الاتحـــــاد الدولـــــي للاتصـــــالات

ITU-T H.235.9

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمة السمعية المرئية والأنظمـــة متعددة الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

إطار الأمن H.323: دعم بوابات الأمن في الأنظمة H.323

التوصيـــة ITU-T H.235.9

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

خصائص أنظمة الهاتف المرئي	H.199–H.100
البنية التحتية للخدمات السمعية المرئية	
اعتبارات عامة	H.219–H.200
تعدد الإرسال والتزامن في الإرسال	H.229–H.220
جوانب الأنظمة	**H.239–H.230**
إجراءات الاتصالات	H.259–H.240
تشفير الصور المتحركة الفيديوية	H.279–H.260
جوانب تتعلق بالأنظمة	H.299–H.280
الأنظمة والتجهيزات المطرافية للخدمات السمعية المرئية	H.349–H.300
معمارية خدمات الأدلة للخدمات السمعية المرئية والخدمات متعددة الوسائط	H.359–H.350
معمارية جودة الخدمات السمعية المرئية والخدمات متعددة الوسائط	H.369–H.360
خدمات إضافية في تعدد الوسائط	H.499–H.450
إجراءات التنقلية والتعاون	
لمحة عامة عن التنقلية والتعاون، تعاريف وبروتوكولات وإجراءات	H.509–H.500
التنقلية لأغراض الأنظمة والخدمات متعددة الوسائط في السلسلة H	H.519–H.510
تطبيقات وخدمات التعاون للوسائط المتعددة المتنقلة	H.529–H.520
الأمن في الأنظمة والخدمات المتنقلة متعددة الوسائط	H.539–H.530
الأمن في تطبيقات وخدمات التعاون للوسائط المتعددة المتنقلة	H.549–H.540
إجراءات التشغيل البيني في التنقلية	H.559–H.550
إجراءات التشغيل البيني للتعاون في الوسائط المتعددة المتنقلة	H.569–H.560
خدمات النطاق العريض وتعدد الوسائط ثلاثي الخدمات	
خدمات متعددة الوسائط بالنطاق العريض على خط المشترك الرقمي فائق السرعة (VDSL)	H.619–H.610

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

التوصيـــة ITU-T H.235.9

إطار الأمن H.323: دعم بوابات الأمن في الأنظمة H.323

ملخص

تحدد هذه التوصية طريقة لاكتشاف بوابات الأمن على مسار التشوير الذي يربط بين كيانين H.323 قيد الاتصال ولتقاسم المعلومات المتعلقة بالأمن بين حارس بوابي ما وبوابات الأمن بهدف الحفاظ على تكاملية التشوير وخصوصية الاتصالات.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) التابعة لقطاع تقييس الاتصالات في الاتحاد على التوصية ITU-T H.235.9 بتاريخ 13 سبتمبر 2005 وذلك بموجب الإجراء الوارد في التوصية ITU-T A.8.

مفردات رئيسية

بوابة، أمن، تشوير

تمهيـــد

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

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

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظـــة

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

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

حقـــوق الملكيـــة الفكريـــة

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، كان 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/.

جدول المحتويات

الصفحة

مقدمة

إن استخدام جدران الحماية و/أو أجهزة ترجمة عناوين الشبكات لتوفير حماية الحركة بين منطقتين في الشبكة تحت مراقبة إدارية مختلفة يخلق مشاكل بالنسبة إلى بروتوكولات تشوير المهاتفة التي ينبغي لها ضمان تبادل عناوين الشبكات بهدف تبادل رسائل التشوير ووسائط الاتصالات.

وتقدم التوصية ITU-T H.235.5 إطاراً تستطيع من خلاله نقطة طرفية وحارس بوابي أو حارسان بوابيان استخدام رسائل التسجيل والقبول والوضع (RAS) المبدئية للتفاوض بشأن مجموعة من الأسرار القوية المتقاسمة واستخدام هذه الأسرار لتجفير أجزاء من رسائل RAS ورسائل تشوير النداء اللاحقة وكذلك لاستيقان هذه الرسائل. ولا تنطبق هذه الطريقة إلا على التشوير المسيّر من الحارس البوابي. وتتناول التوصيات ITU-T H.235.1 وITU-T H.235.2 وITU-T H.235.3 طرائق ومواصفات أمنية مماثلة. وقد يتعارض إجراء الأمن هذا مع بوابات طبقة التطبيق (ALG) التي تصل ما بين مجالات الشبكة وتعالج عناوين التشوير ونقل وسائط الاتصال المحمولة في رسائل RAS و/أو رسائل تشوير النداء H.225.0 وتؤدي إلى فشل استيقان هذه الرسائل المعدّلة عند المقصد.

وتصف هذه التوصية وسيلة بسيطة تمكن الحارس البوابي من الإحاطة علماً ببوابات طبقة التطبيق (ALG) الواقعة على مسير التشوير، وتمكّنه من أن يتقاسم معها مفتاح استيقان التشوير المتفق عليه. وبالتالي يمكن للبوابات ALG أن تعالج بيانات ليست خصوصية؛ لا سيما عناوين النقل، في رسائل التشوير ومن ثم استيقان النتيجة قبل إحالة الرسائل المعدّلة. ويُطلق على هذه النبائط في النص التالي اسم "بوابات الأمن" (SG). وتمكّن هذه التقنية من المحافظة على الخصوصية من طرف إلى طرف لأي من العناصر المجفرة في عملية التشوير.

التوصيـــة ITU-T H.235.9

إطار الأمن H.323: دعم بوابات الأمن في الأنظمة H.323

1 مجال التطبيق

تنطبق هذه التوصية على أي حارس بوابي أو أي نقطة طرفية تستخدم بروتوكولات التسجيل والقبول والوضع (RAS) في إطار H.225.0 في السيناريوهات التي تسلك فيها بوابة أو أكثر من بوابات الأمن السلوك المذكور.

2 المراجع

1.2 المراجع المعيارية

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، فإن جميع المستعملين لهذه التوصية مدعوون إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة بتوصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

- التوصية ITU-T H.225.0 (2003)، *بروتوكولات تشوير النداء وترزيم التدفقات أحادية الوسائط لأنظمة الاتصالات متعددة الوسائط القائمة على الرزم.*
- التوصية ITU-T H.235.0 (2005)، *إطار الأمن H.323: إطار الأمن للأنظمة متعددة الوسائط في السلسلة H (الأنظمة H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.1 (2005)، *إطار الأمن H.323: مواصفة الأمن الأساسي.*
- التوصية ITU-T H.235.2 (2005)، *إطار الأمن H.323: مواصفة الأمن بالتواقيع.*
- التوصية ITU-T H.235.3 (2005)، *إطار الأمن H.323: مواصفة الأمن الهجينة.*
- التوصية ITU-T H.235.5 (2005)، *إطار الأمن H.323: جانبية للاستيقان المأمون خلال تبادل رسائل التسجيل والقبول والوضع (RAS) بواسطة أسرار متقاسمة ضعيفة.*
- التوصية ITU-T H.245 (2005)، *بروتوكول التحكم للاتصالات متعددة الوسائط.*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*

2.2 المراجع الإعلامية

- المعيار IETF RFC 2246 (1999)، *الصيغة 1.0 لبروتوكول أمن طبقة النقل (TLS).*
- المعيار IETF RFC 3546 (2003)، *تمديدات أمن طبقة النقل (TLS).*
- المعيار IETF RFC 2401 (1998)، *معمارية الأمن بالنسبة إلى بروتوكول الإنترنت.*

3 التعاريف

تحدد هذه التوصية المصطلحات التالية:

1.3 بوابة طبقة التطبيق (application level gateway) (ALG): نبيطة متوائمة مع البروتوكولات التي تصل ما بين منطقتين أو أكثر من مناطق الشبكة وباستطاعتها أن تفسر وتعدل بروتوكولات طبقة التطبيق لتوفير ترجمة عناوين النقل

وغيرها من الوظائف. ويمكن لبوابة ALG أن تؤمن وظائف ترجمة عناوين الشبكة (NAT) وجدران الحماية على مستوى النقل داخلياً أو أن تتحكم بها خارجياً.

2.3 عنوان محلي (local address): عنوان نقل يظهر في مجال عنوان محلي.

3.3 بوابة وسائط (media gateway): نبيطة تصل ما بين مجالين أو أكثر من مجالات الشبكة ويمكن أن تتحكم بها نبيطة أخرى (بوابة أمن مثلاً) بهدف توفير تدفقات وسائط محكومة بين مجالين. إن بوابة الوسائط في الواقع تقوم بعملية ترجمة عنوان الشبكة (NAT) أو بوظيفة جدار حماية يعمل في طبقة النقل أو في طبقات أدنى.

4.3 ترجمة عنوان الشبكة (network address translation) (NAT): عملية مطابقة عناوين النقل في الشبكة بين مجال وآخر في الشبكة.

5.3 ثقب دبوس (pinhole): مسير التدفق عبر بوابة الأمن (أو بوابة وسائط خاضعة لها) حيث يُسمح للرزم أو الرسائل سلوكه للانتقال من مجال إلى آخر. ويتميز ثقب الدبوس عموماً بأربعة عناوين نقل (عنوان المصدر في المجال A، عنوان المجال A في بوابة الأمن، وعنوان المجال B في بوابة الأمن، وعنوان المقصد في المجال B)، وبخصائص أخرى مثل بروتوكول النقل والاتجاه. ويمكن عدم تحديد عنوان المصدر (لمنفذ استماع مثلاً).

6.3 المجال (realm): منطقة في شبكة تتقاسم مساحة عنوان مشتركة في شبكة. ويفترض أن مجالات مختلفة تستخدم مساحات عنوان غير متطابقة أو متضاربة أو خاصة.

7.3 بوابة الأمن (security gateway) (SG): نبيطة قائمة بين منطقتين أو أكثر من مناطق الشبكة IP، تقوم بوظائف الأمن مثل التحقق من الصلاحية أو تحديد تدفق الرزم ومطابقة عناوين النقل بين منطقتين في الشبكة. وفي إطار هذه التوصية، يفترض أن بوابة الأمن هي بوابة في طبقة التطبيق (ALG) تكون متوائمة مع بروتوكولات التشوير H.323.

4 المختصرات

تستخدم التوصية الحالية المختصرات التالية:

ALG	بوابة طبقة التطبيق (*application layer gateway*)
GCF	التأكد من الحارس البوابي (*GatekeeperConfirm*)
GK	حارس بوابي (*Gatekeeper*)
GRJ	رفض الحارس البوابي (*GatekeeperReject*)
LCF	تأكيد الموقع (*LocationConfirm*)
LRQ	طلب تحديد الموقع (*LocationRequest*)
MG	بوابة وسائط (*Media Gateway*)
NAT	ترجمة عنوان شبكة (*Network Address Translation*)
OID	معرف الغرض (*Object Identifier*)
RAS	تسجيل وقبول ووضع (*Registration, Admission and Status*)
SG	بوابة الأمن (*Security Gateway*)
UDP	بروتوكول حافظة بيانات المستعمل (*User Datagram Protocol*)

5 الأعراف المتفق عليها

تحدد هذه التوصية مختلف معرفات الأغراض (OID) المعدة لتشوير القدرات المتعلقة بالأمن والإجراءات وخوارزميات الأمن. وتحيل هذه المعرفات إلى تفرعات هرمية من القيم المخصصة التي قد تأتي من مصادر خارجية أو قد تكون جزءاً من تفرعات هرمية من معرفات الأغراض التي يديرها قطاع تقييس الاتصالات في الاتحاد. وتظهر معرفات الأغراض المتعلقة تحديداً بالتوصية ITU-T H.235 في الشكل التالي في النص:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**} حيث تمثل **V** بشكل رمزي عدداً عشرياً بسيطاً يحدد الصيغة المقابلة من التوصية ITU-T H.235؛ أي 1 أو 2 أو 3 أو 4 مثلاً. وتمثل **N** بشكل رمزي عدداً عشرياً يحدد على نحوٍ فريد واقعة معرف الغرض وبالتالي الإجراء أو الخوارزمية أو قدرة الأمن.

وعليه فإن معرف الغرض المرمّز بالنظام ASN.1 يتألف من سلسلة من الأرقام. ومن باب التسهيل، يستخدم لكل معرّف OID تسمية مختزلة مثل "OID" في هذا النص. وثمة علاقة تقابل بين كل سلسلة OID وتتابع الأرقام ASN.1. ولا تستخدم التطبيقات في إطار التوصية ITU-T H.235 إلا الأرقام المشفرة بحسب النظام ASN.1.

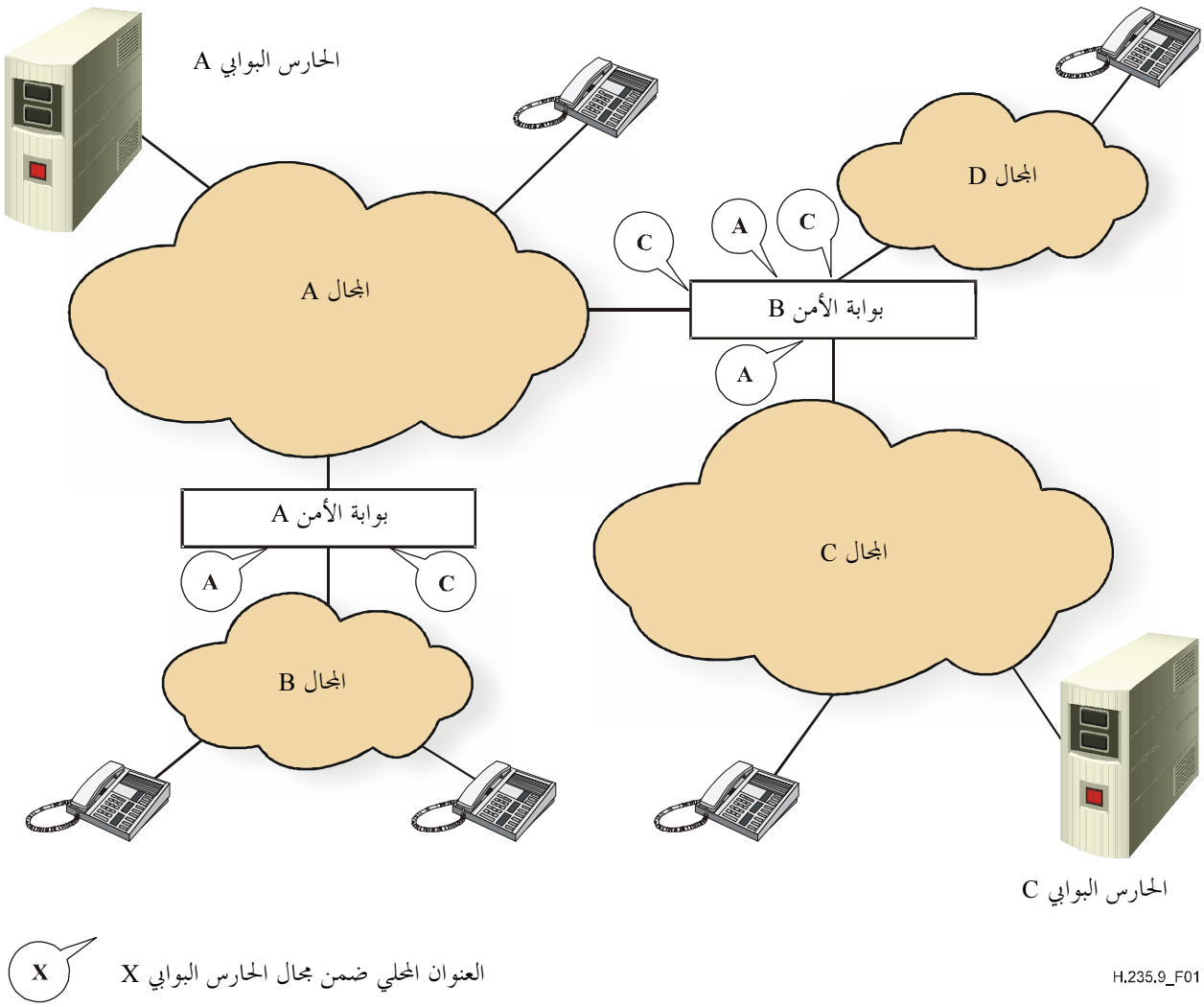
افتراضات أساسية

تتناول هذه التوصية نموذج شبكة بروتوكول الإنترنت تتصل فيه مناطق متعددة من الشبكة يُطلق عليها اسم "مجالات" بواسطة نبائط تُدعى بوابات أمن (SG) تكون متوائمة مع البروتوكول H.323 ومعدة للتحكم في تدفقات المعلومات بين مجالات الشبكة التي تقوم بتوصيلها. ويفترض أن تفحص بوابات الأمن رسائل التشوير المتدفقة بين المجالات وأن تتأكد من صلاحيتها وأن تستخرج المعلومات المتعلقة بعناوين النقل المتبادلة وأن تستخدم هذه المعلومات لإنشاء مسيرات التدفق الملائمة بين المجالات وأن تقوم أخيراً بتعديل عناوين النقل تبعاً للمجال الذي تحال إليه الرسالة. وينبغي لبوابات الأمن طبعاً أن تحرص على أن تمر مسيرات التشوير من خلالها، ولكن يمكنها أن تتحكم بنبيطة أخرى بهدف مناولة أي تدفقات جارية لوسائط الاتصال. ولا تحدد هذه التوصية بروتوكول التحكم المنطبق بين بوابة الأمن و"بوابة وسائط الاتصال".

لكي تكون خدمات حارس بوابي تابعة لمجال ما في متناول نقاط طرفية أو حارسان بوابيان تابعان لمجال آخر، يمكن لبوابة أمن أن توفر عنواناً للكشف عن الحارس البوابي في كل مجال تخدمه، لا يتضمن أي حارس بوابي معروف. وتقوم بوابة الأمن بعدئذ بإحالة أي رسالة اكتشاف تتلقاها في أي من هذه العناوين إلى الحارس البوابي المعني، وذلك بعد القيام بأي معالجة ضرورية للرسالة H.323. وفي الشكل 1 مثال لتشكيل يمثل حارس بوابي يخدم نقاط طرفية في عدة من مجالات الشبكة.

وفي الواقع، ينبغي لبوابات الأمن أن تمثل حارس بوابي في كل مجال من المجالات التي تخدمها (باستثناء ذلك المجال طبعاً الذي يكون فيه حارس بوابي، المجال A مثلاً بالنسبة إلى حارس بوابي A في الشكل). توفر بوابة الأمن B عناوين للكشف عن الحارسين البوابيين اللذين يظهران في الشكل، وبالتالي فهي توفر مسيراً بين حارسين بوابيين لتشوير الرسائل LRQ/LCF. وجدير بالإشارة أيضاً أن ليس من الضروري أن توفر بوابة الأمن النفاذ إلى كل حارس بوابي في كل مجال. إذ في الشكل 1 مثلاً، يمكن تشكيل بوابة الأمن A بحيث لا يتوفر عنوان اكتشاف الحارس البوابي A سوى في المجال B.

يفترض أن كل حارس بوابي يعرف اسماً فريداً لكل بوابة أمن في النظام وأن الكيانين يتقاسمان أيضاً سراً قوياً على المستوى التجفيري يسمح لهما بالاتصال بشكل مأمون. تُبحث فيما يلي طريقة التفاوض وتبادل هاتين الهويتين، والمفتاح المقابل لكل منهما، ولكنها لا تشكل الموضوع الأساسي للتوصية الحالية. وينبغي للأسرار المتقاسمة أن تكون فريدة لكل زوج من بوابة أمن/حارس بوابي. ولكي تمر حركة التسجيل والقبول والوضع (RAS) وحركة تشوير النداء ببوابات الأمن، يفترض أن هذه البوابات تعدل عناوين RAS وعناوين تشوير النداء المتبادلة.



الشكل H.235.9/1 – تشكيل بوابة الأمن

بالإضافة إلى ذلك، تُبحث فيما يلي الوسيلة التي يتم بها إعداد التسيير و/أو ترجمة العنوان بالنسبة إلى عملية الاكتشاف الأولي، وهي ليست الموضوع الرئيسي في هذه التوصية. ويفترض أن تكون عملية إنشاء العناوين اللاحقة، وأي ترجمة ضرورية، جزءاً من عمل بوابات الأمن.

6 العملية الأساسية

يفترض في الوصف التالي أن كل بوابة أمن في النظام مسجلة لدى كل حارس بوابي من المتوقع أن تخدمه. ويرد وصف هذه العملية بشكل تفصيلي لاحقاً. وفيما يتعلق بالعملية الأساسية، يفترض أن بوابة الأمن عرّفت بنفسها لدى كل حارس بوابي وأنها تشاطره سراً فريداً قوياً وتوفر عنواناً أو أكثر من العناوين "المحلية" للكشف عن حارس بوابي هذا. وتبحث التفاصيل المتعلقة بتسجيل بوابة الأمن في فقرة لاحقة. كما تصف الفقرات التالية الطريقة التي تشارك فيها بوابات الأمن في تسجيل النقاط الطرفية بهدف النفاذ إلى مفتاح الاستيقان من طرف إلى طرف الذي يتم التفاوض بشأنه بين حارس بوابي والنقطة الطرفية.

1.6 الكشف عن حارس بوابي من جانب نقطة طرفية

عندما ترسل نقطة طرفية رسالة طلب لحارس بوابي (GRQ) إلى عنوان الكشف عن حارس بوابي، وعندما تُرسل هذه الرسالة إلى حارس بوابي أو أكثر بواسطة البوابة SG، فإن بإمكان هذه البوابة أن تضيف العلامة **ClearToken** إلى العنصر **token** في الرسالة GRQ بما أنها تعالج العناوين داخل هذه الرسالة. ويتم التعرف على العلامة **ClearToken** هذه باعتبارها علامة

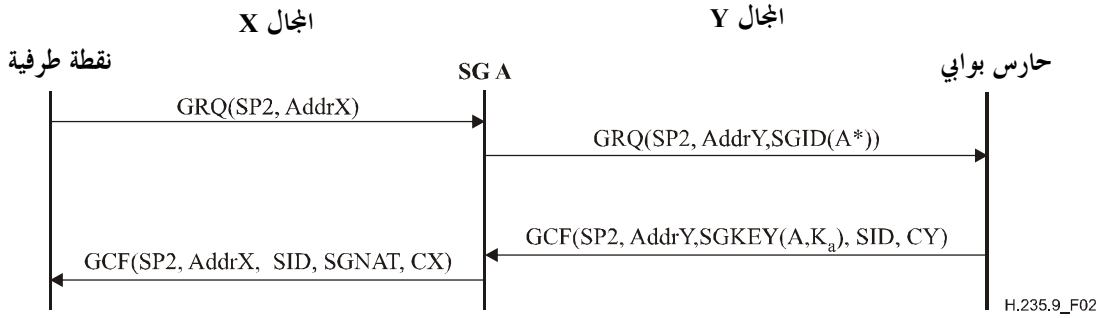
التعرف على البوابة SG (العلامة id-SG) (بواسطة علامتها **tokenOID**) وهي تتضمن سلسلة من المعرفات التي تتعرف بشكل قاطع على البوابة SG. وينبغي للبوابة SG أن تحذف من الجانبية **authenticationCapability** للرسالة GRQ أي آلية **AuthenticationMechanism** معينة (مثال ذلك أمن طبقة النقل TLS وفقاً للمعيارين RFC 2246 أو RFC 3546 أو أمن بروتوكول الإنترنت IPsec وفقاً للمعيار RFC 2401) لا يمكنها تناول إجراء استيقان الرسالة الخاص بها. ومن شأن ذلك أن يضمن قيام الحارس البوابي باختيار مواصفة متوائمة مع بوابة الأمن. وينبغي لأول بوابة أمن تتلقى الرسالة GRQ أن تدرج فيها عنصراً يعرّف عنوان الكشف الذي تلقت عنده رسالة GRQ من النقطة الطرفية.

ومن المفترض ضمنياً أن تعالج كل بوابة SG أي مجالات لعناوين التشوير في داخل الرسالة GRQ وأي رسائل RAS لاحقة بما يضمن مرور كافة رسائل التشوير بالبوابة SG لمعالجة العناوين.

2.6 توزيع مفتاح الاستيقان عند النقطة الطرفية

عندما تصل الرسالة GRQ إلى الحارس البوابي يقوم بمعالجتها، بما في ذلك علامة تعريف بوابة الأمن (SG-id). وبافتراض أنه سيقوم بدور الحارس البوابي بالنسبة إلى النقطة الطرفية، فإنه يعدّ لإرسال رسالة تأكيد حارس البوابة (GCF) إلى النقطة الطرفية. ثم يدرج في هذه الرسالة GCF الآلية **AuthenticationMechanism** المختارة بالإضافة إلى علامة **ClearToken** لمفتاح البوابة SG (المعرّف بواسطة العلامة **TokenOID** الخاصة به) لبوابة الأمن التي تحددها العلامة SG-id المتلقاة. وتتضمن علامة المفتاح عنصر التعرف على البوابة SG والتعرف على الحارس البوابي ومتجه التدميث ومفتاح استيقان الجلسة المجفرة بواسطة متجه التدميث والسر المتقاسم بين البوابة SG والحارس البوابي. ويجري التفاوض بشأن خوارزمية التجفير خلال تسجيل البوابة SG أو تكون جاهزة مسبقاً.

وفي مسير العودة باتجاه النقطة الطرفية، تمر الرسالة GCF بالبوابة SG التي وفرت العلامة SG-id. وتقوم البوابة SG بتحليل الرسالة للحصول على معرّف الجلسة وعلامة المفتاح الخاصة بها. ومن ثم تفك تجفير مفتاح استيقان الجلسة وتستخدمه لاستيقان الرسالة المتلقاة. فإذا كانت الرسالة أصلية، تقوم البوابة SG بمعالجة عناوين النقل حسبما هو ملائم، ثم تعيد إنشاء الرسالة دون علامة المفتاح SG الخاصة بها وتدرج علامة ترجمة عنوان الشبكة SG-NAT إذا لم تكن موجودة ويستيقن الرسالة المنشأة من جديد قبل إرسالها. وينبغي الاحتفاظ بمعرف الجلسة ومفتاح الاستيقان بهدف استخدامهما في رسائل RAS ورسائل تشوير النداء اللاحقة في هذه الجلسة. ويظهر في الشكل 2 التتابع الأساسي للرسائل التي تمر ببوابة أمن وحيدة. وجدير بالذكر أن على بوابة الأمن أن تعد ثقوب الدبوس المحددة انطلاقاً من الرسالة GCF (مثلاً، ثقب لرسائل RAS وأخرى لعناوين الحارس البوابي).



SP2 = جانبية أمن H.235.5

Addrx = عناوين في المجال x

SGID(A*) = علامة ClearToken تدل على وجود بوابة الأمن A

(* تشير إلى أن SGID تشمل عنوان كشف تستخدمه رسالة GRQ)

SID = تعريف الجلسة (يخصصه حارس البوابة)

K_a = مفتاح استيقان الرسالة من أجل SID

SGKEY(A, K_a) = علامة ClearToken لمفتاح بوابة الأمن ويكون تجفير المفتاح K_a بموجب المفتاح السري لدى A

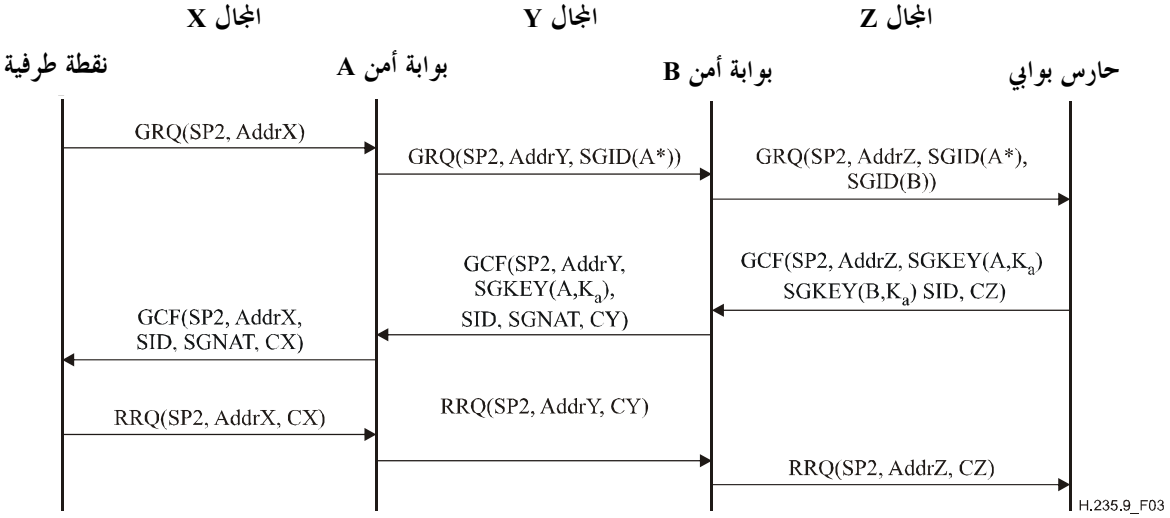
SGNAT = SG-NAT ClearToken

Cx = حاصل مجموع الرسالة (محسوباً على أساس المفتاح K_a المتفق عليه) في المجال x

الشكل H.235.9/2– التبادل الأساسي للرسائل من خلال بوابة الأمن

يمكن تمديد هذا المخطط بسهولة ليشمل سلسلة من البوابات SG بين النقطة الطرفية والحارس البوابي. حيث تضيف كل بوابة SG علامة ClearToken الخاصة بها في الرسالة GRQ عندما تمر هذه الرسالة من خلالها وتنـــزع علامة الاستجابة ClearToken الخاصة بها من الرسالة GCF عندما تعود هذه الأخيرة من الحارس البوابي إلى النقطة الطرفية. وتدرج أول بوابة SG في مسير العودة باتجاه النقطة الطرفية العلامة SG-NAT في الرسالة GCF. ويوضح الشكل 3 هذه العملية. وبالنسبة إلى معالجة رسائل RAS اللاحقة، تبين عملية تحويل عناوين النقل في الرسالة RRQ وحاصل مجموع الرسالة المعاد حسابه.

يمكن القيام بتتابع مماثل في التبادل بين الرسائل LRQ/LCF باستعمال عناصر الرسالة نفسها، ويمكن أن تستعمل النتائج لمعالجة واستيقان رسائل التشوير اللاحقة لهذه الجلسة.



SP2 = جانبية أمن H.235.5

Addrx = عناوين في المجال x

(A*)SGID = علامة ClearToken تدل على وجود بوابة الأمن A

(* تشير إلى أن SGID تشمل عنوان كشف تستخدمه رسالة GRQ)

SID = تعريف الجلسة (يخصصه حارس البوابة)

K_a = مفتاح استيقان الرسالة من أجل SID

(A, K_a)SGKEY = علامة ClearToken لمفتاح بوابة الأمن ويكون تجفير المفتاح K_a بموجب المفتاح السري لدى A

SGNAT = SG-NAT ClearToken

Cx = حاصل مجموع الرسالة في المجال x

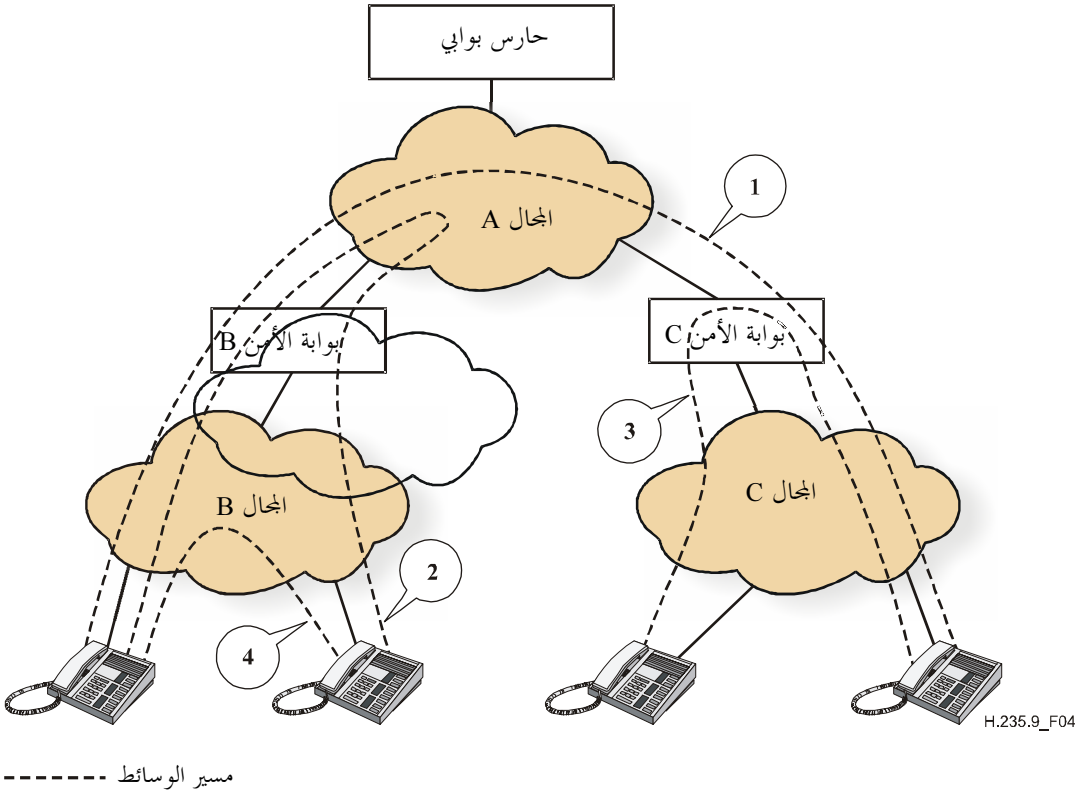
الشكل H.235.9/3 – التبادل عند مستويين للرسائل من خلال بوابتي أمن

3.6 مداولة العناوين

بما أن كل رسالة من رسائل التشوير H.225.0 أو H.245 تمر بالبوابة SG ينبغي لهذه الأخيرة أن تعاين وتعدل كافة عناوين النقل التي تمر من خلالها بحيث تكون صالحة في المجال التالي الذي تمر من خلاله الرسالة. ويعني ذلك أن بوابة الأمن قد تحتاج إلى إحداث ثقوب جديدة لاستيعاب التدفقات المصاحبة من التشوير و/أو الوسائط المصاحبة التي يتعين على العناوين إنشاءها. ويلاحظ أن بعض العناوين تمثل "مراصد استماع" يجب أن تبقى مفتوحة "من قبيل الاحتياط"؛ ولسوف يستحدث ثقب محدد بشكل تام إذا ما وصلت رزمة إلى "مرصد الاستماع".

يجوز لكل بوابة SG أن تعاين كل عنوان نقل لمقصد تتلقاه للتأكد من أنه يمثل فعلاً عنوان مقصد في هذه البوابة. ولنأخذ مثال تشكيل المجالات ومسيرات الوسائط الوارد في الشكل 4. وهنا يتعين على تدفق ما للوسائط بين نقطة طرفية واقعة في المجال B ونقطة طرفية واقعة في المجال C أن يمر عبر بوابتي الأمن B وC، كما يظهر في التدفق "1". وإذا لم تقم بوابة الأمن B بأي

معالجة خاصة، يتبع تدفق الوسائط بين نقطتين طرفيتين في المجال B مسيراً مكافئاً ينقله إلى المجال A ويعيده إلى المجال B، كما يظهر في التدفق "2". وإذا تبين لها أن عنواني المصدر والمقصد المقدمين إلى التدفق في المجال A هما في الواقع عنوانان في بوابة الأمن B، يمكن لهذه البوابة أن "تختصر" التدفق بطريقتين: إما بإرسال التدفق داخلياً، كما يبين التدفق "3" (الذي يمر من بوابة الأمن C بغية التوضيح) وإما، إذا تبيّن لها أن النقطتين الطرفيتين تنتميان إلى المجال B، بتعديل عنواني النقطتين الطرفيتين في المجال B بغية إرسال التدفق مباشرة بين النقطتين، كما يبيّنه التدفق "4". ويلاحظ أن عناوين "النقطة الطرفية" كما تراها بوابة الأمن B قد تكون في الواقع عناوين في بوابة أمن (D مثلاً) ترتبط بمجال آخر. وبعد أن تغيّر بوابة الأمن B العناوين لأداء تسيير "مباشر" بين العناوين في بوابة الأمن D، يمكن لهذه الأخيرة أن "تختصر" التدفقات بالطريقة نفسها.



الشكل H.235.9/4 – مسيّرات الوسائط

وثمة تشكيل لا يظهر في هذا المخطط وهو حالة تدفقات الوسائط التي تمر من منطقة إلى أخرى من خلال عدة بوابات أمن. فإذا ما تسجلت نقطة طرفية ما وتشورت عبر بوابة أمن وتسجلت نقطة طرفية أخرى في المنطقة نفسها وتشورت عبر بوابة أمن ثانية، سيكون من الصعب لأي من البوابتين أن تكتشف أن النقطتين الطرفيتين موجودتان في المجال نفسه، أو أن تحدد العناوين الواجب استعمالها للنقطة الطرفية التي تتشور عبر بوابة الأمن الأخرى. وتجنباً لهذه المشكلة، من الأيسر استخدام بوابة أمن وحيدة بمقدورها أن تعالج المستوى المتوقع من التشوير، ويمكن عندها تحويل عبء معالجة تدفق الوسائط إلى بوابات منفصلة للوسائط تحت مراقبة بوابة الأمن.

7 تفاصيل تتعلق بالتشوير

إن أفضل وسيلة لتعريف تناول هذه الإمكانية على نحو فعال هو إدراج معرف غرض (OID) معياري في علامات ClearToken المعنية. وفي النص التالي، يشار إلى هذه العلامات باسم "الفيش SG". ومن شأن ذلك أن يمكّن أي حارس بوابي مستقبله (أو بوابة وسيطة أو أي نبيطة أخرى لا تشارك في العملية) من تجاهل هذه الإمكانية. ويُستخدم معرف الغرض المخصص لتمييز علامات **ClearToken** التي تتضمن العناصر التالية:

- **tokenOID** – يوضع إزاء معرف الغرض المخصص لهذه الإمكانية، ويسمى "SG1"، انظر الفقرة 11.
- **generalID** – إذا وجد، يوضع إزاء اسم بوابة الأمن التي توجه إليها العلامة **ClearToken** (يستخدم في العلامة SG-key).
- **sendersID** – يوضع إزاء اسم بوابة الأمن التي أنشأت العلامة **ClearToken** (يستخدم في العلامة SG-id).
- **profileInfo** – يتضمن المعلومات المحددة التي ترسلها علامة **ClearToken** هذه، كما هو مبين في الجدول 1.

الجدول H.235.9/1 – عناصر مواصفة الكشف عن بوابة الأمن

اسم العنصر	قيمة معرف العنصر	نمط العنصر (الطول)	وصف العنصر
TokenType	1	بالكامل	0 = SG-id token 1 = SG-key token 2 = SG-NAT token 3 = SG-register token
EncryptedKey	2	أثمونات (16 بالنسبة إلى SP2)	مفتاح استيقان جلسة مواصفة الأمن المشار إليها، المجفر بواسطة السر المتقاسم بين بوابة الأمن (SG) المحددة وحارس البوابي (GK). ويرسل المفتاح في علامة مفتاح البوابة SG. ويتم تحديد متجه التدميث الضروري لفك التجفير في ProfileElement.paramS.
ServedRealm	3	اسم	اسم المجال الذي يمكن/ينبغي لبوابة الأمن أن توفر فيه عنوان الكشف عن الحارس البوابي.

8 اعتبارات تتعلق بتشكيل بوابات الأمن

تعتمد الإجراءات الموصوفة في هذه التوصية على الوسائل التي تستخدمها بوابات الأمن في الشبكة لاكتشاف المسيّرات باتجاه حارس أو حارسان بوابيان التي ينبغي أن توضع خدماته في متناول المستعملين الموجودين في مختلف مجالات الشبكة. وينبغي لكل بوابة أمن أن تكون قادرة على الاتصال بحارسها أو حراسها الموجودين في المجال الأول، وأن توفر النفاذ إلى حراس البوابة هؤلاء انطلاقاً من النقاط الطرفية (أو من حراس بوابة آخرين) الموجودة في المجال الآخر. على سبيل المثال، في الشكل 3، يكون لبوابة الأمن B نفاذ إلى الحارس البوابي في المجال Z. وبإمكانها أيضاً توفير النفاذ إلى الحارس البوابي من العناصر الموجودة في المجال Y. وبالتالي، يمكن لبوابة الأمن A أن تنفذ إلى الحارس البوابي من خلال بوابة الأمن B. وحالما تنفذ بوابة الأمن B إلى الحارس البوابي، يمكنها أن توفر النفاذ إلى كيانات موجودة في المجال X. ويفترض ذلك أن بوابات الأمن نفسها تستخدم بروتوكول كشف مثل RAS. ويمكن استخدام هذه الإجراءات كذلك لمعرفة كل بوابة أمن تتمتع بالنفاذ إلى حارس بوابي ما، وللتفاوض بشأن مجموعة من المفاتيح بهدف حماية تبادل رسائل التشوير بين المستعملين.

1.8 تسجيل بوابات الأمن

يمكن أن تقوم بوابة أمن ما بدور الممثل، في مجال ما، لحارس بوابي في مجال آخر تكون بوابة الأمن قادرة على النفاذ إليه. على سبيل المثال، في الشكل 1، يمكن أن تقدم بوابة الأمن A تمثيلاً (عنوان كشف) في المجال B للحارس البوابي الموجود في المجال A (حالما تعرف عنوان الكشف عن حارس بوابي في المجال A). ويمكن أن تنطبق هذه التقنية في عدة مستويات من بوابة الأمن، وبما أن كل بوابة أمن تكشف عن حارس بوابي (أو ممثل)، فيمكنها أن توفر عنوان الكشف عن الحارس البوابي هذا في مجال جديد أو في عدة مجالات جديدة، وعندئذٍ يمكن لبوابات الأمن الموصولة بهذا المجال أو المجالات أن تكشف عن هذه العناوين الجديدة.

تطبّق بوابات الأمن RAS الإجراءات في إطار التوصية H.225.0 للكشف عن الحارسان البوابيان وللتسجيل لديهم في أي مجال ترغب في تقديم خدمات له باعتبارها بوابات أمن. وتعرف بوابة أمن ما نفسها على أنها نقطة طرفية من نمط **بوابة**.

ويمكنها أن تحدد أنها تتناول البروتوكول H.323 إذا رغبت في تحديد سابقات تحتويها و/أو تحديدات لعرض النطاق، ولكن ذلك ليس إلزامياً. وينبغي استخدام إجراءات أمن مقيسة مثل تلك الواردة في التوصيات ITU-T H.235.1 وITU-T H.235.2 وITU-T H.235.3 وITU-T H.235.5 لاستيقان بوابة الأمن لدى الحارس البوابي وللتفاوض بشأن أسرار متقاسمة مأمونة يتعين استخدامها في الإجراءات الواردة فيما يلي. ويمكن تطبيق الإجراءات H.235.1 وH.235.2 وH.235.3 وH.235.5 للمرور من خلال بوابات أمن أخرى تمتثل للتوصية الحالية. وينبغي لبوابة الأمن أيضاً أن تدرج علامة ClearToken لكي تتسجل في الرسالة RRQ التي ترسلها إلى الحارس البوابي. ويجب أن تتضمن هذه العلامة، التي تستخدم لتعريف البوابة بوصفها بوابة أمن، العنصر **ServedRealm** لكل مجال جديد تنوي بوابة الأمن أن تخدمه. ويمثل كل عنصر عنواناً جديداً محتملاً للكشف عن الحارس البوابي في المجال الخاص به. ويمكن تشكيل كل بوابة أمن بحيث تتحدد فيها المجالات التي تقدم لها عناوين الكشف عن حارس بوابي معين. على سبيل المثال، في الشكل 1، يمكن تشكيل بوابة الأمن B بحيث لا تقدم عنوان الكشف عن الحارس البوابي C في المجال D، مما يرغم النقاط الطرفية في المجال D على أن تسجل نفسها لدى الحارس البوابي A. وإذا كانت بوابة الأمن لا ترسل ولا تتلقى أي نداءات، فإنها لا تحتاج إلى توفير عنوان تشوير النداء خلال تسجيلها بل يمكنها أن تترك "تتابعاً" فارغاً مقابل **callSignalAddress** في الرسالة RRQ. وينبغي للحارس البوابي أن يستجيب بالطريقة نفسها في **callSignalAddress** من الرسالة RCF.

يشير الحارس البوابي إلى المجال أو المجالات التي تقدم لها بوابة الأمن خدمات وذلك بإعادة علامة تسجيل البوابة SG في الرسالة RCF بتضمينها عنصراً واحداً أو أكثر من عنصر **ServedRealm** في الرسالة RRQ لدى بوابة الأمن. وعند انتهاء التسجيل، تفتح بوابة الأمن منفذ استماع لعنوان الكشف عن الحارس البوابي في كل مجال محدد. ويمكن استخدام آليات لا تدخل في إطار هذه التوصية للإعلان عن عنوان الكشف الجديد هذا في المجال المعني. ويمكن للحارس البوابي أن يختار عناوين الكشف التي تقدمها بوابة الأمن من قائمة من العناوين البديلة.

ويمكن استخدام أي مواصفة أمن RAS حالما يُسمح لبوابات الأمن بقراءة ومناولة عناوين التشوير ونقل الوسائط المتبادلة وتكون قادرة على استيقان الرسالة من جديد.

يمكن أن يستخدم الحارس البوابي المعلومات المتعلقة بمجال بوابة الأمن لتحديد مناطق الشبكة والتوصيلية ولاستيقان بوابة الأمن. وبالمقابل، ينبغي للحارس البوابي أن يزود بوابة الأمن بالمعلومات التالية:

- مسوغات هوية الحارس البوابي؛
- عنوان أو عناوين التسجيل التي يمكن لبوابة الأمن أن تستخدمها لإرسال الطلبات RAS الناشئة عن النقاط الطرفية الواقعة في المنطقة أو المناطق التي تخدمها (يجوز للحارس البوابي أن يرفض قبول نقاط طرفية واقعة في منطقة أو أكثر من المناطق التي تخدمها بوابة الأمن).

وينبغي أن يؤدي نجاح تسجيل بوابة الأمن إلى تقاسم مفتاح سري قوي بين بوابة الأمن والحارس البوابي يمكن أن يستخرج منه مفاتيح التجفير و/أو الاستيقان. ويمكن استخدام مفتاح الاستيقان لاستيقان طريقة تسجيل بوابة الأمن، وينبغي استخدام مفتاح التجفير عند تسجيل النقاط الطرفية بغية تجفير مفتاح استيقان جلسة هذه النقاط الطرفية لتوزيعه لدى بوابة الأمن، كما هو موصوف أعلاه.

2.8 مسوغات الهوية من أجل الاستيقان

خلافاً لعدد النقاط الطرفية، يفترض أن يكون عدد بوابات الأمن في شبكة مؤلفة من عدة مناطق ضئيلاً نسبياً. وفي معظم الحالات، يُتوقع تزويد الخدمة على أساس الاشتراك أو أي اتفاق تعاقدي آخر. وبالتالي يكون لدى الحارس البوابي معلومات الاستيقان المتعلقة ببوابات الأمن المحتمل أن تتسجل لديه. وفي أبسط الحالات، يمكن تخصيص كلمات سر لبوابات الأمن كما يمكن تطبيق إجراءات الاستيقان H.235.1 وH.235.2 وH.235.3 وH.235.5 أو إجراءات استيقان "التحدي–الاستجابة". وبالطبع، يتطلب استخدام أسرار متقاسمة سلفاً آلية مأمونة لتوزيعها خارج النطاق.

وهناك طريقة أخرى ممكنة تعتمد على استخدام شهادات المفتاح العمومي يمكن بموجبها وضع نسخ من شهادة الحارس البوابي (أو شهادة تخص الجهة التي وقعت شهادة الحارس البوابي) عند مستوى بوابات الأمن بواسطة طريقة موثوق بها. ولا يزال استخدام أساليب الشهادات هذه بحاجة إلى مزيد من الدراسة.

9 اعتبارات تتعلق بالأمن

تتعرض البروتوكولات من هذا النمط، حيث يمكن تعديل رسالة إبان العبور، لمخاطر التردي. على سبيل المثال، إذا كانت نقطة طرفية ما تقدم إمكانات نقل وسائط مجفرة وغير مجفرة، فقد يحدث لبوابة أمن مؤذية أن تحجب عروض التجفير ولا تقدم إلا العروض غير المجفرة، وبالتالي تبقى تدفقات الإعلام دون تجفير. ويجب أن تتصدى النقاط الطرفية (والحارس البوابي أيضاً) لهذا النوع من المخاطر بأن تقتصر على تقديم قدرات تكون مقبولة وفقاً لسياستها الأمنية الخاصة بها. وفي نهاية المطاف تقع على عاتق النقاط الطرفية ومستعمليها مسؤولية الحفاظ على المستوى الملائم من الأمن. وكذلك الأمر بالنسبة إلى اختيار مواصفة الأمن عند التسجيل، فإذا كانت نقطة طرفية ما تتطلباستيقاناً قوياً ينبغي لها أن توضح ذلك بصراحة في رسالتها GRQ وينبغي ألا تقبل بعرض أضعف من الحارس البوابي.

10 قابلية التطبيق

يمكن تطبيق هذه الطريقة سواء على المواصفات الأمنية H.235.1 وH.235.2 وH.235.3 أم على تلك الموصوفة في التوصية ITU-T H.235.5. ويمكن تناول أي مواصفة أمنية تمكن من استحداث/حساب مفاتيح استيقان مناسبة. وينبغي لبوابات الأمن أن تعاين عناصر الرسائل GRQ/GCF (على سبيل المثال، **authenticationCapability** و/أو **authenticationMode**) لمعرفة ما إذا كان من الممكن تناول نظام الأمن أو استيقان الرسائل المعني.

11 معرف الغرض

معرف الغرض (OID)	قيمة معرف الغرض	الوصف
"SG1"	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 65 }	تتضمن العلامة ClearToken عناصر مواصفة الكشف عن بوابة الأمن.

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 البرامج الإذاعية الصوتية والتلفزيونية 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 المعطيات على الشبكة الهاتفية
السلسلة X	شبكات المعطيات والاتصالات بين الأنظمة المفتوحة والأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا

جنيف، 2006