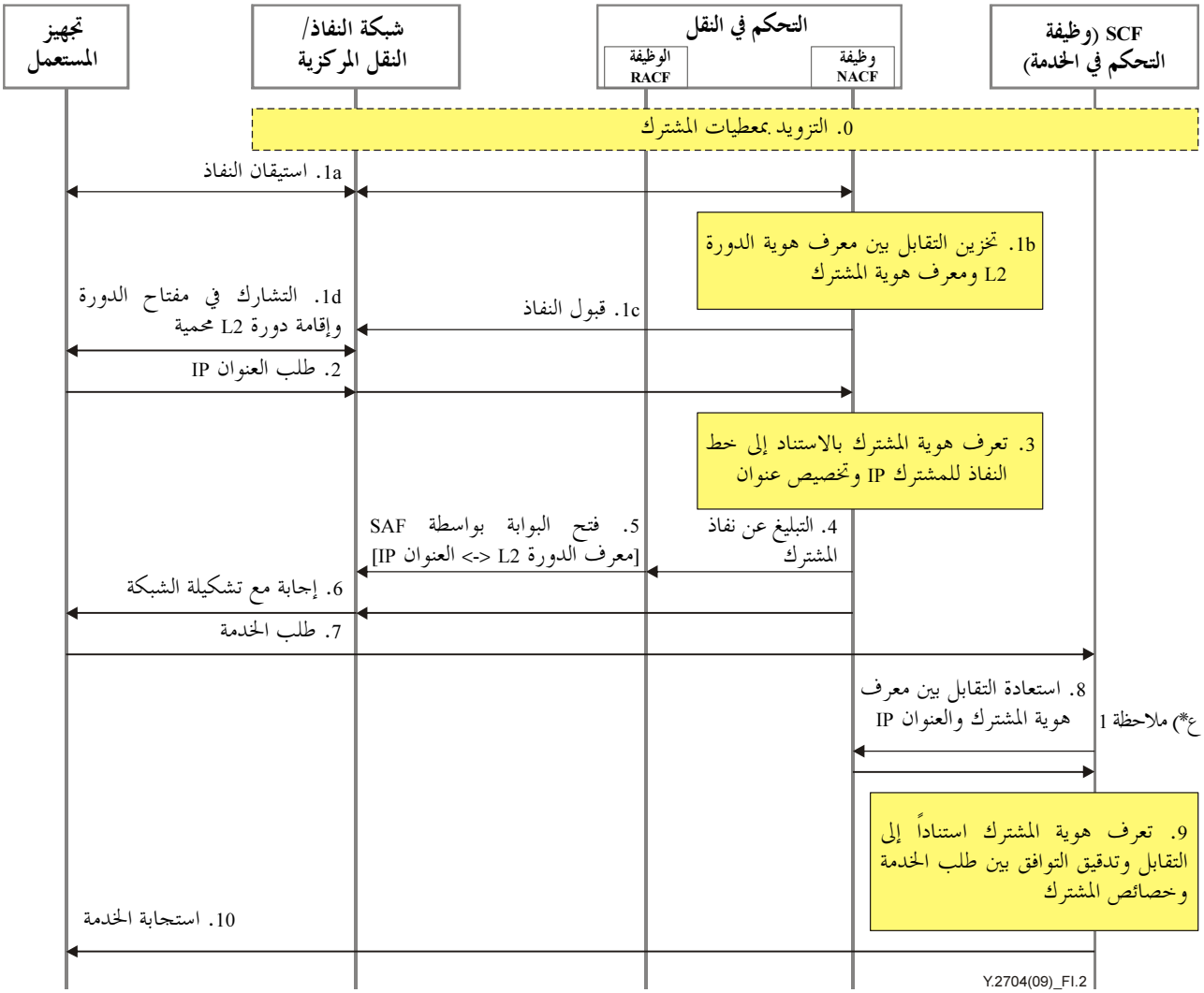
9 تعتبر الوظيفة SCF طلب الخدمة صادراً عن المشترِك المخصوص بمعرِّف هوية المشترِك الذي تحتويه معلومات التقابل المستعادة. وفي حالة اختلاف اسم حيِّز معرِّفات حسابات المشتركين (subscriber IDs) في SCF عنه في NACF، يجب في معرِّف هوية المشترك المستعاد أن يُترجَم إلى معرِّف هوية المشترك في حيز الاسم الذي استعملته SCF بناءً على التقابلات بين هذه المعرِّفات للهوية.

تستخرج الوظيفة SCF قيمة النعوت المناظرة لهوية المشترك (مثلاً: قيمة رأسية "المرسل"، في حالة الخدمات المعتمِدة على بروتوكول فتح الدورة، SIP)، من طلب الخدمة وتدقيقات التوافق بين هذه القيم وخصائص المشترك المناظرة لها.

10 إذا نجح الاستيقان والتخويل، تردّ الوظيفة SCF بالجواب العادي لعرض الخدمة المطلوبة (وهو، مثلاً: "200 OK"، في حالة الخدمات المعتمِدة على بروتوكول فتح الدورة، SIP).

2.I تعرّف هوية المشترك واستيقانه مقروناً باستيقان النفاذ الصريح عند إقامة توصيليةIP

يقدم هذا الجزء مثالاً على تعرف هوية المشترك واستيقانه، يكون فيه العنوان IP نتيجة لاستيقان النفاذ الصريح عند إقامة توصيلية IP. في هذا المثال، لكل مشترك تصاحب دينامي مع دورة طبقة 2 (L2)، يقام وقت استيقان النفاذ. ومن ثَمَّ فإن الآلية الموصوفة في هذا المثال تنطبق على كلا نوعي الخدمات الرحالة وغير الرحالة.



ملاحظة – معلومات التقابل بين العنوان IP وهوية المشترك تستطيع الوظيفة NACF أن تزوّد بها الوظيفة SCF وقتما تخصص الوظيفة NACF هذا العنوان للمشترك.

الشكل I.2 – تدفق الرسائل رفيعة المستوى للمثال 2

شروح

0 خصائص المشترك تكون تشكيلتها مرسلة سلفاً إلى الكيانات الوظيفية (FEs) ذات الصلة (مثل الكيان الوظيفي لخصائص مستعمل النقل (TUP-FE)، والكيان الوظيفي لخصائص مستعمل الخدمة (SUP-FE)) القائمة في وظيفة التحكم بالنفاذ إلى الشبكة (NACF) أو في وظيفة التحكم بالخدمة (SCF). وخلافاً لما ورد في صدد المثال السابق، لا يتوجّب على الوظيفة NACF أن تستبقي التقابلات بين معرِّفات حسابات المشتركين (subscriber IDs) ومعرّفات خطوط النفاذ.

على الوصلات البوابية لشبكة النفاذ/شبكة النقل المركزية، تكون جميع بوابات النفاذ إلى دورات L2 مع تجهيزات المستعمل مشكَّلة في البدء تشكيل إغلاق، بحيث تُسقَط أي رُزَم IP واصلة، باستثناء الرزم الضرورية لربط تجهيز المستعمل بالشبكة (مثل إرسال طلبات عناوين أو طلبات استيقان).

1a حين يطلب تجهيز المستعمل توصيلية مع شبكة NGN، تُنشئ شبكة النفاذ دينامياً دورة L2 مع تجهيز المستعمل هذا، ويُنفَّذ إجراء استيقان للنفاذ، بينه وبين NACF بالاستناد إلى إثباتات المشترك (عادة ما يكون بطريقة استيقان صريحة مثل الطريقة الموصّفة في IEEE 802.1X، وطريقة RADIUS/Diameter). وتعيد الوصلات البوابية إرسال رسائل التشوير المتعلقة بالاستيقان.

1b أثناء إجراء الاستيقان، يُرسَل معرِّف هوية الدورة L2 (مثل VLAN-ID أو عنوان L2 لجهاز المستعمل أو غير ذلك) الذي خُصّ به جهاز المستعمل، إلى الوظيفة NACF. وحين ينجح الاستيقان، تخزّن NACF معرِّف هوية الدورة L2 مع معرِّف هوية المشترك الذي تم استيقانه.

1c تبلِّغ الوظيفة NACF شبكة النفاذ أن تجهيز المستعمل تم استيقانه بنجاح، وخُوِّل النفاذ إلى الشبكة (برسالة قبول النفاذ(ACCESS ACCEPT) مثلاً، في حالة استعمال البروتوكول RADIUS).

1d حالما تستلم شبكة النفاذ التبليغ بنجاح الاستيقان من الوظيفة NACF، تقيم تصاحبا أمنياً (SA) مع تجهيز المستعمل من أجل حماية سلامة الدورة L2 وسريتها. ويتحقق ذلك عادة بفضل آليات اشتقاق مفاتيح الدورة، آليات معرَّفة في IEEE 802.1X، وبفضل إجراء الحماية المعرَّف لكل تكنولوجيا لـ L2 (مثل تكنولوجيا TKIP/CCMP المعرَّفة في IEEE 802.11i من أجل شبكة LAN اللاسلكية المعرَّفة في 802.11).

إن آليات الأمن المتقدم وصفها هذه تحمي دورة L2 من أن يستعملها مشتركون آخرون، وتوفّر الوسائل الضرورية لدرء سرقة العنوان IP بالخديعة.

2 يطلب تجهيز المستعمل تخصيص عنواناً IP له. ويتم عادة تخصيص هذا العنوان بإرسال رسالتي استكشاف وطلب بواسطة بروتوكول التشكيلة لمخدم دينامي (DHCP)، وتُرحَّل هاتان الرسالتان عن طريق الوصلات البوابية إلى الوظيفة NACF.

3 تتعرَّف وظيفة التحكم في النفاذ إلى الشبكة (NACF) هوية المشترك الخاصة بتجهيز المستعمل، استناداً إلى معرِّف هوية الدورة L2 الذي أُرسِل عبره طلب العنوان IP. وعندئذ تخصص الوظيفة NACF عنواناً IP لتجهيز المستعمل، مقدِّم الطلب، وتخزّن التقابل بين معرِّف هوية المشترك والعنوان IP الذي تم تخصيصه.

ومن الجائز أن تُدفَع معلومات التقابل هذه من NACF إلى SCF فتُخزَّن (تحفظ منها نسخة خفية) في SCF. وفي هذه الحالة، يمكن تخطّي المرحلة الثامنة أدناه.

4 تبلِّغ NACF الوظيفةَ RACF (وظيفة التحكم في الموارد والقبول) أن المشترك تم توصيله. وهذا التبليغ يتضمن معرِّف هوية المشترك، ومعرِّف هوية الدورة L2 (المادية/المنطقية)، والعنوان IP الذي تم تخصيصه، وملفات QoS (جودة الخدمة).

5 تتخذ RACF قراراً سياسياً بتخصيص موارد شبكية للمشترك، وتأمر الوصلات البوابية بفتح البوابة أمام دورة L2 مع قواعد ترشيح الرزم، قواعد موضوعة من أجل قبول وإعادة تسيير الرزم IP الواصلة التي عنوانها الأصلي هو العنوان IP الذي خُصِّص للمشترك، وإسقاط سائر الرزم الواصلة.

إن إنفاذ ترشيح العنوان IP الأصلي بالاتساق مع استيقان الوظيفة NACF للنفاذ، ما تقدم وصفه، يضمن أن العنوان IP لا يمكن أن يستعمله إلا المشترك الذي خُصَّ بهذا العنوان.

الخطوات 6 – 10 هي نفس الخطوات التي تقدم شرحها في الفقرة I.1 بخصوص المثال السابق.

التذييل II

أمن التوصيل البيني لخدمة اتصالات الطوارئ (ETS)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II الخلفية

خدمة اتصالات الطوارئ (ETS) هي خدمة وطنية، توفِّر الخدمات لمستعمليها بصفة أولوية في ظروف الكوارث والطوارئ. وإعمال الخدمة ETS مصلحة وطنية. لكن الكوارث/الطوارئ تتجاوز أحياناً الحدود الجغرافية، ومن ثم بات من المحتمل أن تُبرم البلدان/الإدارات اتفاقات ثنائية و/أو متعددة الأطراف للربط بين أنظمتها الخاصة بالخدمة ETS. وتسمح هذه الاتفاقات في حالة إبرامها بخدمات اتصالات أولوية (بالصوت مثلاً أو المراسلة أو الفيديو أو المعطيات) تحت غطاء الخدمة ETS التي يجب، في ظروف الكوارث والطوارئ، تأديتها بين مختلف الشبكات الوطنية الداخلة في اتفاقات ثنائية و/أو متعددة الأطراف. ويكون ضمان اتصالات الخدمة ETS وتيسرها رهناً بأمن المقْدِرات وبالتدابير النافذة في كل شبكة وطنية داخلة في اتصالات من طرف إلى طرف.

2.II مجال التطبيق/الغرض

يقدم هذا التذييل إرشادات تمكّن من دعم الأمن الموفَّر للشبكات من أجل اتصالات الخدمة ETS عبر مختلف الشبكات الوطنية (أي البلدان/الإدارات) التي تؤدي الخدمة ETS.

لا يدخل في مجال تطبيق هذا التذييل وظيفة أمن المستعمل النهائي من ند إلى ند التي تستعمل وظائف خاصة لتحقيق الأمن لتجهيز المستعمل النهائي. إذ إن مجال هذا التذييل مقصور على توفير الأمن للشبكات، من أجل الاتصالات المتعلقة بالخدمة ETS، التي تُجرى عبر شبكات متعددة، وذلك على أساس الحماية من مرحلة إلى أخرى. ومع ذلك، يوصى بأن تكون شبكات الجيل التالي (NGN) قادرة على تأدية وظائف الأمن من ند إلى ند هذه تأدية شفافة.

وليس مقصوداً بهذا التذييل فرض شروط على الأشكال الوطنية لتنفيذ الخدمة ETS. إنما الغرض الرئيسي منه هو تعزيز الأمن الموفَّر للشبكات من أجل اتصالات الخدمة ETS (بالصوت مثلاً أو المراسلة أو الفيديو أو المعطيات) عبر مختلف الشبكات الوطنية (أي البلدان/الإدارات) التي تؤدي هذه الخدمة.

3.II أهداف الأمن والخطوط التوجيهية لإقامة التوصيل البيني للخدمة ETS

يُرجَع بشأن المعلومات عن أهداف الأمن والخطوط التوجيهية لإقامة التوصيل البيني للخدمة ETS، إلى التذييل I من التوصية [ITU-T Y.2701].

4.II الاستيقان والتخويل

يوصى بأن يكون في استطاعة الشبكات الوطنية تأدية وإعمال آليات ومقْدِرات لاستيقان وتخويل مستعمل الخدمة ETS أو الجهاز المستخدَم لها أو المنظومة المكوَّنة من جهاز ومستعمل، بناء على سوية الضمان اللازمة للنفاذ إلى خدمة معيّنة (بالصوت، مثلاً أو المعطيات أو الفيديو) وعلى السياسة المطبَّقة.

ويوصى بأن تُستعمَل حسب الأصول آليات الأمن الموصوفة في متن هذه التوصية لتعرف واستيقان هوية المستعملين وأجهزتهم، من أجل دعم أشكال التنفيذ للخدمة ETS في الشبكات الوطنية، يعني ما يلي:

- تصاحبات IPsec/TLS.
- طريقة التحدي والرد في إطار البروتوكول SIP والشهادات المعرَّفة في التوصية X.509.
- معمارية التمهيد التنوعية.

ويوصى، إضافة إلى ذلك، بإعمال التدابير الأمنية الخاصة بمراقبة النفاذ إلى موارد الخدمة ETS، من أجل كشف وصد الهجمات التي من نوع منع الخدمة.

راجع أيضاً التذييل I للتوصية [ITU-T Y.2702] للوقوف على معلومات عن أمثلة على طرائق الاستيقان والتخويل في إطار الخدمة ETS.

5.II أمن النقل بخصوص التشوير والوظائف OAMP

يوصى بأن تُستعمَل حسب الأصول آليتا الأمن، IPsec وTLS، الموصوفتان في متن هذه التوصية لحماية حركة التشوير والوظائف OAMP للخدمة ETS في الشبكات الوطنية.

6.II حركة الوسائط

يوصى بأن تُستعمَل حسب الأصول، لحماية حركة الوسائط للخدمة ETS في الشبكات الوطنية، آليات الأمن الموصوفة في متن هذه التوصية لتعرّف وحماية حركة الوسائط.

7.II إعمال الخصائص التقييدية بخصوص معرّف هوية الرقم الطالب ومعرّف هوية الاسم الطالب

معرف هوية الرقم الطالب ومعرّف هوية الاسم الطالب هما خَصيصتان موروثتان عن الشبكة الهاتفية التبديلية العمومية، تمكّنان المستعملين من معرفة طالب النداء. ومن شأن نداءات الخدمة ETS أن تخدم مستعملين ينتمون إلى جماعات وطنية مختلفة، ويختلفون من حيث الإدراك لخطورة إفشاء هذه المعلومات للطرف المطلوب. ولذا يوصَى بتوفير آلية ناجعة لإنفاذ سياسة أمنية بشأن عرض أو إفشاء معلومات عن مستعملي الخدمة ETS.

8.II جعل الاقتفاء مستحيلاً

من المهم بخصوص بعض اتصالات الخدمة ETS جعل المعلومات المحددة للموقع المقترنة بطالب النداء أو بمطلوب النداء، غير متيسّرة لسائر الأطراف، وذلك بأقصى درجة ممكنة لمنع التيسّر. وعلى وجه الخصوص، يوصى بشأن أي معلومة عن الموقع أن تُحذف أو، عند اللزوم، أن يُنـــزَل محلها معلومات بلا مغزى، حسبما يناسب، وبناء على سياسة قابلة للتطبيق. والمعلومات المرتبطة بتحديد الموقع تشتمل ولا تقتصر على ما يلي:

1) منطقة خطة الترقيم (NPA) – النقطة المرجعية NXX أو معرِّف الموارد الموحد (URI) لطالب النداء.
2) العنوان الجغرافي لطالب النداء أو مطلوبة.
3) الإحداثيات x-y لكلا الطرفين الطالب والمطلوب.
4) المعلومات الخلوية لكلا الطرفين الطالب والمطلوب، الممكن استعمالها بتضييق مساحة الموقع حتى الخلية.
5) العنوان IP لكلا الطرفين الطالب والمطلوب.
6) المعلومات المتعلقة بالمكتب الطرفي أو بأي مرفق آخر لكلا الطرفين الطالب والمطلوب، التي من شأنها التمكين من تحديد القرب الجغرافي لطالب النداء.

9.II التجفير من ند إلى ند من طرف إلى طرف

قد تطلب طائفة معيّنة من المستعملين تجفير نداءات/دورات الخدمة ETS لتجهيز المستعمل. بخصوص هذه النداءات/الدورات، تنطبق الإجراءات العادية لإقامة نداء/دورة خدمة ETS، وعملية التجفير من طرف إلى طرف يوفّرها تجهيز المستعمل فيما يخص معلومات مقدِرة الحمالة (الصوت، مثلاً) لتجهيز المستعمل الذي عنده ينتهي الاتصال. وعملية التجفير هذه تكون شفافة بالنسبة لشبكات NGN. ولكن يوصى بأن تكون هذه الشبكات قادرة على تأدية الوظائف الخاصة بالتبادل الندي هذه أداء شفافاً.

التذييل III

أفضل الممارسات الأمنية

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.III مقدمة

قد يلزم إعمال آليات أمن إضافة على ما ذُكر في هذه التوصية، إذا أريد الوفاء بالمتطلبات المبيّنة في التوصية [ITU-T Y.2701]. فيستحسن، في سبيل تأمين البنية التحتية لشبكات NGN، استعمال آليات أفضل الممارسات الأمنية مثل المصدّات، وتشديد مناعة نظام التشغيل، ومسح النواحي الضعيفة، وأنظمة كشف الاقتحام (IDS). راجع دليل أنظمة كشف ومنع الاقتحام (IDPS) في المعيار [b-NIST SP 800-94] الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST)، وكذلك الإرشادات الصادرة عنه المتعلقة بمنع ومعالجة حوادث البرمجيات الضارة المبيّنة في المعيار [b-NIST SP 800-83].

يعرض هذا التذييل باختصار بعض الأمثلة على آليات أفضل الممارسات الأمنية التي ينبغي استعمالها.

2.III المِصدّات

المِصدّات (Firewalls) فِدَر أساسية في البنيان الأمني، توفّر عزل الشبكة على الحدود بين القطاعات الشبكية أو بين شبكات مختلفة. وتؤدي المِصدّات العزل بالاعتماد على قواعد نوعية لترشيح الحركة، قائمة تشكيلتها في المِصدّات. وتُستعمل المِصدّات أيضاً بالتضافر مع آليات أمن أخرى لتوفير طبقة من الأمن إضافية. وتسهم إضافة المِصدّات في تحقيق أمن قائم على "دفاع في العمق" حيث يحقق تراكبُ آليات أمن متعددة أمناً أقوى.

يفحص المِصدّ كلتا حركتي الوصول والمغادرة، ويُفترض أن يكون مشكَّلاً بحيث يرفض كل حركة لا تسمح بها قواعد الصدّ صريح السماح. ومن شأن المصدّ أيضاً أن يوفّر تسجيل الحركة وإطلاق الإنذارات عند اكتشافه رزماً غير مخوَّلة. يمكن التزوّد بالمصدات مادياً بصيغة أجهزة مستقلة، كما يمكن التزود بها بصيغة برمجيات تُدخَل على الآلات المضيفة. ومن أنماط المصدّات ما يقوم على ترشيح الرُزم السكوني، وما يعمل في طبقة التطبيق، وما يقوم على ترشيح الرزم المتكيِّف مع الحالة؛ ويتوقف الاختيار على احتياج كل زبون وعلى تفضيله.

المصدات التي تقوم على ترشيح الرُزم السكوني تفحص الرزم الواصلة والمغادرة، وتطبِّق مجموعة من القواعد للبتّ في السماح لها بعبور المصدّ أو في إسقاطها. ويستند البت في هذين الأمرين عادة إلى العنوان IP لكلا مصدر ومقصد الرزم، وإلى نوع البروتوكول، ومنْفَذَيْ المصدر والمقصد لبروتوكول التحكم في الإرسال (TCP). وهكذا، تبعاً للرزمة والمعايير المعتمدة، يُسقِط المصدّ الرزمة أو يعيد تسييرها، ومن الجائز أن يستحدث لها مدخل سجل و/أو يستثير إشارة إنذار بشأنها. ويستطيع بعض المصدّات العاملة بترشيح الرزم السكوني أن يؤدي تفتيشاً معمَّقاً للرزم، وربما وصل بالتفتيش إلى طبقة التطبيق.

المِصدّات التي تعمل في طبقة التطبيق تشغِّل تطبيقات بالنيابة عن الآلات في الشبكة المحمية، وكثيراً ما تُسمّى بالمصدّات "المفوَّضة". إن هذه المِصدّات، إذ تشغِّل التطبيقات المعيّنة، تكتشف النشاط غير السويّ إن وُجد، فلا تمرر المعطيات إلى الآلات التي تحميها. ولذا ينبغي تعزيز هذه المِصدّات العاملة في طبقة التطبيقات بتزويدها بجميع التطبيقات الضرورية، ويجب فيها أن تشغّل هذه التطبيقات نيابة عن جميع الآلات المحمية. ولكن، بسبب هذه المهمة، تؤثر هذه المِصدّات العاملة في طبقة التطبيقات شديد التأثير على أداء الشبكة.

مصدّات ترشيح الرزم المتكيِّف مع الحالة تؤدي وظائف ترشيح للرزم شبيهة بوظائف مصدّات ترشيح الرزم السكوني، وتزيد عليها أنها تستديم معلومات عن حالة توصيلات الحركة. فالمعلومات عن الحالة تمكن المصدّ من اتخاذ قرارات أفضل بشأن السماح للحركة أو ومنعها. مثلاً: المصدّ المتكيّف مع الحالة يمكن تشكيله بحيث يسمح فقط بالحركة التي تصدر عن آلات

واقعة على جانب واحد من الشبكة، من أجل بدء الاتصالات. فهذه الخصيصة تكون بالغة الإفادة حيثما كانت شبكات خاصة موصولة بشبكات عمومية.

وفي حالة استعمال المِصدّات وسيلة إضافية لأمن مستوي المراقبة والتشوير، ينبغي تشكيلها بحيث تسمح فقط بالمرغوب فيه من اتصالات التشوير والمراقبة بين مجموعة من الآلات. ويُفترَض أن تُمنَع أي حركة داخل الشبكة غير الاتصالات المرغوب فيها، ما يوفّر طبقة حماية لهذه الآلات.

يُسترعى الانتباه إلى أن التزوّد بمصدّات لا يخلو من آثار هندسية وإنتاجية على الأنظمة، وأن بعض التطبيقات قد يستدعي جعلَه متكيِّفاً مع المصدّ. ويُسترعى الانتباه أيضاً إلى أن المصدات لا تحمي من جميع الهجمات الأمنية، ولا سيما الهجمات الخداعية التي تستعمل رزم تشوير مشروعة.

3.III تشديد مناعة نظام التشغيل

العناصر المستعملة في الخواديم والشبكات للاضطلاع بوظائف على مستويي التشوير والمراقبة تكون ضعيفة أمام عدد من الهجمات منها ما يلي:

- برامج الهجوم من الباب الخلفي.
- برامج التشمّم.
- أدوات انتزاع وكسر كلمة السر.
- استغلال العيوب الموجودة في خدمات نظام التشغيل.
- منع الخدمة.

ومن هذه الاعتداءات ما هو مبني على تقنيات شائعة، مشفوعة بسيناريوهات وأدوات أخرى متيسّرة تجعل في استطاعة أقل المقتحمين معرفة إحراز مآثر في إيذاء الأنظمة. ومتى تعرض نظام للاختراق تمكّن المقتحم من فعل عدد من الشنائع منها ما يلي:

- تغيير المعلومات أو إتلافها.
- إفشاء معلومات خطيرة.
- تنصيب شفرة خبيثة لجمع معلومات.
- استعمال المخدم المغزوّ لمهاجمة أنظمة أخرى.

إجراءات تشديد مناعة نظام التشغيل تُستعمَل لتحسين مقاومة أنظمة التشغيل للهجمات. وإجراءات تشديد مناعة نظام التشغيل هي بمعظمها ممارسات سليمة تُتّبع أثناء تنصيب نظام تشغيل وتشكيله. وعلى الرغم من أنه لا يوجد نظام مأمون مطلق الأمان، فإن تطبيق إجراءات تشديد مناعة نظام التشغيل يجعل الأنظمة أقوى منعة بوجه الغزاة.

وجل ما يشتمل عليه تشديد مناعة نظام التشغيل هو تقييد الخدمات، والمنافذ، والنفاذ إلى التطبيقات والملفات. وينطوي تشديد مناعة نظام التشغيل أيضاً على حصر انطلاق تشغيل التطبيقات في حساب ذي امتياز ومقيَّد النفاذ إليه، وفي منافذ وخدمات متصفة بالضرورة القصوى. وينبغي استشارة صانعي أنظمة التشغيل للحصول على أحدث إجراءات تشديد مناعة هذه الأنظمة وعلى الوصلات الأمنية الإضافية.

4.III تقييم مدى التعرض

الهدف من إجراء تقييم لمدى تعرّض العناصر الشبكية أمنياً هو اكتشاف ما فيها من المطاعن الأمنية، ونقاط الضعف، والنواحي الخطرة. ويصمم اختبار مدى التعرّض من أجل تجريب الأنظمة وجعلها تُخفِق باستعمال قطع الخدمات، ومداورة المراقبات الأمنية المبتكرة، والتقاط معطيات سرية، والحصول على نفاذ غير مخوَّل إلى النظام، وسرقة الخدمة أو منعها. ويمكن إدراج تقييم مدى التعرّض في إجراءات الصيانة لعناصر الشبكات NGN ضماناً لتحصين أقوى.

يمكن إجراء تقييم مدى التعرّض بخصوص العناصر الشبكية في مرحلة تدقيق المنتَج، ثم بصورة مستمرة كجزء من صيانة الشبكة. لكن إدراج اختبار مدى التعرض في مرحلة تدقيق المنتَج ذو فوائد، على اعتبار أنه يوضع هكذا مسبقاً إجراءٌ لتسجيل النواحي المعرَّضة وتقديم طلبات بشأن التغيير. ثم إن إجراء تقييم مدى التعرّض بصورة متواصلة عادية يفيد أيضاً تعرّف أشكال جديدة من التهديد والمطاعن، ويتيح المبادرة إلى درء هذه التهديدات والتخفيف من مضارّها.

5.III أنظمة كشف الاقتحام

تُستعمَل أنظمة كشف الاقتحام (IDS) لتوفير الحماية من الاقتحام والأفعال غير المخوَّلة. مثلاً: يمكن أن تُستعمَل أنظمة كشف الاقتحام لتنبيه مديري الشبكات إلى إمكان وقوع حادث أمني، مثل اختراق مخدم بروتوكول فتح الدورة (SIP) أو هجمة بمنع الخدمة.

يمكن أن تُصنَّف الأنظمة IDS تصنيفاً إجمالياً وفقاً للمعايير التالية:

- كشف حادث في الوقت الفعلي أو خارج الخط: تجري حركة شبكية لأنظمة IDS مع تسجيل للأحداث في الوقت الفعلي. وعلى أثر وقوع أحداث يقوم نظام IDS خارج الخط بتحليل الاقتحامات على دفعات.
- نظام IDS مخدمي أو شبكي التركيب: النظام IDS الشبكي يشتمل عادة على عدد من أجهزة المراقبة المركّبة على نقاط المرور الاضطرارية في الشبكة، حيث يمكن مراقبة كل حركة بين نقطتين. أما النظام IDS المخدمي فيقتضي تركيب برمجيات تركيباً مباشراً في الخواديم اللازمة حمايتها، فيراقب توصيلات الشبكة ونشاط المستعملين في هذه الخواديم.
- نظام IDS تفاعلي أو منفعل: النظام IDS التفاعلي يتدخل إيجابياً لصد الهجمات بتعديل قواعد اشتغال المصدّات أو مراشيح المسيِّرات، أو بتدابير أخرى. أما النظام IDS المنفعل فيكتفي بتبليغ المشكلة إلى أنظمة الإدارة أو إلى غيرها من الأنظمة الشبكية.

أكثرية الأنظمة IDS المنتجة تجارياً توفِّر توليفة من مقْدِرات المراقبة الشبكية والمخدمية، بفضل جهاز إدارة مركزي يستقبل التقارير من مختلف أجهزة المراقبة ويُصدر إنذارات إلى مدراء الشبكة.

ثبت المراجع

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

[b-ITU-T M.3016.0] Recommendation ITU-T M.3016.0 (2005), *Security for the management plane: Overview.*

[b-ITU-T X.690] Recommendation ITU-T X.690 (2008) | ISO/IEC 8825-1:2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture*.

[b-3GPP TS 33.328] 3GPP TS 33.328, *IP Multimedia System (IMS) media plane security*.

[b-ETSI TS 133 220] ETSI TS 133 220 V9.2.0 (2010), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture.*

[b-IETF RFC 1155] IETF RFC 1155 (1990), *Structure and Identification of Management Information for TCP/IP-based Internets.*

[b-IETF RFC 1212] IETF RFC 1212 (1991), *Concise MIB definitions.*

[b-IETF RFC 1215] IETF RFC 1215 (1991), *A Convention for Defining Traps for use with the SNMP.*

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

[b-IETF RFC 2367] IETF RFC 2367 (1998), *PF_KEY Key Management API, Version 2.*

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

[b-IETF RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE).*

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

[b-IETF RFC 2578] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2).*

[b-IETF RFC 2579] IETF RFC 2579 (1999), *Textual Conventions for SMIv2.*

[b-IETF RFC 2580] IETF RFC 2580 (1999), *Conformance Statements for SMIv2.*

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication.*

[b-IETF RFC 2808] IETF RFC 2808 (2000), *The SecurID® SASL Mechanism.*

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS).*

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

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.

[b-IETF RFC 3410] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework.*

[b-IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

[b-IETF RFC 3413] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[b-IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3417] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol.*

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

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

[b-IETF RFC 3713] IETF RFC 3713 (2004), *A Description of the Camellia Encryption Algorithm.*

[b-IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing.*

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

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

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

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

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

[b-IETF RFC 4422] IETF RFC 4422 (2006), *Simple Authentication and Security Layer (SASL)*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*.

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[b-IETF RFC 4567] IETF RFC 4567 (2006), *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*.

[b-IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams.*

[b-IETF RFC 4590] IETF RFC 4590 (2006), *RADIUS Extension for Digest Authentication.*

[b-IETF RFC 4648] IETF RFC 4648 (2006), *The Base16, Base32, and Base64 Data Encodings.*

[b-IETF RFC 4740] IETF RFC 4740 (2006), *Diameter Session Initiation Protocol (SIP) Application.*

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[b-IETF RFC 5077] IETF RFC 5077 (2008), *Transport Layer Security (TLS) Session Resumption without Server-Side State.*

[b-IETF RFC 5090] IETF RFC 5090 (2008), *Radius Extension for Digest Authentication.*

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

[b-IETF RFC 5282] IETF RFC 5282 (2008), *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol.*

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol.*

[b-ISO/IEC 15946-1] ISO/IEC 15946-1:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.*

[b-ISO/IEC 15946-2] ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures.*

[b-ISO/IEC 15946-3] ISO/IEC 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.*

[b-ISO/IEC 15946-4] ISO/IEC 15946-4:2004: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery.*

[b-ISO/IEC 15946-5] ISO/IEC 15946-5:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation.*

[b-ISO/IEC 18033-3] ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-NIST FIPS 197] NIST Federal Information Processing Standards (FIPS) 197 (2001): *Advanced Encryption Standard.*

[b-NIST FIPS 198-1] NIST Federal Information Processing Standards (FIPS) 198-1 (2008), *The Keyed-Hash Message Authentication Code (HMAC).*

[b-NIST FIPS SP 800-38a] NIST Federal Information Processing Standards (FIPS), *Special Publication 800-38: Recommendation for Block Cipher Modes of Operations. Methods and Techniques, December 2001.*

[b-NIST SP 800-44 v2] NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers.*

[b-NIST SP 800-57] NIST Special Publication 800-57, *Recommendation on Key Management – Part 1: General (Revised).*

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling.*

[b-NIST SP 800-94] NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS).*

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
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، 2010