الاتحـــــاد الدولـــــي للاتصـــــالات

ITU-T H.235.1

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمـــة السمعية المرئيـــة والأنظمة متعددة الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

إطار الأمن H.232: مواصفة الأمن الأساسي

التوصيـــة ITU-T H.235.1

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.235.1

إطار الأمن H.323: مواصفة الأمن الأساسي

الملخص

توفر هذه التوصية حماية الاستيقان والتكامل أو الاستيقان فقط بالنسبة لرسائل H.225.0 (RAS)، ورسائل تشوير النداء، ورسائل H.225.0، والرسائل H.245 المرسلة في قناة نفقية باستعمال حماية شفرة استيقان الرسائل المظللة مع خوارزمية التظليل الآمنة (HMAC-SHAI-96) لرسائل RAS H.225.0 التي تستند إلى كلمة سر، ورسائل تشوير النداء باستعمال تقنيات التحقق التي تستند إلى كلمة سر مؤمَّنة. وتطبق مواصفة الأمن على H.323، مطراف إلى حارس بوابي وحارس بوابي إلى حارس بوابي، وH.323 بوابة تشغيل إلى حارس بوابي وإلى كيانات H.323 الأخرى في بيئات مُدارة بمفاتيح/كلمات سر تناظرية مخصصة.

وفي نسخ سابقة للسلسلة الفرعية H.235، وردت هذه المواصفة في الملحق D/H.235. وتبين التذييلات الرابع والخامس والسادس لـ H.230 الفقرات والأشكال والجداول الكاملة لـ H.235.0. وتعرض الجداول تقابلاً بين الطبقتين 3 و4 من H.235.

المصدر

اعتمدت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات التوصية ITU-T H.235.1 بتاريخ 13 سبتمبر 2005 وفقاً للإجراء المحدد في التوصية A.8.

كلمات مفتاحية

الاستيقان، الشهادة، التوقيع الرقمي، التجفير، التكامل، إدارة المفاتيح، أمن الوسائط المتعددة، مواصفة الأمن.

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).

ملاحظة

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

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "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

التوصيـــة ITU-T H.235.1

إطار الأمن H.323 مواصفة الأمن الأساسي

1 مجال التطبيق

توفر هذه التوصية حماية الاستيقان والتكامل أو الاستيقان فقط بالنسبة لرسائل H.225.0 RAS، ورسائل تشوير النداء ورسائل H.225.0، ورسائل H.245 المرسلة في قناة نفقية باستعمال حماية شفرة استيقان الرسائل المظللة مع خوارزمية التظليل الآمنة HMAC-SHA1-96 1 لرسائل H.225.0 RAS التي تستند إلى كلمة سر، ورسائل تشوير النداء باستعمال تقنيات التجفير المستندة إلى كلمة سر مؤمَّنة. وتطبّق مواصفة الأمن على H.323 مطراف إلى حارس بوابي، وحارس بوابي إلى حارس بوابي وH.323 بوابة تشغيل إلى حارس بوابي وإلى كيانات H.323 الأخرى.

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، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية 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 ووضع قطار متعدد الوسائط في الرزم لأغراض أنظمة الوسائط المتعددة العاملة بأسلوب الرزم.*
- التوصية ITU-T H.235 الإصدار 1 (1998)، *أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235 الإصدار 2 (2000)، *أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.0 (2005)، *إطار أمن للأنظمة متعددة الوسائط من السلسلة H (الأنظمة H.323 وغيرها من النمط H.245)*
- التوصية ITU-T H.235.2 (2005)، *إطار الأمن H.323: مواصفة الأمن بالتوقيع.*
- التوصية ITU-T H.235.4 (2005)، *إطار الأمن H.323: أمن النداءات بالتسيير المباشر والنداءات بالتسيير الاختياري*
- التوصية ITU-T H.235.6 (2005)، إطار الأمن H.323: *مواصفة التجفير الصوتي مع إدارة مفـــاتيح H.235/H.245 الأصلية*
- التوصية ITU-T H.245 الإصدار 10 (2003)، *بروتوكول التحكم لأغراض الاتصالات متعددة الوسائط*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*
- التوصية ITU-T H.323 الملحق واو (1999)، *الأجهزة المطرافية البسيطة.*
- التوصية ITU-T Q.931 (1998)، *مواصفات الطبقة 3 من السطح البيني بين المستعمل وشبكة ISDN للتحكم بالنداء الأساسي*
- التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف*

- المعيار ISO/IEC 7498-2: 1989، *أنظمة معالجة المعلومات – التوصيل البيني للأنظمة المفتوحة – النموذج المرجعي الأساسي – الجزء 2 معمارية الأمن.*
- التوصية ITU-T X.803 (1994) للمعيار ISO/IEC 10745: 1995، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – نموذج الأمن في الطبقات العليا.*
- التوصية ITU-T X.810 (1995) للمعيار ISO/IEC 10181-1: 1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن في الأنظمة المفتوحة: لمحة عامة.*
- التوصية ITU-T X.811 (1995) للمعيار ISO/IEC 10181-2: 1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن في الأنظمة المفتوحة: إطار الاستيقان.*
- المعيار ISO/IEC 10118-3: 2004، *تكنولوجيا المعلومات – تقنيات الأمن – دالات التداخل – الجزء 3: دالات التداخل المخصصة.*

2.2 المراجع الغنية بالمعلومات

[FIPSPUB180-2] المعيار الاتحادي لمعالجة المعلومات FIPS PUB 180-2، معيار التظليل المؤمَّن، وزارة التجارة في الولايات المتحدة، إدارة التكنولوجيا، المعهد الوطني للمعايير والتكنولوجيا، 1 أغسطس 2002.

[OIW] التنفيذ المستقر – الاتفاقات الخاصة ببروتوكولات التوصيل البيني للأنظمة المفتوحة: الجزء 12 – أمن الأنظمة المفتوحة؛ النتائج المستخلصة من ورشة عمل ديسمبر 1994 بشأن منفذي بيئات الأنظمة المفتوحة (OIW)؛
http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt

[RFC2104] IETF RFC 2104(1997)، HMAC: *التظليل بمفاتيح لاستيقان الرسائل.*

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

3 المصطلحات التعاريف

لأغراض هذه التوصية، تنطبق التعاريف الواردة في الفروع H.323/3 وH.225.0/3 وH.245/3 مع التعاريف الواردة في هذا الفرع. وبعض المصطلحات المستخدمة في هذه التوصية معرَّف أيضاً في التوصيات ITU-T REC X.800 | ISO/IEC 7498-2، وISO/IEC 10745 | X.803، وISO/IEC 10181-1 | X.810، وISO/IEC 10181-2 | X.811.

وتستخدم هذه التوصية المصطلحات التالية من أجل توفير خدمات الأمن.

1.3 الاستيقان والتكامل: هذه خدمة أمنية مشتركة تشكل جزءاً من مواصفة الأمن الأساسي التي تدعم تكاملية الرسائل بالاقتران مع استيقان المستعمل. ويمكن للمستعمل أن يضمن الاستيقان من خلال التطبيق السليم لإجراء المفتاح السري المتقاسم. وتوفر آلية الأمن ذاتها خدمتي الأمن المعنيتين على السواء.

2.3 الاستيقان – فقط: هذه الخدمة الأمنية التي تتيحها مواصفة الأمن الأساسي كخيار تدعم استيقان مجالات مختارة فقط، لكنها لا توفر التكاملية الكلية للرسائل. وتطبق مواصفة أمن الاستيقان فقط على تشوير الرسائل التي تَعْبُر أجهزة ترجمة عنوان الشبكة (NAT) /جدران الحماية. ويمكن للمستعمل ضمان الاستيقان من خلال التطبيق السليم لإجراء مفتاح سري متقاسم.

ولدى استخدام تقنيات المفاتيح المجفّرة بالتناظر، لا تطبق خدمات أمن الاستيقان/التكامل إلا على أساس أسلوب قفزة قفزة.

4 الرموز والاختصارات

ASN.1 ترميز تركيب مجرد رقم 1 *(Abstract Syntax Notation One)*

EP النقطة الطرفية *(Endpoint)*

EPID معرِّف هوية النقطة الطرفية *(Endpoint Identifier)*

GK حارس بوابي *(Gatekeeper)*

GKID معرِّف حارس بوابي *(Gatekeeper Identifier)*

GRQ طلب حارس بوابي *(Gatekeeper Request)*

HMAC شفرة استيقان الرسائل المظللة *(Hashed Message Authentication Code)*

ICV قيمة سلامة التحقق *(Integrity Check Value)*

ITU الاتحاد الدولي للاتصالات *(International Telecommunication Union)*

LRQ طلب تحديد الموقع *(Location Request)*

MAC شفرة استيقان الرسائل *(Message Authentication Code)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

OID معرِّف هوية الغرض *(Object Identifier)*

RAS التسجيل والقبول والوضع القانوني *(Registration, Admission and Status)*

RTP بروتوكول الوقت الفعلي *(Real-Time Protocol)*

SHA خوارزمية التظليل الآمنة *(Secure Hash Algorithm)*

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

UTC التوقيت العالمي المنسق *(Universal Time Clock)*

VOIP نقل الصوت باستخدام بروتوكول الإنترنت *(Voice over Internet Protocol)*

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

- "Shall" تشير إلى طلب إلزامي.
- "Should" تشير إلى عمل مقترح ولكنه خياري.
- "May" يجوز تشير إلى عمل خياري وليس توصية بإجراء معين.

تعرف هذه التوصية **مواصفة الأمن الأساسي**. وتوفر هذه المواصفة الأمن الأساسي بوسائل بسيطة من خلال استعمال تقنيات التجفير المستند إلى كلمة سر آمنة. ويمكن استخدام مواصفة الأمن الأساسي بالاقتران مع مواصفات الأمن العامة من مثل H.235.3 وH.235.4 وH.235.5 وH.235.6 وH.235.7.

وتستعمل هذه التوصية مجالات H.235 لتوفير خدمات الاستيقان/التكامل لرسائل التشوير H.323. وتُحدد معرِّفات هويات الأغراض المختلفة (انظر الفقرة 15) أي خدمة أمنية يتم اختيارها فعلياً، وأي صيغة بروتوكول تُستخدم في هذه التوصية. ويحدد الإجراء الأول كيفية تنفيذ خدمات الأمن من قِبل آليات أمن معينة من مثل التقنيات التناظرية (التظليل بمفاتيح). ويشار إلى معرِّفات هوية الغرض من خلال مرجع رمزي في النص (مثل، "A")، وانظر أيضاً الفرع H.235.0/5.

وحيثما كانت خدمة تكامل الرسائل توفر أيضاً استيقان الرسائل على الدوام، فإن العكس ليس دائماً صحيحاً. ففي التطبيق تستعمل الخدمة المشتركة للاستيقان والتكامل نفس مواد المفتاح بدون التسبب في ضعف أمني.

وبالإضافة إلى ذلك، فإن جميع معلومات الأمن قفزة قفزة توضع في العنصر **الإذنة المظللة بالتجفير (CryptoHashedToken)**. ويعاد حساب هذه المعلومات مع كل قفزة.

وتطبّق هذه التوصية تقنيات تجفير تناظري معينة لغرض الاستيقان والتكامل. ويستخدم هذا النص تعبير كلمة السر والسر المتقاسم لدى تطبيق التقنيات المتناظرة.

وبوجه عام، فإن ما هو مشترك بين كلمة السر ومفتاح الدورة والسر المتقاسم فهو أنها تستعمل في التجفير التناظري بين كيانين (أو أكثر). والاختلاف بين كلمة سر ومفتاح دورة سر متقاسم يتمثّل في الكيفية التي تُستخدم بها المفاتيح فعلياً، مثلاً كلمات السر من أجل الاستيقان والتخويل، ومفاتيح الدورة من أجل التجفير. وتعبير "السر المتقاسَم" هو نوع من التعبير المحايد لأنه لا يشير فعلياً إلى أي استعمال خاص.

وتُستخدَم **كلمة السر** (التي يمكن النظر إليها أيضاً باعتبارها سراً متقاسَماً) من أجل توفير الاستيقان/التكامل لرسائل RAS وH.225.0 نظراً لأن هذا البند يمكن إدخاله بواسطة المستعمِل. وكلمة السر عادة هي مجموعة رموز ألفبائية رقمية يستطيع المستعملون تذكُّرها. ولكلمة السر عادة عمر طويل الأجل، وتُعرف كلمة السر مقدّماً ويمكن أن تُحدد باعتبارها جزءاً من عمليات الاشتراك الإجمالية للمستعمِل. ويمكن لبعض الخوارزميات (مثل تسلسل كلمة السر من خلال خوارزمية تظليل) أن تحوِّل كلمة السر من أجل معالجة أكثر ملاءمة في البروتوكولات بغية التوصل إلى طول محدد.

ومن الواضح أن استعمال كلمة السر ينبغي أن يؤدَّى بعناية. فكلمات السر تستطيع توفير قدر كافٍ من الأمن فقط عندما تُختار عشوائياً من حيِّز كبير، وعندما تحمل تشفيراً أنتروبياً بحيث لا يمكن التنبؤ بها، وعندما يتم تغييرها دورياً. ولا تندرج القاعدة الخاصة بوضع كلمة السر والمحافظة عليها في نطاق بحث هذه التوصية.

وثمّة ممارسة جيدة تتعلق بكيفية نشر الفوائد المستمدّة من كلمات السر والأسرار المتقاسَمة. وتتمثل هذه الممارسة في تحويل مجموعة كلمة سر المستعمِل إلى مجموعة بتات ثابتة نظراً لأن السر المتقاسَم يستعمل تظليلاً وحيد الاتجاه قوي التجفير.

وكمثل موصى به عند استعمال مواصفة الأمن الخاصة بهذه التوصية، فإن خوارزمية التظليل الآمنة 1 (SHA1) عندما تُطبّق على مجموعة كلمة السر تُنتج سراً متقاسَماً يصل إلى 20 بايتاً. وتتمثل ميزة في ذلك هي أن النتيجة المظللة لا تخفي كلمة السر الفعلية فقط وإنما تحدد أيضاً نسقاً ثابتاً بطول سلسلة البتات بدون التضحية فعلياً بالتشفير الإنتروبي.

ومن ثم، فإن:

السر المتقاسَم := SHA1 (كلمة السر)

وتتيح الفيشة **ClearToken** H.235 مجالاً يُسمى **Random** يتضمن 32 بتة صحيحة. ويُستخدم هذا المجال على النحو التالي: فالرقم **Random** هو فعلياً رقم متزايد وحيد الوتيرة يبدأ عند أي قيمة ويتزايد مع كل رسالة خارجة. ويُستعمل المجال **Random** كقيمة "عشوائية" إضافية للدخل إلى وظيفة المفاتيح المظللة في الحالة التي تصدر فيها عدة رسائل واحدة بعد الأخرى بفترة قصيرة ومع ذلك تُرسل مجالات دلالة وقت متطابقة. ويمكن أن يحدث هذا عندما لا توفر ميقاتية التوقيت العالمي المنسَّق استبانة ميقاتية كافية. وخُلاصة الأمر، أن قيمة التظليل المنتَجَة أو قيمة فحص التكامل تبدو مختلفة بسبب تغير القيمة **Random**. والغرض من هذا هو مكافحة الهجمات بإعادة التنفيذ. ومن أجل تبسيط التنفيذ، يُفضَّل اللجوء إلى تضاد متزايد إزاء سلسلة عشوائية حقاً هنا. ويمكن للمرسل إليه أن يحتفظ بأزواج مجالات **دلالة الوقت/العشوائية (timestamp/random)** أثناء الفترة التي تحددها نافذة وقت محلية. ويمكن معرفة الهجمات بإعادة التنفيذ عندما تحدث نفس أزواج مجالات **دلالة الوقت/العشوائية** مرتين.

ملاحظة – تعوّض نافذة الوقت عن اختلافات الوقت المتزامن وعن مهلة عبور الشبكة.

وترمي هذه المواصَفَة إلى وضع "تحديد **generalID** في العلامة **ClearToken** إلى معرِّف هوية المرسل إليه". ويعني هذا فعلياً أنه بالنسبة لرسائل RAS الموجهة إلى الحارس البوابي، فإن معرِّف الهوية يكون هو معرّف الحارس البوابي؛ وبالنسبة للرسائل RAS الموجهة إلى النقطة الطرفية يكون هو معرّف النقطة الطرفية، وبالنسبة لرسائل تشوير النداء H.225.0 الموجَّهة إلى

الحارس البوابي، يكون هو معرف هوية الحارس البوابي، وبالنسبة لرسائل تشوير النداء H.225.0 الموجهة إلى النقطة الطرفية يكون هو معرّف النقطة الطرفية المطلوبة، انظر أيضاً الفقرة 14.

وتوضع **SendersID** على سلسلة تعرُّف هوية المُرسل. ويعني هذا فعلياً أنه بالنسبة للرسائل RAS الموجهة إلى الحارس البوابي يكون معرِّف الهوية هو معرِّف النقطة الطرفية؛ وبالنسبة للرسائل بـــ RAS الموجهة إلى النقطة الطرفية يكون هو معرِّف هوية الحارس البوابي؛ وبالنسبة لرسائل تشوير النداء H.225.0 الموجهة إلى الحارس البوابي، يكون هو معرف الحارس البوابي، وبالنسبة لرسائل تشوير النداء H.225.0 الموجهة إلى النقطة الطرفية يكون هو معرِّف النقطة الطرفية المطلوبة، انظر أيضاً الفقرة 14.

ويجوز أن تطبِّق هذه التوصية حماية تكامل الرسائل التي تشمل الرسالة بأجمعها. وبالنسبة لـ H.225.0 RAS، تغطي حماية التكامل الرسالة RAS بأكملها؛ وبالنسبة لتشوير النداء تغطي هذه الحماية رسالة تشوير النداء H.225.0 بأكملها، بما في ذلك الراسيات Q.931.

وتستخدم هذه التوصية مصطلحات الأمن المعروفة جيداً من مثل المفاتيح وإدارة المفاتيح وSET التي لديها معاني مختلفة في سياقات أخرى (مثلاً لوحة مفاتيح اللمس، وإدارة مفاتيح السمة Q.932/Q.931، وبروتوكول الإنجاز الإلكتروني الآمن).

6 لمحة عامة

توفر هذه التوصية حماية الاستيقان والتكامل أو الاستيقان فقط بالنسبة لرسائل H.225.0 RAS، ورسائل تشوير النداء، ورسائل H.225.0، ورسائل H.245 المرسلة في قناة نفقية باستعمال حماية شفرة استيقان الرسائل المظللة مع خوارزمية التظليل الآمنة HMAC-SHA1-96 لرسائل H.225.0 RAS التي تستند إلى كلمة سر، ورسائل تشوير النداء باستعمال تقنيات التجفير المستندة إلى كلمة سر مؤمنة. وتُطبَّق مواصفة الأمن على H.323 مطراف إلى حارس بوابي، وحارس بوابي إلى حارس بوابي، وH.323 وبوابة تشغيل إلى حارس بوابي وإلى كيانات H.323 الأخرى في بيئات مُدارة بمفاتيح تناظرية/كلمات سر تناظرية مخصصة.

1.6 ملخص سمات الأمن

تشمل السمات التي تقدمها هذه المواصفات فيما يلي:

- بالنسبة إلى الرسائل RAS وH.225.0 والرسائل H.254 المدفوعة في نفق:
  - استيقان المستعمل من كيان مطلوب بمعزل عن عدد القفزات التي تحدثها الرسالة إبان التطبيق.

    ملاحظة: تفهم القفزة هنا بمعنى عنصر شبكة H.235 موثوق (مثلاً: بواب، بوابة تشغيل، وحدة تحكم متعددة النقاط (MCU)، وكالة، جدار حماية). ولذلك فإن سوية تطبيق الأمن قفزة قفزة، عندما تستخدم مع التقنيات التناظرية لا توفر أمناً حقيقياً من طرف إلى طرف بين المطاريف.
  - تكامل رسالة التشوير بحد ذاتها، بما فيها الأجزاء (المجالات) الأساسية من الرسائل التي تصل إلى كيان ما بمعزل عن عدد القفزات التي تُحدِثها الرسالة إبان التطبيق.
  - تطبيق استيقان وتكامل رسائل التشوير قفزة قفزة يوفر خدمات الأمن هذه للرسالة بكاملها.

يتم التصدي لعدة أنماط من الاعتداءات بواسطة خدمات الأمن المذكورة أعلاه باستعمالها بشكل ملائم. وهي:

- اعتداءات تستهدف وظيفة رفض الخدمة: ويمكن الوقاية من مثل هذه الاعتداءات بواسطة تحقق سريع من قيم التظليل التجفيرية.
- اعتداءات عن طريق طرف ثالث: ويمكن لاستيقان الرسائل وتكاملها قفزة قفزة عند التطبيق أن يمنعا مثل هذه الاعتداءات عندما يوجد الطرف الثالث كمسيّر معاد مثلاً بين قفزتين إبان التطبيق.
- اعتداءات التكرار: يحمي استخدام طابعات الوقت وأرقام التتابع من مثل هذه الاعتداءات.
- اعتداءات الخداع: يمنع استيقان المستعمل مثل هذه الاعتداءات.

- قرصنة التوصيلات: يحمي استعمال الاستيقان/التكامل لكل رسالة تشوير مثل هذه الاعتداءات.

وهناك جوانب أخرى لمواصفة الأمن البسيط هي:

- استعمال خوارزميات متينة ومشهورة ومنتشرة الاستعمال تستند إلى دراسات المراكز IMTC/ETSI/IETF.
- مقدرة النشر على مراحل تبعاً لاحتياجات أمن النموذج التجاري.
- قابلية التطبيق على سيناريوهات نشر مختلفة مثل الزمر المغلقة والبيئات المتدرجة والمؤتمرات متعددة النقاط.
- يستعمل الأمن القائم على الاستيقان حصراً في حال الرغبة في توفير بعض الأمن للحماية من اجتياز الأجهزة NAT/جدار الحماية.

ويلخص الجدول 1 جميع الإجراءات التي يحددها هذا الملحق تبعاً لمواصفة الأمن المتعلقة بمتطلبات الأمن المختلفة. وتعرض مواصفة الأمن الخيارية بالاستيقان حصراً مع خلفية زرقاء في النسخة الإلكترونية.

الجدول H.235.1/1 – مواصفة الأمن الأساسي

خدمات الأمن	وظائف النداء			
	RAS	H.225.0	H.245 (ملاحظة)	RTP
الاستيقان	كلمة السر HMAC-SHA1-96	كلمة السر HMAC-SHA1-96	كلمة السر HMAC-SHA1-96	
الاستيقان–فقط	كلمة السر HMAC-SHA1-96	كلمة السر HMAC-SHA1-96	كلمة السر HMAC-SHA1-96	
عدم نكران				
التكامل	كلمة السر HMAC-SHA1-96	كلمة السر HMAC-SHA1-96	كلمة السر HMAC-SHA1-96	
السرية				
تحكم بالنفاذ				
إدارة المفاتيح		تخصيص كلمة السر عند الاشتراك		
ملاحظة – H.245 نفقية أو H.245 مدمجة في توصيل H.225.0 سريع.				

ينبغي أن يستخدم المستعمل نظام كلمة السر للاستيقان، وهو نظام يوصى به كثيراً بسبب بساطته وسهولة تطبيقه. وتظليل جميع مجالات الرسائل RAS ورسائل تشوير النداء H.225.0 هي الطريقة الموصى بها لتحقيق تكامل الرسائل (باستعمال نظام كلمة السر أيضاً).

وتجري الكيانات H.323 الأمينة بواسطة مواصفة الأمن هذه، الاستيقان مع التكامل باستخدام نفس آلية الأمن المشتركة.

ولا يرد وصف وسائل التحكم بالنفاذ بشكل صريح، ويمكن تطبيقها محلياً مع مراعاة المعلومة المستقلة المسيّرة في مجالات التشوير H.235 (العلامة ClearToken، العلامة CryptoToken).

لا تصف هذه التوصية الإجراءات المتعلقة بالإدارة وترتيبات تخصيص كلمات السر/المفاتيح السرية عند الاشتراك. ويمكن تنفيذ مثل هذه الإجراءات بطرائق لا ترد دراستها في هذا الملحق.

وتستطيع كيانات الاتصال المعنية تحديد استخدامها لمواصفة الأمن الأساسي أو مواصفة الأمن بالتوقيع بشكل صريح باستخدام تقييم معرفات هوية غرض الأمن المشار إليها في الرسالتين (المعرفات **tokenOID** والمعرفات **algorithmOID**؛ انظر أيضاً الفقرة 15).

2.6 قابلية مواصفة الأمن الأساسي للتطبيق

مواصفة الأمن الأساسي قابلة للتطبيق في سياق يمكن فيه تخصيص كلمات السر/المفاتيح التناظرية الخاصة بالمشترك، للكيانات (المطاريف) H.323 الآمنة، وعناصر الشبكة (حراس بوابيون، والمخدِّمون الوكلاء). وهي توفر الاستيقان والتكامل، أو الاستيقان–فقط بالنسبة لرسائل RAS H.225.0 ورسائل تشوير النداء، والرسائل H.225.0، والرسائل H.245 المرسلة في قناة

نفقية باستعمال حماية شفرة استيقان الرسائل المظلّلة مع خوارزمية التظليل الآمنة (HMAC-SHA1-96 1)، على النحو المحدد في الإجراء I. ويشمل إنشاء النداء H.225.0 باستعمال FastStart (حارس بوابي إلى حارس بوابي أو مِطراف إلى مِطراف) إدارة مفاتيح متكاملة مع Diffie-Hellman.

وتفرض مواصفة الأمن الأساسي إجراء التوصيل السريع وتوصي باستعمال H.245 الإرسال في القناة النفقية داخل H.225.0.

3.6 المتطلّبات H.323

يُفترض بالكيانات H.323 التي تطبق مواصفة الأمن الأساسي هذه أن تدعم سمات H.323 التالية:

- التوصيل السريع؛
- نموذج التسيير عبر الحارس البوابي.

4.6 لمحة عامة عن الإجراءات

وصف الإجراء الواجب استعماله في مواصفة الأمن موضوع الدراسة.

الإجراء I هو آلية استيقان رسائل التشوير التي تستعمل مفاتيح تناظرية من النمط البسيط القائم على كلمة سر معروفة من كيانين اثنين (مثال حارس بوابي ونقطة طرفية H.323). ويوفر هذا الإجراء استيقان الرسائل RAS وQ.931 وH.245 وتكاملها (انظر الفقرة 7).

والإجراء IA هو آلية استيقان بمفرده تستعمل مفاتيح تناظرية من النمط البسيط القائم على كلمة سر معروفة من قبل كيانين (مثال: حارس بوابي ونقطة مطرافية H.323). ويقدم هذا الإجراء الاستيقان دون التكامل التام للرسائل. ويطبق خيار الاستيقان بمفرده على السيناريوهات التي تمر رسائل تشويرها H.323 عبر أجهزة NAT/جدار الحماية.

وقد يكون الاستيقان وحيد الجانب أو متبادلاً تبعاً لسياسة الأمن المختارة، ويمكن تطبيقه على الاستيقان/التكامل في اتجاهات معكوسة كما يستطيع أن يوفي بنفس الوقت درجة أعلى من الأمن. ويقرر الحارس البوابي ضرورة تطبيق الاستيقان/التكامل أيضاً في الاتجاه المعاكس.

ويجيب الحراس البوابيون الذين يكشفون فشل صلاحية الاستيقان و/أو التكامل في رسالة RAS أو رسالة تشوير نداء قادمة من نقطة طرفية أمينة من حارس بوابي ، بإرسالها رسالة رفض مقابلة تشير فيها إلى غياب الأمن وذلك بوضع سبب الرفض على القيمة **securityDenial** أو على أي شفرة خطأ ملائمة أخرى للأمن ومطابقة لما يرد في H.235.0/1.11. وتبعاً لمقدرة الحارس البوابي على التعرف على الاعتداءات وعلى طريقته في التصدي لها فإنه عند استلام رسالة **xRQ** مع معرفات هوية أغراض غير محددة (مثل **tokenOID**، **algorithmOID**) يمكنه الرد بإرسال رسالة **xRJ** غير أمينة مع سبب الرفض أو بإلغاء الرسالة. وينبغي تسجيل حادث الأمن الحاصل. ومن ناحية أخرى ينبغي أن تستبعد النقطة الطرفية الرسالة غير الأمينة التي تم استقبالها وأن تدوّن تاريخ وساعة وصولها ومن ثم تستطيع أن تجري محاولة جديدة مع التفكير بإمكانية اختيار معرفات OID مختلفة. وكذلك يمكن أن يجيب الحارس البوابي الذي يستقبل رسالة H.225.0 SETUP أمينة مع معرفات أغراض غير محددة (**tokenOID**، **algorithmOID**) بإرسال رسالة RELEASE COMPLETE غير أمينة مع سبب الرفض **securityDenied** أو أن يستبعد الرسالة. وينبغي أيضاً تدوين حادث الأمن الحاصل.

وهناك تشوير H.235 ضمني للدلالة على استعمال الإجراء I وآلية الأمن المطبقة القائمة على قيمة معرفات الهوية (انظر أيضاً الفقرة 15) وعلى محتوى مجالات الرسالة.

ولا تستعمل هذه المواصفة المجالات H.235 ICV؛ وبالحقيقة تعالج قيم التحقق من تكامل التجفير على أنها قيم تظليل تجفيري وتوضع في مجالات التظليل في **CryptoToken**.

7 تفاصيل استيقان رسائل التشوير بمفاتيح تناظرية (الإجراء I)

ينبغي في حال استخدام الإجراء I اتباع الإجراءات التالية:

- تولد الخوارزمية HMAC-SHA1-96 قيمة تظليل طولها 12 أثمونا (96 بتة) على أنها مستيقن ناتج. ولإنتاج المفتاح استناداً إلى كلمة السر يجب استعمال الآلية الواردة في الفقرة H.235.0/4.2.8.

الملاحظة 1 – عند تحديد المفتاح السري استناداً إلى كلمة السر التي أدخلها المستعمل، يجب إضفاء طابع عشوائي كافٍ على هذا المفتاح. ويوصى مثلاً باستعمال أسرار عشوائية بالفعل لأغراض المفتاح السري أو بالتأكد من أن كلمات السر العشوائية طويلة بقدر كافٍ.

- ينبغي أن يضم المجال **CryptoH323Token** لكل رسالة H.225.0/RAS المجالات التالية:

– **nestedCryptoToken** ويضم المجال **CryptoToken** الذي يضم بدوره **cryptoHashedToken** مع المجالات التالية:

- **tokenOID** الموضوع على "A" للدلالة على أن حساب الاستيقان/التكامل يشمل جميع مجالات الرسالة H.225.0 RAS ورسالة تشوير النداء.
- **hashedVals** ويضم المجال **ClearToken** الذي يستخدم في المجالات التالية:

– **tokenOID** الموضوع على "T" للدلالة على أن المجال الأساسي **ClearToken** كما هو مبين أدناه، قيد الاستعمال من أجل استيقان الرسالة وحمايتها من التكرار وأيضاً من أجل إدارة المفتاح DH خيارياً كما يرد في الفقرة H.235-6/5.8. ويمكن أيضاً استعمال علامات أخرى **ClearToken** بدلاً من العلامة **ClearToken** الأساسية.

– **timeStamp** ويضم طابعة الوقت.

– **random** ويضم رقم الترتيب المتزايد وحيد الوتيرة. ويتيح هذا العدد إمكانية تمييز رسالتين مطبوعتين بنفس الوقت والساعة (ضمن حدود استبانة الميقاتية).

– **generalID** ويضم معرّف هوية المرسل إليه (في حالة الرسائل أحادية التوزيع).

– **sendersID** ويضم معرّف هوية المرسل.

– **dhkey**، ويستعمل لنقل المعلمات DH من **Setup** إلى **Connect** كما هو محدد في هذه التوصية.

- **halfkey** ويضم مفتاحاً عمومياً عشوائياً في أحد أجزائه.
- **modsize** ويضم DH-prime (انظر الجدول H.235.6/4).
- **generator** ويضم DH-group (انظر الجدول H.235.6/4).

الملاحظة 2 – عند استعمال مواصفة الأمن الأساسي بدون مواصفة الأمن بالتجفير الصوتي، ينبغي عدم إرسال أي معلمة DH وغياب المجال **dhkey**؛ ويستعاض عنهما بوضع **halfkey** و**modsize** و**generator** على {'0'B و'0'B و'0'B}.

– **token** ويضم **HASHED** مع المجالات التالية:

- **algorithmOID** الموضوع على "U" للدلالة على استعمال الشفرة HMAC-SHA1-96؛
- **params** الموضوع على NULL.
- **hash** ويضم المستيقن المحسوب بواسطة الشفرة HMAC-SHA1-96 وبالإمكان حساب المستيقن.

– في مجمل المجالات H.225.0 RAS وتشوير نداء الرسالة إذا كان المعرّف **tokenOID** للمجال **CryptoHashedToken** موضوعاً على "A" (مشيراً بذلك إلى الاستيقان والتكامل).

ويوضع **tokenOID** على "A" لحماية الوحدات H323-UU-PDU المسيرة في النفق بما في ذلك جميع محتويات الرسائل H.245؛ وينبغي أن يشمل حساب التظليل في مجمل رسائل تشوير النداء **H.225.0**، مع العلم أن جميع المجالات مطابقة للإجراء المذكور في الفقرة 3.7.

- ويتم التحقق من المستيقن في نهاية كل آخر مقطع قناة (من EP1 إلى GK1 ومن GK1 إلى GK2 ومن GK2 إلى EP2 ومن EP1 إلى GK2 ومن GK1 إلى EP2 أو من EP1 إلى EP2 حسبما تكون الحالة) ويعاد حسابه قبل إرسال الرسالة إلى المقطع التالي.

الملاحظة 3 – يتم حساب المستيقن لكل رسالة بمفردها.

الملاحظة 4 – يجب استعمال طريقة الملء المشار إليها في المعيار SHA1 (ISO/IEC 10118-3).

الملاحظة 5 – في حال استعمال الاستيقان/التكامل المجتمعين يتم حساب المستيقن في مجمل الرسالة.

الملاحظة 6 – يوصى بشدة، من أجل تفادي حصول الاعتداءات التكرارية، الانتباه عند التطبيق إلى تغيير كلمة السر (المفتاح) قبل اكتمال دورة (أي قبل انتهاء الدورة) رقم التتابع المتزايد بوتيرة واحدة.

الملاحظة 7 – بإمكان المرسل إليه أن يكشف استعمال الإجراء I عن طريق تقييم المعرف **tokenOID** في العلامة المظللة **EncodedGeneralToken** (التي تكشف وجود "A").

1.7 حساب التظليل القائم على كلمة السر

يقوم المرسل والمرسل إليه لرسالة محمية على صعيد الاستيقان/التكامل بحساب التظليل المبعثر بمفتاح محسوب في جميع مجالات الرسالة المشفرة بالترميز ASN.1 (بواسطة المعرف "A" OID). وفيما يخص مواصفة الاستيقان بمفرده، يحسب كلاً من المرسل والمرسل إليه التظليل بالمفتاح في جميع المجالات ClearToken المشفرة بالترميز ASN.1 (باستعمال المعرف "B" OID).

2.7 الشفرة HMAC-SHA1-96

الشفرة HMAC-SHA1-96 هي قيمة مظللة بالتجفير طولها 96 بتة مبتورة من الخوارزمية SHA1 بطول 160 بتة. ويجب استعمال البتات الست والتسعين الأكثر دلالة من ترتيب أثمونات الشبكة لقيمة التظليل للحصول على النتيجة. وتصف الوثيقة RFC 2104 الإجراء بالمفتاح السري *K* الذي تخصص له قيمة السر المشترك (= كلمة سر مظللة SHA1) ومع المجال *text* بقيمة "ذاكرة الرسالة".

3.7 حساب الاستيقان والتكامل والتحقق منهما

بالنسبة للاستيقان وتكامل الرسائل (في حالة المعرّف OID موضوعاً على "A") يكون الإجراء هو التالي.

ينبغي أن يحسب مرسل الرسالة التظليل بالطريقة التالية:

1) وضع قيمة التظليل لنموذج خاص بالتغيب وقدرها 96 بتة، أما دقة تشكيلة البتات فليست هامة جداً ولكن الاختيار المستصوب هو تشكيلة بتات فريدة لا ترد في بقية الرسالة.

2) تشفير مجمل الرسائل بالترميز ASN.1؛ وينبغي أن تشمل هذه العملية فيما يخص الرسائل RAS، مجمل الرسائل RAS H.225.0؛ أما فيما يخص تشوير النداء فتشمل مجمل رسالة تشوير النداء H.225.

3) تحديد موقع التشكيلة بالتغيب في الرسالة المشفرة؛ محو كامل تشكيلة البتات التي تم العثور عليها بواسطة 96 بتة صفر.

الملاحظة 1 – يمكن أن يتضمن هذا الموقع بعض مراحل التجربة والخطأ في الحالة النادرة عندما تحدث التشكيلة بالتغيب أكثر من مرة في الرسالة.

4) حساب قيمة التظليل المجفرة استناداً إلى الرسالة المشفرة بالترميز ASN.1 وذلك باستعمال الشفرة HMAC-SHA1-96 (انظر الفقرة 7.2).

5) الاستعاضة عن تشكيلة التغيب بقيمة التظليل المحسوبة في الرسالة المشفرة.

وينبغي أن يعمل المرسل إليه الذي يستلم الرسالة بالطريقة التالية:

1) فك تشفير الرسالة ASN.1.

2) استخراج قيمة التظليل المستقبلة والحفاظ عليها في قيمة RV متغيرة محلية.

3) البحث عن القيمة RV لقيمة التظليل في الرسالة المشفرة المستقبلة وتحديد موقعها.

ملاحظة 3 – في بعض الحالات النادرة جداً قد يطرأ التسلسل الفرعي لقيمة التظليل عدة مرات في مجمل الرسالة؛ وفي هذه الحالة يجب إعادة إجراء الخطوات من 3) إلى 6) مع نقاط انطلاق بحث مختلفة.

4) محو كامل تشكيلة البتات في الرسالة المشفرة بواسطة 96 صفراً؛

5) حساب قيمة التظليل بالتجفير استناداً إلى الرسالة المشفرة بواسطة التشفير HMAC-SHA1-96 (انظر الفقرة 2.7).

6) مقارنة القيمة RV مع قيمة التظليل المحسوبة. ولا تعتبر الرسالة خالية من الخطأ إلا عندما تكون القيمتان متساويتين؛ وفي هذه الحالة يتم الاستيقان بنجاح وينتهي الإجراء.

7) وإلا فتعاد العمليات من 3) إلى 7) مع البحث عن توافقات أخرى بعد وضع القيمة RV على الموقع السابق. وإذا لم تعط أي من التوافقات مقارنة مرضية بقيم التظليل يكون الاستيقان فاشلاً وتكون الرسالة قد تعرضت للخلل (عرضاً أم قصداً) خلال النقل.

8 الاستيقان–فقط (الإجراء IA)

تستطيع المطاريف أن تختار تطبيق أسلوب الاستيقان فقط (باستعمال المعرف OID "B" انظر الفقرة H.235.2/20). ولا يتم الاستيقان في هذه الحالة إلا في جزء فرعي (**ClearToken** في **CryptoToken**) من الرسالة H.225.0/RAS. وقد يكون أسلوب الاستيقان–فقط مفيداً لاجتياز الأجهزة NAT/حائط الحماية التي تغير العناوين/الموانئ IP في الحمولات النافعة H.323.

ونظراً لأن الاستيقان لا يشمل إلا جزءاً محدوداً جداً من الرسالة، فإن أسلوب الاستيقان–فقط لا يضمن تكامل الرسالة كما هو الحال مع الإجراء I. وهكذا فإن أسلوب الاستيقان–فقط يقدم قدراً أقل من الأمن.

وينبغي، فيما يخص أسلوب الاستيقان–فقط، استعمال المجالات التالية في الرسائل المحمية:

- ينبغي أن يضم المجال **CryptoH323Token** لكل رسالة H.225.0/RAS المجالات التالية:
  - **nestedCryptoToken** ويضم المجال **CryptoToken** الذي يضم بدوره المجال **cryptoHashedToken** الذي يضم المجالات التالية:
    - **tokenOID** موضوعاً على:
      - "B" (انظر الفقرة H.235.2/20) للدلالة على أن حساب عملية الاستيقان–فقط يشمل جميع مجالات **ClearToken**.
    - **hashedVals** ويضم المجال **ClearToken** المستعمل مع المجالات التالية:
      - **tokenOID** موضوعاً على:
        - "T" (مثال ClearToken أساسي لبقية محتوى المجال ClearToken) أو أي معرّف OID مناسب لكل استعمال آخر.
      - **timeStamp** ويضم طابعة الوقت؛
      - **random** ويضم رقم تتابع متزايد بوتيرة واحدة. ويتيح هذا الرقم التمييز بين رسالتين طبع عليهما نفس الوقت والساعة (ضمن حدود استبانة الميقاتية)؛
      - **generalID** ويضم معرّف هوية المرسل إليه (في حالة الرسائل وحيدة المقصد حصراً)؛
      - **sendersID** ويضم معرّف هوية المرسل؛

- **dhkey** ويستعمل في نقل المعلمات DH كما هو محدد في التوصية ITU-T H.235.0 خلال الفترة من **Setup** إلى **Connect**.
  - **halfkey** ويضم المفتاح العمومي العشوائي لأحد أطراف الاتصال؛
  - **modsize** ويضم المعلمة DH-prime (انظر الجدول H.235.6/4)؛
  - **generator** ويضم المعلمة DH-group (انظر الجدول H.235.6/4).

الملاحظة 1 – عند استعمال مواصفة الأمن الأساسي بدون مواصفة الأمن بالتجفير الصوتي ينبغي عدم إرسال أي معلمة DH وغياب المجال **dhkey**؛ ويمكن وضع المعلمات **halfkey** و**modsize** و**generator** على {'0'B و'0'B و'0'B}.

- **token** ويضم **HASHED** مع المجالات:
  - **algorithmOID** موضوعاً على "U" للدلالة على استعمال الشفرة HMAC-SHA1-96؛
  - **params** موضوعاً على NULL؛
  - **hash** ويضم المستيقن المحسوب بواسطة الشفرة HMAC-SHA1-96. ويتم حساب المستيقن في:
    - جميع مجالات **ClearToken** إذا كان **tokenOID** في **CryptoHashedToken** موضوعاً على "B" (مشيراً بذلك إلى أسلوب الاستيقان بمفرده).

- يتم التحقق من المستيقن في نهاية الفرع النهائي للقناة (من EP1 إلى GK1 ومن GK1 إلى GK2 ومن GK2 إلى EP2 ومن EP1 إلى GK2 ومن GK1 إلى EP2 أو من EP1 إلى EP2 حسب الحالة) ويعاد حسابه قبل إرسال الرسالة إلى الفرع اللاحق.

الملاحظة 2 – لا يحسب المستيقن إلا في العلامة **ClearToken**.

الملاحظة 3 – ينبغي استعمال طريقة الحشو التي يرد وصفها في المعيار SHA1 (ISO/IEC 10118-3).

الملاحظة 4 – يوصي بشدة من أجل منع الاعتداءات التكرارية في التطبيقات بتغيير كلمة السر (المفتاح) قبل إنهاء دورة كاملة (أو نهاية الدورة) لرقم التتابع المتزايد بوتيرة واحدة.

الملاحظة 5 – يستطيع المقصد أن يكشف استعمال الإجراء IA عن طريق تقييم المعرف "B" **OID** في العنصر **tokenOID**.

ولا يحسب المستيقن إلا في العنصر **ClearToken** الموجود في **CryptoH323Token** (أي **ClearToken**) من الفيشة **token** للمجال **cryptoHashedToken**. وينبغي حساب التظليل بالتجفير في نفس سلسلة البتات المشفرة بالترميز ASN.1 للعنصر **ClearToken**.

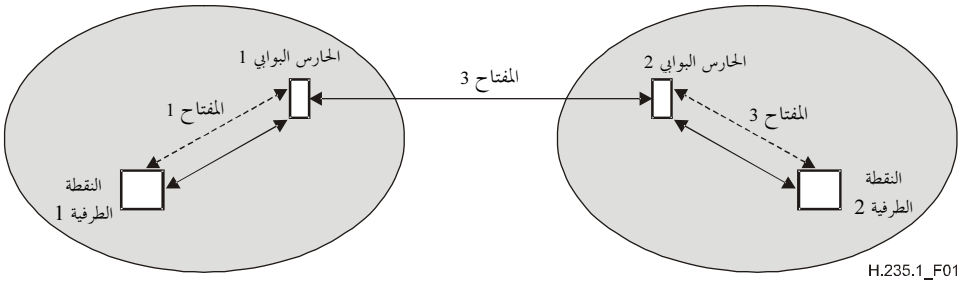
وتستطيع النقاط الطرفية H.235 في الطبعة 1 والطبعة 2، أن تستعمل إجراء الاستيقان بمفرده، حيث ينبغي استعمال المعرفات OID المقابلة للقيمة "B". وينبغي أن تكون النقاط الطرفية H.235 من الطبعة 1 مطابقة للإجراء الوارد في الفقرة 11.

9 عرض استخدام الإجراء I

تبين الأشكال من 1 إلى 3 وجود مفاتيح مشتركة عند نهاية قنوات الاتصال لمختلف تجميعات الحارسات البوابية والقنوات H.225.0 بالتسيير المباشر. والمفتاح المشترك موجود دائماً بين نقطة طرفية وحارسها البوابي بمعزل عن نموذج النداء بغية إتاحة الاستيقان/التكامل للرسالة RAS. وفي حال انتهاء قناة RAS وقناة H.225.0 بين نفس العقدتين (الاثنتين) يمكن استعمال نفس المفتاح للحصول على استيقان/تكامل الرسائل RAS وH.225.0.

ويمثل الشكل 1 السيناريو الأكثر قابلية للقياس حيث تقع كلا النقطتين الطرفيتين داخل مناطق تطبق نموذج التسيير عن طريق الحارس البوابي. وتتقاسم جميع الحارسات البوابية المعنية مفاتيح بعضها البعض. ويوصى باستعمال السيناريو المبين في الشكل 1 لجعله قابلاً للتدرج.

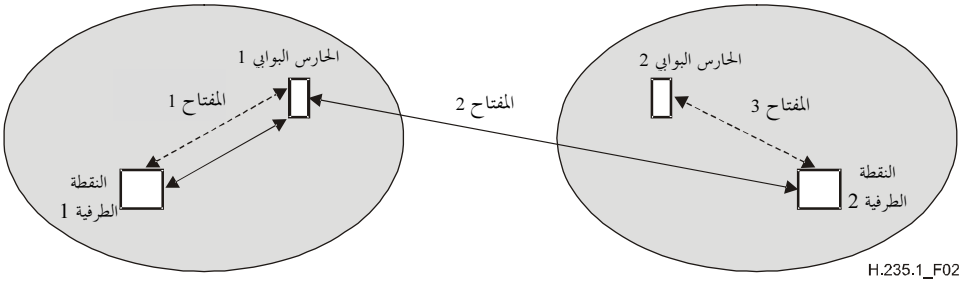
الملاحظة 1 – لا يتيح هذا السيناريو أمناً حقيقياً من طرف إلى آخر بين النقاط الطرفية؛ ولا تتوقف جميع جوانب الأمن إلا على الحارسات البوابية الوسيطة الموثوقة.



--------- رسالة RAS/H.225.0
———— تشوير نداء H.225.0

الشكل H.235/1 – عرض استخدام الإجراء I في سيناريو من حارس GK إلى GK علماً بأن النقطتين الطرفيتين موجودتان في مناطق تسيير الحارسات GK

ويمثل الشكل 2 سيناريو مختلطاً تقع فيه إحدى النقطتين الطرفيتين داخل منطقة تطبق نموذج التسيير بحارس GK بينما تقع النقطة الطرفية الأخرى داخل منطقة تطبق نموذج التسيير المباشر. وقد يحدث هذا السيناريو في بيئات مغلقة حيث يكون عدد النقاط EP2 والحارسات GK1 محدوداً.

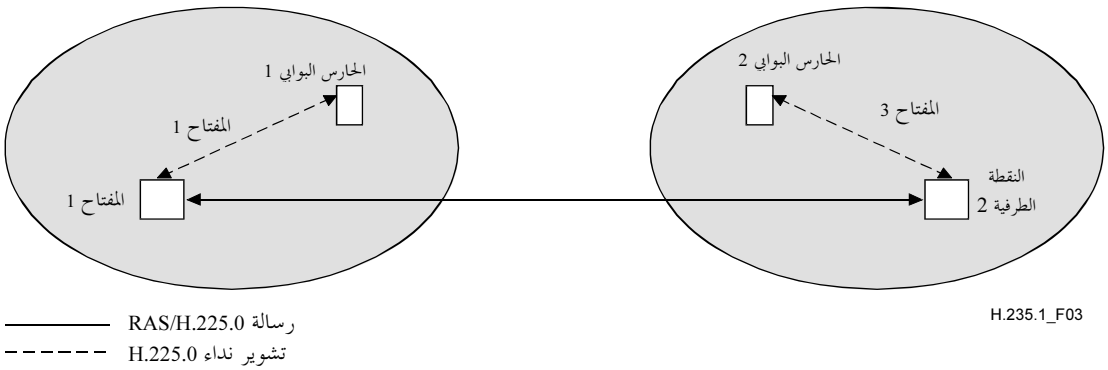


--------- رسالة RAS H.225.0
———— تشوير نداء H.225.0

الشكل H.235/2 – استخدام الإجراء I في سيناريو مختلط بوجود النقطة EP1 ضمن منطقة تسيير بحارس GK والنقطة EP2 ضمن منطقة تسيير مباشر

ويعرض الشكل 3 السيناريو الذي توجد فيه النقطتان الطرفيتان ضمن مناطق تطبق نموذج الحارس GK بالتسيير المباشر. ويكون هذا السيناريو أقل قابلية للقياس عندما تتواجد عدة نقاط طرفية. ويوصى مبدئياً باستعمال الملحق E مع الإجراءين II وIII بدلاً عنه. ولأغراض هذا السيناريو الخاص والإجراءات I أو II أو III من الضروري أيضاً إيجاد تدابير أمن إضافية (تحمي من الاحتيال وسوء الاستعمال بواسطة ترخيص النداء باستعمال علامات نفاذ إلى البوابات H.323 مثلاً). لا يتم تناولها في هذه التوصية، وتتطلب مزيداً من الدراسة.

الملاحظة 2 – يضمن هذا السيناريو أمناً كاملاً من طرف إلى طرف دون الارتباط بالعقد الوسيطة الموثوقة.



الشكل H.235/3 – استعمال الإجراء I لأغراض السيناريو الذي تقع فيه النقاط الطرفية ضمن مناطق تستعمل حارس GK بالتسيير المباشر

فلنأخذ حالة الشكل 1 الذي تتقاسم فيه ثلاث كلمات سر مزدوجة بين النقطة EP1 والحارس GK1 وبين الحارس GK1 والحارس GK2 وبين الحارس GK2 والنقطة EP2. ويتم توليد ثلاثة مفاتيح طول واحدها 20 أثمونا – *key1* و*key2* و*key3* – استناداً إلى كلمات السر هذه القائمة على الإجراء المذكور في الفقرة H.235.0/4.2.8. ومن أجل الحصول على الحد الأقصى من الأمن يوصي بأن تصبح كلمات السر/المفاتيح الثلاثة المختارة بشكل عشوائي مستقلة.

وترد فيما بعد تفاصيل إجراءات استيقان الرسائل RAS وH.225.0 وH245 وتكاملها. ويوضح مثال العرض المعلمات الخاصة لنموذج بالتسيير عبر الحارس GK؛ كما أن هناك مجموعات مفيدة وصالحة أخرى لمعرفات هوية الأغراض في سيناريوهات مختلفة.

الملاحظة 3 – ولا تصلح السيناريوهات المقدمة في الأشكال من 1 إلى 3 للتدرج عندما يكون عدد المفاتيح التناظرية (كلمات السر) المستخدمة بالتقاسم بين الحارسات GK (الشكل 1) أو بين الحارسات GK والنقاط EP (الشكل 2) أو بين النقاط الطرفية (الشكل 3) مرتفعاً جداً.

1.9 استيقان الرسائل RAS وتكاملها

لنأخذ الحالة التي ترغب فيها النقطة EP1 إرسال رسالة RAS – رسالة **ARQ** مثلاً إلى الحارس GK1. تقدم النقطة EP1 الوقت والساعة ورقم التتابع وتدخلها في المجالين **timeStamp** و**random** على التوالي مع لقب الحارس GK في المجال **generalID** ومعرّف النقطة الطرفية في المجال **sendersID**. وتظهر هذه المجالات في المجال **ClearToken** من **hashedVals** الذي يشكل بدوره جزءاً من **cryptoHashedToken** للمجال **CryptoToken** من **cryptoH323Token** من الرسالة **ARQ**.

المجال **tokenOID** من **cryptoHashedToken** موضوع على "A"، مما يدل على أن جميع مجالات الرسالة **ARQ** مظللة. ويوجد في المجال **HASHED** في **token** من **cryptoHashedToken** المجال **algorithmOID** موضوعاً على "U"، مما يدل على استعمال الشفرة HMAC-SHA1-96 والمجال **paramS** موضوعاً على NULL. ثم تحسب النقطة EP1 المستيقن استناداً إلى الشفرة HMAC-SHA1-96 باستعمال المفتاح *key1* الذي يبلغ 20 أثمونا. ويحسب المستيقن في مجمل الرسالة RAS.

وتدرج النقطة EP1 مستيقناً محسوباً في المجال **hash** للمعلمة **token** من المجال **cryptoHashedToken** من **CryptoToken** الموجود في المجال **cryptoH323Token** من الرسالة **ARQ**. ثم ترسل هذه الرسالة إلى الحارس GK1.

وعندما يستقبل الحارس GK1 الرسالة **ARQ** يتحقق من المستيقن استناداً إلى بعض المعايير التي تشمل:

- حداثة **timeStamp** وفرادة **random**؛
- هوية **generalID** ومعرّفه الخاص؛
- توافق مستيقن الرسالة **ARQ** والمستيقن المحسوب في الحارس GK1.

2.9 استيقان الرسالة H.225.0 وتكاملها

لنأخذ الحالة التي ترغب فيها النقطة EP1 إرسال رسالة H.225.0 إلى النقطة EP2 ولتكن رسالة **Setup** مثلاً. وتولد النقطة EP1 الوقت الساعة ورقم التتابع وتدخلهما في المجالين **timeStamp** و**random** على التوالي، مع اسم الحارس GK1 في المجال

generalID ومعرف النقطة EP في المجال **sendersID**. وتحسب النقطة الطرفية EP1 أيضاً نصف المفتاح ديفي–هيلمان وتدرج المعلمات DH: **halfkey** و**modsize** و**generator** في المجال **dhkey** من **ClearToken**. وتوجد هذه المجالات في المجال **ClearToken** من **hashedVals** الموجود بدوره في **cryptoHashedToken** من المجال **CryptoToken** من **cryptoH323Token** من الرسالة **Setup**.

والمجال **tokenOID** من **cryptoHashedToken** موضوع على "A" للدلالة على أن جميع مجالات رسالة تشوير النداء H.225.0 مظللة. وللمجال **HASHED** من **token** في **cryptoHashedToken** مجاله **algorithmOID** الموضوع على "U" للدلالة على استخدام الشفرة HMAC-SHA1-96 والمجال **paramS** الموضوع على NULL. ثم تحسب النقطة EP1 المستيقن على أساس الشفرة HMAC-SHA1 بواسطة المفتاح *key1* البالغ 20 أثمونا. ويتم حساب المستيقن طبقاً لطريق التظليل المختارة (A) مع مراعاة مجمل رسالة تشوير النداء H.225.0.

وتدرج النقطة EP1 المستيقن المحسوب في **hash** للمجال **token** للمجال **cryptoHashedToken** من **CryptoToken** الموجود في المجال **cryptoH323Token** من الرسالة **Setup**. ثم ترسل الرسالة **Setup** بعد ذلك إلى الحارس GK1.

عند استلام الحارس GK1 الرسالة **Setup** يتحقق من المستيقن على أساس عدة معايير تشمل:

- حداثة **timeStamp** وفرادة **random**؛
- هوية **generalID** ومعرّفه الخاص؛
- التحقق من المعلمات ديفي هيلمان كأن يتم التحقق على سبيل المثال، من صحة المعلمتين prime وgenerator البالغتين 1024 بتة. والتحقق من أمن المعلمات DH هو عملية طويلة لا يتم إجراؤها إلا إذا تطلبتها السياسة المحلية؛
- توافق مستيقن الرسالة **Setup** والمستيقن المحسوب في GK1.

إذا كانت نتيجة التحقق من المستيقن إيجابية، يحسب الحارس GK1 مستيقناً جديداً يستعيض به عن المستيقن القديم في الرسالة **Setup** قبل إرساله إلى الحارس GK2 بالطريقة التالية: يستعيض الحارس GK1 عن قيم **timeStamp** و**random** و**sendersID** و**generalID** من المجال **ClearToken** من **hashedVals** بقيم تنطبق على المقطع GK1-GK2. ويضم المجال **timeStamp** طابعة الوقت والساعة النافذة ويضم المجال **random** رقم التتابع المتزايد بانتظام للمقطع GK1-GK2 ويضم المجال **generalID** اسم الحارس GK2 ويضم المجال **sendersID** اسم الحارس GK1. ويدخل GK1 أيضاً المعلمات DH المستقبلة في المجال **dhkey** من **ClearToken**.

ثم يحسب الحارس GK1 المستيقن الجديد لأغراض رسالة تشوير النداء H.225.0 هذه بواسطة المفتاح *key2* والخوارزمية HMAC-SHA1-96 (**algorithmOID**="U") ويدخله في المجال **hash** من **token** ويرسل الرسالة **Setup** إلى GK2.

وعندما يستقبل GK2 الرسالة **Setup** يتحقق من المستيقن ويحسب مستيقناً جديداً بعد تغيير المجالين **ClearToken** من **hashedVals** بطريقة مناسبة ويدخله في المجال **Hash** وينقل الرسالة **Setup** إلى النقطة EP2.

3.9 استيقان الرسالة H.245 وتكاملها

لنأخذ الحالة التي ترغب فيها النقطة EP1 إرسال رسالة H.245 – ولتكن على سبيل المثال رسالة **TerminalCapabilitySet** – إلى النقطة EP2. تتحقق النقطة EP1 مما إذا كان بإمكانها إرسال رسالة H.225.0 إلى الحارس GK1. فإذا صحّ ذلك أرسلت الرسالة H.245 في قناة نفقية داخل هذه الرسالة H.225.0. وللمجالات الموجودة في الرسالة H.225.0 قيماً سبقت الإشارة إليها لأغراض إرسال رسالة H.225.0. ونظراً إلى أن الرسالة H.245 مرسلة في قناة نفقية فإن المجال **h323-uu-pdu** من الرسالة **h323-UserInformation** تتخذ مجالاته القيم التالية:

- يوضع المجال **h323-message-body** على نمط الرسالة H.225.0 أثناء الإرسال؛
- يوضع المجال **h245Tunnelling** على TRUE؛
- يضم المجال **h245Control** سلسلة الأثمونات H.245 PDU.

وتولد النقطة EP1 مجال **CryptoToken** لأغراض الرسالة H.225.0 وتضع **tokenOID** على "A" للدلالة على الاستيقان والتكامل وتضع المعلمات **timeStamp** و**random** و**sendersID** و**generalID** و**tokenOID** على "T" في **ClearToken** من **hashedVals** وتضع **algorithmOID** على "U" للإشارة إلى استعمال الشفرة HMAC-SHA1-96 و**hash** على مستيقن التظليل الذي يحسب في مجمل مجالات رسالة تشوير النداء H.225.0.

غير أنه عند عدم وجود أي إرسال للرسالة H.225.0 بالانتظار فإن الرسالة H.245 تسير في قناة نفقية ضمن رسالة H.225.0 **facility** لهذا الغرض. ويضم المجال **h323-uu-pdu** من الرسالة **h323-UserInformation** القيم التالية:

- يوضع المجال **h323-message-body** على **facility** التي تضم:
  - **reason** موضوعاً على **undefinedReason**؛
  - **tokens** و**cryptoTokens** كما هو الحال بالنسبة إلى كل رسالة H.225.0.
- **h245Tunnelling** موضوعاً على TRUE؛
- يضم المجال **h245Control** سلسلة الأثمونات H.245 PDU.

وتولد النقطة EP1 كما هو مبين أعلاه، مجالاً **CryptoToken** ضمن إطار الرسالة **facility** H.225.0. وترسل الرسالة **facility** بعد ذلك من النقطة EP1 إلى GK1.

ويتحقق GK1 في كلا الحالتين (إرسال الرسالة H.225.0 بالانتظار أو استعمال رسالة **facility** H.225.0 مناسبة) من المستيقن عند استقبال الرسالة. ثم تسير الرسالة H.245 في قناة نفقية في الرسالة H.225.0 إذا كان إرسالها إلى المقطع GK2-GK1 بالانتظار؛ وإلا فإنها تسيّر في قناة نفقية في رسالة **facility** H.225.0 مناسبة. وكما هو الحال بالنسبة إلى جميع إرسالات الرسالة H.225.0 فإن المستيقن الجديد يحسب للرسالة المعنية قبل إرسالها من GK1 إلى GK2. وتتكرر العملية بالنسبة إلى المقطع EP2-GK2.

4.9 سيناريو التسيير المباشر

لا تستطيع الكيانات H.323 الأمنية الاتصال في سياق التسيير عبر حارس بوابي كما يرد في هذه التوصية وحسب بل تستطيع أيضاً أن تطبق نموذج التسيير المباشر. ويتطلب ذلك تدابير أمن إضافية (فيش نفاذ) لا حاجة لها في البيئات الأكثر بساطة التي تعتمد التسيير عبر الحارس البوابي. وتبين التوصية ITU-T H.235.4 كيفية تأمين نموذج التسيير المباشر.

10 توفير خدمة طرفية متخصصة

تستطيع الكيانات H.323 الأمنية استعمال خدمات طرفية متخصصة طبقاً للإجراء الوارد في الفقرة H.235.0/6.1.I.

11 المواءمة مع السياق H.235 الطبعة 1

بالرغم من أن مظاهر الأمن هذه قد أعدت في السياق H.235 طبعة 2 (التوصية ITU-T H.235 (2000)) فإنها قابلة للتطبيق في سياق الطبعة 1 من التوصية المذكورة (التوصية ITU-T H.235 (1998)) مع إدخال بعض التعديلات الطفيفة. ويستطيع المرسل إليه أن يكشف وجود طبعة البروتوكول H.235 الذي يتبعه المرسل عن طريق تقييم معرفات هوية غرض مواصفة الأمن (انظر الفقرة 15).

تطبيقات H.235 طبعة 1 (التوصية ITU-T H.235 (1998)):

- عدم إعطاء قيمة للمجال أو عدم تقييم المجال **sendersID** من **ClearToken**؛
- عدم استعمال الخدمات الطرفية كما هو مبين في الفقرة 10.

12 سلوك التوزيع المتعدد

ينبغي ألا تضم الرسائل متعددة التوزيع H.225.0 مثل الرسائل GRQ أو LRQ المجال CryptoToken المطلوب في الإجراء I باستثناء حالة إرسالها بالتوزيع الأحادي.

13 قائمة رسائل التشوير المؤمِّنة

توفر هذه الفقرة ملخصاً للكيفية التي تؤمِّن بها هذه التوصية مختلف رسائل التشوير H.323، والوسائل التي تؤمِّنها بها.

1.13 H.225.0 RAS

رسالة H.225.0 RAS	مجالات التشوير H.235	الاستيقان والتكامل
أي رسالة	Crypto Tokens	الإجراء I

2.13 تشوير النداء H.235.0

رسالة تشوير النداء H.225.0	مجالات التشوير H.235	الاستيقان والتكامل
UUIE-Alerting وCallProceeding-UUIE UUIE-Connect و Setup- UUIE و Facility- UUIE وInformation-UUIE Progress-UUIE وRelease Complete-UUIE وStatus-UUIE وStatusInquiry-UUIE وSetupAcknowledge-UUIE وNotify-UUIE	Crypto Tokens	الإجراء I

3.13 التحكم بالنداء H.245

ينبغي إما تكديس الرسائل H.245 الآتية من الكيانات H.323 الأمينة أو الذاهبة إليها في إطار التوصيل السريع والأمين وإما تسييرها عبر النفق في رسالة H.224.0 Facility-UUIE أمينة.

14 استعمال المعرّفين sedersID وGeneralID

تضم المعلمة **ClearToken** مجالات المعرّفين بـــ **sendersID** و**GeneralID**. وعندما تتوفر معلومة تعرف الهوية تكون قيمة المعرّف **sendersID** هي قيمة معرف الحارس GK (GKID) للرسالة القادمة من GK وقيمة معرف النقطة الطرفية (EPID) للرسائل القادمة من النقطة EP. عندما تتوفر معلومة تعرف الهوية تكون قيمة معرف الهوية **generalID** هي قيمة المعرف GKID للرسائل القادمة من النقطة الطرفية وقيمة المعرف EPID للرسائل القادمة من الحارس البوابي. وعند عدم تيسُّر معلومة تعرف الهوية أو عندما تلتبس الإذاعة/الإذاعة المتعددة يغيب المجال أو يضم سلسلة من الأصفار. ويُلخص الجدول 2 هذه الحالة.

الجدول H.235.1/2 – استعمال معرفيِّ الهوية SendersID وGeneralID

الرسالة	المعرّف sendersID	المعرف generalID
Unicast **GRQ**	**EPID** إن توفر وإلا **NULL**	**GKID**
Multicast **GRQ**	**EPID** إن توفر وإلا **NULL**	
GCF, **GRJ**	**GKID**	**EPID** إن توفر وإلا **NULL**
Initial **RRQ**	**EPID** إن توفر وإلا **NULL**	**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (EP-to-GK)	**EPID**	**GKID**
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (GK-to-EP)	**GKID**	**EPID**
ARQ, IRQ, RAI	**EPID**	**GKID**
ACF, ARJ, BCF, LCF, LRJ, IRR, IRQ, RAC, LCF, LRJ, IACK, INAK	**GKID**	**EPID**
Unicast **LRQ** (EP-to-GK)	**EPID**	**GKID**
Unicast **LRQ** (GK-to-GK)	**GKID**	**GKID**
Multicast **LRQ**	**EPID**	
ملاحظة – GKID = معرف هوية الحارس البوابي، EPID = معرف هوية النقطة الطرفية. يدل الفراغ على سلسلة تعرف هوية ناقصة أو معدومة.		

15 قائمة معرِّفات هوية الغرض

يعدد الجدول 3 الوارد أدناه جميع المعرّفات OID المذكورة (انظر أيضاً [OIW] و[WEBOIDs]). وهناك معرّفات هوية أغراض للبروتوكولين H.235v1 وH.235v2.

الجدول H.235.1/3 – معرّفات هوية الأغراض

تسمية المعرف	قيمة المعرف	الوصف
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	يُستعمل في الإجراء I لأغراض المعرّف CryptoToken-tokenOID ويدل على أن التظليل يشمل جميع مجالات الرسالة RAS وتشوير النداء H.225.0 (الاستيقان والتكامل).
"E"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 9} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 9}	ClearToken من طرف إلى طرف وهو يسير الهويات ID للمرسلين من أجل التحقق من جهة المرسل.
"T"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 5} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 5}	يستعمل في الإجراءين I وIA مثل ClearToken أساسي لأغراض الاستيقان والحماية من تكرار الرسائل وخيارياً لأغراض إدارة مفاتيح ديفي–هيلمان كما ورد وصفها في الفقرة H.235.6/5.8.
"U"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 6} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 6}	يستعمل في الإجراء I لأغراض معرف الخوارزمية OID ويدل على استعمال الشفرة HMAC-SHA1-96.

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