الاتحـــــاد الـــدولـــــي للاتصـــــــالات

ITU-T H.235.4

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

إطار الأمن H.323: أمن النداءات بالتسيير المباشر والنداءات بالتسيير الاختياري

التوصيـــة ITU-T H.235.4

الاتحاد الدولي للاتصالات ITU

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعدد 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.

التوصية ITU-T H.235.4

إطار الأمن H.323: أمن النداءات بالتسيير المباشر والنداءات بالتسيير الاختياري

ملخص

تقدم هذه التوصية إجراءات أمنية لاستخدام تشوير النداءات بالتسيير المباشر مقرونة بالجانبيتين الأمنيتين (security profiles) H.235.1 وH.235.3. وتقدم هذه الجانبية الأمنية بمثابة خيار ويمكنها أن تكمّل الجانبيتين الأمنيتين في التوصيتين ITU-T H.235.1 وITU-T H.235.3. كما تقدم هذه التوصية تفاصيل بشأن تنفيذ الفقرة 4.8 من التوصية H.235.0 باستخدام تقنيات لإدارة المفاتيح تناظرياً.

في الصيغ السابقة للسلسلة الفرعية H.235، وردت هذه الجانبية في الملحق H.235/I. وتتناول التذييلات IV وV وVI في التوصية H.235.0 كافة الفقرات والأشكال والجداول التي تقابل بين الصيغتين 3 و4 للتوصية H.235.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) التابعة لقطاع تقييس الاتصالات بتاريخ 13 سبتمبر 2005 على التوصية ITU-T H.235.4 بموجب الإجراء الوارد في التوصيةA.8.

مفردات رئيسية

استيقان، تجفير، إدارة المفاتيح، تكاملية، جانبية أمنية، أمن تعدد الوسائط، أمن النداءات بالتسيير المباشر، أمن النداءات بالتسيير الاختياري.

تمهيـــد

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

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

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

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

ملاحظـــة

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

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

حقوق الملكية الفكرية

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

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

© ITU 2006

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

المحتويات

الصفحة

التوصية ITU-T H.235.4

إطار الأمن H.323: أمن النداءات بالتسيير المباشر والنداءات بالتسيير الاختياري

1 مجال التطبيق

تقدم هذه التوصية إجراءات أمنية لاستخدام تشوير النداءات بالتسيير المباشر مقرونة بالجانبيتين الأمنيتين (security profiles) H.235.1 و H.235.3.

وتقدم هذه الجانبية الأمنية بمثابة خيار ويمكنها أن تكمّل الجانبيتين الأمنيتين H.235.1 وH.235.3. كما تقدم هذه التوصية تفاصيل بشأن تنفيذ الفقرة 4.8 من التوصية H.235.0 باستخدام تقنيات لإدارة المفاتيح تناظرياً.

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 ورزمنة التدفقات أحادية الوسائط لأنظمة الاتصالات متعددة الوسائط القائمة على أساس الرزم.*
- التوصية ITU-T H.235 (2003)، *أمن وتجفير المطاريف متعددة الوسائط من السلسلة H (المطاريف H.323 وغيرها من النمط H.245)*، التصويب 1 (2005)، الخطأ 1 (2005).
- التوصية ITU-T H.235.0 (2005)، *إطار الأمن H.323: إطار أمن للأنظمة متعددة الوسائط من السلسلة H (الأنظمة H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.1 (2005)، *إطار الأمن H.323: مواصفة الأمن الأساسي.*
- التوصية ITU-T H.235.3 (2005)، *إطار الأمن H.323: مواصفة الأمن الهجينة.*
- التوصية ITU-T H.235.6 (2005)، *إطار الأمن H.323: مواصفة التجفير الصوتي مع إدارة مفاتيح H.245/H.235 الأصلية.*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*
- التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة لتطبيقات CCITT.*
- المعيار ISO/IEC 7498-2:1989، *أنظمة معالجة البيانات – توصيل بيني للأنظمة المفتوحة – النموذج المرجعي الأساسي– الجزء 2: معمارية الأمن.*

- المعيار ISO/IEC 10118-3:2004، *تكنولوجيا المعلومات – تقنيات الأمن – وظائف التشويش- الجزء 3: وظائف التشويش المكرّسة*.

2.2 المراجع الإعلامية

- التوصية ITU-T H.235.2 (2005)، *إطار الأمن H.323: مواصفة الأمن بالتواقيع*.
- المعيار IETF RFC 4120 (2005)، *خدمة استيقان شبكة كيربيروس (V5)*.

3 المصطلحات والتعاريف

لأغراض هذه التوصية، تطبّق التعاريف الواردة في الفقرة 3 من التوصيات ITU-T H.323 وITU-T H.225.0 وITU-T H.235.0 والمعيار ISO/IEC 7498-2 | X.800.

4 الرموز والمختصرات

تستخدم هذه التوصية المختصرات التالية:

CT	علامة ClearToken
DH	ديفي–هيلمان (*Diffie-Hellman*)
DRC	نداء بتسيير مباشر (*directed-routed call*)
EK_{AG}	مفتاح التجفير المتقاسم بين النقطة الطرفية A وحارس البوابة G
EK_{BH}	مفتاح التجفير المتقاسم بين النقطة الطرفية B وحارس البوابة H
EK_{GH}	مفتاح التجفير المتقاسم بين حارس البوابة G وحارس البوابة H
$ENC_{K;S,IV}(M)$	تجفير محسّن بالتغذية الراجعة للخرج EOFB للنقطة M بواسطة المفتاح السري K ومفتاح التمليح السري S والمتجه الأولي IV
EPID	معرّف النقطة الطرفية (*endpoint identifier*)
GK	حارس البوابة (*gatekeeper*)
GKID	معرّف حارس البوابة (*gatekeeper identifier*)
g^x, g^y	نصف مفتاح ديفي–هيلمان لحارس البوابة G وحارس البوابة H
K_{AB}	مفتاح التجفير المتقاسم بين النقطة الطرفية A والنقطة الطرفية B
K_{AG}	سر متقاسم (H.235.1 وH.235.3) بين النقطة الطرفية A وحارس البوابة G
K_{BH}	سر متقاسم (H.235.1 وH.235.3) بين النقطة الطرفية B وحارس البوابة H
K_{GH}	سر متقاسم (H.235.1 وH.235.3) بين حارس البوابة G وحارس البوابة H
KS_{AG}	مفتاح تمليح سري متقاسم بين النقطة الطرفية A وحارس البوابة G
KS_{BH}	مفتاح تمليح سري متقاسم بين النقطة الطرفية B وحارس البوابة H
KS_{GH}	مفتاح تمليح سري متقاسم بين حارس البوابة G وحارس البوابة H
PRF	وظيفة شبه عشوائية (*pseudo-random function*)

5 صيغ متفق عليها

تستخدم الصيغ التالية في هذه التوصية:

- يشير فعل "يجب" أو صيغة المضارع إلى حكم إلزامي؛
- يشير فعل "ينبغي" إلى إجراء مقترح ولكنه اختياري؛
- يشير فعل "يجوز" إلى إجراء اختياري أكثر منه توصية بإجراء ما.

يشار إلى معرّفات الغرض بمرجع رمزي في النص (مثلاً، "I11" وتحتوي الفقرة 14 على قائمة بالقيم الرقمية الفعلية المقابلة لمعرفات الغرض الرمزية (انظر أيضاً الفقرة 5 من التوصية H.235.0).

6 مقدمة

غالباً ما يستخدم في تنفيذ التوصية H.323 نموذج التسيير بواسطة حارس البوابة (للاستفادة مثلاً من أفضل مزايا الفوترة). كما أن الاستخدام الواسع لنماذج النداء المسيّرة بواسطة حارس البوابة هو السبب في تحديد مختلف الجانبيات الأمنية التي تستند تحديداً إلى هذا النمط من نموذج النداء، في التوصية ITU-T H.235.0 (مثل H.235.1 وH.235.2 وH.235.3).

ولكن نظراً إلى ضرورة دعم عدد متزايد من القنوات المتوازية، يمكن أن يؤدي نموذج النداء بتسيير مباشر مع حارس بوابة إلى أداء أفضل وخصائص توسعية (scalability) أفضل. ويتميز هذا النموذج بأن حارس البوابة يستخدم لتسجيل واعتماد واستبانة العناوين ومراقبة عرض النطاق، بينما تقام النداءات مباشرة بين النقاط الطرفية من طرف إلى طرف.

وتصف هذه التوصية التحسينات الواجب إدخالها في الجانبية الأمنية الأساسية (baseline) H.235.1 والجانبية الأمنية الهجينة (hybrid) H.235.3 بهدف استيعاب النداءات بتسيير مباشر مع حارس بوابة أو أكثر.

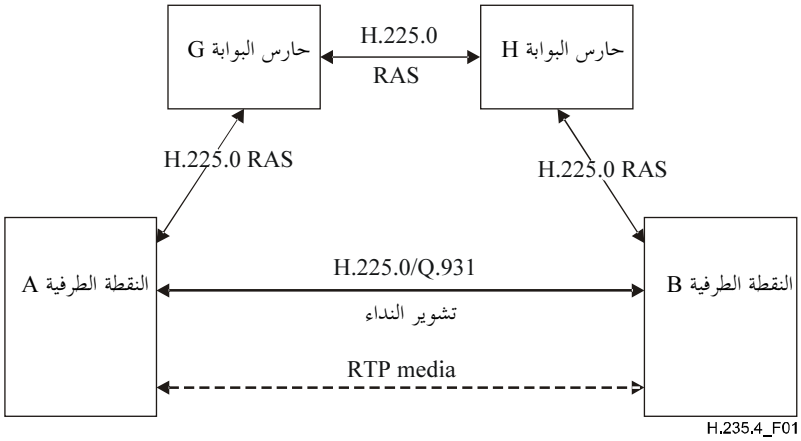
7 نظرة عامة

يطبق كل من الجانبية الأمنية الأساسية H.235.1 والجانبية الأمنية الهجينة H.235.3 سراً متقاسماً (بعد الاتصال الأول) لضمان استيقان و/أو حماية تكاملية الرسائل بطريقة القفزات، باستخدام حارس البوابة كمضيف وسيط موثوق به. ولدى استخدام نموذج النداء بالتسيير المباشر، لا يمكن افتراض وجود سر متقاسم بين النقطتين الطرفيتين. كما أنه من غير العملي استخدام سر متقاسم متفق عليه مسبقاً لضمان أمن الاتصال إذ ينبغي في هذه الحالة، أن تعلم كافة النقاط الطرفية سلفاً ما هي النقطة الطرفية الأخرى التي يستهدفها النداء.

تعالج هذه التوصية السيناريو الموضح في الشكل 1، حيث ترتبط النقاط الطرفية بحارس بوابة وتستخدم تشويراً للنداء بالتسيير المباشر. ويفترض هذا السيناريو، أن شبكة بروتوكول الإنترنت (IP) غير مأمونة في منطقة حارس البوابة.

ويفترض أن لكل نقطة طرفية علاقة اتصال وترابط أمني مع حارس البوابة الخاص بها وأنه تم تسجيل كل نقطة طرفية بطريقة مأمونة مع حارس البوابة باستخدام الجانبية الأمنية الأساسية أو الجانبية الأمنية الهجينة.

وبالتالي، يكون باستطاعة حارس بوابة النقطة الطرفية المصدر (DRC1) أو حارس بوابة النقطة الطرفية المقصد (DRC2) أن يوفر سراً متقاسماً من أجل النقاط الطرفية للاتصال المباشر باستخدام نهج من نمط كيربيروس (انظر المعيار RFC 4120).



الشكل H.235.4/1– سيناريو النداء بالتسيير المباشر

تصف هذه التوصية الإجراءين DRC1 وDRC2 لمختلف البيئات.

ينطبق الإجراء DRC1 (انظر الفقرة 9) في بيئة شركة ما حيث يكون حارس كل بوابة في موقع (محلي) مختلف، علماً بأن كل موقع يلتزم بسياسة أمنية مشتركة في الشركة. وفي مثل هذه البيئة يعتبر من المقبول، أن يحدد حارس البوابة المصدر G السياسة الأمنية الفعالة ليتبعها النداء، وبالتالي، ينتقي ويختار حارس البوابة المصدر G معلمات الأمن المطبقة التي يقبلها حارس البوابة المقصد H.

وينطبق الإجراءان DRC2 (الفقرة 10) وDRC3 (الفقرة 11) في البيئات المشتركة بين الميادين، حيث يكون حارس كل بوابة ضمن ميدان إداري مختلف وحيث يمكن لكل ميدان أن يستخدم سياسة أمنية مختلفة.

وينطبق الإجراء DRC2 في الحالات التي لا تقبل فيها النقطة الطرفية طالبة النداء أو أي من حراس البوابات خوارزمية ديفي–هيلمان. وفي هذه البيئات، يعتبر من المقبول أن يحدد حارس البوابة المقصد H السياسة الأمنية الفعالة ليتبعها النداء، وبالتالي، ينتقي ويختار حارس البوابة المقصد H معلمات الأمن المطبقة التي يقبلها حارس البوابة المصدر G.

وينطبق الإجراء DRC3 في الحالات التي لا تقبل فيها النقطة الطرفية طالبة النداء خوارزمية ديفي–هيلمان، بينما يقبل حارس البوابة في ميدان كل من الجهة الطالبة والجهة المطلوبة خوارزمية ديفي–هيلمان.

وفي بداية تسجيل النداء، توفر الإجراءات وسائل تشوير للتفاوض بشأن انتقاء الإجراء DRC1 أو DRC2 أو DRC3 الذي ينبغي تطبيقه.

8 حدود التوصية

لا تعالج هذه التوصية سيناريوهات التسيير المباشر دون حارس بوابة، وهذه مسألة تستدعي المزيد من الدراسة.

9 الإجراء DRC1 (بيئة شركة)

ينطبق الإجراء الوارد وصفه في هذه الفقرة في بيئة شركة حيث يكون حارس كل بوابة في موقع (محلي) مختلف، علماً بأن كل موقع يلتزم بسياسة أمنية مشتركة في الشركة. وفي مثل هذه البيئة، يعتبر من المقبول أن يحدد حارس البوابة المصدر G السياسة الأمنية الفعالة ليتبعها النداء، وبالتالي، ينتقي ويختار حارس البوابة المصدر معلمات الأمن المطبقة التي يقبلها حارس البوابة المقصد H.

1.9 الطور GRQ/RRQ

تحدد النقاط الطرفية ما إذا كانت قادرة على قبول هذه الجانبية الأمنية عند إرسال الرسالتين **GRQ** و/أو **RRQ** بإدراج علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I10"، وتبقى المجالات الأخرى فيها خالية. ويردّ حارس البوابة

القادر على أداء H.235.4 والمستعد للقيام بهذه الوظيفة برسالة **GCF** أو **RCF** تتضمن علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I10"، وتبقى المجالات الأخرى فيها خالية.

2.9 الطور ARQ

قبل أن تباشر نقطة طرفية A بإرسال رسائل تشوير النداء إلى نقطة طرفية أخرى B مباشرة، تطلب النقطة الطرفية A أو B الدخول لدى حارس البوابة G أو H بواسطة رسالة **ARQ**. وينبغي أن تدرج النقطة الطرفية A في الرسالة **ARQ** علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I10"، وتبقى المجالات الأخرى فيها خالية.

3.9 الطور LRQ

ينطبق هذا الإجراء بالنسبة لحارس بوابة وحيد مشترك لعدة نقاط طرفية أو بالنسبة لسلسلة من عدة حراس بوابات. وفي حالة تعدد حراس البوابات، ينبغي أن يحدد حارس البوابة G – في المنطقة التي يصدر منها النداء – موقع حارس البوابة H بواسطة آلية **LRQ** (متعددة التوزيع) كما هو وارد في الفقرة 6.1.8 من التوصية ITU-T H.323 بعنوان "تشوير اختياري من الجهة المطلوبة". وينبغي توفير أمن الاتصال بين حارسي بوابة وفقاً للتوصية ITU-T H.235.1. ولهذه الغاية يفترض توفر سر متقاسم K_{GH}. وبما أن الرسالة **LRQ** بين حراس البوابات هي عادة رسالة متعددة التوزيع، فإن السر المتقاسم K_{GH} لا يمكن أن يكون بداهةً سراً يتقاسمه كل زوج على حدة وإنما يفترض أن يكون سرّاً تتقاسمه مجموعة داخل السحابة المحتملة من حراس البوابات.

ملاحظة – يحد من هذا الافتراض من إمكانية التوسع (scalability) في الحالة العامة ولا يسمح باستيقان المصدر. ومع ذلك تعتبر مثل هذه العوائق والعوامل المحددة للأمن مقبولة في شبكات الشركات حيث عدد حراس البوابات محدود ومعروف. ويمكن تجاوز هذه العوائق بضمان أمن الاتصالات متعددة التوزيع بين حراس البوابات، بواسطة التوقيعات الرقمية، إلا أن هذه المسألة تستدعي المزيد من الدراسة.

وإذا استخدمت آلية **LRQ** لتحديد موقع حارس البوابة البعيد، عندئذٍ توجّه الرسالة **LRQ** علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I10"، وتبقى المجالات الأخرى فيها خالية. وفي حالة تعدد التوزيع، لا يملأ المجال **generalID** في علامة ClearToken من الرسالة **LRQ**. ويبقى موضوع الاتصال بين حراس البوابات الذي يستند إلى التوصيتين ITU-T H.501 و/أو ITU-T H.510 بحاجة إلى المزيد من الدراسة.

4.9 الطور LCF

يشير EK_{BH} إلى مفتاح التجفير ويشير KS_{BH} إلى مفتاح التمليح اللذين تتقاسمهما النقطة الطرفية B وحارس البوابة H. وكما هو وارد أدناه، يقوم حارس البوابة H والنقطة الطرفية B بحساب بيانات المفاتيح هذه انطلاقاً من السر المتقاسم K_{BH} باستخدام وظيفة شبه عشوائية (PRF).

يقوم حارس البوابة H بتوليد عنصر Challenge-B عشوائي، ثم بيانات مفتاح التجفير EK_{BH} وبيانات مفتاح التمليح KS_{BH}، انطلاقاً من السر المتقاسم K_{BH} باتباع إجراء حساب المفتاح على أساس الوظيفة شبه العشوائية (PRF) الموصوفة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-B ويشتمل الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**keyDerivationOID** على العنصر "AnnexI-HMAC-SHA1-PRF" انظر الفقرة 14.

يشير EK_{GH} إلى مفتاح التجفير ويشير KS_{GH} إلى مفتاح التمليح اللذين يتقاسمهما حارس البوابة G وحارس البوابة H. ويقوم حارس البوابة H بتوليد عنصر Challenge-G عشوائي، ثم بيانات مفتاح التجفير EK_{GH} وبيانات مفتاح التمليح KS_{GH}، انطلاقاً من السر المتقاسم K_{GH} باتباع إجراء حساب المفتاح على أساس الوظيفة PRF الموصوفة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-G. ويشتمل العنصر CT_{HG}→**challenge** على العنصر Challenge-G ويوضع معرّف النقطة الطرفية B في الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID**.

يرسل حارس البوابة H المفتاحين EK_{BH} وKS_{BH} المجفرين إلى حارس البوابة G. ويُستخدم أسلوب التجفير المحسّن بالتغذية الراجعة للخرج (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{GH} الخاص بالنقطة الطرفية. وفيما يلي خوارزميات التجفير القابلة للتطبيق (انظر الجدول 6 في التوصية H.235.6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: بالتغيب وموصى بها؛
- متوافق مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير EOFB، يقوم حارس البوابة H بتوليد قيمة مبدئية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1 OID" و"Z1" OID يشغل المتّجه IV مقدار 64 بتة ويرسل ضمن الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**params**→**iv8**، أما بالنسبة للمعرف "Z2" OID، فإن المتجه IV يشغل 128 بتة ويرسل ضمن الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

ويقوم حارس البوابة H بإدراج $ENC_{EKGH, KSGH, IV}(EK_{BH})$ و$ENC_{EKGH, KSGH, IV}(KS_{BH})$ في العلامة ClearToken CT_{HG} ويملأ فيها المجال **tokenOID** بالرمز "I13". ويرسل النص المجفر $ENC_{EKGH, KSGH, IV}(EK_{BH})$ الذي يتم الحصول عليه في الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**، أما النص المجفر $ENC_{EKGH, KSGH, IV}(KS_{BH})$ فيرسل في الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSaltingKey**. ويشار إلى خوارزمية التجفير في CT_{HG}→**h235Key**→**algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2"). ويوضع العنصر Challenge-B ضمن CT_{HG}→**h235Key**→**secureSharedSecret**→**clearSaltingKey**، ويوضع معرف حارس البوابة G في CT_{HG}→**generalID** أما معرف حارس البوابة H فيوضع في CT_{HG}→**sendersID**.

ويرسل العنصر Challenge-B إلى النقطة الطرفية B بإدراج عنصر **profileInfo** ضمن العلامة **ClearToken** CT_{HG}→**profileInfo**→**elementID** = 0 التي تحدد هذا العنصر المحدد من الجانبية؛

ولا يستعمل CT_{HG}→**profileInfo**→**paramS** بينما يشتمل CT_{HG}→**profileInfo**→**element**→**octets** على العنصر Challenge-B.

وتحتوي الاستجابة **LCF** على العلامة ClearToken CT_{HG}.

5.9 الطور ACF

عندما يتبيّن لحارس البوابة G أن النقطتين الطرفيتين A وB تعملان بهذه التوصية، يقوم بتوليد بيانات المفتاح والعلامات ClearToken، كما هو محدد فيما يلي.

وباستطاعة حارس البوابة أن يستخرج سراً متقاسماً K_{AB} يقوم على النداء، انطلاقاً من رسالة **ARQ** عادية. ومن ثم يمتد هذا السر إلى النقطتين الطرفيتين بواسطة علامات ClearToken. وترسل هذه العلامات ضمن الرسالة **ACF** ثم تُعاد إلى الجهة الطالبة.

تدرج علامتان ClearToken، واحدة CT_A للجهة الطالبة A وأخرى CT_B للجهة المطلوبة B. وتضم كل علامة **ClearToken** معرف OID ("I11" أو "I12") في المجال **tokenOID**، الذي يبيّن ما إذا كانت العلامة معدة للجهة الطالبة ("I11" OID من أجل CT_A) أو للجهة المطلوبة ("I12" OID من أجل CT_B).

يقوم حارس البوابة G بفك التجفير CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** للحصول على المفتاح EK_{BH} كما يفك التجفير CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSaltingKey** للحصول على المفتاح KS_{BH}.

يمكن استعمال العلامة ClearToken المحددة في هذه التوصية بالإضافة إلى جانبيات أمنية أخرى (مثلاً H.235.1 أو H.235.3) تستعمل أيضاً علامات **ClearToken**. وفي مثل هذه الحالة تستخدم ClearToken في إطار هذه التوصية مجالات **ClearToken** الأخرى أيضاً. على سبيل المثال، يتطلب استعمال هذه التوصية مع التوصية ITU-T H.235.1 وجود المجالات **timestamp** و**random** و**generalID** و**sendersID** و**dhkey** واستخدامها كما هو وارد في الجانبية الأمنية H.235.1.

يُدرج معرّف حارس البوابة G في CT_A→**sendersID** وفي CT_B→**sendersID** في حين يحتوي CT_A→**generalID** معرف النقطة الطرفية A ويحتوي CT_B→**generalID** معرف النقطة الطرفية B.

يولّد حارس البوابة G بيانات مفتاح التمليح KS_{GH} وبيانات مفتاح التجفير EK_{GH} انطلاقاً من السر K_{GH} بواسطة إجراء حساب المفتاح القائم على الوظيفة PRF المحددة في الفقرة 12، ويستعاض عن العنصر **challenge** بالعنصر CT_{HG}→**challenge**.

يحسب مفتاحا التجفير EK_{AG} وEK_{BH} بالنسبة للمفتاح المجفر من طرف إلى طرف انطلاقاً من السر المتقاسم بين حارس البوابة والنقطين الطرفيتين (EK_{AG} أو EK_{BH}) بواسطة إجراء حساب المفتاح القائم على الوظيفة PRF المحددة في الفقرة **12**، حيث يحتوي كل من CT_A→**h235Key**→**secureSharedSecret**→**keyDerivationOID** وCT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** على "AnnexI-HMAC-SHA1-PRF" (انظر الفقرة 14) وتضم CT_A→challenge العنصر Challenge-A.

ينسخ حارس البوابة G العنصر Challenge-B من CT_{HG}→**h235Key**→**secureSharedSecret**→**clearSaltingKey** إلى CT_B→**challenge**.

ويحتوي CT_B→**profileInfo** عنصر الجانبية الذي أرسل إلى CT_{HG} **profileInfo** حتى تتمكن النقطة الطرفية B من الحصول على العنصر Challenge-B.

تجفر EK_{AG} (بالنسبة للعلامة CT الموجهة إلى النقطة الطرفية A) أو EK_{BH} (بالنسبة للعلامة CT الموجهة إلى النقطة الطرفية B) سر الجلسة K_{AB} هذا بواسطة خوارزمية التجفير.

يُستخدم أسلوب التجفير المحسّن OFB (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{AG} أو KS_{BH} الخاص بالنقطة الطرفية. وفيما يلي خوارزميات التجفير المطبقة (انظر الجدول H.235.6/6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: خوارزمية بالتغيب وموصى بها؛
- متوافقة مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير المحسّن EOFB، يولّد حارس البوابة G قيمة أولية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1" و"Z1" يَشغل المتّجه IV مقدار 64 بتة ويُرسَل ضمن CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv8**، وضمن CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv8**؛ وبالنسبة للمعرف "Z2" OID، يشغل المتجه IV مقدار 128 بتة ويرسل ضمن CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv16** وضمن CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

يُرسل النص المجفر الذي يتم الحصول عليه $ENC_{EKAG,\ KSAG,\ IV}(K_{AB})$ ضمن CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** ويرسل النص المجفر الذي يتم الحصول عليه $ENC_{EKBH,\ KSBH,\ IV}(K_{AB})$ ضمن CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**. ويشار إلى خوارزمية التجفير في CT_A→**h235Key**→**secureSharedSecret**→**algorithmOID** وفي CT_B→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2").

بالنسبة للعلامة ClearToken الموجهة إلى النقطة الطرفية A، يوضع معرّف النقطة الطرفية B ($EPID_B$) ضمن **CT_A→h235Key→secureSharedSecret→generalID**. وكذلك، بالنسبة للعلامة ClearToken الموجّهة إلى النقطة الطرفية B، يوضع معرّف النقطة الطرفية A ($EPID_A$) ضمن **CT_B→h235Key→secureSharedSecret→generalID**.

بالنسبة إلى خوارزميات التجفير المحسّن EOFB، لا يستخدم العنصر **encryptedSaltingKey**.

يتضمن حارس البوابة G في الوقت نفسه العلامتين ClearToken CT_A وCT_B في الرسالة **ACF** الموجهة إلى النقطة الطرفية A.

6.9 الطور SETUP

تحدد النقطة الطرفية A العلامة CT_A من خلال فحص المعرف **tokenOID** "I11" ضمن ClearToken.

تتحقق النقطة الطرفية A من أن العلامة CT_A حديثة من خلال فحص خاتم الزمن **timestamp**. وتجرى عمليات تحقق أمنية إضافية للتأكد من المجالين **generalID** و**sendersID** في ClearToken والمجال **generalID** في **V3KeySyncMaterial**. فإذا تبين بعد التحقق أن العلامة CT_A المستلمة حديثة، تسترجع النقطة الطرفية A المتجه IV وتحسب EK_{AG} وKS_{AG}، كما هو وارد أعلاه بالنسبة إلى حارس البوابة G. وتقوم النقطة الطرفية A بفك تجفير معلومات **encryptedSessionKey** الموجودة في **secureSharedSecret** من العلامة CT_A للحصول على K_{AB}.

إذا تبين بعد التحقق أن العلامة CT_A المستلمة حديثة فإن النقطة الطرفية A تستطيع إرسال رسالة SETUP إلى النقطة الطرفية B. وتتضمن رسالة SETUP هذه العلامة CT_B. ويجري تأمين هذه الرسالة (توثيقها و/أو حماية تكامليتها) بواسطة الجانبية H.235.1 أو الجانبية H.235.3 من خلال تطبيق السر المتقاسم K_{AB}. ولهذه الغاية، لا يستخدم المجال **generalID** للعلامة ClearToken المظللة في إطار H.235.1 (وليس CT_B!) إلا إذا كانت النقطة الطرفية A تتمتع بمعرف $EPID_B$ (من خلال التشكيل مثلاً أو وضعه في الذاكرة لدى اتصال قديم). وإذا كانت النقطة الطرفية A تستخدم قيمة $EPID_B$ ما للمجال generalID في الرسالة SETUP عندئذ تقبل قيمة المجال sendersID في رسالة تشوير النداء المعاد على أنه المعرف الحقيقي $EPID_B$.

وتتعرف النقطة الطرفية B على العلامة CT_B من خلال فحص المعرف **tokenOID** "I12" ضمن ClearToken.

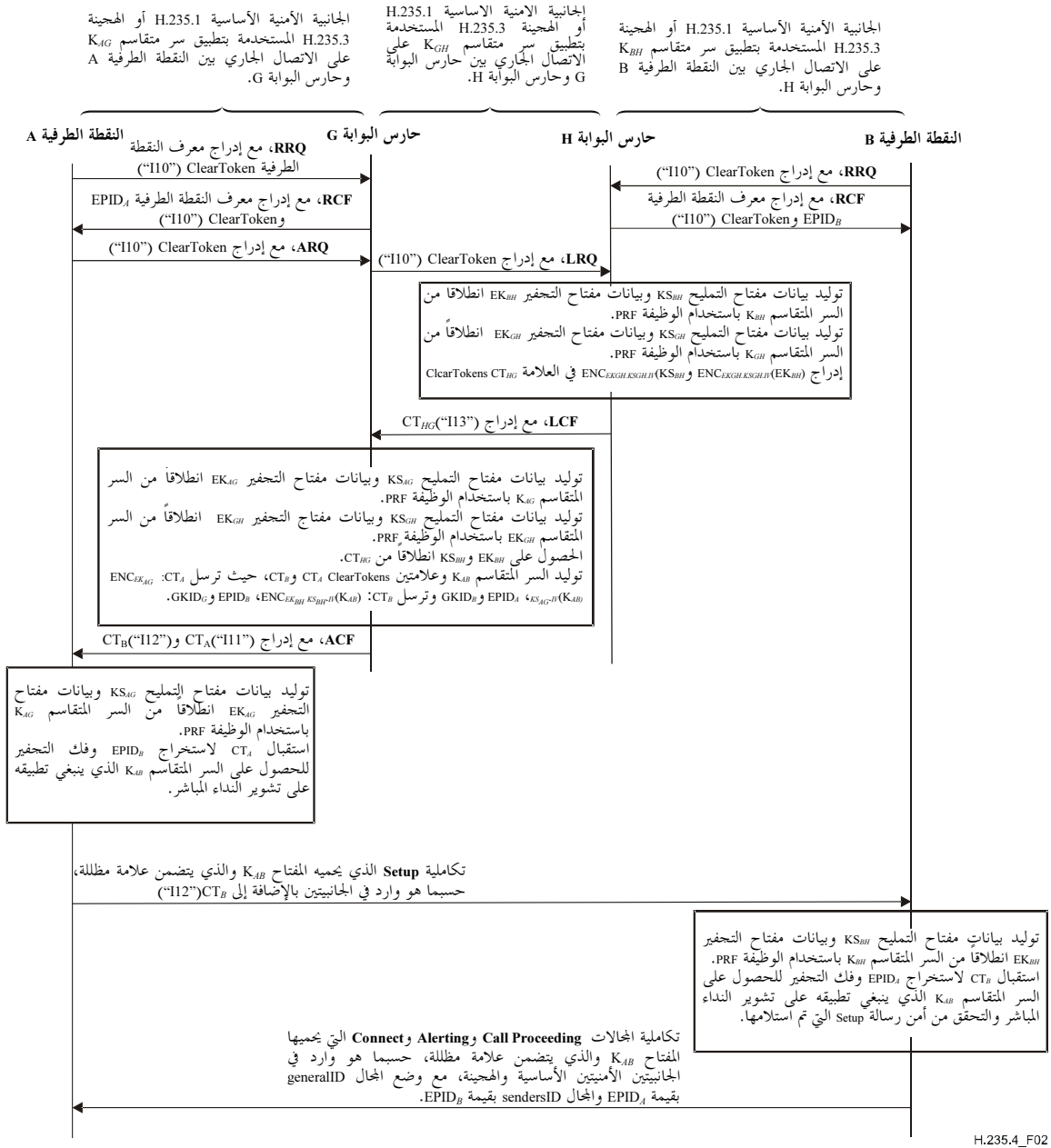
تتأكد النقطة الطرفية B من أن العلامة CT_B المستلمة حديثة بفحص خاتم الزمن **timestamp**. وتجرى عمليات أمنية أخرى للتحقق من المجال **sendersID** في ClearToken والمجال **generalID** ضمن **secureSharedSecret**. وإذا تبيّن بعد التحقق أن العلامة CT_B المستلمة حديثة فإن النقطة الطرفية B تسترجع العنصر Challenge-B من **CT_{HG}→profileInfo→element→octets** وتسترجع المتجه IV وتحسب EK_{BH} وKS_{BH}، بالاستعاضة عن العنصر **challenge** الموصوف في الفقرة 12 بالعنصر Challenge-B، حسبما هو وارد أعلاه بالنسبة لحارس البوابة. وتقوم النقطة الطرفية B بفك تجفير العنصر **encryptedSessionKey** الموجودة ضمن **secureSharedSecret** من العلامة CT_B للحصول على K_{AB}.

وإذا تبين بعد إجراء التحقق أن العلامة CT_B حديثة، تستطيع النقطة الطرفية B متابعة تشوير النداء بالرد برسالة CALL-PROCEEDING أو ALERTING أو CONNECT أو غيرها، حسب مقتضى الحال. وإذا تبين أن العلامة CT_B ليست حديثة، أو أن التحقق من أمن رسالة SETUP ينطوي على مشكلة ما، تستجيب النقطة الطرفية B برسالة RELEASE-COMPLETE، وتضع مقابل العنصر **ReleaseCompleteReason** عبارة خطأ أمني كما هو محدد في الفقرة 1.11 من التوصية H.235.0.

عندما يستدعي الأمر تطبيق أمن وسائط الاتصال (انظر الفقرة 1.6 من التوصية H.235.6)، تتبادل النقطتان الطرفيتان A وB أنصاف مفاتيح ديفي–هيلمان، وفقاً للفقرة 5.8 من التوصية H.235.6 وتنشآن مفتاحاً رئيسياً دينامياً بخصوص جلسة الاتصال يمكن انطلاقاً منه استخراج مفاتيح الجلسة الخاصة بوسائط الاتصال.

تتضمن النقطة الطرفية B المجال **generalID** الذي يملأ بالمعرف $EPID_A$ والمجال **sendersID** الذي يملأ بالمعرف $EPID_B$ لحماية أي رسالة تشوير للنداء H.225.0 موجهة إلى النقطة الطرفية A (من قبيل، Call Proceeding أو Alerting أو Connect).

ويظهر في الشكل 2 المراحل الأساسية لتدفق الاتصال:



الشكل H.235.4/2– المراحل الأساسية لتدفق الاتصال (DRC1)

10 الإجراء DRC2 (بيئة مشتركة بين الميادين)

ينطبق الإجراء الوارد وصفه في هذه الفقرة في بيئة مشتركة بين الميادين حيث يكون حارس كل بوابة في موقع إداري مختلف، وحيث يمكن لكل ميدان أن يستخدم سياسة أمنية مختلفة. وينطبق الإجراء DRC2 في الحالات التي لا تقبل فيها النقطة الطرفية طالبة النداء أو حراس البوابات خوارزمية ديفي–هيلمان.

وفي مثل هذه البيئة، يعتبر من المقبول أن يحدد حارس البوابة المقصد H السياسة الأمنية الفعالة ليتبعها النداء الواجب معالجته، وبالتالي ينتقي ويختار حارس البوابة المقصد H معلمات الأمن المطبقة، ويقبل حارس البوابة المصدر G معلمات الأمن المختارة.

1.10 الطور GRQ/RRQ

تحدد النقاط الطرفية ما إذا كانت قادرة على دعم هذه الجانبية الأمنية عند إرسال الرسالتين **GRQ** و/أو **RRQ** بإدراج علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I20"، وتبقى المجالات الأخرى فيها خالية. ويردّ حارس البوابة القادر على أداء H.235.4 والمستعد للقيام بهذه الوظيفة، برسالة **GCF** أو **RCF** تتضمن علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I20"، وتبقى المجالات الأخرى فيها خالية.

2.10 الطور ARQ

قبل أن تباشر نقطة طرفية A بإرسال رسائل تشوير النداء إلى نقطة طرفية أخرى B مباشرة، تطلب النقطة الطرفية A أو B الدخول لدى حارس البوابة G أو H بواسطة رسالة **ARQ**. وينبغي أن تدرج النقطة الطرفية A في الرسالة **ARQ** علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I20"، وتبقى المجالات الأخرى فيها خالية.

3.10 الطور LRQ

ينطبق هذا الإجراء بالنسبة لحارس بوابة وحيد مشترك لعدة نقاط طرفية أو بالنسبة لسلسلة من عدة حراس بوابات. وفي حالة تعدد حراس البوابات، ينبغي أن يحدد حارس البوابة G – في المنطقة التي يصدر منها النداء – موقع حارس البوابة H بواسطة آلية **LRQ** (متعددة التوزيع) كما هو وارد في الفقرة 6.1.8 من التوصية ITU-T H.323 بعنوان "تشوير اختياري من الجهة المطلوبة". وينبغي توفير أمن الاتصال بين حارسي بوابة وفقاً للتوصية ITU-T H.235.1. ولهذه الغاية يفترض توفر سر متقاسم K_{GH}. وبما أن الرسالة **LRQ** بين حراس البوابات هي عادة رسالة متعددة التوزيع، فإن السر المتقاسم K_{GH} لا يمكن أن يكون بداهةً سراً يتقاسمه كل زوج على حدة وإنما يفترض أن يكون سرّاً تتقاسمه مجموعة داخل السحابة المحتملة من حراس البوابات.

ملاحظة– يحد هذا الافتراض إمكانية التوسع في الحالة العامة ولا يسمح باستيقان المصدر. ومع ذلك تعتبر مثل هذه العوائق والعوامل المحدّدة للأمن مقبولة في شبكات الشركات حيث عدد حراس البوابات محدود ومعروف. ويمكن تجاوز هذه العوائق بضمان أمن الاتصالات متعددة التوزيع بين حراس البوابات بواسطة التوقيعات الرقمية، إلا أن هذه المسألة تستدعي المزيد من الدراسة.

وإذا استخدمت آلية **LRQ** لتحديد موقع حارس البوابة البعيد، عندئذٍ توجّه الرسالة **LRQ** علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I20"، وتبقى المجالات الأخرى فيها خالية. وفي حالة تعدد التوزيع، لا يملأ المجال **generalID** في علامة ClearToken من الرسالة **LRQ**. ويبقى موضوع الاتصال بين حراس البوابات الذي يستند إلى التوصيتين ITU-T H.501 و/أو ITU-T H.510 بحاجة إلى المزيد من الدراسة.

4.10 الطور LCF

عندما يدرك حارس البوابة H أن النقطتين الطرفيتين A وB تعملان بهذه التوصية، يقوم بتوليد بيانات المفاتيح وعلامات ClearToken في الرسالة LCF، كما هو وارد أدناه.

يشير K_{BH} إلى السر المتقاسم بين النقطة الطرفية B وحارس البوابة H. ويشير EK_{BH} إلى مفتاح التجفير ويشير KS_{BH} إلى مفتاح التمليح المتقاسمين بين النقطة الطرفية B وحارس البوابة H. ويقوم حارس البوابة H بتوليد عنصر Challenge-B عشوائي ثم بيانات مفتاح التجفير EK_{BH}، انطلاقاً من السر المتقاسم K_{BH} باتباع إجراء حساب المفتاح على أساس الوظيفة شبه العشوائية PRF الموصوفة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-B ويشتمل الإجراء CT_{HG}→**h235Key→secureSharedSecret→keyDerivationOID** على العنصر "AnnexI-HMAC-SHA1-PRF" (انظر الفقرة 14).

ويولّد حارس البوابة H مفتاح التمليح KS_{BH} انطلاقاً من K_{BH} باتباع إجراء حساب المفتاح على أساس الوظيفة PRF الموصوفة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-B.

ويشير EK_{GH} إلى مفتاح التجفير ويشير KS_{GH} إلى مفتاح التمليح اللذين يتقاسمهما حارس البوابة G وحارس البوابة H. ويقوم حارس البوابة H بتوليد عنصر Challenge-G عشوائي، ثم بيانات مفتاح التجفير EK_{GH} انطلاقاً من السر المتقاسم K_{GH} باتباع إجراء حساب المفتاح على أسس الوظيفة PRF الموصوفة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-G، وحيث يشتمل الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**keyDerivationOID** على العنصر "AnnexI-HMAC-SHA1-PRF" (انظر الفقرة 14).

يولّد حارس البوابة H المفتاح KS_{BH} انطلاقاً من السر المتقاسم K_{GH} باتباع إجراء حساب المفتاح على أساس الوظيفة PRF الموصوفة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-G.

يستحدث حارس البوابة H علامتين ClearToken في الرسالة **LCF**، واحدة CT_{HG} لحارس البوابة G وواحدة CT_B للجهة المطلوبة B. ويحتوي العنصر CT_{HG}→**tokenOID** على المعرف OID "I23" في حين يحتوي العنصر CT_B→**tokenOID** على المعرف OID "I12".

يوضع العنصر Challenge-G في CT_{HG}→**challenge** ويوضع معرف حارس البوابة H في CT_{HG}→**sendersID** ويوضع معرف حارس البوابة G (المستنسخ من الرسالة **LRQ**) في CT_{HG}→**generalID**.

يوضع العنصر Challenge-B في CT_B→**challenge** ويوضع معرف حارس البوابة H في CT_B→**sendersID** ويوضع معرف النقطة الطرفية B في CT_B→**generalID**. إذا كان مجال معرف النقطة الطرفية للرسالة **LRQ** يحتوي على معرف النقطة الطرفية A، عندئذٍ ينسخه حارس البوابة H في الإجراء CT_B→**h235Key**→**secureSharedSecret**→**generalID** وكذلك في الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID**.

تحتوي الاستجابة **LCF** على العلامتين ClearToken CT_{HG} وCT_B إذا كان حارس البوابة H والنقطة الطرفية B يعملان أيضاً بالإجراء DRC2 في هذه التوصية.

بعد أن يتلقى حارس البوابة G الرسالة **LCF** من حارس البوابة H ، يتحقق من العلامتين ClearToken CT_{HG} وCT_B. كما يستخدم حارس البوابة G العنصر Challenge-G كعنصر **challenge** والوظيفة PRF كما هو وارد في الفقرة 12 لحساب KS_{GH} وEK_{GH} انطلاقاً من K_{GH} ومن ثم لفك تجفير CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** والحصول على السر K_{AB} الذي تتقاسمه النقطتان الطرفيتان A وB.

5.10 الطور ACF

يقوم حارس البوابة H بحساب سر K_{AB} على أساس النداء تتقاسمه النقطتان الطرفيتان A وB. ثم يرسل هذا السر إلى النقطتين الطرفيتين بواسطة علامة ClearToken. وتعاد العلامة أولاً إلى حارس البوابة المصدر G الذي يرسل فيما بعد المعلومة إلى الجهة الطالبة ضمن الرسالة **ACF**.

يجفر حارس البوابة H السر K_{AB} انطلاقاً من المفتاح EK_{GH} في شكل $ENC_{EK_{HG},\ KS_{HG},\ IV}(K_{AB})$ ثم يضع السر المجفر K_{AB} في الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

يستخدم أسلوب التجفير بالتغذية الراجعة للخرج (OFB) المحسّن (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{GH} الخاصة بالنقطة الطرفية. وفيما يلي خوارزميات التجفير باستخدام (انظر الجدول 6 في التوصية H.235.6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: بالتغيب وموصى بها؛
- متوافقة مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير EOFB، يولّد حارس البوابة H قيمة مبدئية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1" و"Z1" يشغل المتّجه IV مقدار 64 بتة ويرسل ضمن الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**params**→**iv8**؛ وأما بالنسبة للمعرف "Z2" OID، فإن المتجه IV يشغل 128 بتة ويرسل ضمن الإجراء CT_{HG}→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

ويشار إلى خوارزمية التجفير في CT_{HG}→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2"). أما بالنسبة لخوارزميات التجفير EOFB فلا يستخدم العنصر **encryptedSaltingKey**.

كذلك، يجفّر حارس البوابة H السر K_{AB} انطلاقاً من المفتاح EK_{BH} بشكل $ENC_{EK_{HG}, KS_{HG}, IV}(K_{AB})$ ثم يضع السر المجفر K_{AB} في الإجراء CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

يستخدم أسلوب التجفير المحسّن (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{BH} الخاص بالنقطة الطرفية بالنسبة للنقطة الطرفية B (CT_B). وفيما يلي خوارزميات التجفير المطبقة (انظر الجدول 6 في التوصية H.235.6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: بالتغيب وموصى بها؛
- متوافق مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير EOFB، يولّد حارس البوابة H قيمة مبدئية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1" و"Z1" يشغل المتّجه IV مقدار 64 بتة ويرسل ضمن الإجراء CT_B→**h235Key**→**secureSharedSecret**→ **params**→**iv8**؛ أما بالنسبة للمعرف "Z2" OID، فإن المتجه IV يشغل 128 بتة ويرسل ضمن الإجراء CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

ويشار إلى خوارزمية التجفير في CT_B→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2"). أما بالنسبة لخوارزميات التجفير EOFB فلا يستخدم العنصر **encryptedSaltingKey**.

بالنسبة للاستجابة **ACF** عند النقطة الطرفية A، ينبغي إدراج علامتين ClearToken، واحدة CT_A للجهة الطالبة A وأخرى CT_B للجهة المطلوبة B. وتحتوي الخطوة ClearToken CT_A→**tokenOID** على المعرف "I11" OID.

يولّد حارس البوابة G عنصر Challenge-A واحد ثم يولّد بيانات مفتاح التجفير EK_{AG} انطلاقاً من السر المتقاسم K_{AG} من خلال إجراء حساب المفتاح على أساس الوظيفة PRF المحددة في الفقرة 12، حيث يستعاض عن العنصر **challenge** بالعنصر Challenge-A ويحتوي الإجراء CT_A → **h235Key** → **secureSharedSecret** → **keyDerivationOID** العنصر "AnnexI-HMAC-SHA1-PRF" (انظر الفقرة 14) ويوضع العنصر Challenge-A في الخطوة CT_A→**challenge**.

يجفّر حارس البوابة G السر K_{AB} بواسطة المفتاح EK_{AG} في شكل $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$ باستعمال خوارزمية تجفير ويضع السر المجفر K_{AB} في الإجراء CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

يستخدم أسلوب التجفير المحسّن (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{AG} الخاص بالنقطة الطرفية. وفيما يلي خوارزميات التجفير المطبقة (انظر الجدول 6 في التوصية H.235.6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: بالتغيب وموصى بها؛

– متوافقة مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير EOFB، يولّد حارس البوابة G قيمة مبدئية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1" و"Z1" يشغل المتّجه IV مقدار 64 بتة ويرسل ضمن الإجراء CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv8**؛ أما بالنسبة للمعرف "Z2" OID، فإن المتجه IV يشغل 128 بتة ويرسل ضمن الإجراء CT_A → **h235Key** → **secureSharedSecret** → **params** → **iv16**. ويشار إلى خوارزمية التجفير في CT_A→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2").

يوضع معرف حارس البوابة G في CT_A→**sendersID** ويوضع معرف النقطة الطرفية A في CT_A→**generalID** وينسخ معرف النقطة الطرفية B من CT_B→**generalID** إلى CT_A→**h235Key**→**secureSharedSecret**→**generalID**.

إذا لم يكن حارس البوابة G قد وضع معرف النقطة الطرفية A في المجال endpointIdentifier من الرسالة **LRQ**، عندئذٍ يضعه في CT_B→**h235Key**→**secureSharedSecret**→**generalID**.

بالنسبة إلى خوارزميات التجفير المحسّن EOFB، لا يستخدم بالعنصر **encryptedSaltingKey**.

يمكن استخدام العلامة **ClearToken** المحددة في هذه التوصية بالإضافة إلى جانبيات أمنية أخرى (مثلاً، H.235.1 أو H.235.3) تستعمل أيضاً علامات ClearToken. وفي مثل هذه الحالة، تستعمل علامة ClearToken في إطار هذه التوصية مجالات ClearToken الأخرى أيضاً. على سبيل المثال، يتطلب استخدام هذه التوصية مع التوصية ITU-T H.235.1 وجود المجالات **timestamp** و**random** و**generalID** و**sendersID** و**dhkey** واستخدامها كما هو وارد في الجانبية الأمنية H.235.1.

يدرج معرّف حارس البوابة G في CT_A→**sendersID**، في حين يحتوي العنصر CT_A→**generalID** معرف النقطة الطرفية A.

تتعرف النقطة الطرفية A على العلامة CT_A من خلال فحص المعرّف CT_A→**tokenOID** "I21". وتتأكد من أن العلامة CT_A المستلمة حديثة بفحص خاتم الزمن **timestamp**. وتجرى عمليات أمنية أخرى للتحقق من المجالين **generalID** و**sendersID** في ClearToken والمجال **generalID** ضمن **secureSharedSecret**. وإذا تبين بعد التحقق أن العلامة CT_A المستلمة حديثة تسترجع النقطة الطرفية A المتجه IV وتحسب المفتاحين EK_{AG} وKS_{AG} كما هو وارد أعلاه بالنسبة لحارس البوابة G باستخدام CT_A→**challenge** باعتباره العنصر Challenge-A المستخدم بدل العنصر **challenge** الموصوف في الفقرة 12. وتقوم النقطة الطرفية A بفك تجفير الإجراء CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** للحصول على K_{AB}.

6.10 الطور SETUP

تحدد النقطة الطرفية A العلامة CT_A من خلال فحص المعرّف CT_A →**tokenOID** "I11". وتتحقق من أن CT_A المستلمة حديثة من خلال فحص **timestamp**. وتجرى عمليات أمنية أخرى للتأكد من المجالين **generalID** و**sendersID** في ClearToken والمجال **generalID** في **secureSharedSecret**. فإذا تبين بعد التحقق أن العلامة CT_A المستلمة حديثة عندئذٍ تسترجع النقطة الطرفية A المتجه IV وتحسب المفتاحين EK_{AG} وKS_{AG} كما هو وارد أعلاه بالنسبة إلى حارس البوابة G باستخدام CT_A → **challenge** باعتباره العنصر Challenge-A. وتقوم النقطة الطرفية A بفك تجفير الإجراء CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** للحصول على K_{AG}.

وإذا تبين بعد التحقق، أن العلامة CT_A المستلمة حديثة تستطيع النقطة الطرفية A أن ترسل إلى النقطة الطرفية B رسالة SETUP تحتوي العلامة CT_B. ويجري تأمين هذه الرسالة (توثيقها و/أو حماية تكامليتها) بواسطة الجانبية H.235.1 أو الجانبية H.235.3 من خلال تطبيق السر المتقاسم K_{AB}. ولهذه الغاية، لا يستخدم المجال **generalID** للعلامة ClearToken المظللة في إطار H.235.1 (وليس CT_B!) إلا إذا كانت النقطة الطرفية A تتمتع بمعرف $EPID_B$ (من خلال التشكيل مثلاً أو وضعه في

الذاكرة لدى اتصال قديم). وإذا كانت النقطة الطرفية A تستخدم قيمة $EPID_B$ ما للمجال generalID في الرسالة SETUP عندئذٍ تقبل قيمة المجال sendersID في رسالة تشوير النداء المعاد على أنه المعرف الحقيقي $EPID_B$.

وتتعرف النقطة الطرفية B على العلامة CT_B من خلال فحص المعرف **tokenOID** "I12" ضمن ClearToken.

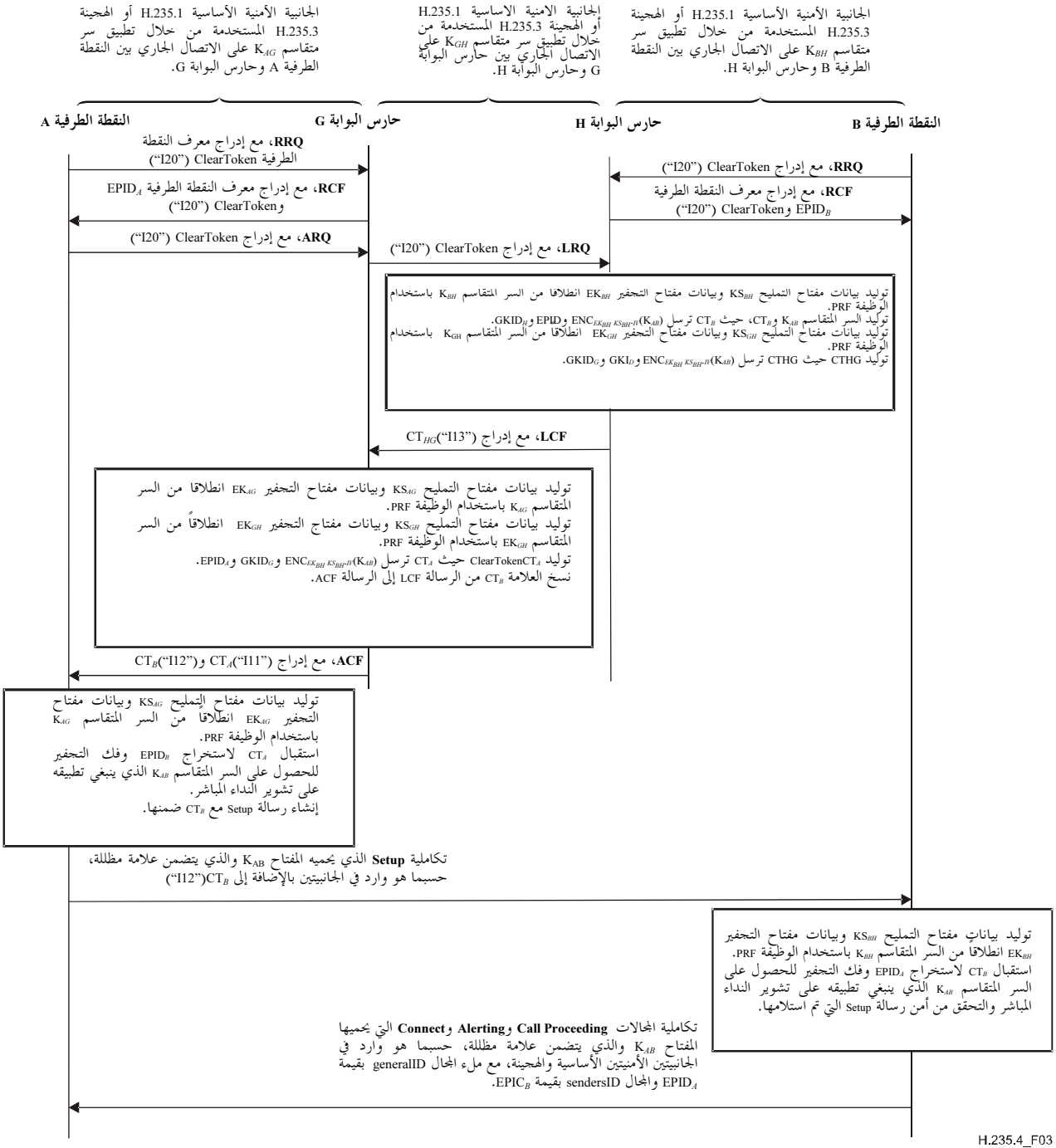
تتأكد النقطة الطرفية B من أن العلامة CT_B المستلمة حديثة بفحص **timestamp**. وتجرى عمليات أمنية أخرى للتحقق من المجال **sendersID** في ClearToken والمجال **generalID** ضمن **secureSharedSecret**. وإذا تبين بعد التحقق، أن العلامة CT_B المستلمة حديثة فإن النقطة الطرفية B تسترجع المتجه IV وتحسب المفتاحين EK_{BH} وKS_{BH} باستخدام CT_B→**challenge** باعتباره العنصر Challenge-B المستعمل مكان العنصر **challenge**، المشار إليه في الفقرة 12، حسبما هو وارد أعلاه بالنسبة لحارس البوابة H. وتقوم النقطة الطرفية B بفك تجفير الإجراء CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** للحصول على K_{AB}.

وإذا تبين بعد التحقق أن العلامة CT_B حديثة، تستطيع النقطة الطرفية B متابعة تشوير النداء بالرد برسالة CALL-PROCEEDING أو ALERTING أو CONNECT أو غيرها، حسب مقتضى الحال. وإذا تبين أن العلامة CT_B ليست حديثة، أو أن التحقق من أمن رسالة SETUP ينطوي على مشكلة ما، تستجيب النقطة الطرفية B برسالة RELEASE-COMPLETE، وتضع مقابل العنصر **ReleaseCompleteReason** عبارة خطأ أمني كما هو محدد في الفقرة 1.11 من التوصية H.235.0.

عندما يستدعي الأمر تطبيق أمن وسائط الاتصال (انظر الفقرة 1.6 من التوصية H.235.6)، تتبادل النقطتان الطرفيتان A وB أنصاف مفاتيح ديفي–هيلمان، وفقاً للفقرة 5.8 من التوصية H.235.6 وتنشآن مفتاحاً رئيسياً دينامياً بخصوص جلسة الاتصال يمكن انطلاقاً منه استخراج مفاتيح الجلسة الخاصة بوسائط الاتصال.

تتضمن النقطة الطرفية B المجال **generalID** الذي يملأ بالمعرف $EPID_A$ والمجال **sendersID** الذي يملأ بالمعرف $EPID_B$ لحماية أي رسالة تشوير للنداء H.225.0 موجهة إلى النقطة الطرفية A (من قبيل، Call Proceeding أو Alerting أو Connect).

ويظهر في الشكل 3 المراحل الأساسية لتدفق الاتصال:



الشكل H.235.4/3 – المراحل الأساسية لتدفق الاتصال (DRC2)

11 الإجراء DRC3 (بيئة مشتركة بين الميادين)

ينطبق الإجراء الوارد وصفه في هذه الفقرة في بيئة مشتركة بين الميادين حيث لا تقبل النقطة الطرفية طالبة النداء خوارزمية ديفي–هيلمان، في حين باستطاعة حارسي البوابتين في ميدان كل من الجهة الطالبة والجهة المطلوبة أن يحسبا ويتبادلا المعلمات DH. وفي مثل هذه البيئة، يحسب مفتاح الجلسة بفضل تبادل المعلمات DH بين حارس البوابة المصدر وحارس البوابة المقصد.

1.11 الطور GRQ/RRQ

يغطي هذا السيناريو حراس بوابات متعددة متسلسلة. وتحدد النقاط الطرفية ما إذا كانت قادرة على قبول هذه الجانبية الأمنية عند إرسال الرسالتين **GRQ** و/أو **RRQ** بإدراج علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I30"،

وتبقى المجالات الأخرى فيها خالية. ويردّ حارس البوابة القادر على أداء H.235.4 والمستعد للقيام بهذه الوظيفة، برسالة **GCF** أو **RCF** تتضمن علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I30"، وتبقى المجالات الأخرى فيها خالية.

2.11 الطور ARQ

قبل أن تتصل النقطة الطرفية A بالنقطة الطرفية B بواسطة الإجراء DRC3، ترسل إلى حارس البوابة G رسالة **ARQ** تحتوي علامة ClearToken منفصلة يملأ فيها المجال **tokenOID** بالرمز "I30"، وتبقى المجالات الأخرى فيها خالية.

3.11 الطور LRQ

عندما يستلم حارس البوابة G الرسالة **ARQ** التي ترسلها النقطة الطرفية A، يرسل بدوره رسالة **LRQ** إلى حارس البوابة H للحصول على عنوان النقطة الطرفية B، باعتبار أن النقطة الطرفية B لا تنتمي إلى ميدان حارس البوابة G. ويفحص حارس البوابة G العلامة ClearToken الواردة في الرسالة **ARQ** ويجد أن المجال **tokenOID** يحتوي "I30". وإذا كان حارس البوابة G يقبل خوارزمية DH عندئذٍ يطبّق بعض القواعد المحددة مسبقاً التي تحدد وجوب استخدام الإجراء DRC3.

ثم يولّد حارس البوابة G رسالة **LRQ** تحتوي ClearToken (في CryptoHashedToken) يملأ فيها المجال **tokenOID** بالرمز "I30" للإشارة إلى حارس البوابة H أن المفاوضة بشأن المفتاح DH ضرورية. ويملأ المجال **dhkey** في العلامة ClearToken بالمعلمات DH للجهة الطالبة (g, p, g^x) التي يولّدها حارس البوابة G، وتبقى المجالات الأخرى فيها خالية.

ثم يرسل حارس البوابة G الرسالة **LRQ** إلى حارس البوابة H. وفي حالة وجود سحابة من حراس البوابات، يرسل حارس البوابة G الرسالة **LRQ** إلى الحارس المجاور له مباشرة، الذي يحيل بدوره الرسالة **LRQ** إلى الحارس المجاور له مباشرة. وتستمر عملية الإحالة، هذه إلى أن تصل الرسالة **LRQ** إلى حارس البوابة H.

في حال تعدد التوزيع، لا يستخدم المجال **generalID** في العلامة CryptoToken للرسالة **LRQ**. وإذا لم يتمكن حارس البوابة G من تحديد موقع النقطة الطرفية البعيدة B، فإنه يعيد الرسالة **ARJ** إلى النقطة الطرفية A. ويتم تأمين الاتصال بين حارسي بوابتين طبقاً للجانبية في التوصية ITU-T H.235.1.

وإذا لم يكن حارس البوابة G يقبل الجانبية، فيمكنه أن يختار إما اللجوء إلى الإجراء DRC2 أو إعادة الرسالة **ARJ** إلى النقطة الطرفية A. فإذا اختار الإجراء DRC2، عندئذٍ يكون الطور **LRQ** والأطوار اللاحقة مماثلة لتلك الواردة في الإجراء DRC2.

4.11 الطور LCF

بعد أن يستلم حارس البوابة H الرسالة **LRQ** من حارس البوابة G، وبعد أن يتبين أن النقطتين الطرفيتين A وB تقبلان هذا الإجراء، يقوم بتوليد مفتاح الجلسة K_{AB} حسبما هو محدد أدناه.

أولاً، يقوم حارس البوابة H بتوليد عنصر عشوائي Challenge-B يوضع في الخطوة CT_B→**challenge** ويشتمل الإجراء CT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** على العنصر "AnnexI-HMAC-SHA1-PRF"، ثم يستعمل حارس البوابة H المفتاح المتقاسم K_{GH} والعنصر Challenge-B لحساب بيانات المفتاح EK_{GH} ومفتاح التمليح KS_{GH} باتباع إجراء حساب المفتاح على أساس الوظيفة PRF.

يوضع العنصر Challenge-B في CT_B→**challenge** ويوضع معرف حارس البوابة H في CT_B→**sendersID** ويوضع معرف النقطة الطرفية B في CT_B→**generalID**. إذا كان المجال Identifierendpoint للرسالة **LRQ** يحتوي معرف النقطة الطرفية A، ينسخه حارس البوابة H في CT_B→**h235Key**→**secureSharedSecret**→**generalID** وفي CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID** أيضاً.

ثم يستحدث حارس البوابة H علامتين ClearToken في الرسالة **LCF**: واحدة CT_{HG} يملأ فيها المجال **tokenOID** بالرمز "I33" بالنسبة لحارس البوابة G وأخرى CT_B يملأ فيها المجال **tokenOID** بالرمز "I12" بالنسبة للنقطة الطرفية B. ويولّد

حارس البوابة H معلمات ديفي–هيلمان للجهة المطلوبة (g, p, g^y). ثم يستخدم معلمات ديفي–هيلمان للجهة الطالبة التي تم الحصول عليها من الرسالة **LRQ** لحساب مفتاح الجلسة $K_{AB} = g^{xy} \bmod p$.

وأخيراً، يجفر حارس البوابة H المفتاح K_{AB} باستخدام المفتاحين EK_{BH} وKS_{BH} في شكل $ENC_{EKBH, KSBH, IV}(K_{AB})$ ويضع المفتاح المجفّر K_{AB} في الإجراء CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** ويضع معلمات ديفي–هيلمان للجهة المطلوبة في المجال **dhkey** من العلامة CT_{HG}.

يستخدم أسلوب التجفير المحسّن (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{GH} الخاص بالنقطة الطرفية. وفيما يلي خوارزميات التجفير المطبقة (انظر الجدول 6 في التوصية H.235.6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: بالتغيب وموصى بها؛
- متوافقة مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير المحسّن EOFB، يولّد حارس البوابة H قيمة مبدئية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1" و"Z1" المتّجه IV يشغل بمقدار 64 بتة ويرسل ضمن الإجراء CT_B→**h235Key**→**secureSharedSecret**→ **params**→**iv8** وبالنسبة للمعرف "Z2" OID، فإن المتجه IV يشغل 128 بتة ويرسل ضمن الإجراء CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

ويشار إلى خوارزمية التجفير في CT_B→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2"). بالنسبة إلى خوارزميات التجفير المحسّن EOFB، لا يستخدم العنصر **encryptedSaltingKey**.

يرسل حارس البوابة H الرسالة **LCF** إلى حارس البوابة G. وفي حالة وجود سحابة من حراس البوابات، يتناقل الرسالة مختلف حراس البوابات. وعلى طول المسار، يستلم كل حارس بوابة الرسالة **LCF** من جاره المباشر السابق ويتحقق من أنها تحتوي العلامة CT_{HG} ويحيلها إلى جاره المباشر اللاحق.

إذا لم يكن حارس البوابة H يقبل خوارزمية ديفي–هيلمان، أو إذا لم تكن سياسة الأمن من استخدام الإجراء DRC3، عندئذٍ يُلجأ إلى الإجراء DRC2، وفي هذه الحالة، يكون الطور **LCF** وكافة الأطوار اللاحقة مماثلة لتلك الموجودة في الإجراء DRC2.

5.11 الطور ACF

بعد أن يستلم حارس البوابة G الرسالة **LCF** وبعد أن يتبين أن المجال **tokenOID** في العلامة ClearToken المنفصلة يحتوي الرمز "I33" يحصل على معلمات ديفي–هيلمان للجهة المطلوبة ويستحدث علامة ClearToken باسم CT_A يملأ فيها المجال **tokenOID** بالرمز "I11" حسبما هو وارد أدناه.

أولاً، يقوم حارس البوابة H بتوليد عنصر Challenge-A عشوائي يوضع في الخطوة CT_A→**challenge** ويشتمل الإجراء CT_A→**h235Key**→**secureSharedSecret**→**keyDerivationOID** على العنصر "AnnexI-HMAC-SHA1-PRF"، ثم يستعمل حارس البوابة G المفتاح المتقاسم K_{AG} والعنصر Challenge-A لحساب بيانات المفتاح EK_{AG} ومفتاح التمليح KS_{AG} باتباع إجراء حساب المفتاح على أساس الوظيفة PRF.

ثم يستخدم حارس البوابة G معلمات ديفي–هيلمان للجهة الطالبة التي تم الحصول عليها في المرحلة **LRQ**، وكذلك معلمات ديفي–هيلمان للجهة المطلوبة، لحساب مفتاح الجلسة $K_{AG} = g^{xy} \bmod p$.

ثم ينسخ حارس البوابة G العلامة CT_B ClearToken، التي يملأ مجالها **tokenOID** بالرمز "I12"، من الرسالة **LCF** إلى الرسالة **ACF**.

وأخيراً، يجفر حارس البوابة G المفتاح K_{AB} باستخدام المفتاحين EK_{AG} وKS_{AG} في شكل $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$ ويضع المفتاح المجفر K_{AB} في الإجراء **CT_A→h235Key→secureSharedSecret→encryptedSessionKey** وينسخ العلامة CT_B من الرسالة **LCF** إلى الرسالة **ACF**.

يستخدم أسلوب التجفير المحسّن (EOFB) (انظر الفقرة 4.8 من التوصية H.235.6) مع مفتاح التمليح السري KS_{AG} الخاص بالنقطة الطرفية.

وفيما يلي خوارزميات التجفير المطبقة (انظر الجدول 6 في التوصية H.235.6):

- DES (56 بتة) بأسلوب EOFB باستخدام معرف "Y1" OID: اختيارية؛
- 3DES (168 بتة) بأسلوب EOFB خارجي باستخدام معرف "Z1" OID: اختيارية؛
- AES (128 بتة) بأسلوب EOFB باستخدام معرف "Z2" OID: بالتغيب وموصى بها؛
- متوافقة مع RC2 (56 بتة) بأسلوب EOFB باستخدام معرف "X1" OID: اختيارية.

بالنسبة لأسلوب التجفير المحسّن EOFB، يولّد حارس البوابة G قيمة مبدئية عشوائية IV. وبالنسبة للمعرفات "X1" OID و"Y1" و"Z1" يشغل المتّجه IV مقدار 64 بتة ويرسل ضمن الإجراء **CT_A→h235Key→secureSharedSecret→params→iv8** وبالنسبة للمعرف "Z2" OID، فإن المتجه IV يشغل 128 بتة ويرسل ضمن الإجراء **CT_A → h235Key → secureSharedSecret → params → iv16**. ويشار إلى خوارزمية التجفير في **CT_A→h235Key→secureSharedSecret→algorithmOID** ("X1" أو "Y1" أو "Z1" أو "Z2").

إذا كان مجال العلامة ClearToken **tokenOID** (في الرسالة **LCF**) يحتوي "I23"، فإن هذا يعني أن عودة قد حصلت باتجاه الإجراء DRC2 وأن لحارس البوابة G الحرية في قبول أو رفض سياسة الأمن التي يتبعها حارس البوابة H. في حال القبول، يكون الطور **ACF** والطور SETUP اللاحق مماثلين للطورين الموصوفين في الإجراء DRC2. أما في حالة الرفض فإن حارس البوابة G يرد برسالة رفض مقابلة تشير إلى قصور من الناحية الأمنية محددة سبب الرفض بعبارة securityDenial.

يرسل حارس البوابة G الرسالة **ACF** إلى النقطة الطرفية A.

6.11 الطور SETUP

تحدد النقطة الطرفية A العلامة CT_A من خلال فحص المعرّف **CT_A →tokenOID** "I11". وتتحقق من أن CT_A المستلمة حديثة من خلال فحص خاتم الزمن. وتجرى عمليات أمنية أخرى للتحقق من المجالين **generalID** و**sendersID** في ClearToken والمجال **generalID** في **secureSharedSecret**. فإذا تبين بعد التحقق أن العلامة CT_A المستلمة حديثة عندئذٍ تسترجع النقطة الطرفية A المتجه IV وتحسب المفتاحين EK_{AG} وKS_{AG} كما هو وارد أعلاه بالنسبة لحارس البوابة G باستخدام **CT_A→challenge** باعتباره العنصر Challenge-A. وتقوم النقطة الطرفية A بفك تجفير الإجراء **CT_A→h235Key→secureSharedSecret→encryptedSessionKey** للحصول على K_{AG}.

وإذا تبين بعد التحقق أن العلامة CT_A المستلمة حديثة عندئذٍ تستطيع النقطة الطرفية A أن ترسل إلى النقطة الطرفية B رسالة SETUP تحتوي العلامة CT_B. ويجري تأمين هذه الرسالة SETUP (توثيقها و/أو حماية تكامليتها) بواسطة الجانبية H.235.1 أو الجانبية H.235.3 من خلال تطبيق السر المتقاسم K_{AB}. ولهذه الغاية، لا يستخدم المجال **generalID** للعلامة ClearToken المظللة H.235.1 (وليس CT_B!) إلا إذا كانت النقطة الطرفية A تتمتع بمعرف $EPID_B$ (من خلال التشكيل مثلاً أو وضعه في الذاكرة لدى اتصال قديم). وإذا كانت النقطة الطرفية A تستخدم قيمة $EPID_B$ ما للمجال **generalID** في الرسالة SETUP، عندئذٍ تقبل قيمة المجال **sendersID** في رسالة تشوير النداء المعاد على أنه المعرف الحقيقي $EPID_B$.

وتتعرف النقطة الطرفية B على العلامة CT_B من خلال فحص المعرف **tokenOID** "I12" ضمن ClearToken.

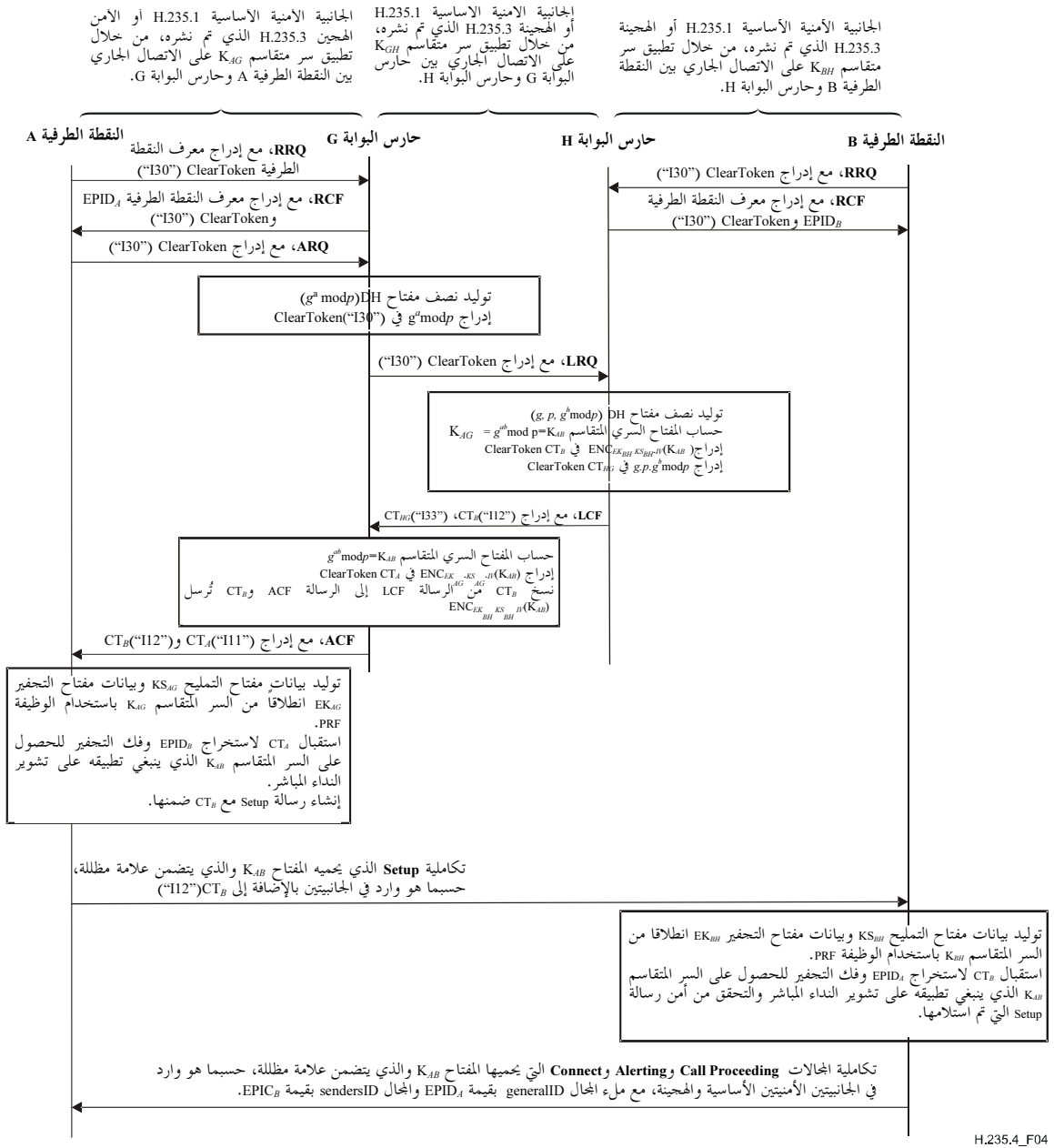
تتأكد النقطة الطرفية B من أن العلامة CT_B المستلمة حديثة بفحص خاتم الزمن **timestamp**. وتجرى عمليات أمنية أخرى للتحقق من المجال **sendersID** في ClearToken والمجال **generalID** ضمن **secureSharedSecret**. وإذا تبيّن بعد التحقق أن العلامة CT_B المستلمة حديثة فإن النقطة الطرفية B تسترجع المتجه IV وتحسب المفتاحين EK_{BH} وKS_{BH} باستخدام **challenge** → CT_B باعتباره العنصر Challenge-B. وتقوم النقطة الطرفية B بفك تجفير الإجراء **CT$_B$→h235Key→secureSharedSecret→encryptedSessionKey** للحصول على K_{AB}.

وإذا تبين بعد التحقق أن العلامة CT_B حديثة، تستطيع النقطة الطرفية B متابعة تشوير النداء بالرد برسالة CALL-PROCEEDING أو ALERTING أو CONNECT، أو غيرها حسب مقتضى الحال. وإذا تبين أن العلامة CT_B ليست حديثة، أو أن التحقق من أمن رسالة SETUP ينطوي على مشكلة ما، تستجيب النقطة الطرفية B برسالة RELEASE-COMPLETE، وتضع مقابل العنصر **ReleaseCompleteReason** عبارة خطأ أمني كما هو محدد في الفقرة 1.11 من التوصية H.235.0.

عندما يستدعي الأمر تطبيق أمن وسائط الاتصال (انظر الفقرة 1.6 من التوصية H.235.6)، تتبادل النقطتان الطرفيتان A وB أنصاف مفاتيح ديفي–هيلمان، وفقاً للفقرة 5.8 من التوصية H.235.6 وتنشآن مفتاحاً رئيسياً دينامياً بخصوص جلسة الاتصال يمكن انطلاقاً منه استنتاج مفاتيح الجلسة الخاصة بوسائط الاتصال.

تتضمن النقطة الطرفية B المجال **generalID** الذي يُملأ بالمعرف $EPID_A$ والمجال **sendersID** الذي يملأ بالمعرف $EPID_B$ لحماية أي رسالة تشوير للنداء H.225.0 موجهة إلى النقطة الطرفية A (من قبيل، Call Proceeding أو Alerting أو Connect).

ويظهر في الشكل 4 المراحل الأساسية لتدفق الاتصال:



الشكل H.235.4/4 – المراحل الأساسية لتدفق الاتصال (DRC3)

12 إجراء حساب المفاتيح بواسطة الوظيفة PRF

تصف هذه الفقرة إجراءً يبيّن كيفية حساب بيانات المفاتيح انطلاقاً من سر متقاسم ومعلمات أخرى.

ويمكّن الإجراء المحدد في هذه الفقرة من حساب مفتاح التجفير ومفتاح التمليح انطلاقاً من مفتاح متقاسم. وهذا الإجراء موحّد بغض النظر عن السر المتقاسم (K_{AG} أو K_{BH} أو K_{GH}).

وللحصول على بيانات المفاتيح المطلوبة (EK_{AG} مثلاً)، تستخدم الوظيفة PRF (انظر الفقرة 10 من التوصية H.235.0) وتؤخذ المعلمات الواردة من الجدول 1، حيث تضبط المعلمة *inkey* إزاء المفتاح المتقاسم المقابل (K_{AG}، مثلاً) وحيث تضبط المعلمة *label* إزاء الثابتة المقابلة (**challenge-A** || 0x2AD01C64 مثلاً)، حيث يشير الرمز || إلى عملية سلسالية. كما تضبط المعلمة *outkey_len* عند الطول المطلوب بالنسبة لبيانات المفاتيح المطلوبة، الأمر الذي يعتمد على خوارزمية التجفير المختارة.

ملاحظة– بالنسبة للمفاتيح EK_{AG} وKS_{AG} وEK_{BH} وKS_{BH}، تأتي الثوابت الصحيحة المكونة من 32 بتة (أي 0x2AD01C64 وهكذا من) الأرقام العشرية للقيمة e (أي 2,71828 وهكذا) وبالنسبة للمفتاحين EK_{GH} وKS_{GH} تأتي الثوابت الصحيحة من الأرقام العشرية للقيمة π (أي 3,14159 وهكذا). وبالنسبة للمفاتيح EK_{AG} وEK_{BH} وKS_{AG} وKS_{BH}، تأتي الثوابت المكونة من 32 بتة من مجموعات من 9 أرقام عشرية، هي

على التوالي المجموعة الأولى والثانية والرابعة والسابعة. أما بالنسبة للمفتاح EK_{GH} فتأتي القيمة من أول عشرة أرقام عشرية للقيمة π، في حين تأتي KS_{GH} من الأرقام العشرية الثمانية اللاحقة للقيمة π.

الجدول 1/ H.235.4– حساب مفاتيح التجفير والتمليح انطلاقاً من سر متقاسم

المفتاح المستهدف	المعلمة inkey للوظيفة PRF	الثابتة || Challenge
EK_{AG}	K_{AG}	0x2AD01C64 || **Challenge-A**
KS_{AG}	K_{AG}	0x150533E1 || **Challenge-A**
EK_{BH}	K_{BH}	0x1B5C7973 || **Challenge-B**
KS_{BH}	K_{BH}	0x39A2C14B || **Challenge-B**
EK_{GH}	K_{GH}	0x54655307 || **Challenge-G**
KS_{GH}	K_{GH}	0x35855C60 || **Challenge-G**

13 إجراء حساب المفاتيح على أساس المعيار FIPS-140

من المزمع أن تصف هذه الفقرة إجراءً يشير إلى كيفية حساب بيانات المفاتيح انطلاقاً من سر متقاسم ومعلمات أخرى بواسطة نموذج تجفير مطابق للمعيار FIPS-140. ويبقى هذا الموضوع بحاجة إلى مزيد من الدراسة.

14 قائمة معرفات الأغراض

الجدول 2/H.235.4– معرفات الأغراض المستخدمة في التوصية ITU-T H.235.4

الإحالة إلى معرف الغرض	قيمة معرف الغرض	الوصف
"I10"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 48}	يستخدم في الإجراء DRC1 خلال تبادل الرسائل GRQ/RRQ وGCF/RCF وARQ لتمكين النقطة الطرفية/حارس البوابة من الإشارة إلى قبول الإجراء DRC1.
"I11"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 49}	يستخدم في الإجراءات DRC1 وDRC2 وDRC3 للعلامة tokenOID في ClearToken، مشيراً إلى أن العلامة ClearToken CT_A تتضمن مفتاحاً من طرف إلى طرف للجهة الطالبة.
"I12"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 50}	يستخدم في الإجراءات DRC1 وDRC2 وDRC3 للعلامة tokenOID في ClearToken، مشيراً إلى أن العلامة ClearToken CT_B تتضمن مفتاحاً من طرف إلى طرف للجهة المطلوبة.
"I13"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 52}	يُستخدم في الإجراء DRC2 للعلامة tokenOID في ClearToken بين حراس البوابات، مشيراً إلى أن ClearToken CT_{HG} تتضمن مفتاح تجفير لحارس البوابة المصدر.
"I20"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 53}	يستخدم في الإجراء DRC2 خلال تبادل الرسائل GRQ/RRQ وGCF/RCF وARQ لتمكين النقطة الطرفية/حارس البوابة من الإشارة إلى قبول الإجراء DRC2.

الإحالة إلى معرف الغرض	قيمة معرف الغرض	الوصف
"I23"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 56}	يستخدم في الإجراء DRC2 للعلامة tokenOID في ClearToken بين حراس البوابات، مشيراً إلى أن ClearToken CT_{HG} تتضمن مفتاح تجفير لحارس البوابة المصدر.
"I30"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 34}	للاستخدام في ClearToken منفصلة في الرسائل GRQ/RRQ وGCF/RCF وARQ إشارةً إلى قبول الإجراء DRC3. للاستخدام في ClearToken منفصلة في رسالة LRQ إشارةً إلى تسيير المعلمات DH للجهة الطالبة.
"I33"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 37}	للاستخدام في ClearToken منفصلة في رسالة LCF إشارةً إلى تسيير المعلمات DH للجهة المطلوبة.
"الملحق "I-HMAC-SHA1-PRF	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 51}	يستخدم في الإجراءات DRC1 وDRC2 وDRC3 للمجال keyDerivationOID في V3KeySyncMaterial إشارةً إلى تطبيق طريقة حساب المفاتيح على أساس الوظيفة شبه العشوائية HMAC-SHA1 المحددة في الفقرة 12.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	**الأنظمة السمعية المرئية والأنظمة متعددة الوسائط**
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات المعطيات على الشبكة الهاتفية
السلسلة X	شبكات المعطيات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2006