الاتحـــــــــاد الـــدولـــــــــي للاتصـــــــالات

ITU-T

H.235.7

(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: استعمال بروتوكول إدارة المفاتيح MIKEY مع بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) في أنظمة H.235

التوصيـــة ITU-T H.235.7

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

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

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

إطار الأمن H.323: استعمال بروتوكول إدارة المفاتيح MIKEY مع بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) في أنظمة H.235

ملخص

الهدف من هذه التوصية هو وصف إجراءات الأمن المطبقة على استعمال الأنظمة الواردة في H.235/H.323 لبروتوكول إدارة المفاتيح MIKEY بالاقتران ببروتوكول النقل المؤمَّن في الوقت الفعلي.

وفي الطبعات السابقة للسلسلة الفرعية H.235، تورد التذييلات IV وV وVI بالتوصية H.235.0 التقابل التام بين جميع الفقرات وجميع الأشكال وجميع الجداول الواردة في الطبعتين 3 و4 للتوصية ITU-T H.235.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 13 سبتمبر 2005 على التوصية ITU-T H.235.7 بموجب الإجراء المحدد في التوصية ITU-T A.8.

الكلمات الرئيسية

تجفير الوسيط، إدارة مفاتيح MIKEY، أمن متعدد الوسائط، بروتوكول النقل المؤمَّن في الوقت الفعلي، ملامح الأمن، بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP).

تمهيـــد

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

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

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

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

مقدمة

تصف هذه التوصية إجراءات الأمن المطبَّقة على استعمال الأنظمة الواردة في H.235/H.323 لبروتوكول إدارة المفاتيح IETF MIKEY بالاقتران ببروتوكول النقل المؤمَّن في الوقت الفعلي IETF SRTP.

وقد تمت صياغة هذه التوصية في شكل ملامح أمنية للتوصية ITU-T H.235 المتاحة كخيار ويمكن أن تستكمل بملامح أخرى للأمن متعدد الوسائط الواردة في التوصية H.235.6.

وتسمح هذه التوصية بتنفيذ أمن وسائط بروتوكول SRTP حيث تتيح إدارة مفاتيح MIKEY المفاتيح ومعلمات الأمن الضرورية للنقاط الطرفية من طرف إلى طرف. ويمكن تنفيذ هذه التوصية ضمن مجال H.323 من بين أنظمة H.323 من نمط H.235.7. وتحدد هذه التوصية تمديدات الأمن المطبَّقة على بروتوكولات إجراءات التسجيل والقبول والحالة (RAS) وتشوير النداء الواردة في التوصية ITU-T H.225.0 وكذلك على بروتوكول H.245 وتحدد أيضاً الإجراءات المقابلة. بالإضافة إلى ذلك، تحدد هذه التوصية القدرات التي تسمح بعدم التشغيل البيني مع كيانات بروتوكول تمهيد الدورة SIP لفريق مهام هندسة الإنترنت IETF التي تقوم بتنفيذ إدارة مفاتيح MIKEY وبروتوكول SRTP.

إطار الأمن H.323: استعمال بروتوكول إدارة المفاتيح MIKEY مع بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) في أنظمة H.235

1 مجال التطبيق

تصف هذه التوصية إجراءات الأمن المطبَّقة على استعمال الأنظمة القائمة على H.235/H.323 لاستعمال بروتوكول إدارة المفاتيح MIKEY بالاقتران ببروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP).

2 المراجع

1.2 المراجع المعيارية

تتضمن توصيات قطاع تقييس الاتصالات (ITU-T) وغيرها من المراجع التي تشكِّل من خلال الإشارة إليها في هذه النص أحكام هذه التوصية. ولدى الطباعة كانت الطبعات المشار إليها سارية المفعول. وتخضع جميع التوصيات وغيرها من المراجع للمراجعة ويشجع بالتالي جميع مستعملي هذه التوصية على التحقق من إمكانية تطبيق أحدث طبعة من التوصيات وغيرها من المراجع التي ترد قائمة بها أدناه. وتنشر بانتظام قائمة بتوصيات القطاع ITU-T السارية المفعول حالياً. ولا تُضفي مجرد الإحالة إلى وثيقة ما ترد في هذه التوصية صفة التوصية على هذه الوثيقة.

- التوصية ITU-T H.225.0 (2003)، *بروتوكولات تشوير النداء ووضع قطار متعدد الوسائط في الرزم لأغراض أنظمة الوسائط المتعددة العاملة بأسلوب الرزم.*
- التوصية ITU-T H.235.0 (2005)، *إطار الأمن H.323: أمن وتخفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.1 (2005)، *إطار الأمن H.323: مظهر جانبي للأمن الأساسي.*
- التوصية ITU-T H.235.3 (2005)، *إطار الأمن H.323: مواصفة الأمن الهجينة.*
- التوصية ITU-T H.235.4 (2005)، *إطار الأمن H.323: أمن النداءات بالتسيير المباشر والنداءات بالتسيير الاختياري.*
- 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 X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة لتطبيقات CCITT.*
- ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*
- IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications.*
- IETF RFC 3711 (2004), *The Secure Real Time Transport Protocol (SRTP).*
- IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing.*

2.2 المراجع الإعلامية وثبت المراجع

- IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

- IETF RFC 2327 (1999)، *(SDP): بروتوكول وصف الدورة (SDP)*.

- IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method*.

- IETF RFC 3261 (2002)، *SIP: بروتوكول استهلال الدورة (SIP)*.

- IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP)*.

- IETF RFC ssss (2005), M. Handley, Van Jacobson, C. Perkins: *SDP: Session Description Protocol*, draft-ietf-mmusic-sdp-new-24.txt.

- IETF RFC wwww (2005), J. Arkko, E. Carrara et al: *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*, Internet Draft draft-ietf-mmusic-kmgmt-ext-14.txt, Work in Progress.

- IETF RFC zzzz (2005), M. Euchner: *HMAC-authenticated Diffie-Hellman for MIKEY*, Internet Draft draft-ietf-msec-MIKEY-DHHMAC-11.txt, Work in Progress.

3 التعاريف

لا توجد.

4 الرموز والاختصارات

تستعمل هذه التوصية الاختصارات التالية:

a, b, e, d مفتاح DH الخصوصي للنقطة الطرفية A، للنقطة الطرفية B، للحارس البوابي E، للحارس البوابي D (*private DH key of EP A, EP B, GK E, GK D*)

Cert شهادة رقمية (الوثيقة RFC 3830) (*digital certificate*)

CP/C نداء جاري توصيله (*CallProceeding-to-Connect*)

CSB حزمة دورات التجفير (الوثيقة RFC 3830) (*Crypto Session Bundle*)

CT_A, CT_B العلامة ClearToken للنقطة الطرفية B، العلامة ClearToken للنقطة الطرفية A (H.235.4) (*ClearToken for endpoint B, ClearToken for endpoint A*)

DRC1 نداء بتسيير مباشر (H.235.4) (*Direct-routed Call*)

$ENC_K(X)$ تشفير X باستعمال المفتاح k (*Encryption of X using key k*)

env_key مفتاح غلاف (RFC 3830) بين النقطة الطرفية B والنقطة الطرفية A (*Envelope key (RFC 3830) between endpoint B and endpoint A*)

EP نقطة طرفية (*Endpoint*)

Esc أمر نهاية الدورة H.245 (*H.245 EndSessionCommand*)

DH ديفي–هيلمان (*Diffie-Hellman*)

DH_A نصف مفتاح DH للنقطة الطرفية A (*DH half-key of endpoint A*)

DH_B نصف مفتاح DH للنقطة الطرفية B (*DH half-key of endpoint B*)

g^a, g^b نصف مفتاح DH للنقطة الطرفية A، للنقطة الطرفية B (*Diffie-Hellman half-key of EP A, EP B*)

g^d, g^e نصف مفتاح DH للنقطة الطرفية E، للنقطة الطرفية D (*Diffie-Hellman half-key of GK E, GK D*)

GK حارس بوابي (*Gatekeeper*)

HDR الحمولة النافعة لرأسية MIKEY (RFC 3830) (*MIKEY header payload*)

ID_A, ID_B هوية النقطة الطرفية A، هوية النقطة الطرفية B (*Identity (i.e., endpoint ID) of endpoint A, Identity of endpoint B*)

IETF فريق مهام هندسة الإنترنت (*Internet Engineering Task Force*)

Imsg رسالة MIKEY للممهد (RFC 3830) (*MIKEY message of the initiator*)

KEMAC رسالة الحمولة النافعة KEMAC MIKEY (*MIKEY KEMAC payload message*)

MAC(k, x) مبرقة MAC بمفتاح k يطبق على x (*Keyed MAC on x using key k*)

Ma مفتاح استيقان MIKEY (RFC 3830) (*MIKEY authentication key*)

Me مفتاح تجفير MIKEY (RFC 3830) (*MIKEY encryption key*)

MIKEY بروتوكول إدارة المفاتيح متعددة الوسائط (*Multimedia Internet Keying*)

NTP البروتوكول المتعلق بالوقت في الشبكة (*Network Time Protocol*)

PKE رسالة الحمولة النافعة MIKEY PKE (RFC 3830) (*MIKEY PKE payload message*)

PKI البنية التحتية لمفتاح عمومي (*Public-Key Infrastructure*)

PRF وظيفة شبه عشوائية (MIKEY-PRF، الفقرات من 2.1.4 إلى 4.1.4 في RFC 3830) (*Pseudo-Random Function*)

Rand غرض حاضر عشوائي (RFC 3830) (*random nonce*)

Rmsg رسالة MIKEY للمستجيب (RFC 3830) (*MIKEY message of the responder*)

Rand() قيمة عشوائية (*random value*)

RSA ريفست وشامير وآديلمان (خوارزمية بمفتاح عمومي) (*Rivest, Shamir and Adleman ((public key algorithm*)

sa, sb السر المتقاسم بين النقطة الطرفية A وحارس بوابي، السر المتقاسم بين النقطة الطرفية B وحارس بوابي (*shared secret among endpoint A and GK, shared secret among endpoint B and GK*)

sl السر المتقاسم بين حارسات بوابية (*shared secret among gatekeepers*)

SDP بروتوكول وصف الدورة (*Session Description Protocol*)

SHA1 خوارزمية التظليل المأمون (ISO/IEC 10118-3) (*Secure Hash Algorithm 1*)

SIP بروتوكول تمهيد الدورة (*Session Initiation Protocol*)

SP سياسة الأمن (RFC 3830) (*Security Policy*)

SRTCP بروتوكول التحكم المؤمَّن للنقل في الوقت الفعلي (*Secure Real-time Transport Control Protocol*)

SRTP بروتوكول نقل مؤمَّن في الوقت الفعلي (*Secure Real-time Transport Protocol*)

SSRC مصدر التزامن (RTP) (*Synchronization source*)

T مُسَجلة الوقت (RFC 3830) (*Timestamp*)

TGK مفتاح توليد الحركة بين النقطة الطرفية A والنقطة الطرفية B (RFC 3830) (*Traffic Generating Key between endpoint A and endpoint B*)

V مجال رسالة التحقق (RFC 3830) (*Verification message field*)

ZZ_{AB} سر H.323 متقاسم دينامي (RFC 3830) (*dynamic shared H.323 secret ZZ_{AB}*)

{ } صفر، حدث واحد أو عدة أحداث (*Zero, one or more occurrences*)

[ ] عنصر اختياري (*Optional element*)

5 الاصطلاحات

تُعيَّن معرِّفات الغرض برمز في النص (أي "G1")، وتُعطى الفقرتان 5.8 و5.9 القيم الرقمية الفعلية المناظرة لمختلف رموز معرِّفات الغرض. وللمزيد من التفاصيل انظر الفقرة 5 للتوصية ITU-T H.235.0.

يحدد الجدول 1 بروتوكولات إدارة المفتاح MIKEY الخمسة المشار إليها في هذه التوصية.

الجدول H.235.7/1 – بروتوكولات إدارة مفاتيح MIKEY

بروتوكول MIKEY	الوصف	قيمة معرِّف الغرض	معرِّف المعلَمة	التنفيذ
MIKEY	أي بروتوكول MIKEY	{التوصية (0) itu-t (8) 235 (0) h الطبعة 3 (0) 76}	76	تنفيذه إلزامي
MIKEY-PS	بروتوكول توزيع المفاتيح المتزامنة باستعمال مفاتيح متزامنة مسبقة التقاسم وشفرات HMAC (انظر RFC 3830)	{التوصية (0) itu-t (8) 235 (0) h الطبعة 3 (0) 72}	72	تنفيذه إلزامي
MIKEY-DHHMAC	بروتوكول اتفاق مفاتيح ديفي – هيلمان باستعمال مفاتيح متزامنة مسبقة التقاسم وشفرات HMAC (انظر RFC zzzz)	{التوصية (0) itu-t (8) 235 (0) h الطبعة 3 (0) 73}	73	تنفيذه اختياري
MIKEY-PK-SIGN	بروتوكول توزيع المفاتيح العمومية (يستند إلى خوارزمية RSA) باستعمال التوقيع الرقمي؛ (انظر RFC 3830)	{التوصية (0) itu-t (8) 235 (0) h الطبعة 3 (0) 74}	74	تنفيذه إلزامي
MIKEY-DH-SIGN	بروتوكول اتفاق مفاتيح ديفي – هيلمان باستعمال التوقيع الرقمي (انظر RFC 3830)	{التوصية (0) itu-t (8) 235 (0) h الطبعة 3 (0) 75}	75	تنفيذه اختياري

يشير تعبير MIKEY (انظر السطر الأول من الجدول 1) إلى عائلة برتوكولات MIKEY بشكل عام، دون الإشارة بالتحديد إلى برتوكول مفتاح إدارة MIKEY معيَّن مثل MIKEY-PS، أو MIKEY-DHHMAC أو MIKEY-PK-SIGN أو MIKEY-DH-SIGN. ويتضمن تنفيذه معالجة رسائل MIKEY بواسطة الحمولة النافعة للرأسية المشتركة MIKEY (القسم 1.6

من الوثيقة RFC 3830) ولكن ذلك لا يقتضي بالضرورة أي تنفيذ لبروتوكول إدارة مفاتيح MIKEY معيَّن أو تنفيذ حمولة نافعة إعلامية معيَّنة MIKEY. وينبغي استعمال معرِّف الغرض ومعرِّف المعلَمة المقابلين في حالة ما إذا كانت النقطة الطرفية H.323 تجهل متغير بروتوكول MIKEY المستعمل بالفعل. وفي كل الأحوال، يوصى باستعمال معرِّف OID محدد ومعرِّف معلَمات خاص بمتغير بروتوكول إدارة مفاتيح MIKEY المستعمل فعلاً.

6 مقدمة

ظهر اهتمام في استعمال خواص الأمن "لبروتوكول النقل المؤمَّن في الوقت الفعلي" IETF SRTP في الأنظمة الواردة في التوصية ITU-T H.235. وإن كانت الطبعات السابقة للتوصية ITU-T H.235 تقدِّم بالفعل خواص أمن مختلفة متعددة الوسائط مثل تجفير الصوت باستعمال فدرة شفرات صوتية واستيقان RTP محدود (خيار مكافحة الرسائل الاقتحامية) وهناك أسباب قوية تدعو إلى تنفيذ SRTP:

- استعمال شفرة تدفق لتحسين الأداء والمتانة والأمن؛
- ضمان التشغيل البيني مع مطاريف SRTP الأخرى، مثل المطاريف متعددة الوسائط القائمة على بروتوكول SIP.

ملاحظة – لا تُحدِّد هذه التوصية إجراءات أمن التشغيل البيني مع بروتوكول SIP (RFC 3261)؛ تتطلب هذه المسألة المزيد من الدراسة؛

- توفير المزيد من الأمن لحماية RTCP؛
- الحصول على تكامل أفضل يغطي رزمة RTCP/RTP؛
- نشر خوارزمية تجفير AES أحدث عهداً؛
- استعمال مفاتيح التجفير/مفاتيح الاستيقان المشتقة من الوظيفة شبه العشوائية للنقطتين الطرفيتين على السواء.

وفضلاً عن ذلك، ظهرت الحاجة إلى تحديد إدارة المفاتيح القائمة على خوارزمية RSA بالإضافة إلى أنظمة مطابقة مفاتيح ديفي–هيلمان المحددة في التوصية ITU-T H.235، وبالمثل اعتبرت تقنيات إدارة المفاتيح غير القائمة على البنية التحتية PKI مفيدة في حالة اعتبار البنية التحتية للمفاتيح العمومية غير مناسبة. وظهر اهتمام أيضاً في تناول الاعتراض المشروع في سياق إدارة المفاتيح.

بذل فريق مهام هندسة الإنترنت IETF الجهود أيضاً لتحديد نظام إدارة المفاتيح في الوقت الفعلي MIKEY (RFC 3830). ويُشكِّل نظام إدارة المفاتيح التنوُّعي هذا سطحاً بينياً ملائماً مع SRTP وهو قادر على توفير مفاتيح عمومية (TGKs) وإما مفاتيح حركة الدورة من طرف إلى طرف أو من طرف إلى وسط/قفزة تلو قفزة. ونظام MIKEY هو بروتوكول إدارة المفاتيح أقرب ما يكون من الكمال ينفَّذ من خلال رسالتين بحد أقصى، مما يجعله مناسباً لإقامة النداء مع بداية سريعة وفقاً للتوصية ITU-T H.323.

وتوفِّر هذه التوصية إجراءات الأمن اللازمة لنشر بروتوكولات إدارة مفاتيح MIKEY الواردة في النظامين H.235/H.323 وذلك بهدف دعم الأمن متعدد الوسائط SRTP. ومن الملاحظ أنه قد تكون هناك وسائل بديلة يمكن بواسطتها دعم SRTP في النظامين H.235/H.323، لكن هذه التدابير لا تتناولها هذه التوصية وتتطلب المزيد من الدراسة.

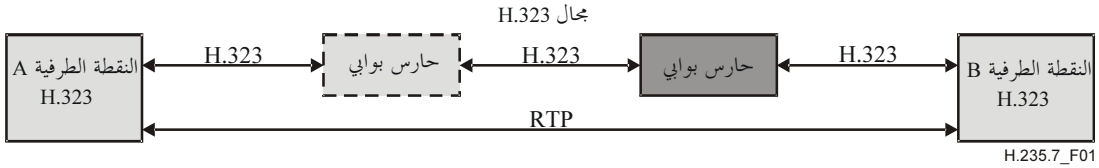
وتحدد هذه التوصية بروتوكولات إدارة مفاتيح MIKEY بطريقة مماثلة من حيث المفهوم للنهج الموصوف في الوثيقة RFC wwww، أو بروتوكول SIP (RFC 3261) الذي يستعمل نظام MIKEY في بروتوكول SDP (RFC 2327 وRFC ssss و RFC 3264).

وتوفِّر هذه التوصية اثنان من ملامح الأمن مع إجراءات الأمن لبنيتين تحتيتين مختلفتين للأمن:

- بنية تحتية للأمن تقوم على مفاتيح متناظرة تدعم حارسات بوابية متعددة (انظر الفقرة 8)؛
- بنية تحتية للأمن تقوم على مفاتيح غير متناظرة (PKI) تدعم حارسات بوابية عديدة (انظر الفقرة 9).

7 نظرة شاملة وسيناريوهات

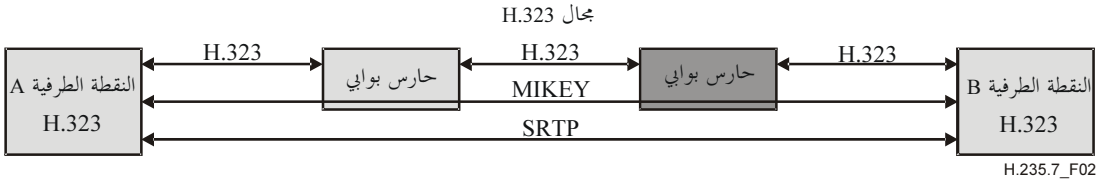
يبيِّن الشكل 1 السيناريو العام الذي تتناوله هذه التوصية. وتشكِّل نقطتان طرفيتان A وB في التوصية H.323 على الأقل جزءاً من هذا السيناريو. والنقطتان الطرفيتان يمكن أن تكونا إما مطاريف H.323 أو بوابات متعددة الوسائط H.323، ويمكن أن تشكِّل الأخيرة سطحاً بينياً مع شبكات أخرى تقوم على الإرسال بالرزم أو على أسلوب آخر للإرسال. بالإضافة إلى ذلك، يفترض أن تتضمن البيئة حارس بوابي واحد على الأقل. وفي حالة وجود حارس بوابي وحيد، يفترض أن جميع النقاط الطرفية H.323 تدخل ضمن منطقة الحارس البوابي الوحيد فقط. وفي حالة وجود حارسات بوابية متعددة، يمكن وضع النقاط الطرفية H.323 ضمن مناطق حارسات بوابية مختلفة. ويفترض من ناحية أخرى أن النقاط الطرفية H.323 تتواصل مباشرة من نقطة إلى نقطة باستعمال البروتوكول المتعدد الوسائط RTP.



الشكل H.235.7/1 – سيناريو

يوضِّح الشكل 2 سيناريو الأمن بشكل عام للدلالة على استعمال بروتوكولات إدارة مفاتيح MIKEY وبروتوكول الأمن متعدد الوسائط SRTP. وتنفذ بروتوكولات إدارة مفاتيح MIKEY بين النقطتين الطرفيتين A وB للتوصية H.323؛ وتغلف بروتوكولات إدارة مفاتيح MIKEY ضمن حاويات في رسائل تصافح التشوير الواردة في التوصية H.245 (رسائل Terminal Capability Set، Request Mode، Open Logical Channel handshakes، MiscellaneousCommand) وهي تعتبر شفافة بالنسبة إلى الحارس (حارسات) البوابي الوسيط.

ويجدر ملاحظة أن النقطة الطرفية في التوصية H.323 يمكن أن تكون بوابة. ويمكن لهذه البوابة، مثلاً، أن توفِّر وظيفة التشغيل البيني التي تشكِّل سطحاً بينياً مع الأنظمة القائمة على SIP. وفي هذه الحالة، لا يتوقَّف تنفيذ بروتوكولات MIKEY بالضرورة على البوابة ولكن هذه البوابة يمكن أن تخدم كمناوب لهذه البروتوكولات وأن تطيلها لضمان إدارة حقيقية للمفاتيح من طرف إلى طرف فيما بين المطاريف متعددة الوسائط المعنية، وتكفل بذلك الأمن متعدد الوسائط من طرف إلى طرف مع بروتوكول SRTP. ويسمح هذا النهج بالتشغيل البيني على مستوى الأمن بين نظامي H.235/H.323 والأنظمة القائمة على SIP. والعنصر الوظيفي الدقيق أو المواصفة الدقيقة لهذه البوابات ليست موضوع هذه التوصية وتتطلب المزيد من الدراسة.



الشكل H.235.7/2 – سيناريو الأمن مع MIKEY وSRTP

تشتمل جميع بروتوكولات إدارة المفاتيح الموصوفة في هذه التوصية على مرحلتين:

- تحدث المرحلة 1 أثناء طور تبادل رسائل RAS وتشوير النداء H.223.0. وبالنسبة لبروتوكولات MIKEY ذات المفاتيح المتناظرة (MIKEY-PS وMIKEY-DHHMAC) تفيد هذه المرحلة في إنشاء سر متقاسم من طرف إلى طرف ZZ_{AB} بين النقطتين الطرفيتين A وB، ويتعلق الأمر بسر متقاسم لبروتوكولات MIKEY. وبالنسبة لبروتوكولات MIKEY غير المتناظرة (MIKEY-PK-SIGN وMIKEY-DH-SIGN) تفيد هذه المرحلة في إنشاء سر متقاسم دينامي بين النقطة الطرفية من القفزة التالية (عادة ما يخدمها حارس بوابي)؛ ولا يرتبط عادة السر المتقاسم الدينامي مع بروتوكولات MIKEY ولكنه يفيد في تأمين تشوير النداء H.225.0 بين النقطة الطرفية والقفزة التالية.

- تحدث المرحلة 2 أثناء طور تشوير النداء H.225.0/وطور تنفيذ بروتوكول H.245. وتفيد هذه المرحلة في التفاوض وفي تنفيذ بروتوكول MIKEY (MIKEY-PS أو MIKEY-DHHMAC أو MIKEY-PK-SIGN أو MIKEY-DH-SIGN) بين النقطتين الطرفيتين A وB وفي إنشاء مفتاح MIKEY TGK. وتستطيع النقاط الطرفية MIKEY أيضاً، خلال المرحلة 2، تنفيذ إعادة حساب المفتاح أو تحديث مفتاح بروتوكول MIKEY لتجديد أو تحديث المفتاح TGK. ويمكن أن يحدث إنهاء نداء ما واستبعاد مفتاح TGK أيضاً أثناء المرحلة 2.

1.7 تشغيل بروتوكولات MIKEY على "مستوى الدورة"

يمكن تنفيذ بروتوكولات إدارة مفاتيح MIKEY على "مستوى الدورة"، أي تطبيق MIKEY TGK على أكثر من تدفق واحد متعدد الوسائط. ويوصى بتشغيل MIKEY على "مستوى الدورة" أثناء تصافح **TerminalCapability**.

ينبغي أن تستعمل **TerminalCapabilitySet**، المجال **h235SecurityCapability** حيث تستعمل **genericH235SecurityCapability** ضمن **encryptionAuthenticationAndIntegrity** على النحو التالي:

- ينبغي أن يشتمل المجال **capabilityIdentifier** على أحدث معرِّفات الغرض MIKEY ضمن المجال **standard**؛
- تبقى **maxbitRate** و**collapsing** غير مستعملتين؛
- تستعمل **nonCollapsing** مع المجموعة التالية **GenericParameters** حينما تنفَّذ بروتوكولات MIKEY على "مستوى الدورة" لجميع القنوات المنطقية:
  - **parameterIdentifier**: في **standard** مع القيمة 0 للإشارة إلى أن بروتوكولات MIKEY تنفذ على "مستوى الدورة"؛
  - **parameterValue** مع الرسالة المشفَّرة الاثنينية (I أو R) MIKEY في **octetString**؛
  - **supersedes** تظل خالية/غير مستعملة؛
- تبقى **nonCollapsingRaw** غير مستعملة؛
- **transport** (غير مستعملة أو معلَمات النقل بالتغيب).

ينبغي على **OpenLogicalChannel** و**OpenLogicalChannelAck** ألا تستعمل **encryptionSync** عندما تنفذ بروتوكولات MIKEY على "مستوى الدورة". وبالمثل، ينبغي على **RequestMode** ألا تستعمل **genericModeParameters** و**ModeElement** من أجل بروتوكولات MIKEY عندما تنفذ هذه البروتوكولات على "مستوى الدورة".

ينبغي على **MiscellaneousCommand** أن يستعمل **encryptionUpdate**، وتستعمل **genericParameter** على النحو التالي:

- **parameterIdentifier**: في **standard** باستعمال القيمة 0 للإشارة إلى إعادة حساب MIKEY TGK وتحديث CSB على "مستوى الدورة"؛
- **parameterValue** مع الإشارة المشفرة الاثنينية (I أو R) ضمن **octetString**.
- تبقى **supersedes** خالية/غير مستعملة.

ينبغي تجاهل **LogicalChannelNumber** لبروتوكولات MIKEY على مستوى الدورة ويمكن أن تكون لها أي قيمة.

ينبغي على **RequestMode** أن تستعمل **capabilityIdentifier** في **genericModeParameters** من **ModeElement** على النحو التالي:

- يأخذ **capabilityIdentifier** أحد معرِّفات الغرض MIKEY في **standard**؛
- **maxbitRate** و**collapsing** تبقى غير مستعملتين؛

- **nonCollapsing** مع المجموعة التالية **GenericParameters** حينما تنفذ بروتوكولات MIKEY على "مستوى الدورة" لقناه منطقية معينة:
  - **parameterIdentifier**: في **standard** باستعمال القيمة 0 للإشارة إلى أن بروتوكولات MIKEY تنفذ على "مستوى الدورة"؛
  - **parameterValue** مع الرسالة المشفَّرة الاثنينية (I أو R) MIKEY في **octetString**؛
  - **supersedes** تبقى خالية/غير مستعملة؛
- **nonCollapsingRaw** تبقى غير مستعملة؛
- **transport** (غير مستعملة أو معلَمات النقل بالتغيب).

2.7 تشغيل MIKEY على "مستوى متعدد الوسائط"

وبالمثل، يجوز تشغيل بروتوكولات إدارة مفاتيح MIKEY بالتناوب على "مستوى متعدد الوسائط"؛ أي يُطبَّق MIKEY TGK على قناة منطقية محددة فقط على تدفق متعدد الوسائط. وينبغي استعمال التصافح **TerminalCapability** للتفاوض على بروتوكول MIKEY في حين ينبغي استعمال **OpenLogicalChannel/Ack** لنقل الرسالة المشفَّرة MIKEY.

ينبغي أن تستعمل **TerminalCapabilitySet**، **h235SecurityCapability** حيث **genericH235SecurityCapability** تستعمل ضمن **encryptionAuthenticationAndIntegrity** على النحو التالي:

- ينبغي أن يشتمل **capabilityIdentifier** على أحد معرِّفات الغرض MIKEY OID ضمن **standard**؛
- **maxbitRate** و**nonCollapsing** و**collapsing** تبقى غير مستعملة؛
- **nonCollapsingRaw** (غير مستعملة أو معلَمات النقل بالتغيب)؛
- **transport** (غير مستعملة أو معلَمات النقل بالتغيب).

ينبغي على **OpenLogicalChannel** أو **OpenLogicalChannelAck** أن تستعمل **genericParameter** ضمن **encryptionSync** على النحو التالي:

- **parameterIdentifier**: في **standard** مع قيمة معرِّف الغرض (انظر الجدول 1) المقابلة لبروتوكول MIKEY المتفاوض بشأنه؛
- **parameterValue** مع الرسالة المشفَّرة الاثنينية MIKEY (I أو R) في **octetString**؛
- **supersedes** تبقى خالية/غير مستعملة؛
- ينبغي وضع **synchFlag** و**encryptionSync** على رقم الحمولة النافعة الدينامية. ينبغي ألا تستعمل هذه التوصية h235key وينبغي أن تكون سلسلة اتمونات خالية. ينبغي ألا يستعمل المجال **escrowentry**.

ينبغي على المجال **MiscellaneousCommand** أن يستعمل **encryptionUpdate** حيث يستعمل المجال **genericParameter** ضمن **encryptionSync** على النحو التالي:

- **parameterIdentifier**: في المجال **standard** مع قيمة معرِّف الغرض (انظر الجدول 1) المقابلة لبروتوكول MIKEY المتفاوض بشأنه؛
- **parameterValue** مع الرسالة المشفَّرة الاثنينية MIKEY (I أو R) في المجال **octetString**؛
- تبقى **supersedes** خالية/غير مستعملة.

ينبغي على **RequestMode** أن تستعمل **capabilityIdentifier** ضمن **genericModeParameters** للمجال **ModeElement** على النحو التالي:

- يجب أن يشتمل المجال **capabilityIdentifier** على أحد معرِّفات الغرض MIKEY ضمن المجال **standard**؛

- تبقى **maxbitRate** و**collapsing** غير مستعملتين؛
- **nonCollapsing** مع المجموعة التالية للمعلَمات **GenericParameters** عندما تنفذ بروتوكولات MIKEY على "مستوى متعدد الوسائط" من أجل قناة منطقية معينة:
  - **parameterIdentifier**: في المجال **standard** باستعمال قيمة معرِّف المعلَمة (انظر الجدول 1) المقابلة لبروتوكول MIKEY المتفاوض بشأنه؛
  - **parameterValue** مع الرسالة المشفَّرة الاثنينية MIKEY (I أو R) في المجال **octetString**؛
  - تبقى **supersedes** خالية/غير مستعملة.
- تبقى **nonCollapsingRaw** غير مستعملة؛
- **transport** (غير مستعملة أو معلَمات النقل بالتغيب).

3.7 التفاوض على قدرات MIKEY

إذا نقلت بروتوكولات MIKEY في آن معاً رسائل التصافح Request Mode/Capability Set وOpen Logical Channel، تلغى معلومات MIKEY المتضمنة في الرسالة Open Logical Channel وتحل محل المعلومات المتعلقة بإدارة المفاتيح التي تم الحصول عليها من قبل في الرسالتين Terminal Capability Set وRequest Mode.

ولما كانت النقاط الطرفية لا تنفذ بالضرورة المجموعة الكاملة لبروتوكولات إدارة مفاتيح MIKEY، بل لا تنفذ أياً منها (وبعبارة أخرى يمكن ألا تدعم بعض النقاط الطرفية هذه التوصية على الإطلاق)، فقد لا تعرف بعض النقاط الطرفية الطالبة قدرات MIKEY المدعمة عند النقطة الطرفية الطالبة. وبالتالي، يوصى بالتفاوض بشأن قدرات إدارة مفاتيح MIKEY بواسطة رسائل التصافح Terminal Capability Set.

وأثناء التفاوض على قدرات المطاريف، ينبغي أن تشير النقطة الطرفية الطالبة إلى بروتوكولات إدارة مفاتيح MIKEY التي تدعمها والتي يمكن أن تقبلها. ولتحقيق هذا الغرض، ينبغي أن تشير النقطة الطرفية الطالبة إلى قدرات أمن MIKEY التي تدعمها. وفي المجال **genericH235SecurityCapability**، يجب على النقطة الطرفية أن تضع **capabilityIdentifier** على قيمة معرِّف الغرض (انظر الجدول 1) المقابلة لملامح الأمن وإدارة مفاتيح MIKEY المفضلة. وتشجع النقاط الطرفية الطالبة أيضاً على الإشارة إلى بروتوكولات MIKEY الأخرى التي تدعمها، بحسب الترتيب التنازلي المفضل لسياستها وقيودها الأمنية.

يجب على أي نقطة طرفية طالبة لا تدعم هذه التوصية أن ترفض النداء باستعمال **ReleaseComplete** مع وضع **ReleaseCompleteReason** على **securityDenied** أو أن تستمر بطريقة غير آمنة إذا سمحت بذلك قواعد السياسة الأمنية. وإذا لاحظ الطالب أن المطلوب لا يدعم قدرة MIKEY بالتفتيش على القدرة المعادة، فإنه يمكن أن يخلُص إلى أن الطالب لا يدعم قدرة MIKEY المطلوبة.

يجب على أي نقطة طرفية طالبة تدعم هذه التوصية ولكنها لا تدعم قدرة بروتوكول MIKEY المطلوبة أن تشير إلى بروتوكولات MIKEY التي تدعمها وتقبلها أثناء تصافح المفاوضة Terminal Capability Set.

ترسل أي نقطة طرفية طالبة تدعم هذه التوصية وبروتوكول MIKEY المطلوب، ولكنها لا تدعم تركيبة معينة من خوارزميات ومعلَمات أمن SRTP/MIKEY (أي سياسة أمن MIKEY)، رسالة أخطاء MIKEY كرد (انظر الوثيقة RFC 3830، الفقرات 1.1.5 و2.1.5 و2.1.6). وينبغي أن تدرج النقطة الطرفية الطالبة سياسة أمن MIKEY التي تدعمها وتقبلها مع خوارزمية ومعلَمات أمن SRTP/MIKEY.

يستعمل في هذه التوصية التمرير النفقي لرسائل H.245 في رسائل تشوير النداء H.225.0 وذلك بهدف تأمين رسائل تشوير النداء H.225.0. ويمكن أيضاً عدم استعمال التمرير النفقي لرسائل H.245، ولكن يجب في هذه الحالة استعمال نقل آمن لحماية التكامل على الأقل (IPsec، TLS) لتأمين رسائل H.245. ولا ترد المزيد من التفاصيل بشأن هذا المتغير في هذه التوصية.

ومن المفضل في هذه التوصية استعمال التوصيل السريع، الذي تغلف بموجبه رسائل H.245 الممررة في النفق في الرسالتين Call Signalling Setup وCallProceeding-to-Connect. ويسمح هذا الإجراء بإتمام تصافح MIKEY ضمن رحلتي ذهاب وإياب.

تتقيد النقطة الطرفية المطابقة لهذه الملامح بالإجراء الموصوف في الفقرة 15.6 من الوثيقة RFC 3830، التي يقوم الطالب بموجبها بإقامة قائمة بمعرِّفات بروتوكول إدارة المفاتيح MIKEY (KMIDs) وذلك للوقاية من الاعتداءات الناجمة عن التنـــزيل أثناء التفاوض بشأن القدرة؛ (انظر الفقرة 3.8 من الوثيقة RFC wwww) وتدرج هذه القائمة في الحمولة النافعة للتمديد العام MIKEY لكل بروتوكول MIKEY مقدم.

وفي حالة القناة المزدوجة الكاملة، يستطبق بروتوكول SRTP مرتين، مرة واحدة في كل اتجاه؛ في حين يتم التفاوض بشأن مفتاح واحد عمومي MIKEY دينامي بين النقاط الطرفية H.323. وتستطبق النقاط الطرفية مفاتيح دورة SRTP في كل اتجاه بتطبيق معرِّفات دورة تجفير MIKEY المتميزة لحساب مفتاح MIKEY وSRTP.

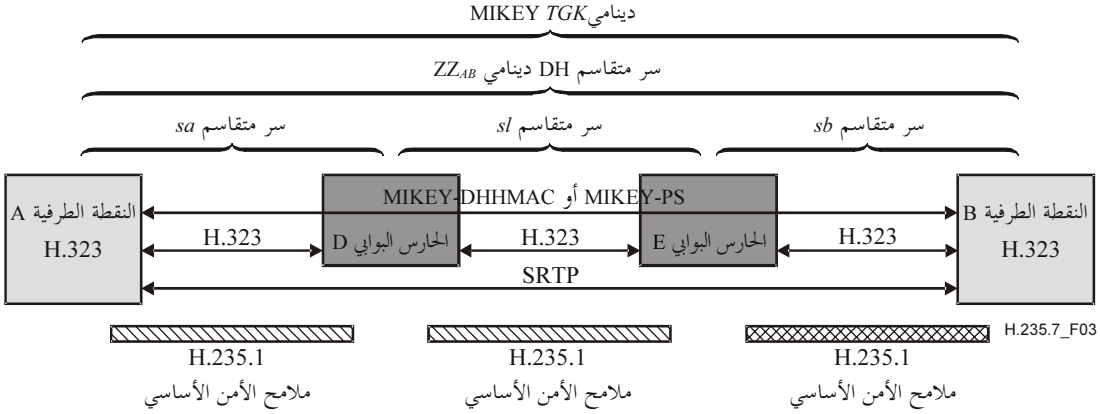
8 مواصفة الأمن باستعمال تقنيات الأمن المتناظر

يصف هذا القسم مواصفة الأمن الخاصة بهذه التوصية التي تنفذ في إطارها تقنيات الأمن المتناظر فقط.

ويوضِّح الشكل 3 سيناريو يفترض وجود أسرار متقاسمة قفزة بقفزة بين كيانات H.323 في مجال H.323 (*sa* و*sb* و*sl*)؛ ومن ثم تسمح بتنفيذ أمن الخط الأساسي H.235.1 (استيقان و/أو تكامل الرسائل) رسائل التشوير المتبادلة بين النقطتين الطرفيتين B وA، ينبغي تنفيذ الأمن الأساسي H.235.1 قفزة بقفزة.

ويفترض في النقطة الطرفية B أن تكون متناظرة نسبياً من حيث الوقت مع النقاط الطرفية الأخرى في H.323؛ وبعبارة أخرى، لا يمكن تنفيذ بروتوكول MIKEY بطريقة مؤمَّنة.

ملاحظة – لا تصف هذه التوصية أي وسيلة تسمح بتناظر الميقاتيات (بطريقة مؤمَّنة) بين الكيانات المعنية. ويفترض بشكل عام إمكانية الحصول على التناظر الزمني في إطار شبكات المنشآت.



الشكل H.235.7/3 – سيناريو قفزة بقفزة فقط مع الأسرار المتقاسمة

ويستند النهج الأساسي لهذا السيناريو إلى واقع أن بروتوكول توزيع مفاتيح MIKEY-PS (متناظر مع أسرار متقاسمة)، أو في حالة السر التام الأمامي، ينفذ بروتوكول اتفاق المفاتيح MIKEY-DHHMAC (ديفي–هيلمان مع HMAC) في مجال H.323. وتوفِّر RFC zzzz كخيار يُكمِّل MIKEY، انظر التذييل I.

عندما تطلب النقطة الطرفية B (ممهد MIKEY) النقطة الطرفية A (مستجيب MIKEY)، يقام سر متقاسم دينامي ZZ_{AB} بين النقطتين الطرفيتين A وB في إطار إجراءات H.225 RAS وSetup من أجل النداء. ويستعمل هذا السر فيما بعد كسر متقاسم

مسبق MIKEY، يشتق منه MIKEY في نقطتي مفاتيح التشفير EP A وEP B التحفير المتناظر ومفاتيح الاستيقان (غير مبيَّنة في هذا الشكل).

تولِّد النقطة الطرفية الطالبة B مفتاح MIKEY TGK (وهو في الواقع المفتاح العمومي) للنقطة الطرفية القرينة A. تقوم النقطة الطرفية B بإنشاء رسائل بروتوكول MIKEY وتغلفها بالكامل في إطار حاوية في الرسالة **TerminalCapabilitySet/OpenLogicalChannel** النفقية. وفي سياق تسيير بواسطة حارس بوابي GK E، لا يقوم الحارس البوابي سوى بإرسال الحاوية MIKEY إلى النقطة الطرفية الأخرى A بدون أي تشفير لمعلومات MIKEY في حد ذاتها. وتنهي النقطة الطرفية A بروتوكول MIKEY في مجال H.323.

وهكذا تقوم النقطتان الطرفيتان B وA بإنشاء مفتاح *TGK*.

وينفذ بروتوكول MIKEY-PS أو MIKEY-DHHMAC بين النقطتين الطرفيتين B وA، مما يسمح لهما بالحصول على مفتاح *TGK* وحساب مفاتيح الدورة SRTCP/SRTP. ويطبق البروتوكولان SRTP وSRTCP مفاتيح الدورة من طرف إلى طرف هذه.

الملاحظة 1 – يوفّر بروتوكول MIKEY جميع المعلَمات اللازمة لبروتوكول SRTP (الخوارزمية، أطوال المفتاح، أجل المفتاح، إلخ) كجزء من سياسات تسيير MIKEY.

ولا تشارك الحارسات البوابية بنشاط في معالجة MIKEY وتعملن كمخزن مرحل لإحالة رسائل MIKEY المغلقة.

والإجراء المماثل في حالة إنشاء النداء الصادر عن النقطة الطرفية A في الاتجاه المعاكس على اعتبار أن النقطة الطرفية A هي الممهد والنقطة الطرفية B هي المقصد.

الملاحظة 2 – يبيِّن الشكل 3 أيضاً دعم نموذج تشوير النداء بالتسيير المباشر مع حارس (حارسات) بوابي بدون تسيير. وفي بيئة التسيير المباشر هذه، ترسل رسائل تشوير النداء H.225.0 (Setup، إلخ) من طرف إلى طرف ضمن مجال H.323 دون أن يسيرها حارس بوابي. انظر التذييل II للاطلاع على الأشكال التي توضِّح كيفية استعمال H.235.4 لهذا الغرض.

الملاحظة 3 – يستعمل بروتوكول MIKEY مسجلات الوقت ضمن بروتوكول الأمن كوسيلة لضمان الحماية من إعادة تنفيذ رسالة إدارة المفاتيح. ويتطلب ذلك أن تكون ميقاتيات النقاط الطرفية متزامنة وقتياً على نحو ملائم نسبياً (ضمن حدود معقولة). ومن المعتقد أنه يمكن تحقيق هذا التزامن الوقتي باستعمال ميقاتيات زمنية مشَكَّلة يدوياً أو بروتوكول تزامن الشبكة (NTP RFC 1305 مثلاً). وينبغي أن يكون التزامن الوقتي، بحد ذاته، ممكناً في شبكات المنشآت على الأقل؛ انظر الفقرتان 4.5 و3.9 في الوثيقة RFC 3830.

الملاحظة 4 – لا يوصى بتركيبة البدء السريع والوسائط المتعددة المبكرة مع بروتوكول MIKEY-DHHMAC. وإذا كان البدء السريع والوسائط المتعددة المبكرة مطلوبة عندئذ ينبغي ألا تستعمل النقاط الطرفية MIKEY-DHHMAC بل بالأحرى MIKEY-PS.

الملاحظة 5 – يعتبر السيناريو بحارس بوابي واحد فقط حالة خاصة للسيناريو الممثَّل بعدد من الحارسات البوابية. وفي هذه الحالة ليس من الضروري القيام باكتشاف النقطة الطرفية للحارس البوابي البعيد بواسطة رسائل LCF/LRQ.

يرد فيما يلي المزيد من التفاصيل فيما يتعلق بتدفق الرسائل المرتبط بالسيناريو الوارد في الشكل 3، ويفترض هذا السيناريو حارس بوابي أو أكثر ضمن مجال H.323 حيث يجرى التسيير النفقي لرسائل H.245 ضمن H.225.0 ويطبق البدء السريع.

الملاحظة 6 – تغطي مخططات التدفق حالة التسيير المباشر أيضاً (مع حارس بوابي بدون تسيير) يتم فيها تبادل رسائل تشوير النداء H.225.0 مباشرة بين النقاط الطرفية دون أن يرسلها الحارس البوابي، انظر التذييل II.

ينشئ الإجراء الموصوف في هذه الفقرة سر متقاسم من طرف إلى طرف ZZ_{AB} بين النقطتين الطرفيتين A وb في H.323 أثناء المرحلة 1 وذلك باستعمال اتفاق مفتاح ديفي–هيلمان. وتطبق هذه الطريقة أثناء طور تسجيل وقبول RAS في H.225.0، وفي حالة وجود حارسات بوابية متعددة، أثناء تبادل رسائل **LCF/LRQ**. ويستعمل السر المتقاسم ديفي–هيلمان كمفتاح استيقان من طرف إلى طرف ويستمر طوال النداء. وينفذ بروتوكول MIKEY-PS (أو MIKEY-DHHMAC) بشكل منفصل أثناء المرحلة 2 خلال إنشاء النداء مما يسمح بإنشاء أسرار MIKEY تقوم على النداء من أجل القناة الحمالة.

يصف التذييل II الإجراء البديل والاختياري باستعمال إجراء DRC1 للتوصية H.235.4 بحيث يتمكَّن الحارس البوابي من توليد السر المتقاسم وتوزيعه على النقطتين الطرفيتين A وB.

يوضِّح المخطط الوارد في الشكل 4 أيضاً ملامح الأمن للخط الأساسي H.235.1 التي تؤمن في إطارها الرسالة بأسرها (الاستيقان والتكامل). بيد أن تدفق الرسائل يكون متماثلاً عندما يطبق خيار الاستيقان فقط لملامح أمن الخط الأساسي (غير مبيَّنة في الشكل). وفي هذه الحالة، لا تحسب شفرة HMAC على الرسالة بأكملها بل على جزء (**ClearToken** داخل **CryptoToken**) من الرسالة H.225.0/RAS.

ويوضِّح مثال تدفق الرسائل حالة النقطة الطرفية B (ممهد MIKEY) وهي تطلب النقطة الطرفية A (مستجيب MIKEY) باستعمال البدء السريع (انظر الشكل 4). والنقطتان الطرفيتان A وB في H.323 تبدآن بالتسجيل لدى حارس بوابي بواسطة الرسالة **RRQ** وتقدمان نصف مفتاحهما DH (g^a وg^b). وتستعمل العلامة **ClearToken** (ضمن العلامة **CryptoHashedToken**) لإرسال نصف مفتاح ديفي–هيلمان أثناء تبادل رسائل **RRQ** و**ACF**. ولهذا السبب ينبغي ألا يستعمل المجال **challenge**.

يُسيِّر نصف مفتاح ديفي–هيلمان في **dhkey** كجزء من **ClearToken**. يستعمل **ClearToken** معرِّف الغرض OID "TG" (انظر الفقرة 5.8) بدلاً من معرف الغرض "T" **ClearToken**، مشيراً بذلك إلى أن ملامح الأمن هذه جاري استعمالها إلى جانب H.235.1. يحتفظ الحارس البوابي بكل نصف مفتاح طالما كانت النقطة الطرفية مسجلة. وعندما تنفذ النقاط الطرفية إبقاء التسجيل أو استعمال إعادة تسجيل خفيفة الوزن (re-RRQ). ينبغي عليها عدم إدراج نصف مفتاح ديفي–هيلمان. ينبغي الإشارة إلى أن الحارس البوابي يدعم مواصفة الأمن هذه.

تحاول النقطة الطرفية B توجيه نداء إلى النقطة الطرفية A وتطلب القبول من الحارس البوابي D (**ARQ**). ينبغي على الرسالة **ARQ** أن تستعمل معرِّف الغرض TG في **ClearToken**. وينبغي أن يستعمل معرِّف الغرض "TG" هذا في جميع رسائل RAS في **ClearToken**.

يغطي السيناريو حارسات بوابية عديدة ومتسلسلة ولكنه يمكن أن يدعم حارس بوابي وحيد. ويتم اكتشاف النقطة الطرفية البعيدة وفقاً للفقرة 1.8 من التوصية H.323 "التشوير الاختياري بواسطة النقطة الطرفية الطالبة" وذلك باستعمال **LCF/LRQ**. ويتعلق الأمر بالطريقة التي تحدد بها النقطة الطرفية للمصدر موقع منطقة الحارس البعيد وتحصل بها على نصف مفتاح ديفي–هيلمان من النقطة الطرفية الطالبة المستهدفة. وإذا احتاج الحارس البوابي E إلى تحديد موقع منطقة الحارس البعيد، يقوم بإرسال رسالة **LRQ**. وفي حالة الإرسال المتعدد، ينبغي ألا يستعمل المعرِّف **generalID** في CryptoToken في الرسالة **LRQ**. وإذا كان الحارس D لا يدعم هذه الملامح، فإنه يعيد الرسالة **LRJ**. وإلا، فإنه يعيد الرسالة **LCF** متضمنة نصف مفتاح ديفي–هيلمان للنقطة الطرفية A. ثم يرد الحارس البوابي E برسالة **ACF** تتضمن نصف مفتاح ديفي–هيلمان للنقطة الطرفية A، وإذا لم يتمكن من تحديد م وقعها من النقطة الطرفية البعيدة A، عندئذ يقوم بإعادة الرسالة **ARJ**.

يؤمَّن الاتصال بين اثنتين من الحارسات البوابية وفقاً للتوصية ITU-T H.235.1. ولتحقيق هذه الغاية، يفترض تيسر سر متقاسم مشترك *sl*. ولما كانت الرسالة **LRQ** بين الحارسات البوابية تعتبر عادة رسالة توزيع متعدد، لا يمكن للسر المتقاسم *sl* أن يكون عادة سراً متقاسماً بين اثنين ولكن يفترض أن الأمر يتعلق بسر متقاسم بواسطة مجموعة داخل سحابة ممكنة من الحارسات البوابية. ويُحد هذا الافتراض من إمكانية التطور في الحالة العامة ولا يسمح باستيقان للمصدر. غير أن من المعتقد أن شبكات المنشآت تشتمل على عدد ضئيل من الحارسات البوابية المعروفة تماماً، ولذلك تبقى هذه القيود والحدود الأمنية مقبولة. ويسمح تأمين الاتصالات ذات التوزيع المتعدد بين الحارسات البوابية بواسطة التوقيع الرقمي بالتغلُّب على هذه القيود؛ غير أن هذه المسألة تتطلب المزيد من الدراسة.

تحصل النقطة الطرفية B على نصف مفتاح ديفي–هيلمان للنقطة الطرفية A (**ACF**). ينبغي أن تتضمن الرسالة **ACF** نصف مفتاح ديفي–هيلمان للنقطة الطرفية المطلوبة في dhkey ضمن الخط الأساسي **ClearToken** في H.235.1، ويستعمل هذا الأخيرة معرِّف الغرض "TG" وليس معرِّف الغرض "T". وينبغي أن تترك جميع المجالات الأخرى **ClearToken** كما هي من أجل مواصفة الأمن هذه.

الملاحظة 7 – تعمل النقاط الطرفية مع نصف مفتاح ديفي–هيلمان الذي يكون ساكناً طوال مدة التسجيل ولجميع النداءات. وينبغي ألا يعتبر هذا الإجراء بمثابة ضعف على المستوى الأمني حيث تطبق كل نقطة طرفية أنصاف مفاتيح ديفي–هيلمان عشوائية حقيقة.

بيد أن النقاط الطرفية ينبغي أن توفِّر قيمة عشوائية جديدة ذات 512 بتة (أي 64 أثمونة) داخل **challenge** في الوقت ذاته الذي يوفِّر فيه نصف مفتاح ديفي–هيلمان الخاص بها، انظر الفقرة 3.2 من الوثيقة RFC 2631. وقيم **challenge** هذه تقوم على النداء، وتسمح بأن يكون توليد مفاتيح ديفي–هيلمان بطريقة عشوائية في الوقت الفعلي، على النحو المطلوب.

عندئذ تكون النقطة الطرفية للمصدر B قادرة على حساب g^{ab} ثم السر المتقاسم الدينامي ZZ_{AB} بواسطة **challenge** عشوائي، مع الناتج الناشئ عند MIKEY-RRF (**challenge** || 0x12F905FE ,g^{ab}) (انظر الفقرات من 2.1.4 إلى 4.1.4 في RFC 3830). ويكون MIKEY قادراً على اشتقاق التجفير (*Me*) ومفاتيح الاستيقان (*Ma*) باستعمال MIKEY-PRF (انظر الفقرات من 2.1.4 إلى 4.1.4 في الوثيقة RFC 3830).

وخلال المرحلة 2، ينبغي أن تولِّد النقطة الطرفية للمصدر B مفتاحاً جديداً MIKEY *TGK* ثم تقوم بإنشاء رسالة MIKEY I Imsg، وفقاً لبروتوكول MIKEY-PS باستعمال *Me* و*Ma*؛ كما يمكن اشتقاق مفاتيح دورة SRTP انطلاقاً من مفتاح TGK على النحو الموصوف في الفقرة 3.4 من الوثيقة RFC 3711 (غير مبيَّنة في الأشكال).

وتكون رسالة MIKEY I_message مشفَّرة اثنينياً.

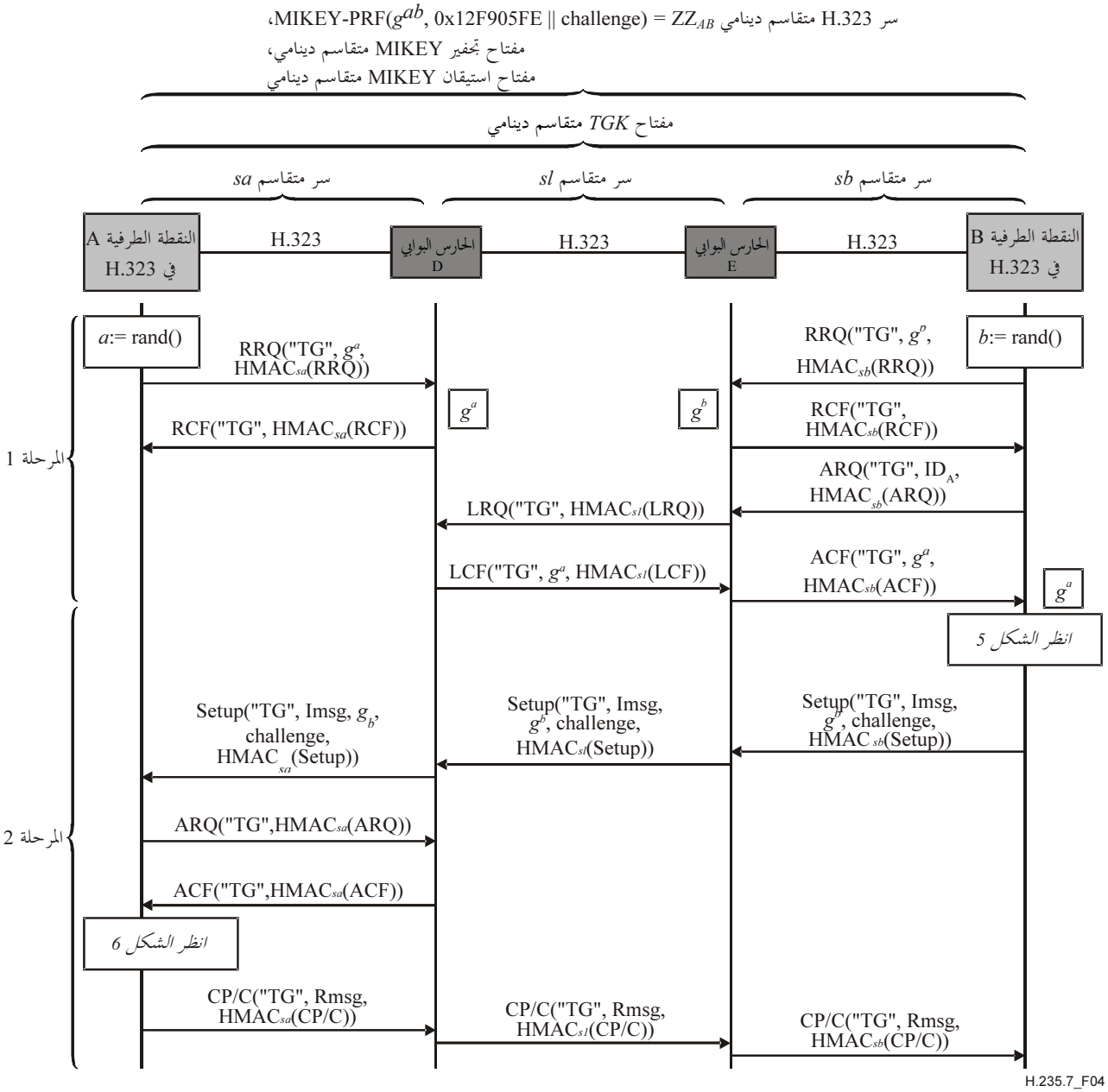
ينبغي أن تشتمل النقطة الطرفية للمصدر B دائماً على نصف مفتاحها DH في **dhkey** في علامة **ClearToken**، مما يسمح أيضاً بدعم نموذج التسيير المباشر مع الحارسات البوابية. وينبغي أن تدرج العلامة **ClearToken** في الرسالة Setup وينبغي أن ترسل إلى النقطة الطرفية القرينة A. ينبغي لحارس بوابي التسيير أن يرسل **ClearToken** المحوَّلة (بدون تعديل رسائل MIKEY) إلى القفزة التالية.

عندئذ تحسب النقطة الطرفية للمقصد A قيمة g^{ab} والسر المتقاسم الدينامي ZZ_{AB} انطلاقاً من MIKEY-PRF (**challenge** || 0x12F905FE , g^{ab}) (انظر الفقرات 2.1.4 إلى 4.1.4 من الوثيقة RFC 3830). تسمح الوظيفة MIKEY-PRF فيما بعد بحساب مفاتيح التجفير (*Me*) ومفاتيح الاستيقان (*Ma*) باستعمال MIKEY-PRF (انظر الفقرات من 2.1.4 إلى 4.1.4 في الوثيقة RFC 3830). عندئذ يمكن استرجاع مفاتيح TGK المحوَّلة.

وانطلاقاً من المفتاح *TGK*، يمكن أن تشتق النقطة الطرفية للمقصد A مفاتيح دورة SRTP على النحو الموصوف في الفقرة 3.4 من الوثيقة RFC 3711 (غير مبيَّنة في الأشكال).

يمكن للنقطة الطرفية A أن تبني رسالة _R مماثلة، Rmsg، ولكنها لا تستطيع أن تفعل ذلك إلا بناء على طلب النقطة الطرفية B أو عند الضرورة (DH). وتحوَّل هذه الرسالة _R في رسالة CallProceeding-to-Connect message (CP/C).

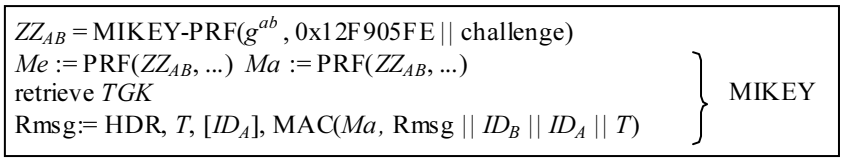
ترسل الرسالة CallProceeding-to-Connect إلى النقطة الطرفية B.



الشكل H.235.7/4 – مثال لمناداة النقطة الطرفية B للنقطة الطرفية A (التسيير بواسطة حارس بوابي) مع MIKEY-PS مسبق التقاسم

challenge:= rand()
ZZ_{AB} = MIKEY-PRF(g^{ab}, 0x12F905FE || challenge)
Me := PRF(ZZ_{AB}, ...), *Ma* := PRF(ZZ_{AB}, ...)
TGK := rand()
I := HDR, *T*, challenge, [ID_B], {*SP*}, ENC$_{Me}$(*TGK*)
Imsg:= *I*, MAC(*Ma, I*)
} MIKEY

الشكل H.235.7/5 – معالجة التقاسم المسبق MIKEY بواسطة النقطة الطرفية B



الشكل H.235.7/6 – معالجة التقاسم المسبق MIKEY بواسطة النقطة الطرفية A

1.8 إنهاء نداء H.323

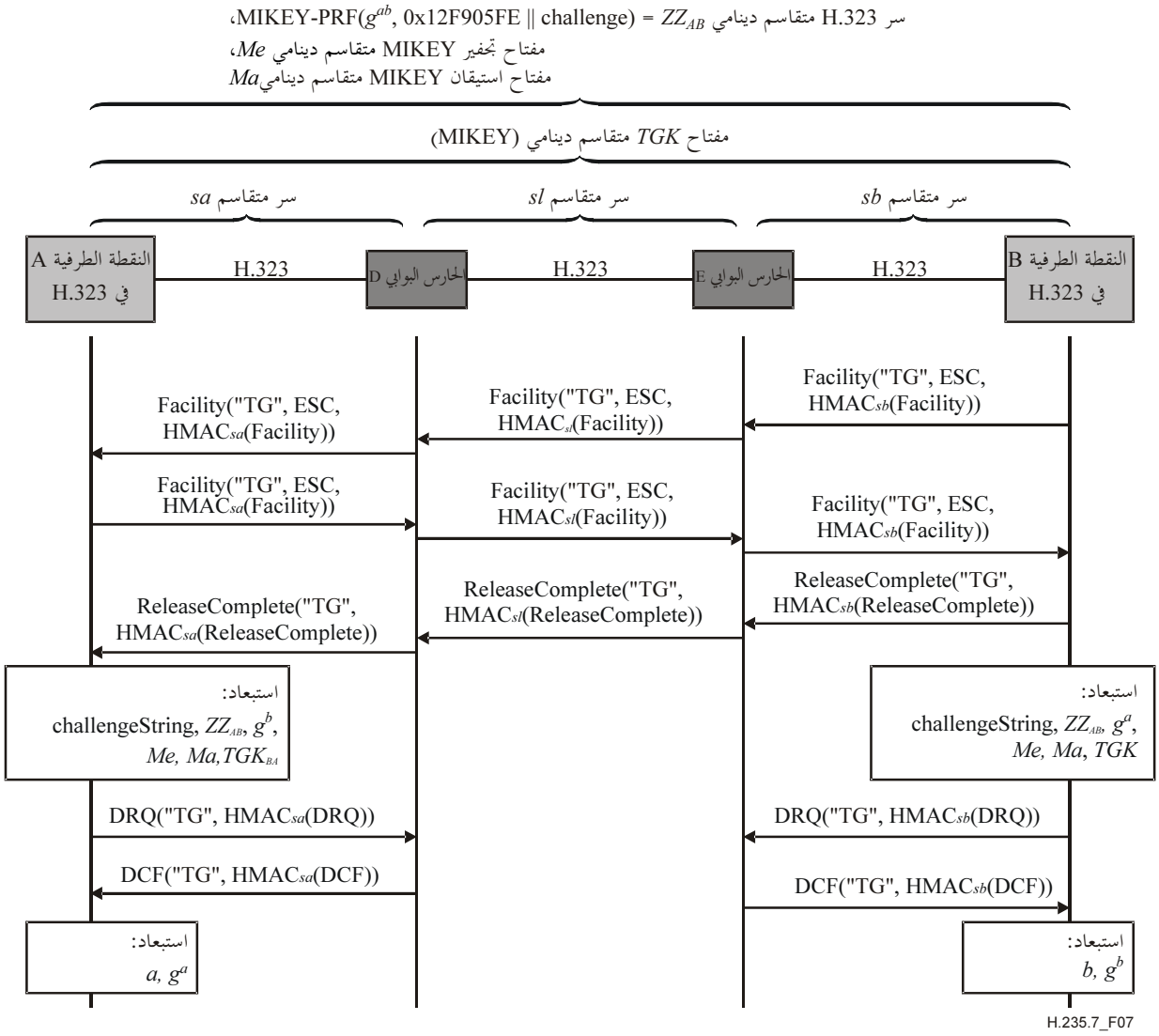
لما كانت النقاط الطرفية المعنية تحتفظ بالحالة للبروتوكولين MIKEY وSRTP، من الأساسي وجود إجراء خاص للإنهاء. ويورد الشكل 7 مثالاً لتدفق الرسائل في حالة إنهاء النقطة الطرفية B (ممهد MIKEY) لنداء معين. ويكون التدفق أساساً وفقاً للفقرة 5.8 من التوصية ITU-T H.323 "الطور E – إنهاء النداء".

ملاحظة – يبيِّن الشكل 7 إجراءات الانسحاب الاختيارية لهذه الحالة التي تلغى فيها النقاط الطرفية تسجيلها تماماً. عندئذ ينبغي أن تستبعد النقاط الطرفية المفتاح الخصوصي DH (a أو b) ونصف المفتاح DH العمومي (g^a أو g^b) أيضاً.

ولما كان إجراء إنهاء نداء معين مستقلاً عن مواصفة الأمن هذه، يمكن استعمال أي معرِّف للغرض منطبق على مواصفة الأمن الكامنة (H.235.1، H.235.3)؛ ومن ثم لا يشير الشكل 7 على أي معرِّف للغرض.

وإذا سجلت النقطة الطرفية مجدداً لدى حارس بوابي، ينبغي عندئذ توليد نصف مفاتيح جديدة ديفي–هيلمان. بيد أن إلغاء التسجيل الكامل غير ضروري في أي ظرف من الظروف لمجرد إنهاء النداء. قررت النقطة الطرفية أن تبقى مسجلة لدى الحارس البوابي، يمكن مواصلة استعمال نصف مفاتيح ديفي–هيلمان السكونية.

وفي الحالة التي تبقى فيها النقاط الطرفية مسجلة و لم يطبق الانسحاب، ينبغي أن تستبعد النقاط الطرفية المعلومات المرتبطة بالنداء فحسب، بما في ذلك نصف مفاتيح ديفي–هيلمان القرينة، **challenge**، ومفاتيح MIKEY، *Me* و*Ma* و*TGK* ومعلومات الدورة SRTP ذات الصلة.



الشكل H.235.7/7 – مثال لنقطة طرفية B تنهي نداء

2.8 إعادة حساب المفتاح TGK وتحديث حزمة CSB

يدعم بروتوكول MIKEY ذاتياً إعادة حساب مفتاح TGK و/أو تحديث معلومة CSB. وينبغي أن تستعمل مواصفة هذه التوصية إجراء MIKEY-PS الوارد في الفقرة 5.4 من الوثيقة RFC 3830، أو في حالة السر التام نحو الأمام، تسمح الفقرة 1.3 من الوثيقة RFC zzzz لهذا الغرض بتحديث مفتاح TGK قبل انقضائه أو تحديث المعلومات الأخرى بدون تعديل مفتاح TGK.

وتفيد آلية إعادة حساب مفتاح TGK وتحديث حزمة CSB في حماية حزمة من القنوات المنطقية بموجب السياسة الأمنية ذاتها. ولتحقيق هذا الغرض، يوصى بتنفيذ بروتوكول MIKEY مسبق التقاسم (بالكامل) على النحو الموصوف في الفقرة 8 من أجل القناة المنطقية الأولى فقط. وينبغي على أي قناة منطقية لاحقة تطبق آلية السياسة الأمنية MIKEY ذاتها أو مفتاح TGK ذاته، أن تستعمل آلية تحديث CSB بدون آلية إعادة حساب مفتاح TGK الواردة في هذه الفقرة وذلك بالإشارة على معرِّف CSB للمصدر مع حذف بيانات تحديث مفتاح TGK. ويسمح ذلك بإنشاء قنوات منطقية أو دورات تحفير MIKEY بطريقة أكثر فعالية مما يسمح به التنفيذ التام لبروتوكول MIKEY لكل قناة منطقية.

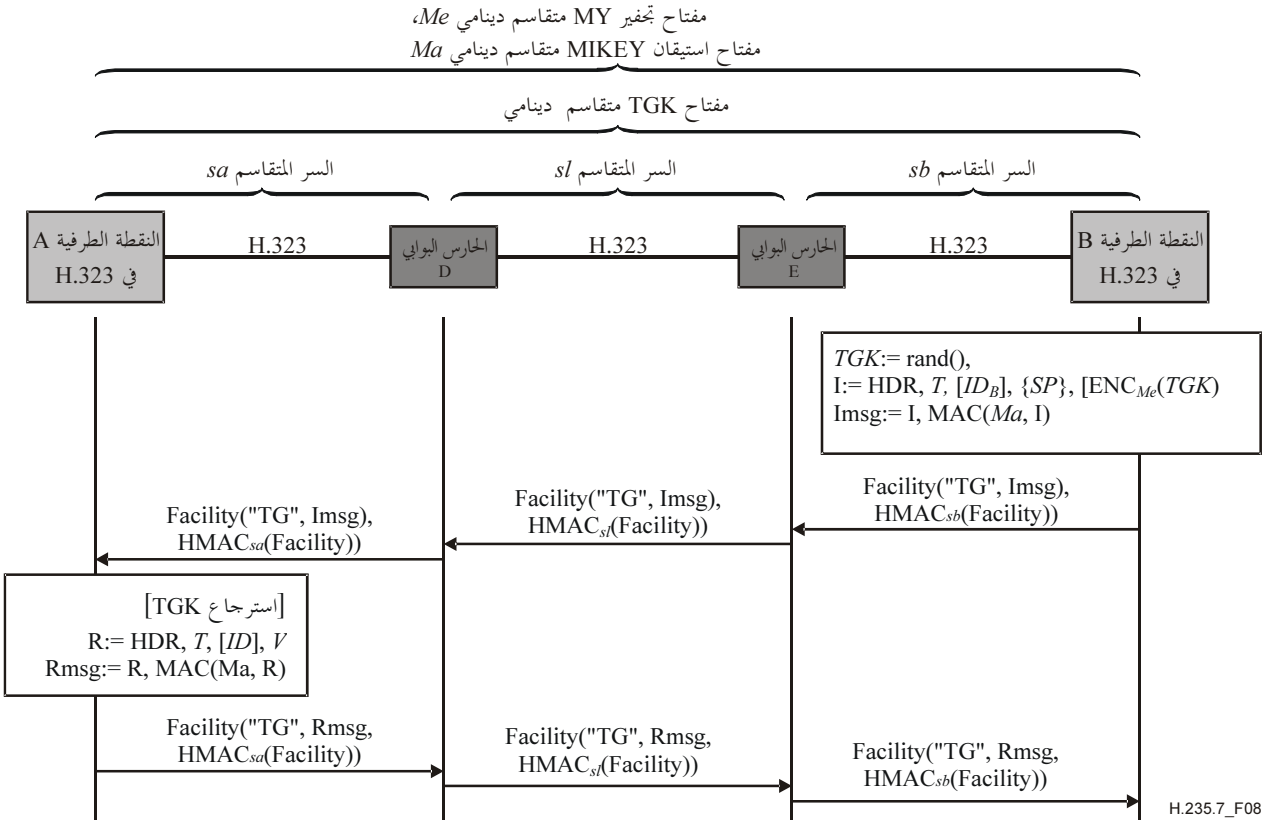
ينبغي تغليف رسائل إعادة حساب مفتاح MIKEY TGK أو رسائل تحديث CSB وتسير في **MiscellaneousCommand** ضمن رسالة Facility. ويضبط **tokenOID** الخاص بالعلامة **ClearToken** على "TG".

إذا نفذ بروتوكول MIKEY على "مستوى الوسائط"، ينبغي أن تحدد النقطة الطرفية B القناة المنطقية التي يتعين تطبيق إعادة حساب مفتاح TGK عليها و/أو تحديث CSB. وتستعمل النقطة الطرفية A بوصفها المستجيب أيضاً **MiscellaneousCommand** في Facility لتسيير رسالة MIKEY R_message (إن وجدت).

ولإعادة حساب مفتاح TGK (انظر الشكل 8)، ينبغي أن تولِّد النقطة الطرفية بوصفها المصدر MIKEY مفتاحاً جديداً TGK.

ويمكن أن تؤكد النقطة الطرفية A بوصفها المستجيب رسالة إعادة حساب مفتاح TGK الناتجة عند الضرورة بناءً على طلب النقطة الطرفية B. وتقوم النقطة الطرفية A بإنشاء رسائل R_messages ضمن رسالة Facility نحو النقطة الطرفية A.

ولتحديث CSB، يعتبر الإجراء مماثل للإجراء الوارد أعلاه باستثناء أن رسالة MIKEY ينبغي ألا تتضمن مفتاح TGK.



الشكل H.235.7/8 – مثال لنقطة طرفية B تقوم بتحديث مفتاح

ملاحظة – تعتبر الرسالة Facility لتأكيد النقطة الطرفية A عند النقطة الطرفية B اختيارية وهي ليست ضرورية سوى في حالة ما إذا طلبت النقطة الطرفية B أيضاً رسالة تحقق MIKEY R_message بواسطة راية V في MIKEY HDR.

ولا تحدد هذه التوصية أية إجراءات في حالة تمسك المستجيب بإعادة حساب مفتاح TGK و/أو تحديث CSB؛ وتقتضي هذه المسألة المزيد من الدراسة.

3.8 دعم التمرير النفقي H.245

وإذا اقتضى الأمر إضافة قنوات منطقية أخرى أثناء دورة ما، ينبغي تنفيذ أسلوب التمرير النفقي الوارد في H.245، التي تسير فيها رسائل H.245 النفقية في الرسالة Facility.

4.8 خوارزميات SRTP

تستعمل هذه المواصفة الأمنية خوارزمية HMAC-SHA1-32 المبتورة مع طول واسم استيقان *n_tag* يساوي 32 بتة باعتباره خوارزمية استيقان بالتغيب لبروتوكول RTP. وينبغي دعم أطوال واسم الاستيقان أخرى على غرار تلك المحددة في الوثيقة RFC 3711 كما ينبغي التفاوض بشأنها بواسطة السياسة الأمنية MIKEY وفقاً للاحتياجات.

5.8 قائمة معرِّفات الغرض

"TG"	{التوصية (0) itu-t (0) h (8) 235 (0) الطبعة 70 3 (0)}	تشير إلى علامة **ClearToken** للخط الأساسي H.235 في سياق هذه التوصية. ويشير معرِّف الغرض هذا أيضاً إلى أن السر المتقاسم ZZ_{AB} يحسب أيضاً بواسطة الوظيفة MIKEY-PRF.

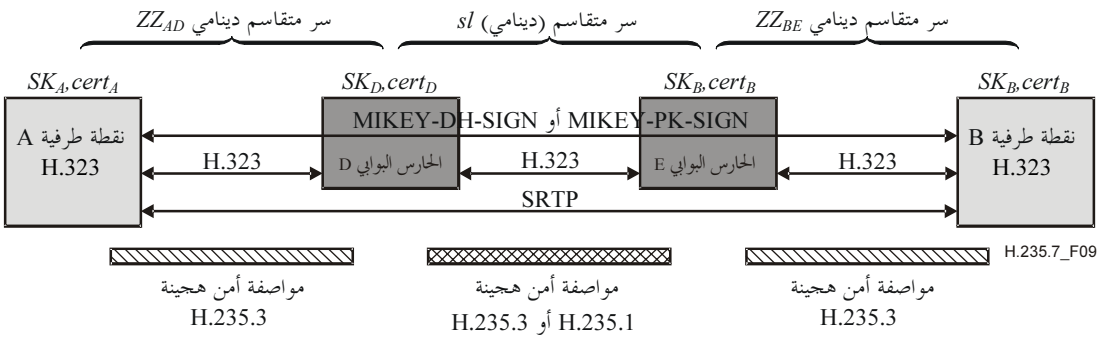
9 ملامح الأمن باستعمال تقنيات الأمن اللا تناظري

تصف هذه الفقرة ملامح الأمن الخاصة بهذه التوصية التي تنفذ في إطارها تقنيات الأمن اللا تناظري. ويتيح هذا السيناريو إمكانية تدرج أكبر.

قد لا يكون وجود كيانات وسيطة (أي حارسات بوابية) قادرة على اعتراض مفتاح MIKEY TGK و/أو مفاتيح دورة SRTP، مقبول دائماً. ويبيِّن الشكل 6 أدناه سيناريو لبنية تحتية لمفتاح عمومي (PKI) لإنشاء مفاتيح وسيطة SRTP كاملة من طرف إلى طرف.

الافتراضات: يفترض أن كلتا النقطتين الفرعيتين A وB تمتلكان مفتاحاً خصوصياً وكذلك مفتاح عمومي معتمد (*Cert*). بيد أن النقطة الطرفية A والحارس البوابي E والنقطة الطرفية B والحارس البوابي D يمكن أن يتقاسما السر المتقاسم (المدار/المشكل) في حالة ما إذا كانت الرسائل RAS وتشوير النداء H.225.0 مؤمَّنة بواسطة H.235.1. ويفترض أيضاً أن النقطة الطرفية A والنقطة الطرفية B متزامنتين وقتياً على نحو مناسب، وخلاف ذلك لا يمكن تنفيذ بروتوكول MIKEY بطريقة آمنة.

ويمكن إنجاز رسالة الاستيقان/التكامل إما باستعمال السر المتقاسم قفزة–قفزة مسبق التشكيل (*sa* و*sb* و*sl*) ومواصفة خط الأمن الأساسي H.235.1، أو بطريقة أعم، مع بنية تحتية PKI لإنشاء أسرار متقاسمة دينامية مع ملامح الأمن الهجينة H.235.3.



الشكل H.235.7/9 – سيناريو من طرف إلى طرف باستعمال البنية التحتية PKI (حارسات بوابية متعددة)

النقطتان الطرفيتان A وB تنفذان بروتوكول MIKEY-PK-SIGN أو بروتوكول MIKEY-DH-SIGN من طرف إلى طرف، مما يسمح لهما بإنشاء مفتاح MIKEY TGK وتحسب انطلاقاً من هذا المفتاح الأنظمة الطرفية مفاتيح دورة SRTP.

الملاحظة 1 – يستوفي بروتوكول MIKEY-PK-SIGN متطلبات إدارة المفاتيح القائمة على خوارزمية RSA.

الملاحظة 2 – من المؤكد أن استعمال تقنيات PKI يتكيف على نحو أفضل مع بيئة H.323 العامة التي يوجد فيها عدد من الحارسات البوابية بالتسلسل، من البنى التحتية المحدودة والأقل تدرجاً باستعمال تقنيات الأمن المتناظرة.

الملاحظة 3 – لا يوصى بالجمع بين البدء السريع والوسيط المبكر مع بروتوكول MIKEY-DH-SIGN. وإذا كانت البدء السريع والوسيط المبكر مطلوبين عندئذ ينبغي ألا تستعمل النقاط الطرفية MIKEY-DH-SIGN بل MIKEY-PK-SIGN بالأحرى.

تقدم الفقرات التالية مزيداً من التفاصيل بشأن تدفق الرسائل الواردة في الشكل 9. ويبيِّن هذا السيناريو حارسات بوابية متعددة ضمن مجال H.323.

تفترض الأشكال التالية وجود حارس بوابي للتسيير (نموذج حارس بوابي للتسيير) حيث ترسل رسائل H.235 في نفق ضمن H.225.0 (بدء سريع).

الملاحظة 4 – تغطى مخططات تغطي مخططات التدفق حالة التسيير المباشر أيضاً (مع حارس بوابي بدون تسيير) يجرى في إطارها تبادل رسائل تشوير النداء H.225.0 بطريقة مباشرة بين النقطتين الطرفيتين بدون أن يرسلها أي حارس بوابي.

ويبيِّن الشكل أيضاً ملامح الأمن الهجينة H.235.3 حيث يجرى تأمين رسائل RAS الأولية بالكامل (الاستيقان والتكامل) باستعمال التوقيعات الرقمية والشهادات الاختيارية. ويتعلق الأمر بإنشاء أسرار متقاسمة دينامية ZZ_{BE} وZZ_{AD} بين النقاط الطرفية والحارس البوابي للقفزة التالية، مما يجعل الأسرار المتقاسمة السكونية زائدة عن الحاجة. ومع ذلك، يكون تدفق الرسائل مماثلاً عندما يطبق خيار الاستيقان فقط على ملامح أمن التوقيعات (غير مبيَّنة).

ويوضح مثال تدفق الرسائل حالة النقطة الطرفية B (ممهد MIKEY) توجه نداءً إلى النقطة الطرفية A (مستجيب MIKEY) (انظر الشكل 10).

وخلال المرحلة 1، تبدأ النقاط الطرفية H.323 بالتسجيل لدى الحارس البوابي للقفزة التالية وتقدم نصف مفتاحها (g^a وg^b).

وتحاول النقطة الطرفية B نداء النقطة الطرفية A، ولذلك تطلب القبول من الحارس البوابي E. وتستطيع النقطة الطرفية B أن تطلب شهادة من نظيرها *CertC* وذلك بإدراج عنصر الملامح الأمنية في **ClearToken** إذا لم يكن في حوزتها معلومات الشهادة. وينبغي أن يستعمل عنصر ملامح الأمن المجالات التالية:

- يوضع **elementID** على 7 للإشارة إلى عنصر طلب الشهادة؛ يوضح الشكل 10 ذلك بواسطة CertFlag؛
- تبقى **paramS** غير مستعملة؛
- يشتمل **element** على عنصر حيث توضع **flag** على TRUE.

تؤمِّن رسائل ARQ ورسائل RAS وتشوير النداء في التوصية H.225.0 التالية بواسطة السر المتقاسم الديناميي ZZ_{BE} عن طريق ملامح الأمن الأساسية H.235.1. إذا طلبت النقطة الطرفية B البحث عن الشهادات، يقوم الحارس البوابي E باستخلاص CertC من قائمة الشهادات المحلية أو غيرها ويقدم النتيجة (النتائج) كجزء من رسالة ACF في **certificate**، **ClearToken** ويقوم بإدراج عنصر ملامح الأمن. وينبغي أن يستعمل هذا العنصر المجالات التالية:

- يوضع **elementID** على 8 للإشارة إلى عنصر استجابة الشهادة؛ يوضِّح الشكل 10 ذلك بواسطة certFlag؛
- تبقى **paramS** غير مستعملة؛
- يشتمل **element** على عنصر حيث توضع **flag** على TRUE.

في حالة ما إذا حصل الحارس البوابي على شهادات متعددة من نقطة طرفية/UA قرينة، تتضمن الرسالة ACF في الواقع عدة علامات ClearToken، تتضمن كل منها شهادة واحدة في **certificate**. عندئذ تختار النقطة الطرفية ما يناسبها. بيد أنه قد يستغرق البحث عن الشهادات وقتاً طويلاً، وهو ما يحدث في حالة الاتصال بالأدلة الخارجية. وإذا لم يتمكن الحارس البوابي من

تقديم الشهادة (الشهادات) في الوقت المناسب، أو تقديمها على الإطلاق، تعاد الرسالة ACF مع **certificate** خالية في **ClearToken** الذي يتضمن عنصر ملامح الأمن حيث:

- يوضع **elementID** على 8 للإشارة إلى عنصر استجابة الشهادة.
- تبقى **paramS** غير مستعملة؛
- يشتمل **element** على عنصر حيث توضع **flag** على FALSE.

وتقع على النقطة الطرفية عندئذ مهمة إما التخلي أو محاولة تحديد موقع الشهادة المناسبة بوسائل غير محددة في هذه التوصية. وإذا كان الحارس البوابي قادراً على الحصول على شهادة خارج الفترة الزمنية اللازمة للاستجابة، ينبغي أن يشير الحارس البوابي إلى هذه الحالة بترك **certificate** خالية وبإدراج عنصر ملامح الأمن في ClearToken حيث:

- يوضع **elementID** على 8 للإشارة إلى عنصر استجابة الشهادة؛
- تبقى **paramS** غير مستعملة؛
- يشتمل **element** على عنصر وتوضع **flag** على TRUE.

وفي هذه الحالة ينبغي أن يعيد الحارس البوابي ClearToken في رسالة ACF.

وأثناء المرحلة 2، تكون النقطة الطرفية للمصدر B (ممهد MIKEY) قادرة على توليد مفتاح جديد MIKEY TGK وعلى حساب رسالة MIKEY I، Imsg المرتبطة بها وذلك بتطبيق بروتوكول إدارة مفاتيح MIKEY-PK-SIGN (انظر الشكلان 11 و12) أو إذا تعلَّق الأمر بسر تام نحو الأمام، بروتوكول إدارة المفاتيح MIKEY-DH-SIGN (ديفي–هيلمان مع التوقيعات الرقمية). ويتاح MIKEY-DH-SIGN كخيار.

ويمكن الحصول على مفاتيح دورة بروتوكول SRTP انطلاقاً من مفتاح TGK الموصوف في الفقرة 3.4 من الوثيقة RFC 3711 (غير مبيَّنة في هذه الأشكال).

الملاحظة 5 – يوضِّح الشكلان 11 و12 جزئياً بروتوكول MIKEY، وبعض الأجزاء غير مبيَّنة في الصورة.

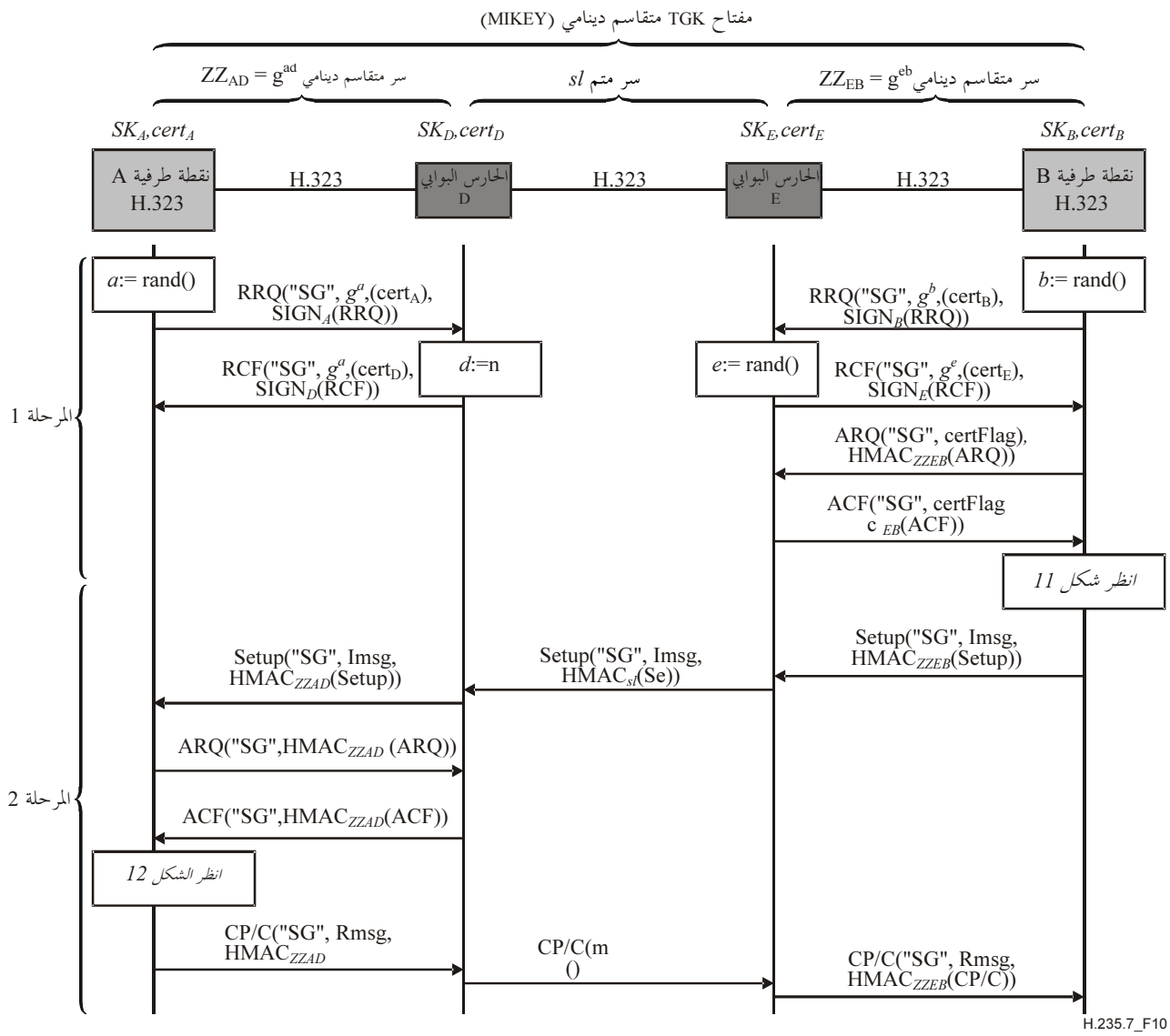
الرسالة MIKEY I_message مجفرة اثنينياً ثم تغلف في **OpenLogicalChannel** وفقاً للتوصية ITU-T H.245.

تدرج **ClearToken** في الرسالة Setup وترسل إلى النقطة الطرفية A. يعيد الحارس البوابي للتسيير إرسال رسالة MIKEY I_message (بدون تعديل رسالة MIKEY) إلى القفزة التالية.

وفي حالة وجود حارسات بوابية عديدة للتسيير، يمكن تأمين رسائل تشوير النداء بين الحارسات البوابية وذلك بتطبيق السر المتقاسم الإداري واستعمال التوصية ITU-T H.235.1 أو ITU-T H235.3 والمفاتيح العمومية/الخصوصية.

ومن ثم تكون النقطة الطرفية A قادرة على اشتقاق مفاتيح الدورة SRTP على النحو الموصوف في الفقرة 3.4 من الوثيقة RFC 3711 (غير مبيَّنة في الأشكال).

وتكون النقطة الطرفية A بوصفها مستجيب MIKEY قادرة على تجميع الرسالة MIKEY R_message، Rmsg، باستعمال مفتاح MIKEY *Ma* وإدراجه في الرسالة CallProceeding-to-Connect (CP/C).



الشكل H.235.7/10 – مثال لنقطة طرفية B توجه نداء إلى النقطة الطرفية A
(تسيير بواسطة حارسات بوابية متعددة) مع MIKEY-PK-SIGN

TGK := rand()
env-key:= rand()
Me, Ma := PRF(env-key,…|| Rand)
PKE := ENC_{PK-A}(env-key,…|| Rand)
K := ENC_{Me}(*ID*$_B$ || [*TGK*])
KEMAC:= ENC_{Me}(*ID*$_B$ || [*TGK*])
M := HMAC-SHA1(Ma, K)
I:= HDR, *T*, rand(), [*ID*$_B$ | *Cert*$_B$], {*SP*}, [chash], *KEMAC*, *PKE*
Imsg:= *I*, $Sign_{SK-B}$(*I*)

الشكل H.235.7/11 – معالجة MIKEY-PK-SIGN بواسطة النقطة الطرفية B

Retrieve env-key, TGK
Ma := PRF(env-key,…|| Rand),
Rmsg:= HDR, *T*, [ID_A], HMAC-SHA1(Ma, Rmsg || ID_A || ID_B || *T*)

الشكل H.235.7/12 – معالجة MIKEY-PK-SIGN بواسطة النقطة الطرفية A

يعتبر السيناريو بحارس بوابي وحيد حالة خاصة للسيناريو الممثل بحارسات بوابية متعددة. وفي هذه الحالة، ليس من الضروري القيام باكتشاف الحارس البوابي/النقطة الطرفية البعيدة بواسطة الرسائل LCF/LRQ.

1.9 إنهاء نداء H.323

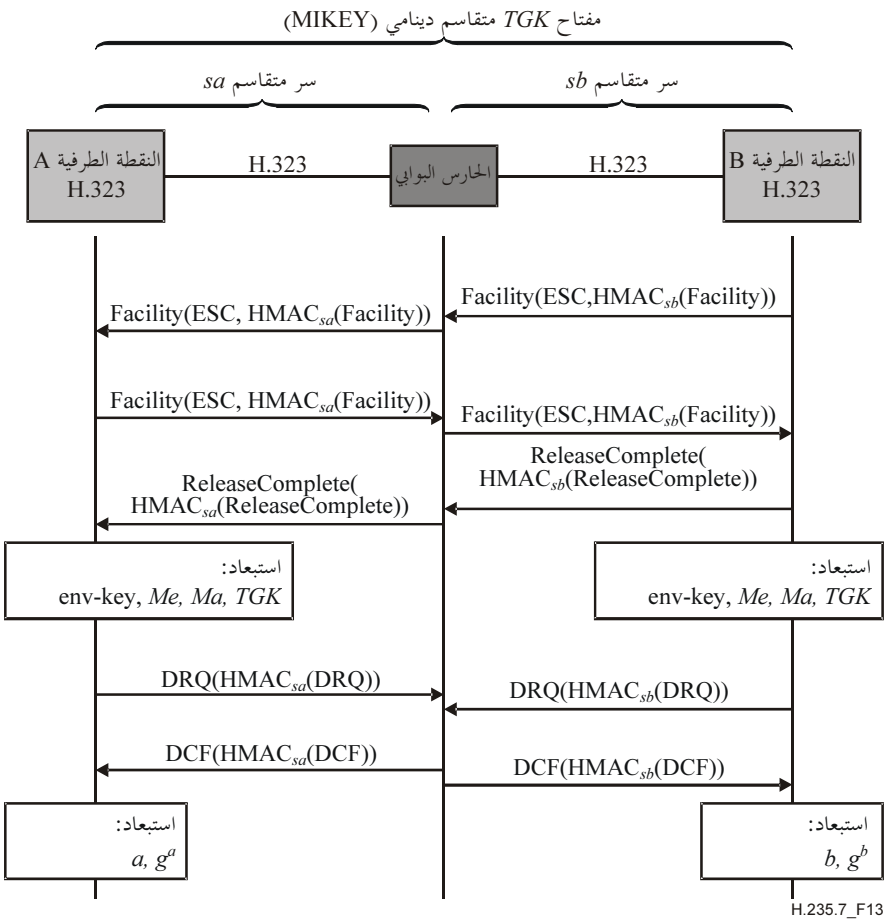
لما كانت النقاط الطرفية المعنية تحتفظ بحالتها للبروتوكولين MIKEY وSRTP، من الأساسي وضع إجراء خاص للإنهاء ويورد الشكل 13 مثالاً لتدفق الرسائل في حالة إنهاء النقطة الطرفية B (ممهد MIKEY)لنداء معين. ويتوافق التدفق، أساساً، مع الفقرة 5.8 من التوصية H.323 "الطور E، إنهاء النداء".

ملاحظة – يوضِّح الشكل 13 إجراءات الانسحاب الاختيارية لهذه الحالة، عندما تلغى النقاط الطرفية تسجيلها تماماً. عندئذ ينبغي أن تستبعد النقاط الطرفية المفتاح الخصوصي DH (a أو b) ونصف المفتاح العمومي DH (g^a أو g^b).

ولما كان إجراء إنهاء نداء معين مستقلاً عن ملامح الأمن هذه، يمكن استعمال أي معرِّف غرض OID ينطبق على ملامح الأمن الكامنة؛ وبالتالي لا يبيِّن الشكل 13 أي معرِّف غرض.

إذا سجلت نقطة طرفية مجدداً مع حارس بوابي، ينبغي توليد نصف مفاتيح جديدة. بيد أن إلغاء التسجيل التام غير ضروري في جميع أحوال إنهاء النداء. إذا قررت النقطة الطرفية أن تبقى مسجلة لدى الحارس البوابي، يمكن مواصلة استعمال نصف مفاتيح DH السكونية.

وفي الحالة التي تبقى فيها جميع النقاط الطرفية مسجلة، ولم يطبق الانسحاب، ينبغي أن تستبعد النقاط الطرفية المعلومات المرتبطة بالنداء، بما في ذلك نصف مفاتيح ديفي–هيلمان القرينة، **challenge**، مفاتيح MIKEY، *Me*، *Ma*، *TGK* ومعلومات الدورة SRTP ذات الصلة.



الشكل H.235.7/13 – مثال لنقطة طرفية تنهي نداء

2.9 إعادة حساب مفتاح TGK وتحديث حزمة CSB

يدعم بروتوكول MIKEY ذاتياً إعادة حساب مفتاح TGK و/أو تحديث معلومات حزمة CSB. ولتحقيق هذه الغاية، ينبغي استعمال إجراء MIKEY-PK-SIGN الوارد في الفقرة 4.5 من الوثيقة RFC 3830، الذي يسمح بتحديث مفتاح TGK قبل انقضاء أجله أو تحديث المعلومات الأخرى (CSB) بدون تغيير TGK.

وتفيد آلية إعادة حساب مفتاح TGK وتحديث حزمة CSB في حماية مجموعة من القنوات المنطقية ذات الصلة بالسياسة الأمنية ذاتها. ولتحقيق هذه الغاية، يوصى بتنفيذ بروتوكول MIKEY-PK-SIGN (تماماً) على النحو الموصوف في الفقرة 8 من أجل القناة المنطقية الأولى فقط. وينبغي على أي قناة منطقية لاحقة أن تطبق آلية تحديث CSB بدون إعادة حساب مفتاح TGK الواردة في هذه الفقرة وذلك بالإشارة على معرِّف الحزمة CSB الأولية وحذف بيانات تحديث مفتاح TGK. ويسمح ذلك بإنشاء قنوات منطقية أو دورات تجفير MIKEY بطريقة أكثر فعالية مما يسمح به التنفيذ التام لبروتوكول MIKEY لكل قناة منطقية.

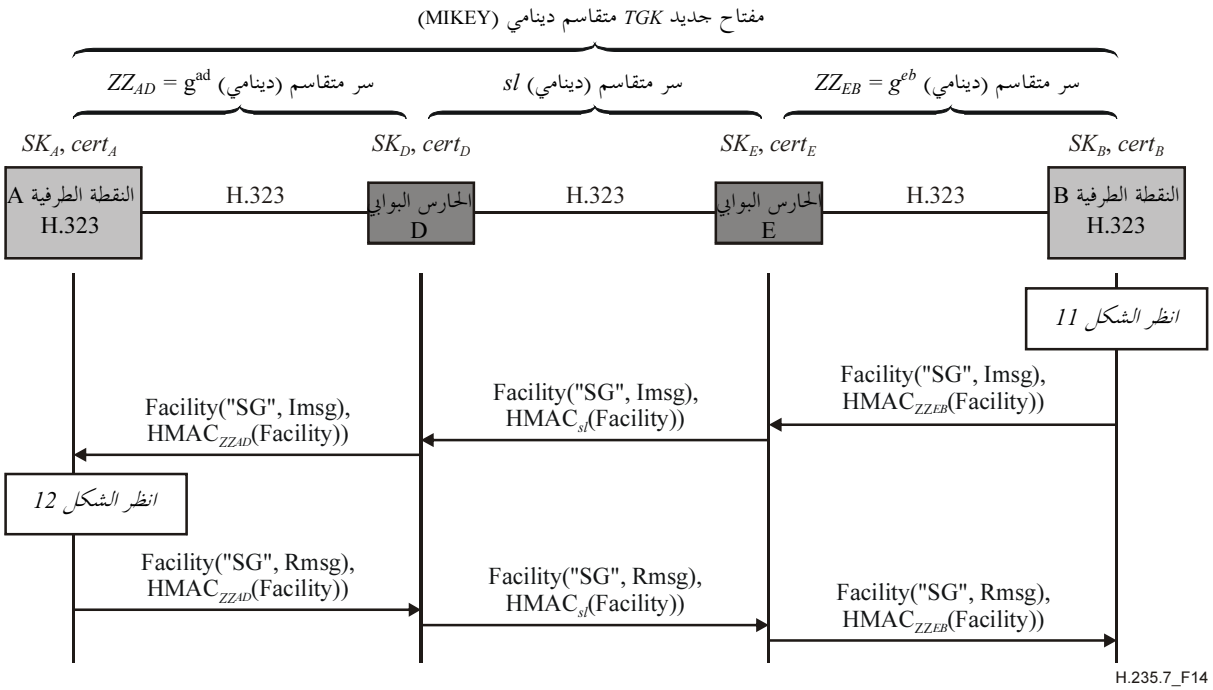
وينبغي أن تدرج رسائل حساب مفتاح TGK أو رسائل تحديث MIKEY CSB في الأمر **MiscellaneousCommand** لرسالة Facility. ويوضِّح المعرِّف **tokenOID** التابع للعلامة **ClearToken** على "SG".

وإذا نفذ بروتوكول MIKEY على "مستوى متعدد الوسائط"، ينبغي أن تحدد النقطة الطرفية B القناة الم نطقية التي يجدر تطبيق إعادة حساب مفتاح TGK عليها و/أو تحديث حزمة CSB. وتستعمل النقطة الطرفية A بوصفها المستجيب وكذلك الأمر **MiscellaneousCommand** في Facility لتسيير رسالة MIKEY R_message (إن وجدت).

ولإعادة حساب مفتاح TGK (انظر الشكل 14)، ينبغي أن تولِّد النقطة الطرفية B بوصفها الممهد مفتاحاً جديداً TGK. وينبغي أن تتضمن **mikey**، رسالة MIKEY I_message المقابلة.

ويمكن أن يؤكد المستجيب (النقطة الطرفية A) رسالة إعادة حساب مفتاح TGK الناتجة عند الضرورة بناءً على طلب النقطة الطرفية B. وتقوم النقطة الطرفية A بإنشاء رسالة R_message مماثلة، Rmsg. وترسل هذه الرسالة R_message ضمن رسالة Facility. Rmsg هي رسالة استجابة MIKEY المقابلة وينبغي تسييرها في **octetString** للمعلَمة **GenericParameter**. وترسل النقطة الطرفية A رسالة Facility إلى النقطة الطرفية B.

ولتحديث حزمة CSB التي يطلقها الممهد، يعتبر الإجراء مماثلاً للإجراء الوارد أعلاه باستثناء أن رسالة MIKEY ينبغي ألا تتضمن مفتاح TGK (انظر الشكل 14).



الشكل H.235.7/14 – مثال لنقطة طرفية B (الممهد) تقوم بإعادة حساب مفتاح TGK وتحديثه

ملاحظة – تعتبر الرسالة Facility لتأكيد النقطة الطرفية A عند النقطة الطرفية B اختيارية وهي ليست ضرورية سوى في حالة ما إذا طلبت النقطة الطرفية B أيضاً رسالة تحقق (MIKEY I_message) باستعماله راية V في MIKEY HDR.

ولا تحدد هذه التوصية أية إجراءات في حالة تمسك المستجيب بإعادة حساب مفتاح TGK و/أو تحديث CSB؛ وتقتضي هذه المسألة المزيد من الدراسة.

3.9 دعم التسيير النفقي [إعادة الترزيم بهدف تحسين التسيير] التوصية H.245

إذا توجب إضافة قنوات منطقية أخرى أثناء دورة معينة، ينبغي تنفيذ أسلوب التسيير النفقي الوارد في التوصية H.245، حيث تجرى تسيير رسائل H.245 نفقية في إطار الرسالة Facility.

4.9 خوارزمية SRTP

ينبغي أن تستعمل هذه الملامح الأمنية طريقة HMAC-SHA1-32 المبتورة مصحوبة بطول واسم الاستيقان *n_tag* البالغ 32 بتة بوصفه خوارزمية استيقان بالتغيب لبروتوكول RTP. كما ينبغي دعم أطوال واسم استيقان أخرى على غرار تلك المحددة في الوثيقة RFC 3711 أيضاً وينبغي التفاوض بشأنها عن طريق ملامح السياسة الأمنية MIKEY وفقاً للاحتياجات.

5.9 قائمة معرِّفات الغرض

"SG"	{التوصية (0) itu-t (0) 235 (8) h (0) الطبعة 71 3 (0)}	تشير إلى ClearToken أساسية H.235.3 في سياق هذه التوصية

التذييل I

خيار MIKEY-DHHMAC

يصف هذا التذييل كيفية تنفيذ خيار إدارة المفاتيح MIKEY-DHHMAC في هذه الملامح الأمنية.

يفترض خيار إدارة المفاتيح هذا وجود بنية تحتية أمنية فقط تتيسر فيها المفاتيح المتقاسمة. ويتيح الخيار MIKEY-DHHMAC (RFC zzzz)، بوصفه أحد الملامح الأمنية، السر التام نحو الأمام (RFS) وذلك بسبب القدرة الملازمة لآلية ديفي–هيلمان. وهكذا، ينطبق خيار إدارة المفاتيح هذا عندما يطلب السر التام نحو الأمام (RFS) وعندما لا تتيسر البينة التحتية PKI أو الشهادات الرقمية.

ويفترض في هذا السياق وجود الحارسات البوابية ضمن مجال H.323.

والإجراء الموصوف في هذه الفقرة يفترض إنشاء سر متقاسم من طرف إلى طرف بين نقطتين طرفيتين A وB للتوصية H.323 باستعمال مخطط اتفاق مفاتيح ديفي–هيلمان. ويطبق هذا المخطط أثناء طور تسجيل RAS في H.225.0، أو في حالة وجود حارسات بوابية متعددة، أثناء تبادل رسائل LCF/LRQ بين الحارسات البوابية. ويفيد السر المتقاسم ديفي–هيلمان المولد كمفتاح استيقان من طرف إلى طرف ويستمر طوال فترة النداء. ويسمح بروتوكول MIKEY-DHHMAC المنفذ اتفاق إنشاء النداء، بإنشاء أسرار MIKEY القائمة على النداء من أجل القناة الحمالة.

يبيِّن الشكل 1.I مثالاً للنقطة الطرفية B توجه نداءً إلى النقطة الطرفية A عن طريق حارسات بوابية للتسيير. والتدفق مماثل للتدفق المبيَّن في الشكل 4 باستثناء تنفيذ بروتوكول MIKEY-DHHMAC، ويفترض السيناريو وجود حارس بوابي واحد أو أكثر للتسيير (نموذج حارس بوابي للتسيير)، حيث يجرى تسيير رسائل نفقية H.245 ضمن H.225.0 (بداية سريعة). وتمرير تشوير النداء يمكن أن يمر أو لا يمر عن طريق الحارس البوابي؛ ولذلك يعتبر الحارس البوابي للتسيير غير ضروري لدعم هذا السيناريو.

الملاحظة 1 – يغطي مخطط التدفق أيضاً حالة التسيير المباشر (مع حارسات بوابية بدون تسيير) يتم فيها تبادل رسائل تشوير النداء H.225.0 مباشرة بين النقاط الطرفية بدون أن تقوم الحارسات البوابية بإرسالها.

يوضِّح المخطط الوارد في الشكل 1.I أيضاً ملامح الأمن الأساسية H.235.1 حيث تؤمّن في إطارها كل رسالة بالكامل (الاستيقان والتكامل). ومع ذلك يكون تدفق الرسائل مماثلاً عندما يطبق خيار الاستيقان فقط لملامح الأمن الأساسية (غير مبيَّن في الشكل). وفي هذه الحالة، لا تحسب HMAC على الرسالة بأكملها بل بالأحرى على جزء (**ClearToken** ضمن **CryptoToken**) من رسالة RAS في H.225.0.

يطابق تدفق الرسائل المبيّن الحالة التي توجه فيها النقطة الطرفية B (ممهد MIKEY) نداءً إلى النقطة الطرفية A (مستجيب MIKEY) بواسطة البداية السريعة (انظر الشكل 1.I). وتبدأ النقطتان الطرفيتان A وb، أثناء المرحلة 1، بالتسجيل لدى الحارس البوابي بواسطة الرسالة **RRQ** وتقدمان نصف مفتاحهما DH (g^a وg^b). وينبغي استعمال **ClearToken** (ضمن **CryptoHashedToken**) لإرسال نصف مفتاح ديفي–هيلمان أثناء تبادل رسائل **ACF/RRQ**. ولهذا السبب، ينبغي عدم استعمال المجال **challenge**.

وينبغي تسيير نصف مفتاح ديفي–هيلمان في **dhkey** كجزء من **ClearToken**. ويستعمل ClearToken معرِّف OID "TG" (انظر الشكل 5.8) بدلاً من معرِّف الغرض "T" لعلامة ClearToken الخط الأساسي H.235.1، مشيراً إلى استعمال ملامح الأمن هذه إلى جانب ملامح H.235.1. ويحتفظ الحارس البوابي بكل نصف مفتاح طوال مدة تسجيل النقطة الطرفية. وعندما تنفذ النقاط الطرفية المحافظة على التسجيل أو تستعمل إعادة التسجيل المبسط (re-RRQ)، ينبغي عليها ألا تدرج نصف مفتاح ديفي–هيلمان. وينبغي أن تستعمل الرسالة **RCF** معرِّف الغرض "TG" ضمن ClearToken للإشارة إلى أن الحارس البوابي يدعم ملامح الأمن هذه.

تحاول النقطة الطرفية B مناداة النقطة الطرفية A، ولتحقيق ذلك، تطلب القبول من الحارس البوابي D (**ARQ**). ينبغي أن تستعمل الرسالة **ARQ** معرِّف هوية الغرض "TG" ClearToken. وينبغي أن يستعمل معرِّف هوية الغرض هذا "TG" في كل الرسائل الأخرى RAS ضمن ClearToken.

يغطي هذا السيناريو حارسات بوابية متسلسلة. وينبغي إجراء اكتشاف النقطة الطرفية البعيدة وفقاً للفقرة 6.1.8 من التوصية ITU-T H.323 "التشوير الاختياري بواسطة النقطة الطرفية المطلوبة" باستعمال الرسائل **LCF/LRQ**. وهذه هي الطريقة التي تحدد بها النقطة الطرفية الممهدة موقع منطقة الحارس البوابي البعيد وتحصل بذلك على نصف مفتاح ديفي–هيلمان من النقطة الطرفية المطلوبة المستهدفة. إذا احتاج الحارس البوابي E إلى تحديد موقع منطقة الحارس البوابي البعيد، عندئذ يرسل الحارس البوابي E رسالة **LRQ**. وفي حالة التوزيع المتعدد، ينبغي عدم استعمال المعرِّف generalID في CryptoToken الرسالة **LRQ**. وإذا كان الحارس البوابي D لا يدعم هذه الملامح، عندئذ يقوم بإعادة الرسالة **LRJ**. وفي حالة العكس، يعيد الحارس البوابي D الرسالة **LCF** متضمنة نصف مفتاح ديفي–هيلمان للنقطة الطرفية A. ويرد الحارس البوابي E برسالة **ACF** تتضمن نصف مفتاح ديفي–هيلمان للنقطة الطرفية A. أو إذا تعذَّر على الحارس البوابي A تحديد موقع النقطة الطرفية، فإنه يعيد الرسالة **ARJ**.

ينبغي أن تكون الاتصالات بين اثنين من الحارسات البوابية مؤمَّنة وفقاً للتوصية ITU-T H.235.1. ولتحقيق ذلك، يفترض تيسر سر متقاسم مشترك *sl*. ولما كانت الرسالة **LRQ** بين الحارسات البوابية رسالة توزيع متعدد عموماً، لا يمكن أن يكون السر المتقاسم *sl* سراً متقاسماً بين اثنين بل يفترض أن المر يتعلق بسر متقاسم قائم على مجموعة ضمن سحابة محتملة من الحارسات البوابية. ويحد هذا الافتراض من التطورية في الحالة العامة ولا يسمح بإجراء استيقان في المصدر. بيد أنه من المعتقد أن شبكات المنشآت تشتمل على عدد صغير من الحارسات البوابية المشهورة، ولذلك تعتبر هذه القيودات والتحديدات مقبولة. وتسمح الاتصالات المؤمَّنة بتوزيع متعدد بين الحارسات البوابية باستعمال التوقيعات الرقمية بالتغلب على هذه القيودات؛ ولا تزال هذه المسألة تتطلب المزيد من الدراسة.

تحصل النقطة الطرفية B على نصف مفتاح ديفي–هيلمان من النقطة الطرفية A. وينبغي أن يشتمل مفتاح ديفي–هيلمان على النقطة الطرفية المطلوبة في **dhkey** ضمن **ClearToken** في الخط الأساسي H.235.1، ولكن باستعمال المعرِّف OID "TG" بدلاً من "T". وينبغي عدم تعديل أي مجال آخر ضمن ClearToken بواسطة هذه الملامح الأمنية.

الملاحظة 2 – تشغل النقاط الطرفية مع نصف مفتاح ديفي–هيلمان وهو سكوني طوال فترة التسجيل ولجميع النداءات. ولا يتعلق الأمر بضعف أمني طالما تطبق كل نقطة طرفية نصف مفاتيح عشوائية حقيقة.

بيد أنه ينبغي أن تقدم النقاط الطرفية قيمة عشوائية جديدة من 512 بتة (أي 64 اتمونة) ضمن **challenge**، في الوقت ذاته التي تقدم فيه ن صف مفاتيحها DH (انظر الفقرة 3.2 من الوثيقة RFC 2631). وتسمح قيم **challenge**، التي تستند إلى النداء، بضمان توليد مفاتيح ديفي–هيلمان بطريقة عشوائية وفي الوقت المناسب.

وتكون النقطة الطرفية للمصدر B قادرة على حساب g^{ab} ثم السر المتقاسم الدينامي ZZ_{AB} بواسطة **challenge** عشوائي، مع الناتج الناشئ عن MIKEY-PRF (**challenge** || 0x12F905FE , g^{ab}) (انظر الفقرات من 2.1.4 إلى 4.1.4 في الوثيقة RFC 3830) ثم تسمح الوظيفة MIKEY-PRF بحساب مفتاح الاستيقان (*Ma*) (انظر الفقرات من 2.1.4 إلى 4.1.4 من الوثيقة 3830).

وأثناء المرحلة 2، ينبغي أن تولِّد النقطة الطرفية للمصدر B قيم عشوائية MIKEY جديدة *y* مع نصف مفتاح g^y المقابل ثم تقوم بإنشاء رسالة MIKEY، Imsg، وفقاً لبروتوكول MIKEY-DHHMAC باستعمال *Ma*.

تكون رسالة MIKEY I مجفرة اثنينياً.

ينبغي أن تتضمن النقطة الطرفية للمصدر B دائماً نصف مفتاح ديفي–هيلمان في **dhkey** ضمن **ClearToken**، مما يسمح أيضاً بدعم نموذج التسيير المباشر مع الحارسات البوابية. وينبغي إدراج **ClearToken** في الرسالة Setup وترسل إلى النقطة

الطرفية القرينة. وينبغي أن يرسل الحارس البوابي مع التسيير علامة ClearToken (بدون تعديل رسائل MIKEY) مع القفزة التالية.

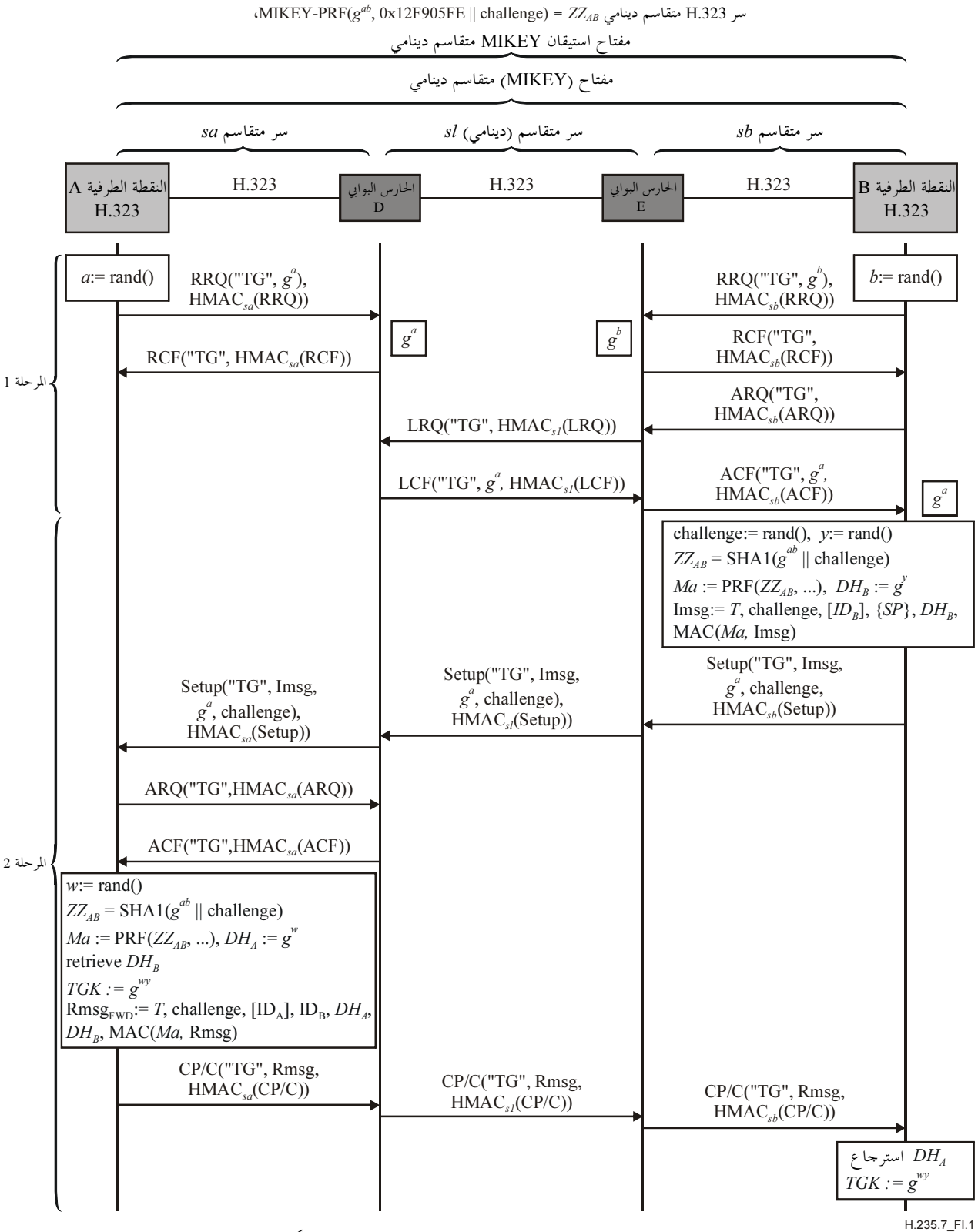
ثم تحسب النقطة الطرفية للمقصد A، g^{ab} والسر المتقاسم الدينامي ZZ_{AB} انطلاقاً من MIKEY-PRF (g^{ab} , 0x12F905FE || **challenge**) (انظر الفقرات من 2.1.4 إلى 4.1.4 من الوثيقة RFC 3830). وتسمح الوظيفة MIKEY-PRF فيما بعد بحساب مفتاح الاستيقان (*Ma*) (انظر الفقرات من 2.1.4 إلى 4.1.4 من الوثيقة RFC 3830). وتولِّد النقطة الطرفية A قيمة عشوائية MIKEY *w* وتُحسب g^w. ثم تحسب مفتاح *TGK* باستعمال نصف مفاتيح ديفي–هيلمان المستقبلة.

وانطلاقاً من *TGK*، تكون النقطة الطرفية للمقصد A قادرة على حساب مفاتيح الدورة SRTP على النحو الموصوف في الفقرة 3.4 من الوثيقة RFC 3711 (غير مبيَّنة في الشكل).

تقوم النقطة الطرفية A بإنشاء رسالة R_message، Rmsg مماثلة. تسير الرسالة R_message هذه ضمن رسالة CallProceeding-to-Connect message (CP/C) نحو النقطة الطرفية B.

وترسل الرسالة CallProceeding-to-Connect message (CP/C) نحو النقطة الطرفية B.

تسترجع النقطة الطرفية B نصف مفتاح ديفي–هيلمان وتحسب المفتاح *TGK*.ثم تحسب مفاتيح الدورة SRTP انطلاقاً من مفتاح TGK على النحو الموصوف في الفقرة 3.4 من الوثيقة RFC 3711 (غير مبيَّنة في الشكل).



الشكل H.235.7/1.I – مثال توجه في إطاره النقطة الطرفية B نداءً إلى النقطة الطرفية A (تسيير بواسطة حارسات بوابية) مع MIKEY-DHHMAC

1.I إنهاء نداء H.323

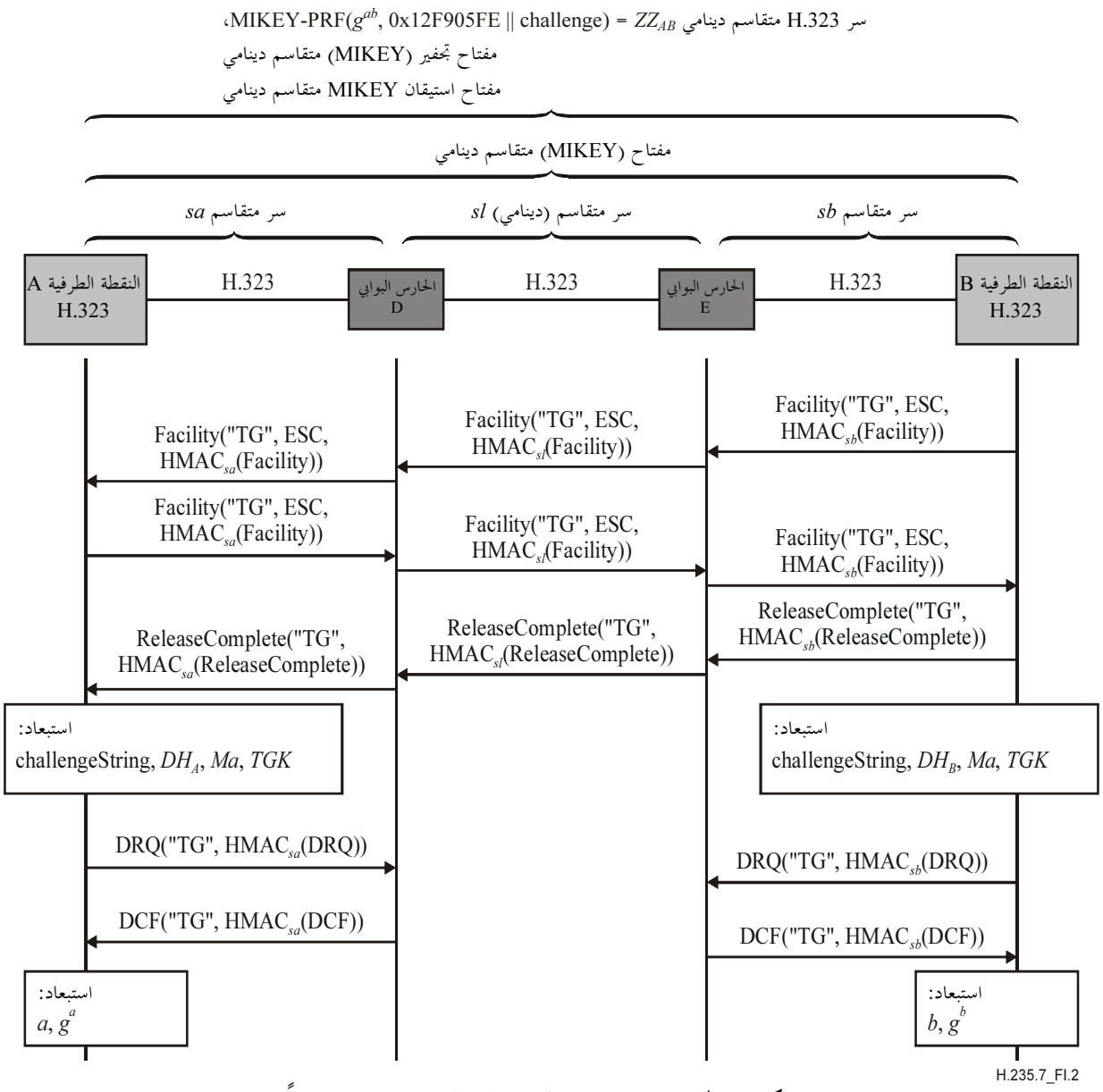
لما كانت النقاط الطرفية المعنية تحتفظ بالحالة للبروتوكولين MIKEY وSRTP، من الأساسي وجود إجراء خاص للإنهاء. ويورد الشكل 2.I مثالاً لتدفق الرسائل في حالة إنهاء النقطة الطرفية B (ممهد MIKEY) لنداء معين. ويكون التدفق، أساساً، وفقاً للفقرة 5.8 من التوصية H.323 "الطور E: إنهاء النداء".

ملاحظة – يبيِّن الشكل 2.I إجراءات الانسحاب الاختيارية للحالة التي تلغى فيها النقاط الطرفية تسجيلها تماماً. وعندئذ ينبغي أن تستبعد النقاط الطرفية المفتاح الخصوص DH (a أو b) ونصف مفتاح DH العمومي (g^a أو g^b).

ولما كان إجراء إنهاء نداء معين مستقلاً عن مواصفة الأمن هذه، يمكن استعمال أي معرِّف للغرض ينطبق على ملامح الأمن الكامنة (H.235.1، H.235.3، إلخ)؛ ومن ثم لا يشير الشكل 2.I إلى أي معرِّف للغرض.

وإذا سجلت النقطة الطرفية مجدداً لدى حارس بوابي، ينبغي عندئذ توليد نصف مفاتيح ديفي–هيلمان جديدة. بيد أن إلغاء التسجيل الكامل غير ضروري في أي ظرف من الظروف لمجرد إلغاء النداء. وإذا قررت النقطة الطرفية أن تبقى مسجلة لدى الحارس البوابي، يمكن مواصلة استعمال نصف مفاتيح ديفي–هيلمان السكونية.

وفي الحالة التي تبقى فيها النقاط الطرفية مسجلة ولم يطبق الانسحاب، ينبغي أن تستبعد النقاط الطرفية المعلومات المرتبطة بالنداء فحسب، بما في ذلك نصف مفاتيح ديفي–هيلمان القرينة، **challenge**، ومفاتيح MIKEY، *Me* و*Ma* وTGK ومعلومات الدورة SRTP ذات الصلة.



الشكل H.235.7/2.I – مثال لنقطة طرفية B تنهي نداءً

2.I إعادة حساب المفتاح TGK وتحديث CSB

يدعم بروتوكول MIKEY ذاتياً إعادة حساب مفتاح TGK و/أو تحديث معلومة CSB. وينبغي أن تستعمل ملامح هذه التوصية إجراء MIKEY-DHHMAC الواردة في الفقرة 1.3 من الوثيقة RFC zzzz لهذا الغرض بما يسمح بتحديث مفتاح TGK قبل انقضائه، أو تحديث المعلومات الأخرى بدون تعديل مفتاح TGK.

وتفيد آلية إعادة حساب مفتاح TGK وتحديث CSB في حماية حزمة من القنوات المنطقية بموجب السياسة الأمنية ذاتها. ولتحقيق هذا الغرض، يوصى بتنفيذ بروتوكول MIKEY-DHHMAC (بالكامل) على النحو الموصوف أعلاه من أجل القناة المنطقية الأولى فقط. وينبغي على أي قناة منطقية لاحقة أن تطبق آلية السياسة الأمنية MIKEY ذاتها أو مفتاح TGK ذاته، وأن تستعمل آلية تحديث CSB بدون آلية إعادة حساب مفتاح TGK الواردة في هذه الفقرة وذلك بالإشارة على معرِّف CSB للمصدر مع حذف مفاتيح ديفي–هيلمان المحدَّثة.ويسمح ذلك بإنشاء قنوات منطقية أو دورات تجفير MIKEY بطريقة أكثر فعالية مما يسمح به التنفيذ التام لبروتوكول MIKEY لكل قناة منطقية.

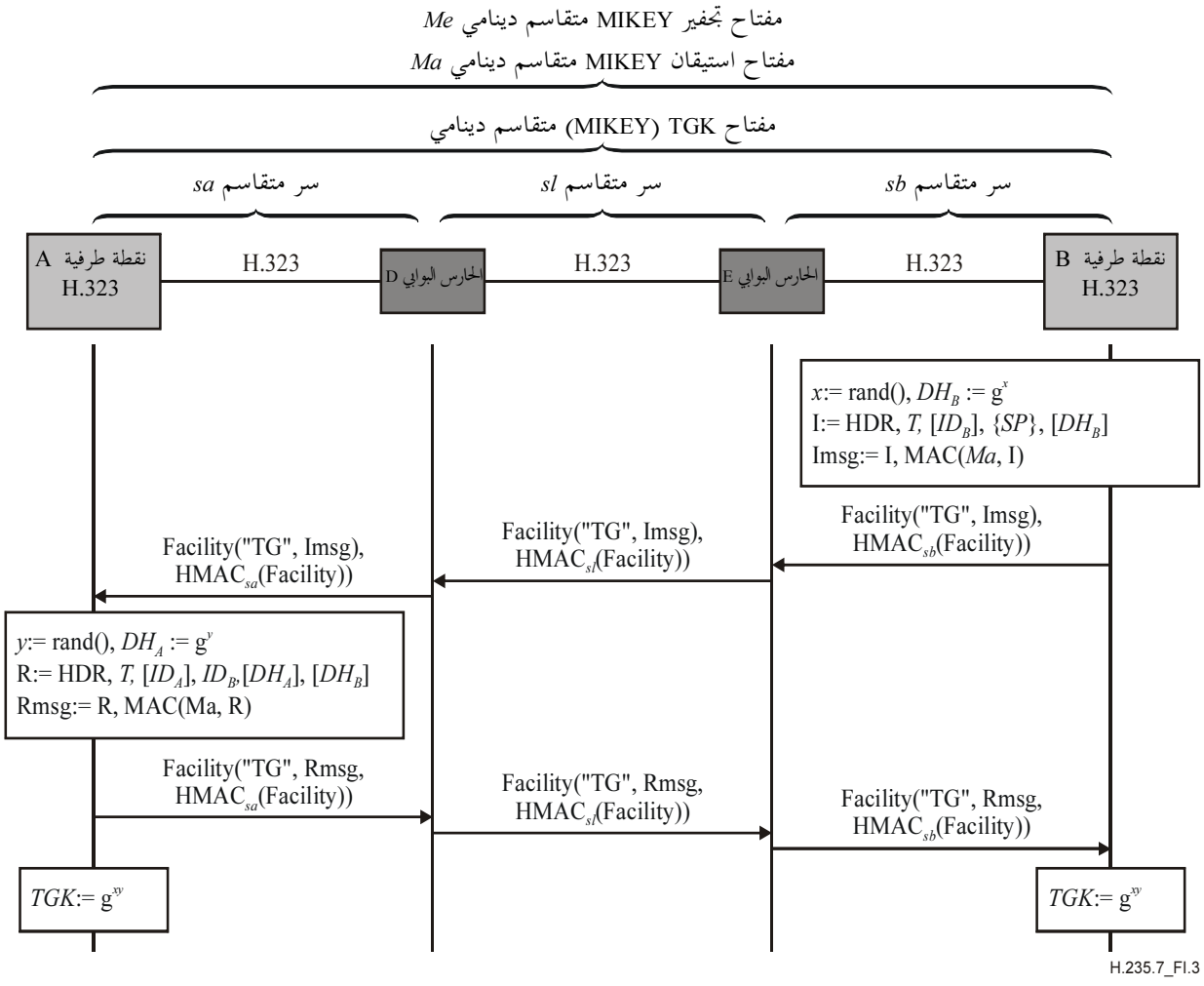
وينبغي تغليف رسائل إعادة حساب مفتاح MIKEY TGK أو رسائل تحديث CSB وتسير في **MiscellaneousCommand** ضمن رسالة Facility. ويضبط المعرِّف **tokenOID** الخاص بالعلامة **ClearToken** على "TG".

إذا نفذ بروتوكول MIKEY على"مستوى متعدد الوسائط"، ينبغي أن تحدد النقطة الطرفية B القناة المنطقية التي يتعين تطبيق إعادة حساب مفتاح TGK عليها و/أو تحديث CSB. وتستعمل النقطة الطرفية A بوصفها المستجيب أيضاً **MiscellaneousCommand** ضمن Facility لتسيير رسالة MIKEY R_message (إن وجدت).

ولإعادة حساب مفتاح TGK (انظر الشكل 3.I)، ينبغي أن تولِّد النقطة الطرفية B بوصفها المصدر MIKEY مفتاحاً جديداً TGK. ينبغي أن تتضمن القيمة **parameterValue**، رسالة مقابلة I اثنينية مجفرة.

ويمكن أن تؤكد النقطة الطرفية A بوصفها المستجيب رسالة إعادة حساب مفتاح TGK الناتجة عند الضرورة بناءً على طلب النقطة الطرفية B. وتقوم النقطة الطرفية A بإنشاء رسائل R مماثلة. وتسير النقطة الطرفية B الرسالة R_message ضمن رسالة Facility نحو النقطة الطرفية B.

ولتحديث CSB، يعتبر الإجراء مماثلاً للإجراء الوارد أعلاه باستثناء أن رسالة MIKEY ينبغي ألا تتضمن أي مفتاح TGK.



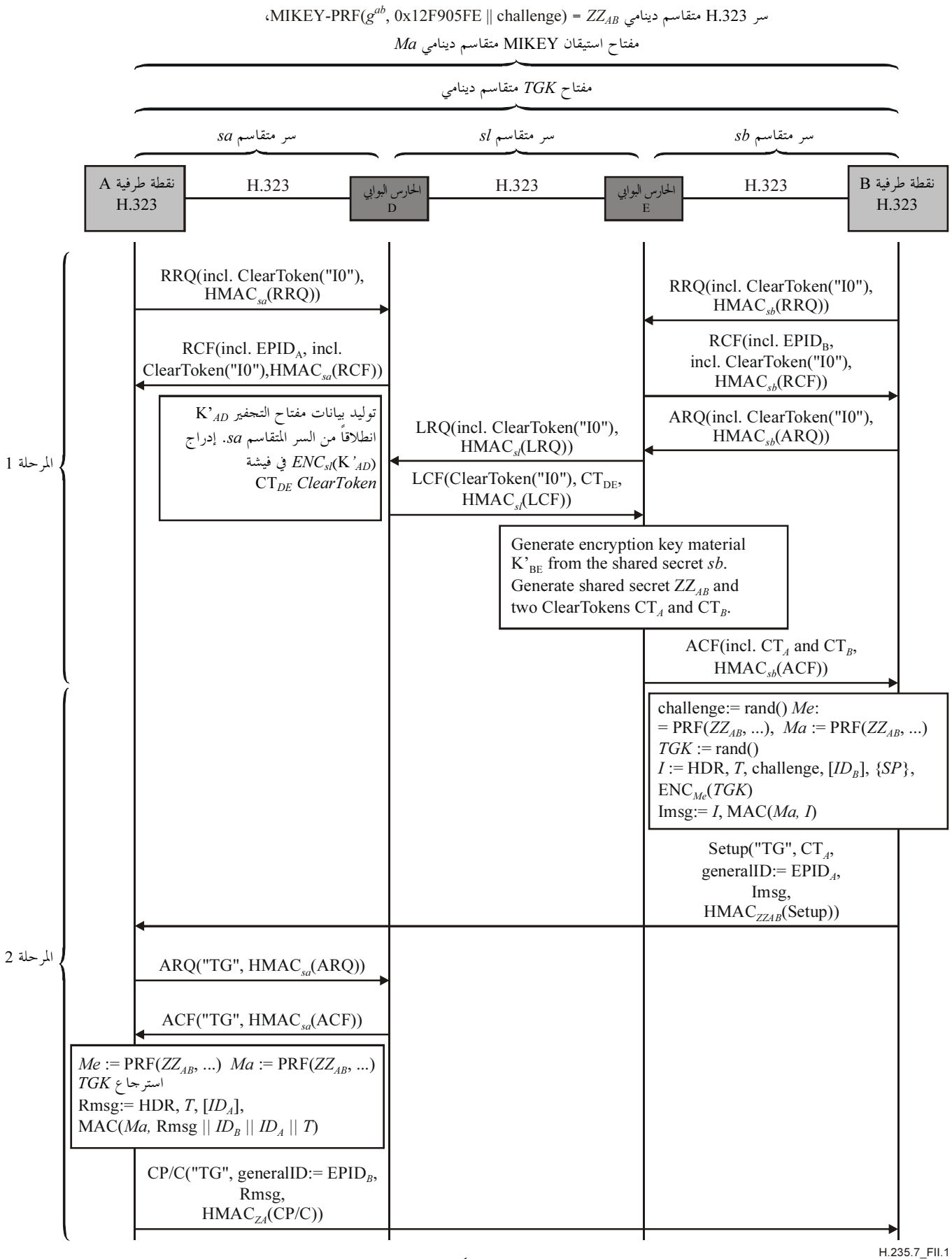
الشكل H.235.7/3.I – مثال لنقطة طرفية B تقوم بتحديث مفتاح

التذييل II

استعمال H.235.4 لإنشاء سر متقاسم مسبق

يحدد هذا التذييل كيفية تنفيذ الإجراء DRC1 الوارد في التوصية ITU-T H.235.4 لإنشاء سر متقاسم مسبق ZZ_{AB} بين النقطتين الفرعيتين B وA، بافتراض عدم وجود سر من طرف إلى طرف في المقام الأول. وتنطبق الطريقة الموصوفة في هذا التذييل على سيناريو بحارس بوابي وحيد أو حارسات بوابية متعددة. ولا ينطوي الإجراء الوارد في هذا التذييل على حسابات ديفي–هيلمان أثناء إجراءات التسجيل والقبول والحالة RAS بل تنفي التجفير المتناظر بالأحرى.

يبيِّن الشكل 1.II مثالاً لمخطط تدفق نقطة طرفية B توجه نداءً إلى نقطة طرفية A.



الشكل H.235.7/1.II – مثال لنقطة طرفية B توجه نداءً إلى نقطة طرفية A (تسيير بدون حارس بوابي) مع سر متقاسم مسبق MIKEY-PS وDRC1 في التوصية H.235.4

1.II إنهاء نداء H.323

يشرع في إجراء إنهاء نداء H.323 على النحو الموصوف في الفقرة 1.8.

2.II إعادة حساب مفتاح TGK وتحديث CSB

يشرع في إجراء إعادة حساب مفتاح TGK وتحديث CSB على النحو الموصوف في الفقرة 2.8.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة B	وسائل التعبير: التعاريف والرموز والتصنيف
السلسلة C	الإحصائيات العامة للاتصالات
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

طُبعت في سويسرا
جنيف، 2006