الاتحـــــاد الدولـــــي للاتصـــــالات

ITU-T H.235.3

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمة السمعية والمرئية والأنظمة متعددة الوسائط

البنية التحتية للخدمات السمعية والمرئية – جوانب الأنظمة

إطار الأمن H.323: مواصفة الأمن الهجينة

التوصيـــة ITU-T H.235.3

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية والمرئية 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

للحصول على مزيد من التفاصيل يرجى الرجوع إلى قائمة توصيات القطاع ITU-T

التوصيـــة ITU-T H.235.3

إطار الأمن H.323: مواصفة الأمن الهجينة

ملخص

إن الهدف من هذه التوصية هو وصف مواصفة أمن هجينة تطورية وتتوافر فيها الكفاءة وتقوم على بنية تحتية ذات مفتاح عمومي (PKI) بالنسبة للطبعة 2 من التوصية ITU-T H.235.0 أو التوصيات اللاحقة. وتستفيد المواصفة المشار إليها في هذه التوصية من مواصفات الأمن المذكورة في التوصيتين ITU-T H.235.1 وITU-T H.235.2 من خلال تطبيق التوقيعات الرقمية من التوصية ITU-T H.235.2 ونشر مواصفة الأمن الأساسي من التوصية ITU-T H.235.1.

في الطبعات السابقة من السلسلة الفرعية H.235، تضمن في الملحق H.235/F هذه المواصفة. كما تُظهر التذييلات IV وV وVI للتوصية H.235.0 التقابل بين جميع الفقرات والأشكال والجداول بين الطبعتين 3 و4 من التوصية ITU-T H.235.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات على التوصية ITU-T H.235.3 في الاتحاد بتاريخ 13 سبتمبر 2005 بموجب الإجراء الوارد في التوصية ITU-T A.8.

مفردات رئيسية

استيقان، شهادة التوقيع الرقمي، تجفير، تكامل، إدارة المفاتيح، أمن تعدد الوسائط، 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).

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

إطار الأمن H.323: مواصفة الأمن الهجينة

1 مجال التطبيق

إن الهدف من هذه التوصية هو وصف مواصفة أمن هجينة تطورية وتتوافر فيها الكفاءة وتقوم على بنية تحتية ذات مفتاح عمومي (PKI) بالنسبة للطبعة 2 من التوصية ITU-T H.235.0 أو التوصيات اللاحقة. وتستفيد المواصفة المشار إليها في هذه التوصية من مواصفات الأمن المذكورة في التوصيتين ITU-T H.235.1 وITU-T H.235.2 من خلال تطبيق التوقيعات الرقمية من التوصية ITU-T H.235.2 ونشر مواصفة الأمن الأساسي من التوصية ITU-T H.235.1.

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 وترزيم تدفقات الوسائط لأنظمة الاتصالات متعددة الوسائط القائمة على الرزم.*
- التوصية ITU-T H.235، الطبعة 1 (1998)، *أمن وتجفير المطاريف المتعددة الوسائط من السلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235، الطبعة 2 (2000)، *أمن وتجفير المطاريف المتعددة الوسائط من السلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.0 (2005)، *أمن H.323: أمن وتجفير المطاريف المتعددة الوسائط من السلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.1 (2005)، *أمن H.323: مواصفة الأمن الأساسي.*
- التوصية ITU-T H.235.2 (2005)، *أمن H.323: مواصفة الأمن مع التوقيع.*
- التوصية ITU-T H.235.6 (2005)، *أمن H.323: مواصفة التجفير الصوتي مع الإدارة الأصلية للمفاتيح H.245/H.235.*
- التوصية ITU-T H.245 (2005)، *بروتوكول التحكم لأغراض الاتصالات متعددة الوسائط.*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*
- التوصية ITU-T Q.931 (1998)، *تحديد الطبقة 3 من السطح البيني لمستعمل الشبكة الرقمية متكاملة الخدمات (ISDN).*

- التوصية ITU-T X.509 (2005) | ISO/IEC 9594-8:2005، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أطر عامة لشهادات المفاتيح العمومية والنعوت.*
- التوصية ITU-T X.800 (1991)، *معمارية أمن التوصيل البيني للأنظمة المفتوحة لتطبيقات CCITT.*
- المعيار ISO 7498-2:1989، *أنظمة معالجة البيانات – التوصيل البيني للأنظمة المفتوحة – النموذج المرجعي الأساسي– الجزء 2: معمارية الأمن.*
- التوصية ITU-T X.803 (1994) | ISO/IEC 10745:1995، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – نموذج الأمن للطبقات العليا.*
- التوصية ITU-T X.810 (1995) | ISO/IEC 10181-1:1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: نظرة عامة.*
- التوصية ITU-T X.811 (1995) | ISO/IEC 10181-2:1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار الاستيقان.*
- المعيار IETF RFC 3280 (2002)، *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

2.2 المراجع الغنية بالمعلومات

[ISO|IEC 14888-3] ISO/IEC 14888-3:1998، *تكنولوجيا المعلومات – تقنيات الأمن – توقيعات رقمية مع تذييل؛ الجزء 3: آليات قائمة على الشهادة.*

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; October 1, 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; .http://www.rsa.com/rsalabs/pubs/PKCS/index.html

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm.*

3 المصطلحات والتعاريف

تنطبق على هذه التوصية التعاريف الواردة في الفقرة 3 من التوصية H.323 والفقرة 3 من التوصية H.225.0 والفقرة 3 من التوصية H.245. وبعض المصطلحات المستخدمة في هذه التوصية معرّفة أيضاً في التوصيات ITU-T X.800 | ISO 7498-2 وX.803 | ISO/IEC 10745 وX.810 | ISO/IEC 10181-1 وX.811 | ISO/IEC 10181-2 وH.235.0.

4 الرموز والمختصرات

تستخدم هذه التوصية المختصرات التالية:

ALG بوابة عند سوية التطبيق (*Application Level Gateway*)

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

BRJ نبذ عرض النطاق (*Bandwidth Reject*)

BRQ طلب عرض النطاق (*Bandwidth Request*)

CA سلطة إصدار الشهادات (*Certification Authority*)

CRL قائمة إبطال الشهادات (*Certificate Revocation List*)

DB قاعدة بيانات (*Database*)

DH ديفي–هيلمان (*Diffie-Hellman*)

DN اسم متميّز (*Distinguished name*)

EP نقطة طرفية (*Endpoint*)

GCF تأكيد الحارس البوابي (*Gatekeeper confirm*)

GK حارس بوابي (*Gatekeeper*)

GKID معرف (هوية) حارس بوابي (*Gatekeeper identifier*)

GKSP معالج أمن حارس بوابي (*Gatekeeper security processor*)

GRJ رفض حارس بوابي (*Gatekeeper reject*)

GRQ طلب حارس بوابي (*Gatekeeper request*)

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

ICV قيمة التحقق من التكامل (*Integrity check value*)

ID معرف (الهوية) (*Identifier*)

IP بروتوكول الإنترنت (*Internet protocol*)

LDAP بروتوكول سريع للنفاذ إلى الدليل (*Lightweight directory access protocol*)

LRQ طلب تحديد الموقع (*Location request*)

MCU وحدة تحكم متعدد النقاط (*Multipoint Control Unit*)

MD5 ملخص الرسالة 5 (*Message digest 5*)

NAT ترجمة عنوان الشبكة (*Network address translation*)

OID معرّف هوية الغرض (*Object Identifier*)

PDU وحدة بيانات البروتوكول (*Protocol data unit*)

PKI بنية تحتية ذات مفتاح عمومي (*Public Key Infrastructure*)

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

RCF تأكيد التسجيل (*Registration Confirm*)

RRJ رفض التسجيل (*Registration reject*)

RRQ طلب التسجيل (*Registration request*)

RSA خوارزمية تحفير تريفست وشامير وأدلمان (*Rivest, Shamir and Adleman encryption algorithm*)

RTP بروتوكول النقل في الوقت الفعلي (*Real-time transport protocol*)

SHA خوارزمية التظليل المأمون (*Secure Hash Algorithm*)

UDP بروتوكول داتا غرام المستعمل (*User Datagram Protocol*)

URQ طلب إلغاء التسجيل (*Unregistration Request*)

VoIP المهاتفة باستخدام بروتوكول الإنترنت (*Voice-over-IP*)

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

- "Shall" تشير إلى طلب إلزامي.
- "Should" تشير إلى عمل مقترح ولكنه خياري.

– "May" تشير إلى عمل خياري وليس توصية.

تستخدم مواصفة الأمن الهجينة المصطلحات والتعاريف الواردة في التوصيتين ITU-T H.235.1 وITU-T H.235.2.

في حين توفر خدمة تكامل الرسائل دائماً استيقان الرسائل، فإن العكس ليس صحيحاً على الدوام. وفي أسلوب الاستيقان فقط، لا يشمل التكامل المأمون إلا مجموعة فرعية معينة من مجالات الرسائل. وينطبق ذلك على خدمات التكامل التي تؤمنها الوسائل لاتناظرية (على سبيل المثال، التوقيعات الرقمية). ومن ثم، من الناحية العملية، تستخدم لاستيقان وتكامل خدمة مزدوجة البيانات المفتاحية نفسها من دون توهين مستوى الأمن.

وتطبق مواصفة الأمن هذه في البيئات التي يحتمل أن تتضمن مطاريف كثيرة، لا يمكن فيها تخصيص كلمة سر سكونية/ مفتاح تناظري، مثلاً في السيناريوهات الواسعة النطاق أو ذات النطاق الشامل. وبدلاً من ذلك، تفترض المواصفة إلى تيسر بنية تحتية ذات مفتاح عمومي مع شهادات مخصصة ومفاتيح خاصة أو عمومية وأدلة، إلخ. وبالإضافة إلى ذلك، تستخدم هذه المواصفة للأمن تقنيات تناظرية مجفَّرة، حسب مقتضى الحال.

وتستحدث مواصفة الأمن هذه المصطلحين "الرسالة الأولى" و"الرسالة الأخيرة" المرسلتين. وتختلف حماية الرسالة الأولى (وربما أيضاً الرسالة الأخيرة) عن حماية أمن الرسائل المتبقية الأخرى.

وتُعتبر "الرسالة الأولى" المرسلة بمثابة رسالة تنتقل بين كيانين H.323 وتنشئ سياقاً للأمن. وهي تضع تحت تصرف هذين الكيانين بيانات المفتاح التناظري وتحدد بداية الاتصال. وفي حالة الرسائل RAS H.225.0 فإن الرسالة الأولى تمثِّل طلب التسجيل RRQ ورسالة الاستجابة المتعلقة به. وفي حال تشوير النداء H.225.0 الذي يستخدم الانطلاق السريع، فإن الرسالة الأولى هي SETUP وCONNECT.

وتنهي "الرسالة الأخيرة" سياق الأمن الذي تم إنشاؤه. ويجب إتلاف البيانات المفتاحية المنشأة. وبالنسبة للرسالة RAS H.225.0، فإن الرسالة الأخيرة تمثل طلب إلغاء التسجيل URQ ورسالة الاستجابة المتعلقة به، أما بالنسبة إلى تشوير النداء H.225.0، فإن الرسالة الأخيرة هي RELEASE-COMPLETE.

6 لمحة عامة

تصف هذه التوصية مواصفة أمن هجينة تطورية وتتوافر فيها الكفاءة وتقوم على بنية تحتية ذات مفتاح عمومي (PKI)، وتستخدم التوقيعات الرقمية في التوصية ITU-T H.235.2 ومواصفة الأمن الأساسي في التوصية ITU-T H.235.1. وتقترح هذه التوصية على أنها خيار. ويجوز لكيانات الأمن H.323 (المطاريف والحارسات البوابية والبوابات ووحدات التحكم بالنقاط المتعددة، إلخ.) أن تطبق مواصفة الأمن الهجينة هذه لتحسين الأمن كلما دعت الحاجة إلى ذلك.

وفي هذا النص، يعني المصطلح "هجين" أن إجراءات الأمن من مواصفة التوقيعات في التوصية ITU-T H.235.2 تطبق فعلياً بقدر من المرونة وأن التوقيعات الرقمية لا تزال مطابقة لإجراءات الرسالة RSA. غير أن التوقيعات الرقمية لا تُستخدم إلا في حالات الحاجة القصوى بينما في الظروف العادية، تستخدم تقنيات الأمن التناظرية عالية الكفاءة لمواصفة الأمن الأساسي الواردة في التوصية ITU-T H.235.1.

وتطبّق مواصفة الأمن الهجينة على المهاتفة "العالمية" التطورية باستخدام بروتوكول الإنترنت، وهي تتخطى حدود مواصفة الأمن الأساسي البسيط في التوصية ITU-T H.235.1 عند تطبيقها بشكل دقيق. وفضلاً عن ذلك، تتجاوز هذه المواصفة بعض العقبات من التوصية ITU-T H.235.2 مثل الحاجة إلى عرض نطاق أكبر وأداء متزايد في المعالجة، عند تطبيقها بشكل دقيق. وعلى سبيل المثال، لا تعتمد مواصفة الأمن الهجينة على الإدارة (السكونية) لأسرار القفزات المتقاسمة بالتبادل في مختلف المجالات. وبالتالي، يستطيع المستعملون أن يختاروا بسهولة مزود المهاتفة VoIP الخاص بهم. ومن ثم تقبل مواصفة الأمن هذه نوعاً من تنقلية المستعمل أيضاً. من جهة أخرى، لا يطبق التجفير التناظري مع التوقيعات والشهادات إلا عند الضرورة، وفي غير ذلك من الحالات تستخدم تقنيات تناظرية أكثر سهولة وكفاءة. وهي تتيح إرسال رسائل H.245 في قناة نفقية من أجل تكاملها وتطبق أيضاً بعض الأحكام من أجل عدم إنكار الرسائل.

وإن مواصفة الأمن الهجينة يلزم نموذج التسيير القائم على الحارس البوابي ويقوم على تقنيات إرسال رسائل H.245 في قناة نفقية. ويحتاج استخدام نماذج التسيير غير القائمة على الحارسات البوابية إلى مزيد من الدراسة.

تشمل الخصائص التي توفرها هذه المواصفة ما يلي:

بالنسبة للرسائل RAS وH.225.0 وH.245:

- استيقان المستعمل إزاء الكيان المطلوب، بغض النظر عن عدد القفزات على المستوى التطبيقي التي تجتازها الرسالة.

الملاحظة 1 – يعني المصطلح "قفزة" في هذه الحالة عنصر الشبكة الموثوق H.235 (مثل الحارس البوابي والبوابة ووحدة التحكم بالنقاط المتعددة ومخدم الذاكرة الوسيطة (proxy) وجدران الحماية). وبالتالي، فإن المستوى التطبيقي للأمن بالقفزة تلو القفزة لا يؤمن أمناً فعلياً من طرف إلى طرف بين المطاريف، عند استخدامه مع التقنيات التناظرية.

- تكامل كافة الأجزاء (المجالات) أو الأجزاء الحرجة للرسائل التي تصل إلى كيان، بغض النظر عن عدد القفزات على المستوى التطبيقي التي تجتازها الرسالة. ويؤمَّن تكامل الرسالة نفسها باستخدام رقم عشوائي قوي يقترح كخيار.
- إن ما تتميز به الرسالة من استيقان وتكامل وعدم رفض (إلى حد ما) على المستوى التطبيقي بالقفزة تلو القفزة يوفر خدمات الأمن للرسالة بأكملها.
- بفضل تيسر البنية التحتية، ذات المفتاح العمومي، يمكن أن يختار المستعملون مزود الخدمة. ويتم إدماج إدارة المفاتيح لتوزيع مفاتيح الدورة إدماجاً جيداً في مواصفة الأمن الهجينة.

إن خدمات الأمن الواردة أعلاه تسمح بالتصدي، على نحو مرضٍ، لأنواع مختلفة من الهجمات بما في ذلك:

- *هجمات اعتراضية لفرد*: إن استيقان الرسائل وتكاملها بالقفزة تلو القفزة على المستوى التطبيقي يحولان دون هجمات من هذا القبيل عندما يتواجد عامل معترض، مثلاً مخدم معادٍ، بين قفزتين على المستوى التطبيقي.
- *هجمات بإعادة التنفيذ*: إن استخدام الطابعات الزمنية وأرقام التتابع يحول دون هذه الهجمات.
- *التزوير*: يحول استيقان المستعمل دون هذه الهجمات.
- *سرقة التوصيلات*: إن استعمال الاستيقان/التكامل لكل رسالة تشوير يحول دون هذه الهجمات.

تستند مواصفة الأمن إلى نموذج النداء القائم على الحارس البوابي، حيث تطبق منهجية تشوير النداء بالتوصيلة السريعة. وتوجه رسائل التحكم بالنداء H.245 بشكل آمن عبر قناة نفقية في رسائل تشوير النداء H.225.0 وتستفيد بالتالي من خطة الحماية الأمنية H.225.0.

تسمح مواصفة الأمن مع التوقيع بأن ترسل عبر قناة نفقية بشكل آمن وحدات PDU للتحكم بالنداء H.245 في رسائل facility H.225.0. وتتطلب آليات التحيين والتزامن للمفاتيح H.245 إرسالاً عبر قناة نفقية للرسالة FACILITY لتحيين المفتاح التي يتعين تشويرها، وهي مقيدة على سبيل المثال بالنسبة للنداءات الطويلة الأمد.

تشير المنطقة المظللة في الجدول 1 إلى آليات الأمن التي تستخدمها مواصفة الأمن الهجينة.

الملاحظة 2 – لا تشكل الشهادات RSA مع تظليل (MD5([RFC 1321 جزءاً من مواصفة الأمن هذه.

يجوز استخدام مواصفة الأمن بالتجفير الصوتي في التوصية ITU-T H.235.6 (انظر الفقرة 1.6 من التوصية H.235.6) بشكل اختياري، إلى جانب مواصفة الأمن الهجينة. ويتم التفاوض بشأن استخدامها في سياق تشوير إقامة النداء.

الجدول H.235.3/1 – لمحة عامة لمواصفة الأمن الهجينة

خدمات الأمن	وظائف النداء			
	التسجيل والقبول والوضع القانوني	H.225.0	H.245 (الملاحظة 3)	بروتوكول النقل بالوقت الفعلي
الاستيقان	التوقيع الرقمي RSA (SHA1)	التوقيع الرقمي RSA (SHA1)	التوقيع الرقمي RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
عدم الإنكار	(ممكن عند الرسالة الأولى فقط)	(ممكن عند الرسالة الأولى فقط)		
التكامل	التوقيع الرقمي RSA (SHA1)	التوقيع الرقمي RSA (SHA1)	التوقيع الرقمي RSA (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
السرية				
التحكم بالنفاذ				
إدارة المفاتيح	تخصيص شهادة	تخصيص شهادة		
	تبادل مفاتيح ديفي–هيلملن الموثوقة	تبادل مفاتيح ديفي–هيلملن الموثوقة		

الملاحظة 1 – يجب أن تدعم الكيانات H.235 الأخرى (مثل الحارسات البوابية والبوابات ومخدمات الذاكرة الوسيطة H.235) مواصفة الأمن الهجينة.
الملاحظة 2 – يمكن أن تحدد بتات استخدام المفتاح المتيسر في الشهادة خدمة الأمن التي يوفرها مطراف ما (مثلاً، تأكيد عملية عدم الإنكار).
الملاحظة 3 – الرسالة H.245 المرسلة عبر قناة نفقية أو الرسالة H.245 المدمجة في إطار التوصيلة السريعة H.225.0.

يجوز أن تطبق هذه التوصية حماية تكامل الرسالة التي تغطي الرسالة بكاملها. بالنسبة للرسالة RAS H.225.0، تغطي حماية التكامل الرسالة RAS بكاملها. أما بالنسبة إلى رسالة تشوير النداء فإنها تغطي رسالة تشوير النداء H.225.0 بكاملها، بما في ذلك الرأسيات Q.931.

بالنسبة إلى الاستيقان، ينبغي للمستعمل أن يستخدم نظام توقيع بمفتاح عمومي أو خاص. ويوفر عادة مثل هذا النظام تكاملاً أفضل.

لا تحدد هذه التوصية إجراءات التسجيل أو الشهادة أو تخصيص الشهادات من مركز ثقة ولا تقوم بتخصيص المفاتيح الخاصة أو العمومية بالنسبة إلى خدمات الدليل والمعلمات CA المحددة وإلغاء الشهادات وتحيين أزواج المفاتيح أو استعادتها. كما أنها لا تحدد إجراءات التشغيل أو إدارة الشهادات الأخرى، مثلاً تسليم الشهادات أو المفاتيح العمومية/الخاصة ووضعها في المطاريف. ويجوز لمثل هذه الإجراءات أن تجري من خلال وسائل لا تكون جزءاً من هذه التوصية.

باستطاعة كيانات الاتصال المعنية أن تحدد ضمنياً استخدام مواصفة الأمن الأساسي H.235.1 أو مواصفة الأمن مع التوقيع H.235.2 أو مواصفة الأمن الهجينة، من خلال تقييم معرفات أغراض الأمن المشار إليها في الرسالتين (**tokenOID** و**algorithmOID**، انظر أيضاً الفقرة 10 من التوصية H.235.2).

1.6 المتطلبات H.323

من المتوقع أن تدعم الكيانات H.323 التي تطبّق مواصفة الأمن الهجينة هذه الخصائص H.323 التالية:

- التوصيل السريع؛
- إرسال رسائل H.245 عبر قناة نفقية؛
- نموذج التسيير بالحارس البوابي.

2.6 الاستيقان والتكامل

تستخدم هذه التوصية المصطلحات التالية في إطار توفير خدمات الأمن.

الاستيقان والتكامل: خدمة أمن مزدوجة تدعم تكامل الرسالة بالإضافة إلى استيقان المستعمل. يوثّق المستعمل هويته إما باستخدام التوقيع الرقمي الصحيح على بيانات ما بواسطة مفتاح خاص، وإما بتطبيق سر متقاسم مماثل بشكل صحيح. إضافة إلى ذلك، يتم حماية الرسالة من الإتلاف. وتوفر آلية الأمن نفسها خدميّ الأمن. ولا يمكن الدمج بين الاستيقان والتكامل إلا في حالة القفزة تلو القفزة.

ملاحظة – إن استخدام التواقيع الرقمية يسمح بدعم خدمة أمنية لعدم الإنكار. ويتوقف ذلك أيضاً على قيمة بتات استخدام مفتاح التوقيع في الشهادة (انظر أيضاً RFC 3280).

الإجراءات المعدة للاستعمال في هذه المواصفة هي التالية.

يقوم الإجراء IV على التواقيع الرقمية باستخدام زوج من المفاتيح العمومية/الخاصة ونشر التقنيات الرمزية التناظرية لتوفير الاستيقان والتكامل للرسائل RAS وQ.931 وH.245. ويجوز للمطاريف أن تستخدم هذه المنهجية إذا تطلب ذلك أمناً فعالاً وقابلاً للتكيّف.

ووفقاً لسياسة الأمن، يجوز للاستيقان أن يكون أحادياً أو متبادلاً (أي تطبيق الاستيقان/التكامل في الاتجاهين، مما يزيد الأمن). ويقوم الأسلوب الأفضل على استخدام الاستيقان الثنائي.

عندما تكتشف الحارسات البوابية فشلاً في صلاحية الاستيقان و/أو التكامل في رسالة RAS أو رسالة تشوير نداء من مطراف أو حارس بوابي مناظر، فإنها ترد برسالة رفض مماثلة تشير إلى غياب الأمن من خلال وضع سبب الرفض عند **securityDenial** أو أي شفرة خطأ آخر مناسب، وفقاً للفقرة 1.11 من التوصية H.235.0. وفقاً للقدرة على الكشف عن الهجمات والطريقة الأنسب للتصدي لها، أنه ينبغي للحارس البوابي الذي يستلم رسالة **xRQ** مأمونة تتضمن معرفات أغراض غير محددة (**tokenOID** أو **algorithmOID**) أن يرد برسالة **xRJ** غير مأمونة وأن يضع سبب الرفض على **securityDenial** أو يمكنه أن يطرح هذه الرسالة جانباً. وتحذف النقطة الطرفية الرسالة الواردة غير المأمونة وتؤخرها ثم تسعى إلى القيام بمحاولة أخرى باختيار معرفات أغراض مختلفة. والأمر سيان بالنسبة إلى الحارس البوابي الذي يستلم رسالة SETUP لتشوير النداء H.225.0 المأمون مع معرفات أغراض غير محددة (**tokenOID** أو **algorithmOID**) أن يرد برسالة RELEASE COMPLETE غير مؤمَّنة وأن يوضع سبب الرفض على **securityDenial** أو يمكنه أن يطرح هذه الرسالة جانباً، في حين ينبغي للحارس البوابي الذي يستلم رسالة FACILITY H.225.0 مؤمَّنة تتضمن معرفات أغراض غير محددة (**tokenOID** أو **algorithmOID**) أن يرد برسالة FACILITY غير مأمونة وأن يوضع السبب على **undefinedReason** أو يمكنه أن يطرح هذه الرسالة جانباً. وعلى غرار ذلك، ينبغي تسجيل أي حدث أمني. وكجزء من الاستجابة العائدة، يجوز للمرسل أن يقدم قائمة بالشهادات المقبولة في فيش منفصلة، عملاً على تسهيل عملية اختيار شهادة مناسبة من جانب المرسل إليه.

وهناك تشوير H.235 ضمني للدلالة على استعمال الإجراء IV وآلية الأمن المطبقة القائمة على قيمة معرفات الأغراض (انظر أيضاً الفقرة 13) وعلى محتوى مجالات الرسالة. في هذه التوصية، يتم الإحالة إلى معرفات الأغراض بشكل رمزي بأحرف (مثلاً "A").

ولا تستعمل هذه المواصفة المجالات H.235 ICV؛ وبالحقيقة توضع قيم التحقق من تكامل التجفير في المجال **signature** من الفيشة **token** في **cryptoSignedToken** عند الإحالة إلى التوصية ITU-T H.235.2 أو توضع قيم التحقق من التكامل في مجالات التظليل في **CryptoToken** عند الإحالة إلى التوصية ITU-T H.235.1.

7 الإجراء IV

إذا استخدمنا الإجراء IV للأمن بالقفزة تلو القفزة، من الضروري الامتثال للإجراءات الواردة فيما يلي. يجمع هذا الإجراء الإجراء I من الفقرة 7 في التوصية H.235.1 والإجراء II من الفقرة 7 في التوصية H.235.2.

بالنسبة إلى الرسالة الأولى، التي تتضمن الرد المناسب، والمرسلة في كل اتجاه، يُستخدم الإجراء II في التوصية H.235.2 (الاستيقان والتكامل بالقفزة تلو القفزة، انظر الفقرة 7 في التوصية H.235.2) مع القيم التالية:

- معرف الغرض "A1" بدلاً من "A" ومعرف الغرض "S1" بدلاً من " S". ويسمح استعمال معرفات الأغراض OID تحديد مواصفة الأمن الهجينة.
- يوضع المعرف **algorithmOID** في **tokenOID** عند "W" للإشارة إلى استخدام التوقيع RSA-SHA1.
- يتضمن المجال **signature** التوقيع RSA المرمز بأسلوب ASN.1 (انظر الفقرة 12 من التوصية H.235.2).
- ينبغي أن يتضمن المجال **certificate** **شهادة** مستعمل المرسل إذا لم تكن متيسرة إلى المرسل إليه بشكل آخر، ويتضمن المجال **type** معرف الغرض "W" للإشارة إلى أن احتواء شهادة RSA-SHA1 أو معرف الغرض "P" (انظر الفقرة 20 في التوصية H.235.2) للإشارة إلى أن المجال **certificate** يتضمن عنواناً URL.

في حالة وجود مجال إداري وحيد، يتم تحديد "الرسالة الأولى/الرد الأول" على أنها (أنه) الرسالة/الرد الأول RAS H.225.0، وهو يقابل إجمالاً إما الرسالة GRQ/GCF أو الرسالة RRQ/RCF. أما في حالة تعدد المجالات الإدارية، فيتم تحديد أول رسالة/رد داخل كل مجال كما هو وارد أدناه وتحدد الرسالة الأولى فيما بين المجالات على أنها الرسالة SETUP.

عند إرسال شهادة رقمية إلى رسالة ما، يقوم الكيان الذي يستلمها بمقارنة هوية المرسِل بهوية الشهادة، وفقاً للإجراء المشار إليه في الفقرة 14 في التوصية H.235.2، سعياً لتجنب الهجمات التي يقوم بها فرد يكون موقعه بين طرفين.

يتبادل ويحسب المرسِل والمرسل إليه سلسلة سرية ثنائية وموثوقة ديفي–هيلمان. يوفر الجدول H.235.6/4 مثالاً من معلمات مجموعة ديفي–هيلمان ويوصي باختيار الرقم الأصم عند 1024 بتة لأسباب أمنية، حسب مقتضى الحال. يُحسب السر ديفي–هيلمان لكل مقطع، بغض النظر عن استخدام مواصفة للتجفير الصوتي أو عدم استخدامه.

وانطلاقاً من السلسلة الثنائية المشتركة التي يحسبها الطرفان، فإنهما تستنتجان سراً ذا 160 بتة بأخذ البتات ال160 الأقل دلالة. ويُستخدم هذا السر بمثابة كلمة مرور/سر متقاسم يتم استخدامها في التوصية ITU-T H.235.1.

في حالة وجود الحارسات البوابية في المجالات الإدارية المنفصلة، يستخدم المرسِل والمرسل إليه فيشتين في كل اتجاه لتشوير النداء H.225.0:

- تُستخدم فيشة **ClearToken** في **CryptoToken** لحساب مفتاح الوسائط المتقاسمة بين المطاريف (انظر الفقرة 5.8 في التوصية H.235.6). وهذا ضروري فقط في حالة استخدام التجفير الصوتي.
- تُستخدم فيشة **ClearToken** منفصلة لحساب مفتاح الوصلة الذي يتقاسمه المرسل والمرسل إليه لحماية وصلة التشوير. ويحل مفتاح الوصلة محل كلمة المرور المتقاسمة بين حراس البوابات في التوصية ITU-T H.235.1. ويوضع المعرف **tokenOID** للفيشة **ClearToken** عند "Q" للإشارة إلى استعمال تبادل ديفي–هيلمان ومواصفة الأمن الهجينة. ويجري حساب مفتاح الوصلة بالطريقة نفسها التي يجري فيها حساب مفتاح الوسائط (انظر الفقرة 5.8 من التوصية H.235.6).

الملاحظة 1 – في بيئات التسيير المباشر، تتقابل الكيانات ومطاريف المرسل/المرسل إليه. وفي بيئات التسيير بالحارس البوابي، يتقاسم كل زوج من الحارسات البوابية المناظرة مفتاح الوصلة القفزة تلو القفزة، في حين يتم تقاسم مفتاح الوسائط من طرف لآخر.

وفي بيئات التسيير بالحارس البوابي، يرسل الحارس البوابي الفيشة ديفي–هيلمان التي استلمها من النقطة الطرفية إلى القفزة التالية.

يُستخدم الإجراء H.235.1/I (انظر الفقرة 7 في التوصية H.235.1) لكافة الرسائل/الردود المرسلة في كل اتجاه، ما عدا الرسالة الأولى/الرد الأول. وينطبق هذا الإجراء كذلك عندما تتواجد عدة حارسات بوابية في نفس المجال الإداري. وفي هذه الحالة، لا حاجة لإدارة تناظرية للمفاتيح وتكون التوصية ITU-T H.235.1 كافية.

يمكن استخدام هذه التوصية مع أنظمة الطبعة 1 من التوصية H.235 إذا أخذنا بعين الاعتبار الاستخدام المحدود للمعرفين **sendersID** و**generalID**، كما هو وارد في الفقرة 19 في التوصية H.235.2.

ومن المتوقع ألا يستلم الحارس البوابي إلا رسالة واحدة **RRQ** تتضمن فيشة ديفي–هيلمان مع توقيع رقمي ناتج عن نقطة طرفية ثابتة محددة. إلا أن الرسائل **RCF/RRJ** الضائعة أو المتأخرة يمكن أن تؤدي إلى إعادة إرسال رسالة أخرى **RRQ** موقعة.

إذا لم يصل رد التسجيل المقابل في الوقت المطلوب إلى النقطة الطرفية، يمكن لهذه الأخيرة أن تحاول مجدداً. ولهذه الغاية، تستخدم الفيشة ديفي–هيلمان الأحدث، ولكنها تستخدم رقماً تسلسلياً جديداً وطابعة زمنية جديدة.

بالنسبة إلى نقطة طرفية ثابتة محددة، يستخدم الحارس البوابي الرسالة **RRQ** الموقعة التي تم استلامها حديثاً ويستنتج السر المتقاسم انطلاقاً من الفيشة DH، بغض النظر عما إذا كان الحارس البوابي يملك سراً متقاسماً متيسراً أم لا. وبالتالي، يستبدل الحارس البوابي أي سر متقاسم قائم بسر تم استنتاجه مؤخراً. يرد الحارس البوابي برسالة **RCF** موقعة تتضمن فيشة الرد DH. ومن الأفضل توليد فيشة الرد DH من جديد.

الملاحظة 2 – إن الطريقة الموصى بها والمفضلة لتحييد المفاتيح هي التي تستخدم الرسالة FACILITY كما هو وارد في الفقرة 9. غير أنه يمكن إجراء عملية تحيين المفاتيح باستخدام رسالة **RRQ** إضافية أخرى موقعة مع فيشة جديدة DH.

الملاحظة 3 – يستجيب الحارس البوابي الذي يملك سراً متقاسماً إلى رسالة **RRQ** تحميها الشفرة HMAC (وفقاً للتوصية ITU-T H.235.1) برسالة استجابة تحميها الشفرة HMAC.

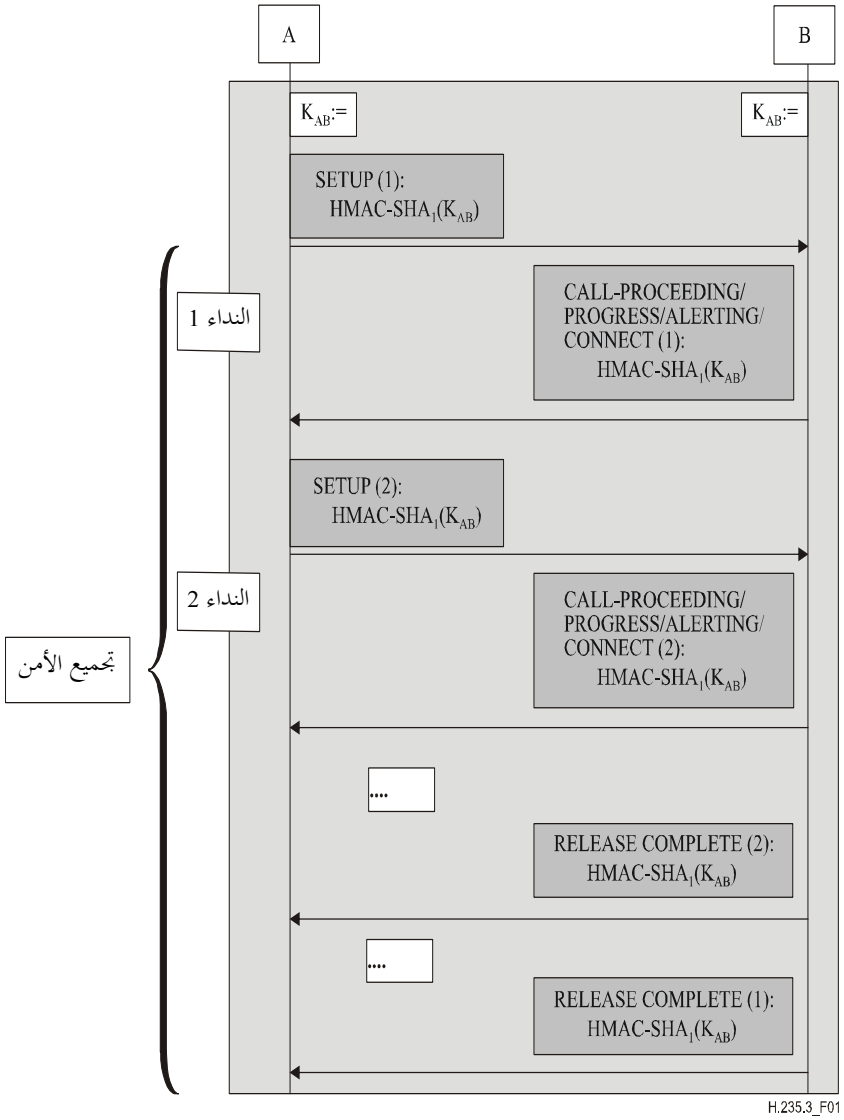
8 جمع الأمن فيما يتعلق بالنداءات المتلازمة

يتم توفير استمثال للحالات التي يعالج فيها زوج ثابت من الكيانات عدة نداءات مستقلة بالتوازي بواسطة قناة واحدة لتشوير النداء. وعوضاً عن إنشاء عدة مفاتيح وصلة مع تبادل ديفي–هيلمان لكل نداء، تم تحديد اتحاد أمن ينطبق على عدة نداءات متزامنة.

بشكل أدق، يغطي اتحاد الأمن كافة النداءات بين كيانين ثابتين طالما أن قناة تشوير النداء قائمة. تستخدم الكيانات العلم **multipleCalls** في الرسالة Setup للإشارة إلى قدرة تشوير النداءات المتعددة على توصيلة واحدة لتشوير النداء (انظر الفقرة 3.7 في التوصية H.323).

إذا تم استخدام توصيلة وحيدة لتشوير النداء، لا يجوز إنشاء إلا مفتاحاً واحداً للوصلة المشتركة (انظر الشكل 1).

من جهة أخرى، إذا وضع العلم **multipleCalls** للرسالة SETUP عند "0"، تحسب مفتاح الوصلة فردياً لكل نداء جديد.



الشكل H.235.3/1 – جمع الأمن للنداءات المتلازمة

9 تحيين المفتاح

يسمح الإجراء الاختياري لتحيين المفتاح لكل كيان من كيانات الاتصال (حارس بوابي أو مطراف) بإنعاش مفتاح الدورة المعمول به باستبداله بمفتاح جديد. ومن المتوقع إطلاق عملية التحيين هذه من جانب أحد الكيانين الذي يشعر بالحاجة إلى ذلك. ويمكن تحفيز تحيين المفتاح إما من خلال مفتاح الدورة الحرجة أو الشعور بأن مفتاح الدورة لا يوفر ولن يوفر الأمن، وإما لعوامل أخرى ترتبط بسياسة الأمن. وجميع هذه الجوانب خارجة عن مجال تطبيق هذه التوصية.

إن الكيان الذي يتمسّك بتحيين المفتاح يستخدم الرسالة FACILITY التي تتضمن فيشة جديدة ديفي–هيلمان وشهادة رقمية اختيارية وتوقيعاً رقمياً خاصاً به. وعندما يستلم المرسل إليه الرسالة FACILITY، يجيب برسالة FACILITY مماثلة عبر إرسال الفيشة DH وشهادة رقمية اختيارية وتوقيعاً رقمياً خاصاً به. عند انتهاء إجراء تحيين المفتاح، يستعمل الكيانان مفتاح الوصلة الجديد المحسوب.

– يوضع المجال **tokenOID** في الفيشة **ClearToken** في الرسالة FACILITY عند "Q" للإشارة إلى استعمال التبادل DH ومواصفة الأمن الهجينة. ويتم حساب مفتاح الوصلة بالطريقة نفسها التي يتم فيها حساب مفتاح دورة الوسائط (انظر الفقرة 5.8 في التوصية H.235.6).

يتم حماية الرسالة FACILITY لتحيين المفتاح وفقاً للإجراء H.235.2/II. ولا تُستخدم أي رسالة أخرى FACILITY من دون فيشة DH لتحيين المفتاح وهي محمية وفقاً للإجراء I من الفقرة 7 في التوصية H.235.1.

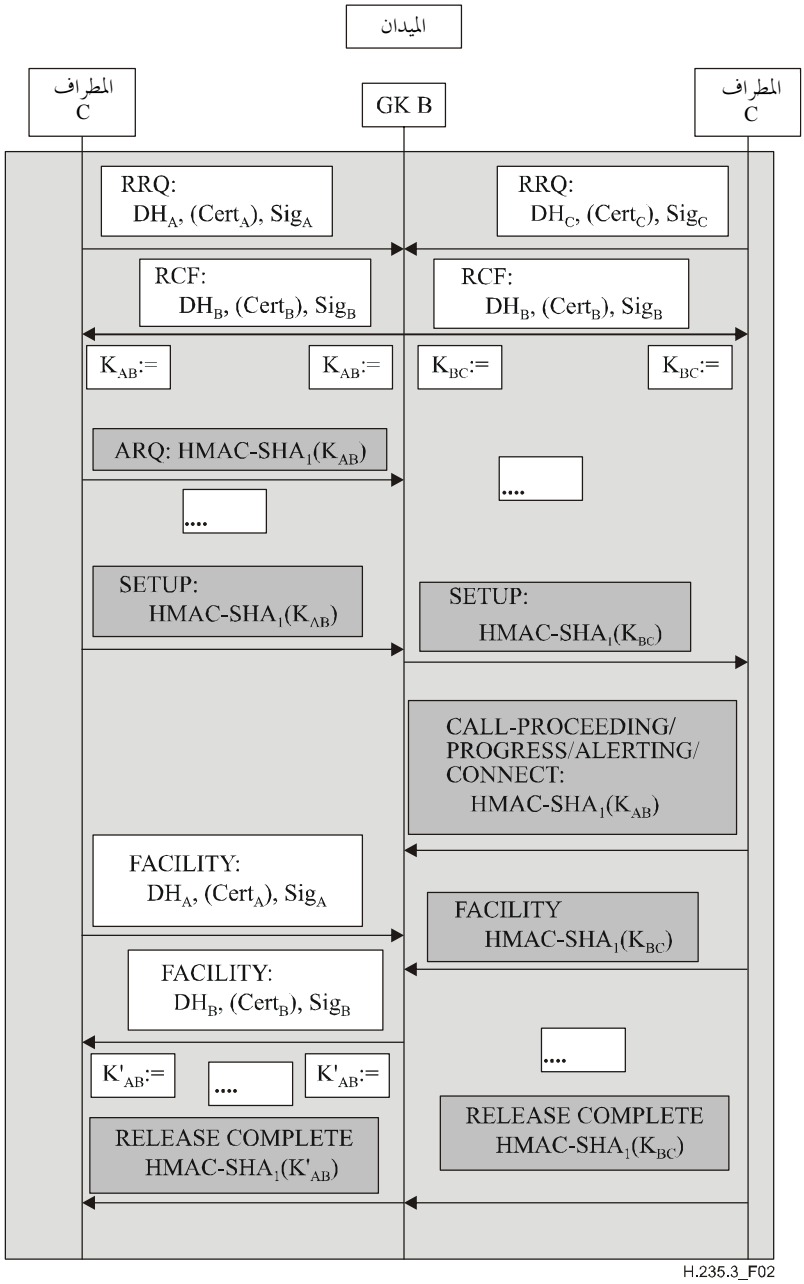
10 استخدام التقنيات ذات المنحني الإهليلجي

بحاجة لمزيد من الدراسة.

11 أمثلة توضيحية

يوضح المخططان البيانيان الواردان في الشكلين 2 و3 استخدام مواصفة هذه التوصية في تدفق أساسي للرسائل. وتجدر الإشارة إلى أن المخططات البيانية لا تظهر التدفق الكامل للرسائل وأن الكثير من الرسائل تم إسقاطها لدواعي التبسيط. إن الرسائل المظللة باللون الرمادي الفاتح تتعلق بالمواصفة مع التوقيع H.235.2 والرسائل المظللة باللون الرمادي الداكن تتعلق بمواصفة الأمن الأساسي H.235.1. ويشدد الشكلان على الأجزاء المتعلقة بالأمن (الأكثر أهمية) في كل رسالة (H.235 CryptoTokens، الفيش) في حين يتم إسقاط التفاصيل.

ويظهر المخطط البياني الوارد في الشكل 2 تدفقاً أساسياً للرسائل في حالة حارس بوابي في مجال إداري وحيد. وإذا اعتبرنا أن شهادة الحارس البوابي معروفة من قبل جميع المطاريف المعنية وأن المطاريف على علمٍ أيضاً بشهادة الحارس البوابي، ليس من الضروري إرسال الشهادات داخل النطاق خلال إجراء التسجيل.



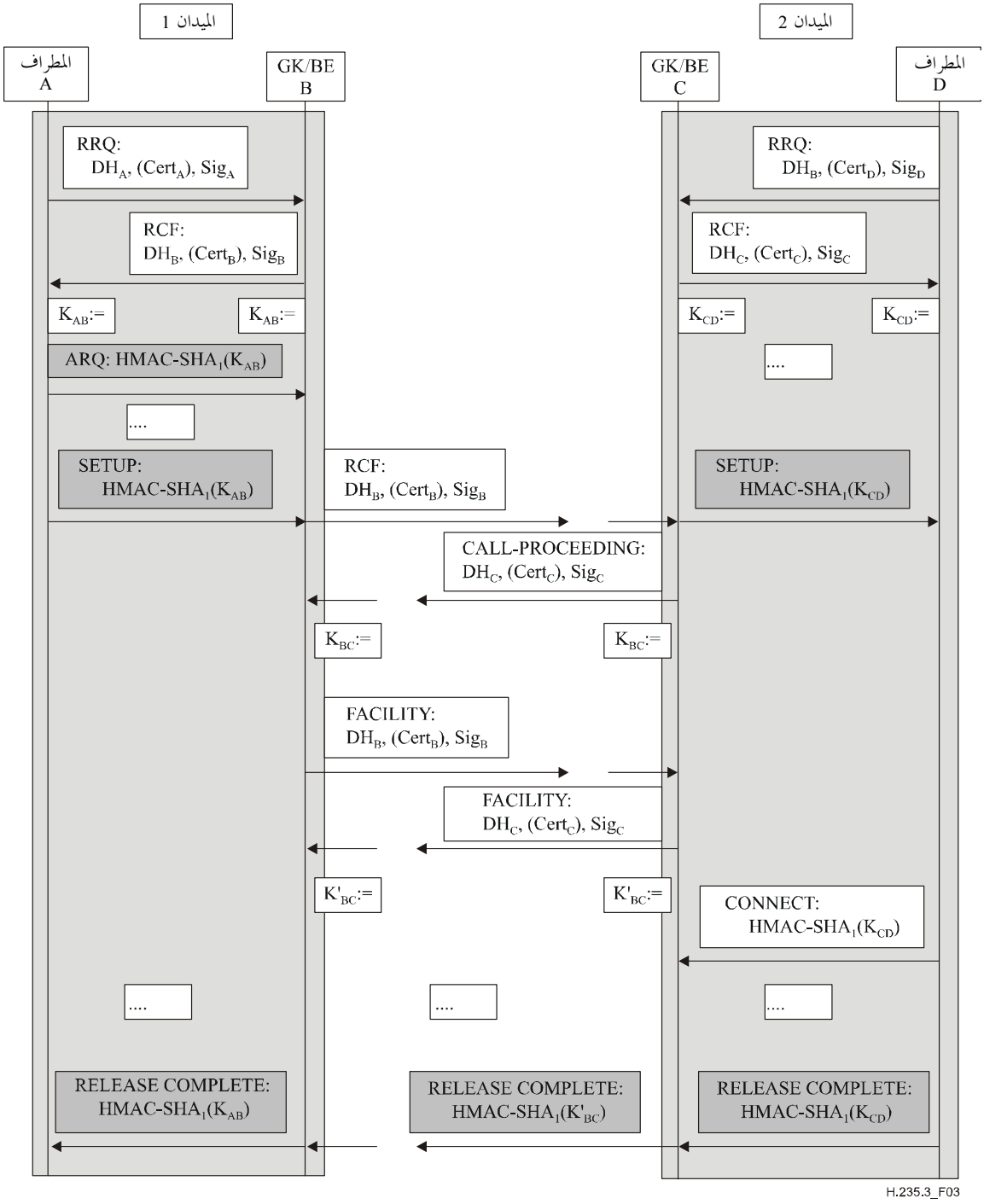
Cert	شهادة المستعمل	K, K'	مفتاح وصلة تناظري
DH_A	فيشة ديفي–هيلمان $g^a \bmod p$	Sig	توقيع رقمي
DH_B	فيشة ديفي–هيلمان $g^b \bmod p$		
EP	نقطة طرفية (مطراف)		
GK	الحارس البوابي		

الشكل H.235.3/2 – تدفق الرسائل في حالة ميدان إداري وحيد

الملاحظة 1 – يشمل الشكلان 2 و3 أيضاً إجراء الانطلاق السريع عندما تتضمن رسائل تشوير النداء SETUP وCALL PROCEEDING/PROGRESS/ALERTING/CONNECT فيشة الانطلاق السريع (انظر الفقرة 7.1.8 في التوصية H.323)، وإلا يكون الأسلوب المتوقع هو أسلوب الانطلاق غير السريع وفقاً للفقرة 1.3.7 في التوصية H.323. كما يشير الشكل 2 إلى إجراء تحيين المفتاح بين المطراف A والحارس البوابي B بواسطة الرسالة FACILITY.

ويقدم الشكل 3 مثالاً على تدفق الرسائل في حالة عدة ميادين إدارية. وفي حين تنطبق مواصفة الأمن الهجينة في كل ميدان بين المطراف والحارس البوابي، كما هو وارد في الشكل 2، يجوز لمواصفة الأمن الهجينة أن تنطبق على كلا الميدانين خلال طور إنشاء النداء.

الملاحظة 2 – يسقط الشكل 3 أي اتصال بين العناصر الحدية (BE) وأي اتصال بين الحارس البوابي وعنصر حدي. ومن جهة أخرى، يشير الشكل 3 إلى إجراء تحيين المفتاح بين كلا الميدانين بواسطة الرسالة FACILITY.



الشكل H.235.3/3 – تدفق الرسائل في حالة عدة ميادين إدارية

12 سلوك التوزيع المتعدد

تتضمن الرسائل H.225.0 ذات التوزيع المتعدد مثل **GRQ** و**LRQ** المجال **CryptoToken** وفقاً للإجراء II عندما لا يتم تحديد المعرف **generalID**. عند إرسال هذه الرسائل إلى جهة واحدة، يجب أن تتضمن الرسالة المجال **CryptoToken** مع معرف **generalID** محدد.

13 قائمة برسائل التشوير الأمينة

يستخدم الإجراء IV الإجراء I في التوصية H.235.1 أو الإجراء II في التوصية H.235.2، استناداً إلى السيناريو والرسالة الفعلية، كما هو مشار إليه أدناه.

1.13 الرسائل RAS H.225.0

الرسالة RAS H.225.0	مجالات التشوير H.235	الاستيقان والتكامل	عدم الإنكار
GatekeeperRequest, GatekeeperConfirm, GatekeeperReject إذا انطبق اكتشاف حارس البوابة RegistrationRequest, RegistrationConfirm, RegistrationReject إذا لم ينطبق اكتشاف حارس البوابة	CryptoToken، ClearToken	الإجراء II	الإجراء II
أي رسالة RAS أخرى (الملاحظة 2)	CryptoToken	الإجراء I	
الملاحظة 1 – بالنسبة إلى الرسائل المرسلة إلى جهة واحدة، ينطبق الإجراء II مع مجالات الأمن المحددة في العلامة CryptoToken. **الملاحظة 2** – لا ترسل رسائل اكتشاف الحارسات البوابية والرسائل ذات التوزيع المتعدد.			

2.13 رسائل تشوير النداء H.225.0 (ميدان إداري وحيد)

رسالة تشوير النداء H.225.0	مجالات التشوير H.235	الاستيقان والتكامل	عدم الإنكار
Setup-UUIE، Connect-UUIE (الملاحظة1)، Facility-UUIE (الملاحظة 2)، Alerting-UUIE، CallProceeding-UUIE، Facility-UUIE، Progress-UUIE، Information-UUIE، ReleaseComplete-UUIE، Status-UUIE، StatusInquiry-UUIE، SetupAcknowledge-UUIE، Notify-UUIE	CryptoToken، ClearToken	الإجراء I	
Facility-UUIE (الملاحظة 3)	CryptoToken	الإجراء II	الإجراء II
الملاحظة 1 – باعتبار أن كل رسالة تكون الأولى في كل اتجاه. **الملاحظة 2** – غير مستخدمة بالنسبة لتحيين المفتاح. **الملاحظة 3** – مستخدمة بالنسبة لتحيين المفتاح.			

3.13 رسائل تشوير النداء H.225.0 (عدة ميادين إدارية)

رسالة تشوير النداء H.225.0	مجالات التشوير H.235	الاستيقان والتكامل	عدم النبذ
Setup-UUIE، Connect-UUIE (الملاحظة1)، Alerting-UUIE (الملاحظة 2)، CallProceeding-UUIE، Facility-UUIE (الملاحظة 3)، Progress-UUIE، Information-UUIE، ReleaseComplete-UUIE	CryptoToken، ClearToken	الإجراء II	الإجراء II
Alerting-UUIE (الملاحظة 4)، CallProceeding-UUIE، Facility-UUIE (الملاحظة 5)، Progress-UUIE، Information-UUIE، ReleaseComplete-UUIE، StatusInquiry-UUIE، Status-UUIE، SetupAcknowledge-UUIE، Notify-UUIE	CryptoToken، ClearToken	الإجراء I	الإجراء I
الملاحظة 1 – باعتبار أن كل رسالة تكون الأولى في كل اتجاه.			
الملاحظة 2 – تحدث أي رسالة من هذه الرسائل باعتبارها الرسالة الأولى في أي الاتجاهين.			
الملاحظة 3 – مستخدمة بالنسبة لتحيين المفتاح.			
الملاحظة 4 – لا تحدث أي رسالة من هذه الرسائل باعتبارها الرسالة الأولى في أي الاتجاهين.			
الملاحظة 5 – غير مستخدمة بالنسبة لتحيين المفتاح.			

14 قائمة معرّفات هوية الغرض

يعدد الجدول 2 جميع المعرّفات OID المذكورة.

الجدول H.235.3/2 – معرفات هوية الغرض

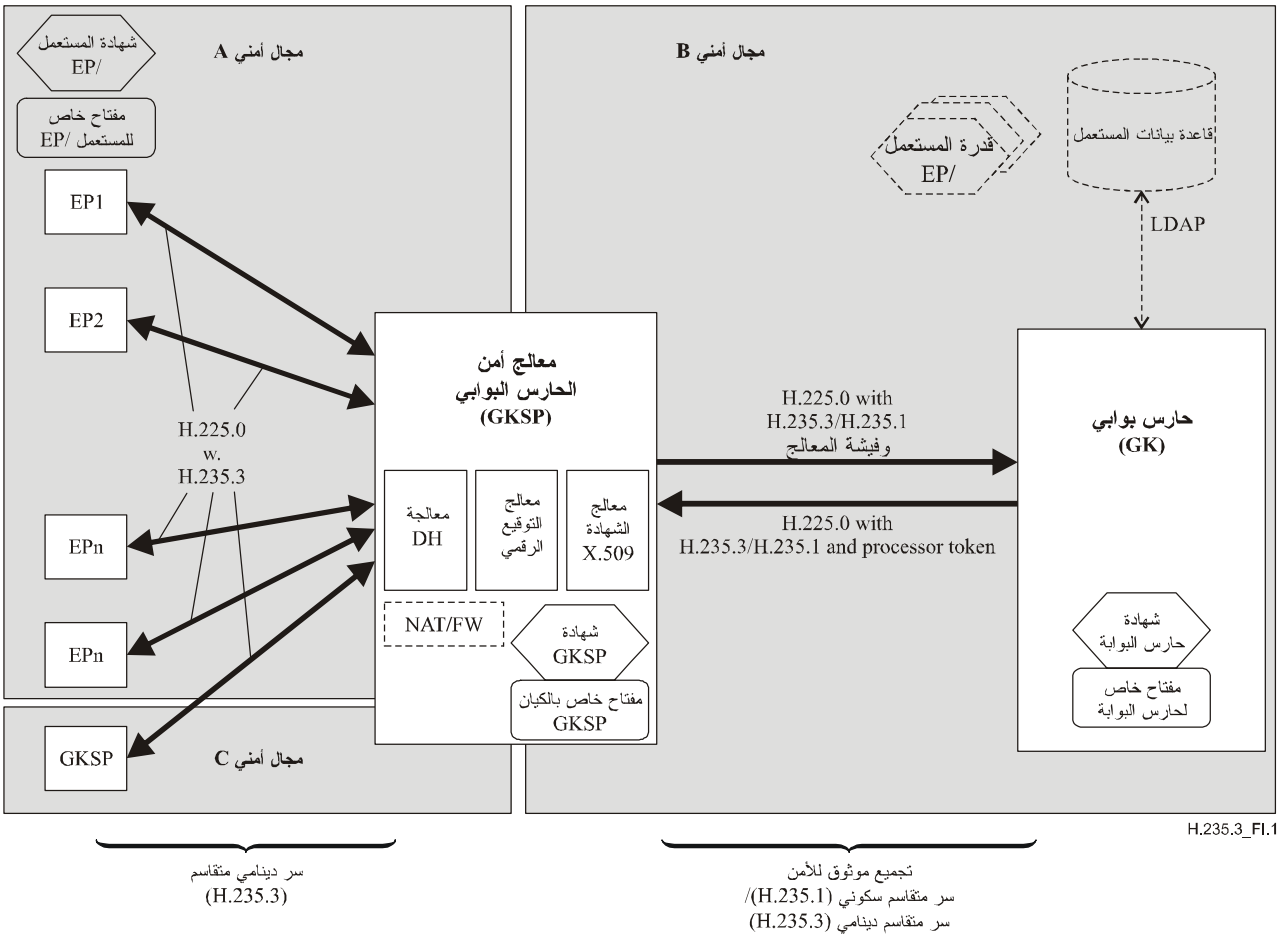
الإحالة إلى معرف هوية الغرض	قيمة (قيم) معرف هوية الغرض	الوصف
"A1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 20}	يُستعمل كبديل للمعرف "A" في الإجراء II من التوصية ITU-T H.235.2 للمعرف CryptoToken-tokenOID، للدلالة على أن التوقيع أو التظليل RSA يغطي كافة مجالات الرسالة RAS أو رسالة تشوير النداء H.225.0 (الاستيقان والتكامل).
"S1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 21}	يُستعمل كبديل للمعرف "S" في الإجراء II من التوصية ITU-T H.235.2 للمعرف CryptoToken-tokenOID، للدلالة على أن المجال ClearToken يستخدم لاستيقان الرسالة وتكاملها. ويشير المعرف في المجال CryptoToken من طرف لآخر أيضاً ضمنياً إلى استخدام تبادل DH خلال إجراء الانطلاق السريع.
"Q"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 22}	يُستعمل في الإجراء IV للدلالة على أن المجال ClearToken للوصلة بالقفزة قفزة يرسل الفيشة DH.
"W"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 23}	يُستعمل في الإجراء IV لمعرف الخوارزمية OID للدلالة على استخدام التوقيع الرقمي القائم على الخوارزمية RSA SHA1.

التذييل I

معالج أمن الحارس البوابي مخوَّل H.235.3

يصف هذا التذييل الزاخر بالمعلومات مثالاً لتطبيق معالج أمن حارس بوابي مخوّل H.235.3 (GKSP) بالاقتران مع حارس بوابي. ويهدف المعالج GKSP إلى نقل بعض المهام الأمنية H.235.3 مثل تنفيذ بعض العمليات الأمنية الخاصة مثل عمليات DH مطولة للغاية وحسابات للتوقيع الرقمي وعمليات تحقق ومعالجة للشهادة X.509 من حارس بوابي أحادي (monolithic) إلى كيان وظيفي جديد ومنفصل يُعرف باسم "معالج أمن حارس بوابي". وهناك على الأقل كيان واحد GKSP لكل حارس بوابي، ولكن يجوز أن يخدم حارس بوابي واحد عدة كيانات GKSP لزيادة عدد النقاط الطرفية المخدومة وتحسين صلابة النظام ككل.

يظهر الشكل 1.I معمارية حارس بوابي مفكك حيث يحتوي الكيان GKSP وظائف الأمن H.235.3.



١

الشكل H.235.3/1.I – معمارية معالج أمن حارس بوابي

الملاحظة 1 – يمكن أن يتضمن الكيان GKSP وظائف أخرى، منها على سبيل المثال وظيفة ترجمة عنوان الشبكة (NAT) وجدران الحماية وبوابة عند سوية التطبيق (ALG)، الخ. إن هذه الوظائف التي يمكن أن تكون جزءاً من معالجة الأمن أو التي يمكن أن تُدرج باعتبارها وظائف داخلية منفصلة، لا يرد وصفها في هذه الفقرة وتبقى بحاجة لمزيد من الدراسة.

يخدم الكيان GKSP عدداً معيناً من النقاط الطرفية في ميدان إداري للأمن A. ويمكن لهذا الكيان أن يتصل بكيان آخر ينتمي إلى ميدان إداري آخر للأمن C (لا يظهر في الشكل).

الملاحظة 2 – عملياً، ليس من الضروري أن تكون ميادين الأمن الإدارية الثلاثة منفصلة. ويجوز أن يوضع الكيان GKSP كلياً في الميدان الإداري للأمن B الذي ينتمي إليه الحارس البوابي أو يمكن وضعه في مجال الأمن A أو في مجال أمن نظيف ومنفصل (لا يظهر في الشكل).

باستخدام الكيان GKSP، لن يحتاج الحارس البوابي إلى المشاركة في تنفيذ عمليات الأمن كثيفة الحسابات. ويستمر هذا الحارس في تحديد التخويل والقبول من خلال مقارنة مسوغات تأهيل لهوية ملائمة (اسم مستعار/اسم DN/رقم تسلسلي للشهادة أو شهادة X.509) مع البيانات التي تظهر في قاعدة البيانات (الداخلية/الخارجية) للمستعملين المشتركين مع تراخيصهم ومسوِّغات تأهيلهم. وتحدد الفقرة 3.I مسوِّغات التأهيل المناسبة التي يتعين على الكيان GKSP H.235.3 المخوَّل استخدامها.

الملاحظة 3 – لا تحدد هذه التوصية سطحاً بينياً ممكناً LDAP بين الحارس البوابي وقاعدة بيانات المشتركين/المستعملين. من جهة أخرى، يبقى على سياسة الحارس البوابي أن تحدد المعايير ومسوغات التأهيل (اسم مستعار/اسم DN/رقم تسلسلي للشهادة) التي ينبغي استخدامها للتحكم بالنفاذ. ويترك لتقدير قاعدة بيانات المستعمل أمر تحديد أي مسوغات التأهيل (اسم مستعار/اسم DN/رقم تسلسلي للشهادة) يُخزَن في قاعدة البيانات.

الملاحظة 4 – لا يحتاج الكيان GKSP إلى المشاركة في المسائل المتعلقة بالتشكيل أو بإدارة المستعملين/المشتركين ولا يحتاج GKSP إلى النفاذ إلى قاعدة بيانات المستعملين.

الملاحظة 5 – تتضمن النقاط الطرفية من النمط H.235.3 والكيان GKSP عادة شهادة جذرية (لا تظهر في الشكل 1.I). وتسمح الشهادة الجذرية للكيان بالتحقق من شهادة الكيان المعني (النقطة الطرفية، المعالج GKSP).

ويكون الاتصال بين معالج الأمن GKSP والحارس البوابي أو بين المعالجين GKSP مأموناً. على سبيل المثال، تطبّق المواصفة H.235.1 عند استخدام سر متقاسم مشكّل سكونياً، ويسمح بإنشاء سر متقاسم دينامي. وفي كلتا الحالتين، من المتوقع أن يكون الحارس البوابي والمعالج GKSP قد قاما بإرساء علاقة ثقة متبادلة، أكان ذلك في إطار تجميع أمني سكوني أو دينامي.

وبالتالي، يعهد الحارس البوابي إلى المعالج GKSP بتطبيق إجراءات الاستيقان الطرفية ولتنفيذ الإجراءات الأمنية بشكل صحيح. ويبلّغ المعالج GKSP نتيجة المعالجة الأمنية إلى الحارس البوابي في توكيد بسيط للأمن باستخدام فيشة المعالج.

ومن المتوقع أن تتضمن كل نقطة طرفية مخوَّلة من النمط H.235.3 والمعالج GKSP شهادة X.509 تصل بشكل موثوق هوية حائز شرعي للمفتاح العمومي مع مفتاح خاص مناظر للتوقيع.

الملاحظة 6 – لا يظهر المفتاح العمومي المناظر للمفتاح الخاص بوضوح في الشكل 1.I؛ ويُرسل المفتاح العمومي المعتَمد عادة في شهادة المستعمل/النقطة الطرفية X.509.

الملاحظة 7 – لا تظهر كافة الشهادات/المفاتيح الخاصة للنقاط الطرفية/المعالج GKSP.

الملاحظة 8 – عادة، تكون شهادة المعالج GKSP شهادة مخدم.

يتوجب على حارس البوابة أن يتضمن شهادة منفصلة ووحيدة بالإضافة إلى مفتاح خاص فقط إذا طبق الحارس البوابي المواصفة H.235.3 للاتصالات مع المعالج GKSP.

إن المعالج GKSP عبارة عن مخدم ذاكرة وسيطة ذي حالات متعددة يعمل بين النقاط الطرفية والحارس البوابي أو بين اثنين من الحارسات البوابية. وهناك على الأقل معالج GKSP لكل حارس بوابي ولكن يجوز للحارس البوابي أن يخدم عدة من معالجات الأمن GKSP لزيادة عدد النقاط الطرفية المخدومة وتحسين صلابة النظام بكامله. ويمكن وضع كيانات GKSP H.235.3 بتسلسل خطي كما يظهر في الشكل 2.I أو وفقاً لمعمارية هرمية كما يظهر في الشكل 3.I.

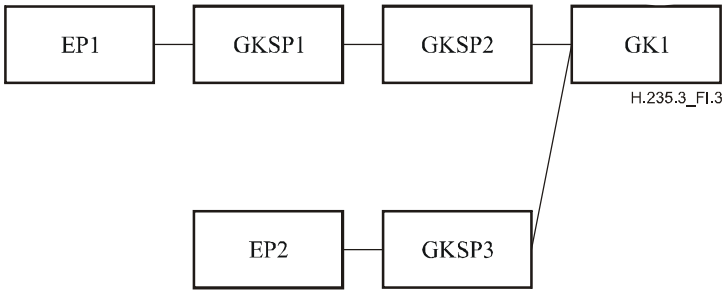
وهناك على الأقل كيان نمطي واحد GKSP لكل حارس بوابي ولكن يجوز لحارس بوابي أن يخدم عدة كيانات GKSP نمطية لزيادة عدد النقاط الطرفية المخدومة وتحسين صلابة النظام بكامله. ويمكن وجود كيان نمطي واحد GKSP أو أكثر بين نقطة طرفية وحارس بوابة، وبالتالي فإن التشكيلات الخطية أو الهرمية مع عدة حارسات بوابية تكون ممكنة مبدئياً. تنشئ نقطة طرفية دائماً علاقة ثقة مع حارس البوابة المصاحب لها من خلال كيان واحد أو أكثر من الكيانات GKSP. ويمكن لحارس بوابي أن يتمتع بعدة علاقات ثقة مع عدة نقاط طرفية.

يظهر الشكل 2.I معمارية كيانات GKSP بتسلسل خطي.

الشكل H.235.3/2.I – المعمارية مسلسلة للمعالجات GKSP

في الشكل 2.I، يستقين المعالج GKSP1 الرسالة RRQ التي تسلمها من النقطة EP1، في حين أن الحارس البوابي GK1 أو GK2 يقرر منح الترخيص للنقطة EP1. ويعتمد المعالجان GKSP1 وGKSP2 (المقابلين للمعالجين GKSP3 وGKSP4) على رسائل التشوير H.323 بين النقطة EP1 والحارس البوابي GK1 (المقابلين للحارس البوابي GK1 والحارس البوابي GK2).

ويظهر الشكل 3.I معمارية ذات عناصر تراتبية للمعالجات GKSP المتسلسلة.



الشكل H.235.3/3.I – المعمارية التراتبية للمعالجات GKSP

يكون للمعالج GKSP على الأقل عنوان IP واحد ويكون عادة عبارة عن جهاز أمني طرفي يقع عند الحدود بين مجالين إداريين منفصلين للأمن. وبالتالي، يمكن للكيان GKSP أن يتمتع بعنوانين IP، عنوان باتجاه النقاط الطرفية H.323/المعالج GKSP المناظر (المجالان الإداريان للأمن A وC) وعنوان IP مختلف موجه داخلياً باتجاه الحارس البوابي (المجال الإداري للأمن B).

1.I اكتشاف معالج أمن الحارس البوابي

يمكن الافتراض أنه ليس من المطلوب من نقطة طرفية H.323 أن تعرف بوجود معالج GKSP. ويمكن للنقطة الطرفية أن تكون قد شكلت العنوان IP للمعالج GKSP باعتباره نقطة الاتصال بالحارس البوابي. ويكون للنقطة الطرفية نفس السلوك في حالة وجود معالج GKSP من عدمه. ويمكنها أن تستخدم طور اكتشاف الحارس البوابي باستخدام الرسالة **GRQ** لتحديد موقع المعالج GKSP الذي يخدمها.

وفي حالة وجود معالج GKSP يخدم النقطة الطرفية الطالبة، ينبغي للمعالج GKSP أن يحدد ما إذا كان الحارس البوابي يدعم معالج الأمن.

وإذا كان في نية المعالج GKSP أن يستخدم المواصفة H.235.1 باتجاه الحارس البوابي من دون أن يكون تم تشكيل أي سر متقاسم بين المعالج GKSP والحارس البوابي، يقوم المعالج GKSP بإرسال الرسالة **GRJ** إلى النقطة الطرفية مع **السبب (reason)** عند **securityDenial/securityDenied**. وفي الحالة العكسية، يقوم المعالج GKSP بإعادة إرسال الرسالة **GRQ** ويدرج فيها فيشة معالج ClearToken ويضع عنصر المواصفة من النمط elementID عند 0، كما هو محدد في الجدول 1.I. وفي هذه الحالة، يدعم الحارس البوابي المعالج GKSP ويعيد الرسالة **GCF/GRJ** يدرج فيه فيشة معالج.

وإذا كان في نية المعالج GKSP أن يستخدم المواصفة H.235.3 باتجاه الحارس البوابي، يقوم المعالج GKSP بإرسال الرسالة **GRQ** إلى الحارس البوابي ويدرج فيها فيشة معالج ClearToken ويضع عنصر المواصفة ID عند 0 كما هو محدد في الجدول I.1. ويستجيب الحارس البوابي المزوّد بالمعالج GKSP والذي يتقبل إجراء هذا التذييل بإرسال رسالة **GCF** ويدرج فيها فيشة معالج ClearToken.

إن الحارس البوابي الذي لا يدعم معالج الأمن أو حارس بوابي لم يطبق هذا التذييل لا يعترف بفيشة المعالج ويرد برسالة **GCF/GRJ**. ويستطيع المعالج GKSP أن يتعرف إلى هذه الحالة بما أن الرسالة **GRQ/GRJ** لا تتضمن فيشة المعالج. وعندئذٍ، يرسل المعالج GKSP رسالة **GRJ** إلى النقطة الطرفية مع **السبب (reason)** عند **securityDenial/securityDenied**.

إن الحارس البوابي الذي يتلقى رسالة **GRQ** مباشرة من نقطة طرفية من دون المرور بمعالج GKSP وحيث يعرف الحارس GK معالجاً GKSP، فإنه يستجيب برسالة **GRJ** مع **السبب (reason)** موضوعاً عند **securityDenial/securityDenied** (من دون إدراج فيشة معالج).

2.I عملية معالج أمن الحارس البوابي

يؤدي معالج أمن الحارس البوابي على الأقل الوظائف التالية:

- ينهي تنفيذ لبروتوكول H.235.3 مع النقاط الطرفية H.323 أو مع المعالج GKSP الند كما يحدده الإجراء IV.
- يدير البروتوكول H.235.3 ديفي–هيلمان تجاه النقاط الطرفية H.323/مع المعالج GKSP الند، أي ينفذ عمليات ديفي–هيلمان النموذجية الأسية.
- يتحقق من التوقيعات الرقمية الصادرة عن النقاط الطرفية H.323 أو من المعالج GKSP الند في الرسائل المأمونة H.235.3.
- يتحقق من أمن الشهادات الرقمية X.509 المتلقاة: التحقق من المسير ومراقبة الصلاحية والتحقق من القائمة CRL، وما إلى ذلك.
- قبل إعادة إرسال رسالة ما إلى الحارس البوابي أو إلى معالج GKSP آخر، يولّد GKSP فيش جديدة H.235 (H.235.1 أو H.235.3) ويستخدم المعرف الخاص به في المجال **sendersID** والمعرف الخاص بالحارس (GKID) في المجال **generalID** في فيشة H.235 ClearToken الأساسية.
- بالنسبة إلى الرسائل الصادرة عن النقطة الطرفية H.323، يدرج GKSP فيشة معالج. وبالنسبة إلى الرسالة **RRQ/GRQ** الأساسية، تتضمن فيشة المعالج عنصر مواصفة الأمن من النمط 0 ElementID الذي يشير إلى طريقة الاستيقان الموجودة. ويمكن للمعالج GKSP أيضاً أن يدرج عنصر مواصفة الأمن مع العنصر 0 ElementID في رسالة RAS أخرى و/أو رسالة تشوير النداء H.225.0.

بالإضافة إلى ذلك، تتضمن فيشة المعالج عنصراً واحداً أو عدة عناصر لمواصفة الأمن ترسل مسوغات التفويض.

إن مسوغات التفويض المحددة في هذا التذييل هي التالية:

- العنصر 1 ElementID لتوفير الموضوع الموجود في الشهادة X.509.
- العنصر 2 ElementID لتوفير الموضوع AltName الموجود في الشهادة X.509.
- العنصر 3 ElementID لتوفير رقم التسلسل الموجود في الشهادة X.509.
- العنصر 4 ElementID لتوفير اسم المصدر الموجود في الشهادة X.509.
- العنصر 5 ElementID لتوفير معرف هوية النقطة الطرفية للمطراف H.323.

ملاحظة – يجوز للحارس البوابي أن يفسر العنصر المستعار H.323 للرسائل H.225.0 باعتباره مسوغ التفويض. وبما أن هذا العنصر موجود على أي حال في الرسائل، فليس من الضروري تحديد عنصر مستعار منفصل داخل عنصر مواصفة الأمن.

عند حدوث خطأ، يدرج المعالج GKSP كذلك عنصراً لمواصفة الأمن من النمط ElementID 6 للإشارة إلى هذا الخطأ. إذا نجح الاستيقان بين النقطة الطرفية H.323 والمعالج GKSP، عندئذٍ يجوز للمعالج GKSP أن يدرج عنصراً لمواصفة الأمن من النمط ElementID 6 للإشارة إلى عدم وجود أي خطأ.

- إذا صادف المعالج GKSP أخطاء للأمن (توقيع رقمي خاطئ أو عدم إثبات صلاحية الشهادة، إلخ.) في رسالة تم استلامها من النقطة الطرفية H.323 أو من المعالج GKSP الند، يقوم المعالج GKSP بتسجيل الخطأ ويعيد إرسال الرسالة إلى الحارس البوابي بعد تضمينها فيشة المعالج مع عنصر مواصفة الأمن من النمط ElementID 6 للإشارة إلى نمط الخطأ ويترك للحارس البوابي حرية اتخاذ القرار والعمل وفقاً لذلك.
- إذا صادف المعالج GKSP أخطاء للأمن في رسالة صادرة عن الحارس البوابي أو أي معالج GKSP آخر، يقوم بتسجيل الخطأ ويتلف الرسالة.
- يحسب التوقيعات الرقمية للرسالة H.235.3 الخارجة الموجهة للنقاط الطرفية H.323 أو المعالج GKSP الند.
- يعيد إرسال الرسالة H.225.0 بين النقطة الطرفية H.323 والحارس البوابي أو المعالج GKSP في اتجاه أو آخر وينفذ العمليات التالية على الفيش:

  - يتصل بالحارس البوابي بواسطة البروتوكول H.225.0 حيث تم انتزاع الفيش H.235.3 الصادرة عن النقاط الطرفية H.323 أو المعالج GKSP الند في الرسالة الأولى للاتصال.
  - يتم التحقق من الفيش H.235.1 المدمجة الصادرة عن النقاط الطرفية H.323 أو عن المعالج GKSP الند وينتزعها قبل إعادة إرسال الرسائل إلى الحارس البوابي.
  - ينهي تطبيق البروتوكول H.235.1/H.235.3 مع الحارس البوابي الخاص به.
  - يدرج الفيش H.235.1/H.235.3 باتجاه النقاط الطرفية H.323 أو المعالج GKSP الند للرسائل الخارجة.
  - يترك الرسائل H.225.0 الصادرة عن النقاط الطرفية H.323 أو عن الحارس البوابي شبه كاملة ولا يعيد سوى كتابة الفيش كما هو محدد فيما يلي.
  - يكون البروتوكول H.225.0 بين المعالج GKSP والحارس البوابي التابع له مأموناً بواسطة مواصفة الأمن الأساسي H.235.1 أو مواصفة الأمن الهجينة H.235.3.

- في حال قام معالج GKSP وحارس بوابي أو معالج GKSP ومعالج آخر GKSP بتنفيذ مواصفة الأمن الهجينة H.235.3، ينفذ المعالج GKSP ما يلي:

أ) ينفذ البروتوكول H.235.3 مع الحارس البوابي أو المعالج GKSP لإنشاء مفتاح دينامي جديد عند استلام أول رسالة صادرة عن النقطة الطرفية الأولى أو عن المعالج GKSP الند.

ب) استهلال تنفيذ البروتوكول H.235.3 تجاه الحارس البوابي أو المعالج GKSP لإنشاء مفتاح دينامي جديد قبل أن تبدأ نقطة طرفية أخرى H.323 أو المعالج GKSP الند عملية الاتصال. ويسمح ذلك بوضع سر دينامي متقاسم جاهز للتطبيق لحماية رسائل الاتصال الأولى الصادرة عن المطراف H.323 أو المعالج GKSP الند، ويسمح ذلك بالتالي بتقصير المدة الإجمالية لإنشاء تجميعات الأمن.

- لا يرسل المعالج GKSP أي رسائل خاصة FACILITY H.235.3 لتحيين المفتاح.
- في حال قام المعالج GKSP والحارس البوابي أو المعالج GKSP ومعالج آخر GKSP بتنفيذ مواصفة للأمن الأساسي H.235.1، يطبق الكيان GKSP المفتاح السكوني المتقاسم لحماية الرسائل RAS و/أو رسائل تشوير النداء H.225.0.

- يترك أثراً لتجميعات الأمن، أي إنه ينشئ سراً متقاسماً DH ويحتفظ بالأسرار الدينامية المتقاسمة. ووفقاً للسياسة الأمنية التي يتبعها، يجوز للمعالج GKSP أن يطلب إعادة حساب المفتاح للسر (الأسرار) الدينامي (الدينامية) المتقاسم (المتقاسمة) المحفوظ (المحفوظة) بواسطة الرسائل FACILITY. وعندما يزيل المطراف H.323 أو المعالج GKSP المناظر التسجيل، ينبغي للمعالج GKSP أن يستبعد المفتاح الدينامي المتقاسم وألا يعتبر ثمة وجود لأي تجميع أمني.
- يصمم تخطيط منافذ النقل ثنائية الاشتراك (نقطة طرفية–معالج GKSP ومعالج GKSP–نقطة طرفية) للبروتوكول الخاص بالرسائل RAS و/أو بروتوكول تشوير النداء H.225.0.

3.I علامة المعالج

عندما يستلم المعالج GKSP رسالة RAS و/أو رسالة تشوير النداء H.225.0 مأمونة تتضمن شهادة X.509 وتوقيعاً رقمياً، يقوم بحذف الفيش H.235.3 ويدرج علامة المعالج المنفصلة في الرسالة التي يعيد إرسالها إلى الحارس البوابي التابع له أو إلى المعالج GKSP المحتمل.

مع وجود فيشة المعالج، يشير المعالج GKSP إلى طريقة الاستيقان الموجودة أو معرف النقطة الطرفية الموجود أو الاسم الموجود في الشهادة (الاسم أو الموضوع AltName) ورقم التسلسل الموجود في الشهادة X.509 واسم المرسل الموجود في الشهادة X.509 أو الإشارة إلى خطأ. وتقوم فيشة المعالج بتأكيد بسيط للأمن حول ما إذا كانت علاقة الأمن قائمة أم لا بين المعالج GKSP والنقاط الطرفية H.323 باتجاه الحارس البوابي.

يستطيع الحارس البوابي الكشف عن المعالج GKSP من خلال التحقق من الرسالة المستلمة والإقرار بأنها تتضمن علامة المعالج. ويفسر الحارس البوابي غياب أي علامة معالج للإشارة إلى غياب أي معالج GKSP.

إن فيشة المعالج هي علامة ClearToken مع استخدام المجالات التالية:

- تتضمن العلامة **tokenOID** معرف الهوية "PT"، انظر الجدول 2.I.
- يتضمن المجال **generalID** إما:
  - معرف النقطة الطرفية للنقطة الطرفية H.323 في حال رسالة مؤمَّنة H.235 صادرة عن نقطة طرفية H.323؛
  - وإما معرف الحارس البوابي في حالة رسالة مؤمَّنة H.235 صادرة عن الحارس البوابي.
- يجوز **للشهادة** اختيارياً أن تتضمن الشهادة H.235.2/H.235.3 الصادرة عن النقطة الطرفية H.323 أو المعالج GKSP الند. وإذا طُبّق هذا الخيار، يعيد المعالج GKSP إرسال الشهادة إلى الحارس البوابي.

  ومن الأفضل استخدام المجال subject/subjectAltName أو معرف النقطة الطرفية أو رقم تسلسل الشهادة أو أي مسوغ تفويض بدلاً من إدراج الشهادة بأكملها في المجال **certificate**. ويعود هذا في الواقع، إلى أن الشهادات X.509 تتجه إلى احتواء بيانات ضخمة، وإلى أن هناك مشكلة محتملة تتمثل في تجزؤ الرسائل عندما تُدرج الشهادات في الرسائل H.225.0 التي ينقلها بروتوكول داتاغرام المستعمل (UDP).
- يتضمن المجال **profileInfo** على الأقل عنصراً واحداً للمواصفة.

  يجوز أن تتضمن علامة المعالج عدة عناصر للمواصفة محدد بعضها في الجدول 1.I:

وتظل أي مجالات أخرى في العلامة ClearToken لمعالج أمن الحارس البوابي دون استخدام.

الجدول H.235.3/1.I – مواصفات عناصر المنهج العام للمواصفة

قيمة ElementID	الوصف	المواصفة
0	يشير إلى عنصر المواصفة الذي يرسل طريقة الاستيقان. يكون استخدام هذا العنصر إلزامياً بالنسبة إلى رسالة الإتصال الأولية (GRQ أو RRQ) واختيارياً في الحالات الأخرى.	• يبقى العنصر **paramS** دون استخدام. • يتضمن المجال **element** عنصراً يوضع فيه المجال **integer** على إحدى القيم التالية للإشارة إلى طريقة الاستيقان الموجودة عند مستوى النقطة الطرفية H.323 أو المعالج GKSP الند: 1) طريقة استيقان أخرى غير محددة وغير مقيَّسة؛ 2) لا شيء (أي لا استيقان)؛ 3) سر متقاسم H.235.1 (غير محدد في هذا التذييل)؛ 4) H.235.2؛ 5) H.235.3؛ 6) H.235.5 (غير محدد في هذا التذييل)؛ 7) H.235.4 (غير محدد في هذا التذييل)؛ 8) H.530 (غير محدد في هذا التذييل).
1	يشير إلى المواصفة الذي يتضمن المجال **subject** للشهادة المتلقاة. واستخدام هذا العنصر اختياري.	• لا يبقى العنصر **paramS** دون استخدام • يتضمن المجال **element** عنصراً يتضمن فيه المجال **name** أو **octets** المجال **subject** للشهادة المتلقاة. **ملاحظة** – قد يحتاج المعالج GKSP إلى إعادة تشفير المجال **subject** الممثل باسم X.509 بسلسلة **octets** أو باسم BMP **name**.
2	يشير إلى عنصر المواصفة الذي يتضمن المجال **subjectAltName** للشهادة المستلمة. واستخدام هذا العنصر اختياري.	• يبقى العنصر **paramS** دون استخدام. • يتضمن المجال **element** عنصراً يتضمن فيه المجال **name** أو **octets** المجال **subjectAltName** للشهادة المتلقاة. **ملاحظة** – يجوز للمعالج GKSP أن يعيد تشفير المجال **subjectAltName** الممثل باسم X.509 بسلسلة **octets** أو باسم BMP **name**.
3	يشير إلى عنصر المواصفة الذي يتضمن رقم تسلسل الشهادة. واستخدام هذا العنصر إلزامي.	• يبقى العنصر **paramS** دون استخدام. • يتضمن المجال **element** عنصراً يتضمن فيه المجال **integer** المجال **CertificateSerialNumber** للشهادة X.509 المتلقاة.
4	يشير إلى عنصر المواصفة الذي يتضمن اسم مرسل الشهادة. واستخدام هذا العنصر إلزامي.	• يبقى العنصر **paramS** دون استخدام. • يتضمن المجال **element** عنصراً يتضمن فيه المجال **name** أو **octets** اسم **issuer** للشهادة X.509 المتلقاة. **ملاحظة** – قد يحتاج المعالج GKSP إلى إعادة تشفير المجال **issuer** الممثل باسم X.509 بسلسلة **octets** أو باسم BMP **name**.

5	يشير إلى عنصر المواصفة الذي يتضمن معرف النقطة الطرفية/المطراف الأصلي. واستخدام هذا العنصر اختياري.	• يبقى العنصر **paramS** دون استخدام. • يتضمن المجال **element** عنصراً يتضمن فيه المجال **name** معرف النقطة الطرفية/المطراف الأصلي.
6	يشير إلى عنصر المواصفة الذي يتضمن إشارة إلى خطأ. واستخدام عنصر المواصفة هذا إلزامي في حالة أي خطأ (> 0) ولكنه اختياري للإشارة إلى عدم وجود أخطاء (0).	• يبقى العنصر **paramS** دون استخدام. • يتضمن المجال **element** عنصراً يتضمن فيه المجال **integer** إحدى قيم الأخطاء المشفرة التالية: 0: عدم وجود أخطاء 1: securityDenied 2: securityWrongSyncTime 3: securityReplay 4: securityWrongGeneralID 5: securityWrongSendersID 6: securityMessageIntegrityFailed 7: securityWrongOID 8: securityDHmismatch 9: securityCertificateExpired 10: securityCertificateDateInvalid 11: securityCertificateRevoked 12: securityCertificateNotReadable 13: securityCertificateSignatureInvalid 14: securityCertificateMissing 15: securityCertificateIncomplete 16: securityUnsupportedCertificateAlgOID 17: securityUnknownCA 18: خطأ أمني غير محدد 19: معالج GKSP غير موفَّر.

4.I مثال توضيحي للمعالج GKSP

تظهر هذه الفقرة أمثلة عن مخططات تدفق الرسائل (انظر الشكلين 4.I و5.I) لمعالج أمن الحارس البوابي الذي يعمل في ميدان إداري للأمن. وتجدر الإشارة إلى أن الشكلين 4.I و5.I يظهران فقط الرسائل الحاسمة بالنسبة للمواصفة H.235.3. وعملياً، يمكن وجود الكثير من الرسائل RAS و/أو رسائل تشوير النداء H.225.0.

وفي كلا الشكلين، يطبّق المطراف A H.323 المخوَّل من النمط H.235.3 والمعالج GKSP مواصفة الأمن الهجينة H.235.3، وبالتالي لا يتقاسم المطراف A والمعالج GKSP B أي سر سكوني متقاسم. وفي الشكل 4.I، يطبق المعالج GKSP والحارس

البوابي مواصفة الأمن الأساسي H.235.1 لحماية الرسائل RAS ورسائل تشوير النداء H.225.0. ويمثل المفتاح K_{BC} السر السكوني المتقاسم بين المعالج GKSP B والحارس البوابي C.

ويظهر الشكل 4.I إجمالي نداءً كاملاً صادراً عن المطراف A عبر المعالج GKSP B والحارس البوابي C. ويقوم حارس بوابي بتسيير النداء. وفي البداية، يتفاوض المطراف A والمعالج GKSP B بشأن مفتاح الوصلة الدينامي K_{AB} وفقاً للتوصية H.235.3 خلال تسجيل الرسالة RAS. لذلك، يولّد المطراف A الرسالة **RRQ** التي ترسل نصف مفتاح ديفي–هيلمان DH_A للمطراف A والذي يتضمن الشهادة A (اختيارية) والتوقيع الرقمي للمطراف A على كامل الرسالة **RRQ** أو على جزء منها.

يتلقى المعالج GKSP B **الرسالة RRQ** ويتحقق من التوقيع الرقمي ويشمل هذا (صلاحية الشهادة الرقمية X.509 المرسلة والتحقق منها (إذا كانت مدرجة) على ضوء شهادة جذرية للمطراف A والتحقق من المسير والتأكد من القائمة CRL، إلخ.)

يعيد المعالج GKSP إرسال الرسالة **RRQ** إلى الحارس البوابي C بعد إضافة علامة المعالج (PT) التي تتضمن العناصر التالية لمواصفة الأمن:

- 0 يشير إلى H.235.3 (5)؛
- 2 يتضمن المجال subjectAltName شهادة المطراف A؛
- 3 يتضمن الرقم المتسلسل شهادة المطراف A؛
- 5 يتضمن معرف النقطة الطرفية للمطراف A،

وتطبق مواصفة الأمن الأساسي H.235.1 مع المفتاح المتقاسم K_{BC} ويتم التحقق من تكامل HMAC-SHA1 إما على كامل الرسالة **RRQ** وإما على أجزاء منها.

في حال عدم التثبت من صحة الشهادة أو التوقيع الرقمي، لا يمكن لمعالج المطراف GKSP B أن يستيقن ويخوِّل المطراف A وبالتالي، يسجل المعالج خطأ ويعيد إرسال الرسالة **RRQ** غير الصحيحة إلى الحارس البوابي C.

ويتلقى الحارس البوابي C الرسالة **RRQ** ويتحقق من التكامل من خلال تطبيق المفتاح K_{BC} ويعالج علامة المعالج PT مع عناصر المواصفة المدرجة فيه. وإذا كان باستطاعة الحارس البوابي C أن يخوِّل بنجاح الرسالة **RRQ**، فإن الحارس البوابي C يخوِّل المطراف A. ثم يستجيب الحارس البوابي C برسالة **RCF** ترسل إلى المعالج GKSP B.

ويتلقى المعالج GKSP B الرسالة **RCF** ويتأكد من أن الحارس البوابي C قام بنجاح بتخويل المطراف A وأعاد إرسال الرسالة **RCF** إلى المطراف A بعد حساب نصف المفتاح ديفي–هيلمان DH_B وإدراجه وبعد إدراج شهادته (الاختيارية) وتوقيع الرسالة **RRQ** (كلياً أو جزئياً) بمفتاحه الخاص. ويصدِّق المطراف A على استيقان الرسالة **RCF** المتلقاة.

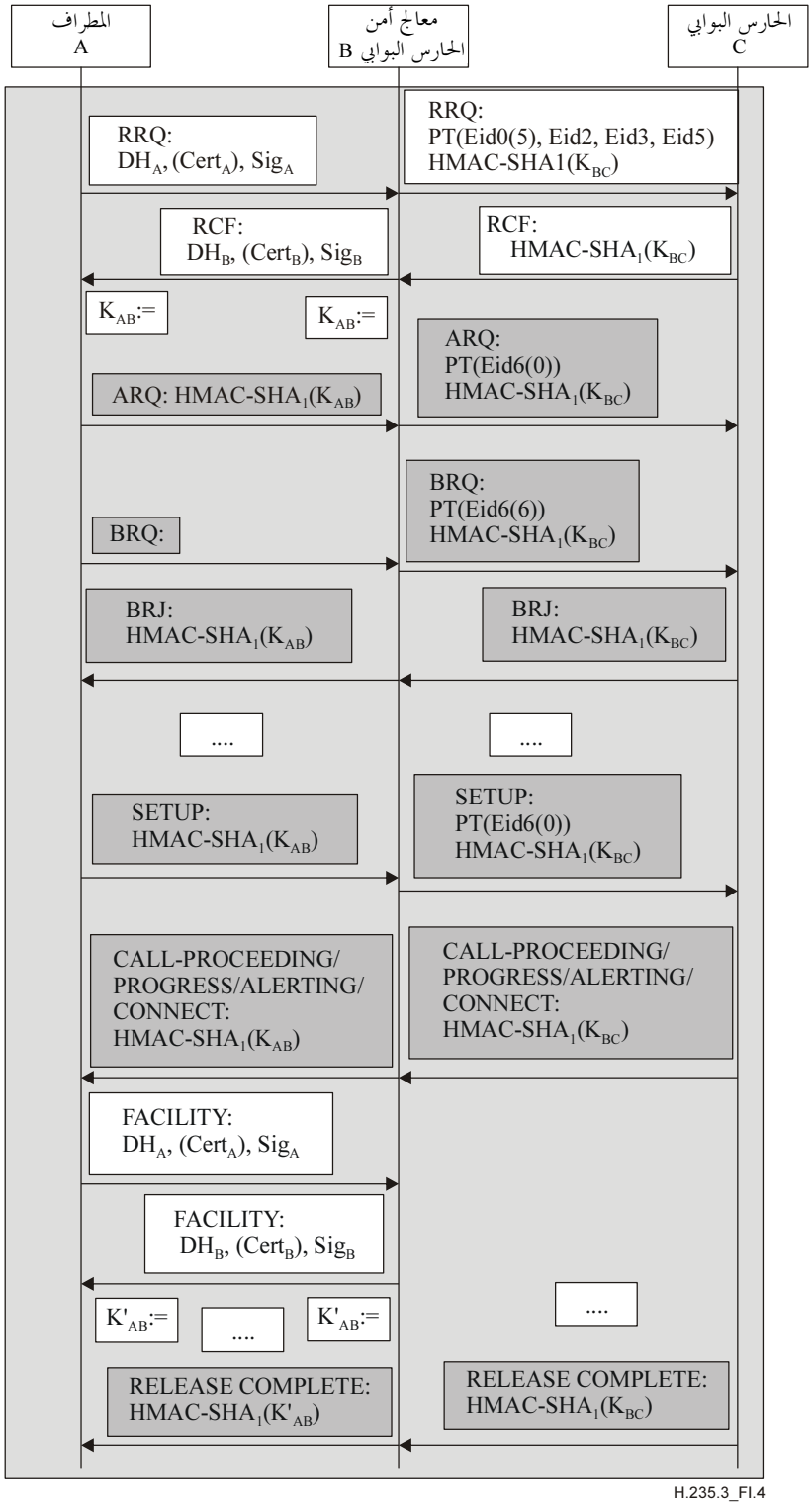
في حال استطاع المعالج GKSP B أن يستيقن المطراف A ويخوِّله بنجاح، فإن المعالج B والمطراف A يحسبان السر المتقاسم الدينامي K_{AB}. ويمثل هذا السر علاقة الثقة القائمة بين المطراف A والمعالج GKSP B. وإلا في الحالة التي لا يخول فيها الحارس البوابي C المطراف A، فإن المعالج GKSP B يقوم بإرسال الرسالة **RCF** إلى المطراف A من خلال حساب نصف المفتاح ديفي–هيلمان DH_B وإدراجه، وبعد إدراج شهادته (الاختيارية) وتوقيع الرسالة **RRQ** (كلياً أو جزئياً) بمفتاحه الخاص. وبما أنه لم يتم تخويل المطراف A، فإن المعالج GKSP B لا يحتفظ طويلاً بالمفتاح K_{AB}. ويمكن للمعالج GKSP B أن يسجل الرسالة الفاشلة **RCF** في ملف التسجيل.

يستخدم المطراف A والمعالج GKSP B السر الدينامي المتقاسم K_{AB} لحماية الرسائل RAS ورسائل تشوير النداء H.225.0 باستعمال مواصفة الأمن الأساسي H.235.1. ويستخدم المعالج GKSP B والحارس البوابي C مواصفة الأمن الأساسي H.235.1 لحماية جميع الرسائل RAS ورسائل تشوير النداء H.225.0.

وفي حالة تسلّم المطراف A رسالة **RCF**، لا يتابع المطراف A إنشاء النداء.

يظهر الشكل 4.I أيضاً حالة خطأ حيث يرسل المطراف A (أو جهة أخرى) رسالة **BRQ** غير محمية إلى المعالج GKSP. ويمكن أن تتأتى هذه الرسالة من هجوم قام خلاله المهاجم بإزالة حماية الأمن H.235.1 أو تعريضها للخطر بشكل أو بآخر. ويكشف المعالج GKSP عن فشل التحقق من التكامل ويعيد إرسال الرسالة **BRQ** مع فيشة معالج إلى الحارس البوابي، ويشير عنصر مواصفة الأمن إلى securityMessageIntegrityFailed (6). ويدرك الحارس البوابي انتهاك الأمن ولا يخوِّل طلب عرض النطاق وذلك برفضه مع رد **BRJ**.

وبعد فترة من إنشاء النداء، يقرر المطراف A استرداد المفتاح K_{AB} بأداء إجراء تحيين للمفتاح K_{AB} مع المعالج GKSP B، ويمثل المفتاح K'_{AB} مفتاح التحيين الجديد. وعند نهاية النداء، ينهي الحارس البوابي C النداء.



Cert	شهادة المستعمل	GKSP	معالج أمن حارس بوابي
DH_A	$g^a \bmod p$ فيشة ديفي–هيلمان	HMAC-SHA1	القيمة المحسوبة للتحقق من التكامل
DH_B	$g^b \bmod p$ فيشة ديفي–هيلمان	K, K'	مفتاح وصلة تناظرية
Eid*n*	*n* معرف عنصر مواصفة الأمن مع القيمة	PT	فيشة المعالج
EP	نقطة مطرافية (مطراف)	Sig	توقيع رقمي
GK	الحارس البوابي		

الشكل H.235.3/4.I – إجراء النداء مع معالج أمن الحارس البوابي وحماية الرسالة H.235.1

(المعالج GKSP إلى الحارس البوابي)

في الشكل 5.I، يطبق المعالج GKSP والحارس البوابي مواصفة الأمن الهجينة H.235.3 لحماية الرسائل RAS ورسائل تشوير النداء H.225.0. ويمثل المفتاح K_{BC} السر الدينامي المتقاسم الذي يتفاوض بشأنه أولاً المعالج GKSP والحارس البوابي ومن ثم يتقاسمانه بهدف استخدامه أيضاً في مواصفة الأمن الأساسي H.235.1 لحماية الرسائل RAS ورسائل تشوير النداء H.225.0. ويبين الشكل 5.I كذلك مطرافاً H.323 D مخولاً من النمط H.235.1 يتقاسم سراً متقاسماً سكونياً K_{DB} مع المعالج GKSP B الخاص به.

ويبين الشكل 5.I إجراء نداء كامل صادر من المطراف 5.I عبر المعالج GKSP B والحارس البوابي C. ويقول الحارس البوابي بتسيير النداء. وفي الشكل 5.I، يُفترض أن المطراف A هو في الواقع النقطة الطرفية الأولى التي تسجّل بجانب الحارس البوابي عبر المعالج GKSP.

يستخدم المطراف A والمعالج GKSP B السر الدينامي المتقاسم K_{AB} لحماية الرسائل RAS ورسائل تشوير النداء H.225.0 بواسطة مواصفة الأمن الأساسي H.235.1. ويستخدم المعالج GKSP B والحارس البوابي C مواصفة الأمن الأساسي H.235.1 لحماية الرسائل RAS الأخرى ورسائل تشوير النداء H.225.0 بواسطة السر الدينامي المتقاسم K_{BC}.

وفي البداية، يتفاوض المطراف A والمعالج GKSP B بشأن مفتاح دينامي للوصلة K_{AB} وفقاً للتوصية ITU-T H.235.3. وخلال التبادل الأول لرسائل الاتصال **RRQ/RCF** بين المطراف A والمعالج GKSP الذي ينشئ خلاله المعالجان سراً دينامياً متقاسماً K_{AB}، يطبق المعالج GKSP والحارس البوابي أيضاً التوصية ITU-T H.235.3 لإنشاء سر دينامي متقاسم K_{BC}.

ويعيد المعالج GKSP إرسال الرسالة **RRQ** التي تلقاها من المطراف A، ويضيف فيشة المعالج (PT) التي تتضمن العناصر الثلاثة التالية لمواصفة الأمن:

- 0 يشير إلى H.235.3 (5)؛
- 3 يشير إلى رقم تسلسل الشهادة A؛
- 6 يشير إلى غياب الأخطاء (0)،

ويطبق مواصفة الأمن الهجينة H.235.3. وبما أن المعالج GKSP B والحارس البوابي C لا يتقاسمان أي سر متقاسم بعد، فإنهما يطبقان البروتوكول H.235.3 وينشئان سراً دينامياً متقاسماً K_{BC}.

وبعد فترة من الوقت، يسجّل المطراف D نفسه عند المعالج GKSP B بواسطة الرسالة **RRQ** المؤمَّنة H.235.1. ويعيد المعالج GKSP B إرسال الرسالة **RRQ** إلى الحارس البوابي C بعد إضافة فيشة المعالج (PT) التي تتضمن العناصر الثلاثة التالية للمظهر الجانبي للأمن:

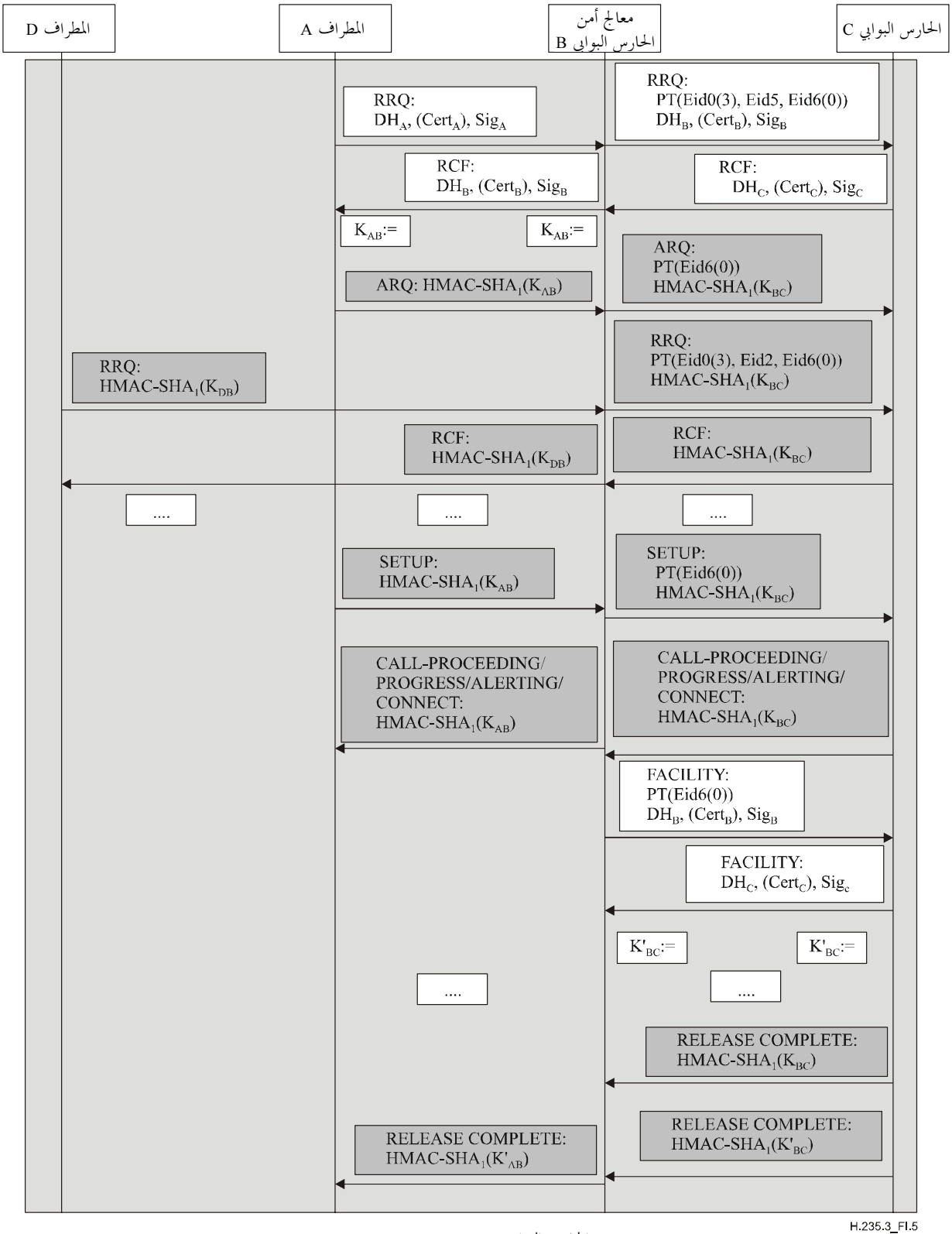
- 0 يشير إلى H.235.1 (3)؛
- 5 يوفر معرف النقطة الطرفية D؛
- 6 يشير إلى غياب الأخطاء (0)،

ويطبق مواصفة الأمن الهجينة H.235.3. وبما أن السر الدينامي المتقاسم K_{BC} H.235.3 تم إنشاؤه من قبل، فإن المعالج GKSP يؤمّن الرسالة **RRQ** المعاد إرسالها باستخدام H.235.1 من خلال تطبيق المفتاح K_{BC}. ويخوِّل الحارس البوابي C المطراف D، ويرد برسالة **RCF** مؤداها المعالج GKSP يعيد إرسالها إلى المطراف D.

بعد فترة من إنشاء النداء الصادر عن المطراف A والذي يمر بالحارس البوابي C، يقرر المعالج B استرداد المفتاح K_{BC} بأداء إجراء تحيين للمفتاح K_{BC} مع الحارس البوابي C، ويمثل المفتاح K'_{BC} مفتاح التحيين الجديد.

ويبين الشكل 5.I أيضاً حالة وجود خطأ يتلقى خلالها المعالج GKSP رسالة RELEASE-COMPLETE من الحارس البوابي. ويكشف المعالج GKSP B فشل التحقق من التكامل، ولا تستخدم هذه الرسالة المفتاح الجاري. ومن الممكن أن تتأتى الرسالة عن إعادة تطبيق أو تحويل من جانب مهاجم أو أن يستخدم حارس البوابة مفتاحاً قديماً. ويسجّل المعالج GKSP B حدث الأمن ويتخلص من الرسالة بدون إعادة إرسالها إلى المطراف A.

عند نهاية النداء، ينهي الحارس البوابي C النداء.



Cert	شهادة المستعمل	GK	الحارس البوابي
DH_A	$g^a \bmod p$ علامة ديفي–هيلمان	GKSP	معالج امن حارس بوابي
DH_B	$g^b \bmod p$ علامة ديفي–هيلمان	HMAC-SHA1	القيمة المحسوبة للتحقق من التكامل
DH_C	$g^c \bmod p$ علامة ديفي–هيلمان	K, K'	مفتاح وصلة تناظرية
Eid*n*	*n* معرف عنصر مواصفة الأمن مع القيمة	PT	علامة المعالج
EP	نقطة مطرافية (مطراف)	Sig	توقيع رقمي

الشكل H.235.3/5.I– إجراء النداء مع معالج أمن الحارس البوابي وحماية الرسالة H.235.3
(المعالج GKSP إلى الحارس البوابي)

5.I قائمة معرفات الأغراض

يشير الجدول 2.I إلى معرف الغرض المذكور والذي يتعين استخدامه إلى جانب الجدول 1.I.

الجدول 2.I – معرفات الأغراض التي يستخدمها التذييل I

تعيين معرف هوية الغرض	قيمة (قيم) معرف هوية الغرض	الوصف
"PT"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 15}	يُستعمل للإشارة إلى الفيشة ClearToken لمعالج الحارس البوابي من أجل الاتصالات من المعالج GKSP إلى الحارس البوابي.

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