الاتحـــــاد الدولـــــي للاتصـــــالات

ITU-T H.235.8

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمة السمعية المرئية والأنظمة المتعددة الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

إطار الأمن H.323: تبادل المفاتيح في بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) باستعمال قنوات التشوير المؤمَّنة.

التوصيـــة ITU-T H.235.8

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: تبادل المفاتيح في بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) باستعمال قنوات التشوير المؤمَّنة

ملخص

تهدف هذه التوصية إلى وصف إجراءات الأمن التي تنطبق على تبادل المفاتيح في البروتوكول SRTP باستعمال التشوير المؤمَّنة في الشبكات H.323/H235.

وتستند هذه التوصية إلى التوصيتين ITU-T H.323 وITU-T H.225.0 (الطبعتان 4 أو اللاحقتان).

المصدر

وافقت لجنة الدراسات 16 (2005-2008) التابعة لقطاع تقييس الاتصالات في الاتحاد على التوصية ITU-T H.235.8 بتاريخ 13 سبتمبر 2005 وذلك بموجب الإجراء الوارد في التوصية ITU-T A.8.

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

جـــدول المحتـــويات

الصفحة

إطار الأمن H.323: تبادل المفاتيح في بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) باستعمال قنوات التشوير المؤمَّنة

1 مجال التطبيق

تهدف هذه التوصية إلى تقديم توصيات بشأن إجراءات الأمن التي تسمح بدعم بروتوكول النقل المؤمن في الوقت الفعلي (SRTP) بين نقطتين طرفيتين H.323 في الحالات التي تنقل فيها البيانات المجفرة المصاحبة لقناة الوسائط في قناة تشوير مؤمنة، مثلاً IPsec (RFC 2401) أو TLS (RFC 2246) أو أية آليات أخرى H.235. وتقدم إجراءات الأمن هذه باعتبارها بديلاً عن إجراءات الأمن الأخرى H.235 التي تدعم البروتوكول SRTP.

تصف هذه التوصية الإجراءات التي تهدف إلى دعم بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) لفريق مهام هندسة الإنترنت (IETF) في أنظمة التوصية ITU-T.H.323. ويوفر البروتوكول SRTP خدمات أمنية للوسائط RTP ويعتمد على بروتوكولات منفصلة لتأمين خدمات إدارة المفاتيح والتفاوض بشأن معلمات التجفير. وينبغي الاستخدام هذه الإجراءات عندما تنتهي قناة التشوير المؤمنة إلى نظام وسيط، وفي هذه الحالات، ينبغي أن تنقل بيانات تجفير البروتوكول SRTP بواسطة آلية مؤمَّنة من طرف إلى طرف.

تدعم هذه الإجراءات التشوير والتفاوض والنقل المتعلقين بمفاتيح تجفير البروتوكول SRTP ومعرفات الخوارزميات والاستيقان والتجفير وغيرها من معلمات الدورة بين نقطتين طرفيتين H.323.

ويتمثل جانب رئيسي لهذه الإجراءات في أنه ينبغي أن يكون التابع H.245 والرئيس H.245 قادرين على توليد المفاتيح التجفيرية وتوزيعها.

من الممكن تبادل قدرات الأمن في بروتوكول SRTP من خلال تبادل القدرات بين مطرافين بواسطة المدخلات h235securityCapability في جدول capabilityTable الوارد في الرسالة TerminalCapabilitySet H.245. ويتضمن المجال genericH235SecurityCapability الموجود في المجال encryptionAuthenticationAndIntegrity من المدخل h235SecurityCapability المجال SrtpCryptoCapability الذي يحدد التسلسلات التجفيرية SRTP.

وتحدد معلمة SRTP "crypto" للإشارة إلى المعلمات التجفيرية لبروتوكول SRTP والتفاوض بشأنها. وينحصر تعريف المعلمة "crypto" في هذه التوصية في تدفقات الوسائط أحادية التوزيع بين كيانين، على أن يملك كل مصدر مفتاحاً تجفيرياً وحيداً. ويحتاج دعم تدفقات الوسائط متعددة التوزيع أو التدفقات المتعددة النقاط أحادية التوزيع مزيداً من الدراسة.

والمقصود من المعلمة SRTP "crypto" أن تمكّن من إنشاء المعلمات التجفيرية SRTP عند تبادل رسالة واحدة أو عند تبادل رسالة في كل اتجاه. في حالة تبادل الرسالة في كل اتجاه، يمكن التفاوض بشأن المعلمات التجفيرية. مثلاً، في التوصيلة السريعة، ترسل النقطة الطرفية الطالبة H.323 مجموعة من المعلمات SRTP "crypto" المقدمة إلى النقطة الطرفية H.323المستجيبة، ويكون كل عرض مكبسل في رسالة OpenLogicalChannel H.245 منفصلاً. ثم يمكن للنقطة الطرفية H.323 المستجيبة أن تقبل إحدى المعلمات المقدمة وأن ترد باستجابة تتضمن مجموعة فرعية من المعلمات المختارة المكبسلة في الرسالة OpenLogicalChannel H.245.

في حالة تبادل رسالة واحدة، لا يجري أي تفاوض. وترسل النقطة الطرفية الطالبة H.323 المعلمات SRTP "crypto" إلى النقطة الطرفية H.323 المستجيبة، التي إما أن تقبل المعلمات المقدمة أو ترفض النداء.

يمكن إضافة الإجراءات التجفيرية ذات المفتاح العمومي بهدف تأمين السرية والاستيقان من طرف إلى طرف لبيانات مفتاح الدورة SRTP المتبادلة بين النقطتين الطرفيتين H.323 من خلال تجفير بيانات المفتاح SRTP وتوقيعها في حال لا يُشغّل بروتوكول أمن الكبسلة (مثلاً، IPsec، TLS) إلا عند جهاز وسيط وبالتالي، لا يوفر الأمن من طرف إلى طرف.

2 المراجع

1.2 المراجع المعيارية

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

- التوصية ITU-T H.225.0 (2003)، *بروتوكولات تشوير النداء وترزيم التدفقات أحادية الوسائط لأنظمة الاتصالات متعددة الوسائط القائمة على الرزم.*
- التوصية ITU-T H.235.0 (2005)، *إطار الأمن H.323: أمن وتجفير المطاريف المتعددة الوسائط من السلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*
- التوصية ITU-T H.460.11 (2004)، *إنشاء نداء مؤجّل في الأنظمة H.323.*
- المعيار IETF RFC 2246 (1999)، *الصيغة 1.0 لبروتوكول أمن طبقة النقل (TLS).*
- المعيار IETF RFC 2401 (1998)، *معمارية الأمن بالنسبة إلى بروتوكول الإنترنت.*
- المعيار IETF RFC 2733 (1999)، *نسق تحميل RTP للتصحيح الأمامي النمطي للخطأ.*
- المعيار IETF RFC 3280 (2002)، *شهادة الإنترنت X.509 للبنية التحتية للمفتاح العمومي والملمح العام لقائمة إبطال الشهادة.*
- المعيار IETF RFC 3550 (2003)، RTP: *تطبيقات بروتوكول النقل في الوقت الفعلي.*
- المعيار IETF RFC 3711 (2004)، *بروتوكول المؤمَّن في الوقت الفعلي (SRTP).*
- المعيار IETF RFC 3852 (2004)، *تركيب رسالة مجفرة (CMS).*

2.2 المراجع الإعلامية

- IETF Draft، F. Andreasen، M. Baugher، D Wing: *أمن بروتوكول وصف الدورة، أوصاف تدفقات وسائط الإعلام،* <draft-ietf-mmusic-sdescriptions-11.txt>.

3 الرموز والمختصرات

تستخدم هذه التوصية المختصرات التالية:

AES خوارزمية تجفير متطورة (*Advanced Encryption Algorithm*)

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

CA سلطة الترخيص (*Certificate Authority*)

CEK مفتاح تجفير المحتوى (*Content Encryption Key*)

CMS تركيب الرسالة المجفرة (*Cryptographic Message Syntax*)

EP نقطة طرفية (*Endpoint*)

FEC تصحيح أمامي للأخطاء (*Forward Error Correction*)

FFS بحاجة لمزيد من الدراسة (*For Further Study*)

F8 خوارزمية تجفير UMTS (*UMTS Encryption Algorithm*)

GK حارس بوابة (*Gatekeeper*)

GW بوابة (*Gateway*)

HMAC شفرة استيقان الرسائل المظلة بمفتاح (*Keyed-Hash Message Authentication Code*)

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

KDR معدل اشتقاق المفتاح (*Key Derivation Rate*)

MAC شفرة استيقان الرسالة (*Message Authentication Code*)

MKI معرف المفتاح الرئيسي (*Master Key Identifier*)

OID معرف الغرض (*Object identifier*)

OLC فتح قناة منطقية (*Open Logical Channel*)

PKI البنية التحتية للمفتاح العمومي (*Public Key Infrastructure*)

RAS تسجيل وقبول ووضع (*Registration, Admission, Status*)

ROC عدّاد الدورات الكاملة (*Roll-over Counter*)

RTCP بروتوكول التحكم في النقل في الوقت الفعلي (*Real-Time Transport Control Protocol*)

RTP بروتوكول النقل في الوقت الفعلي (*Real-Time Transport Protocol*)

SHA1 خوارزمية التظليل المؤمَّن رقم 1 (*Secure Hash Algorithm 1*)

SRTCP بروتوكول التحكم في النقل المؤمن في الوقت الفعلي (*Secure Real-Time Transport Control Protocol*)

SRTP بروتوكول النقل المؤمَّن في الوقت الفعلي (*Secure Real-Time Transport Protocol*)

SSRC مصدر التزامن (*Synchronization Source*)

TLS أمن مستوى النقل (*Transport Level Security*)

WSH بيان حجم النافذة (*Window Size Hint*)

4 وصف المعلمات

يجري تبادل القدرات التجفيرية والبيانات المفتاحية في البروتوكول SRTP بواسطة معلمتين:

- يحتوي العنصر **SrtpCryptoInfo** ضمن **StrpCryptoCapability** التسلسل التجفيري ومعلمات الدورة. وتُنقل المعلمة **SrtpCryptoInfo** إلى المعلمة **genericH235SecurityCapability** H.245 للإشارة إلى المعلمات التجفيرية SRTP والتفاوض بشأنها.
- يحتوي العنصر **SrtpKeyParameters** ضمن **SrtpKeys** على البيانات المفتاحية SRTP. وينقل حاوي **SrtpKeys** في المعلمة **h235Key** H.245 معلمة واحدة أو عدة معلمات **SrtpKeyParameters** بالإضافة إلى المفاتيح SRTP.

يقتصر استخدام المعلمات التجفيرية SRTP في هذه التوصية على تدفقات الوسائط أحادية التوزيع بين كيانين، حيث يملك كل مصدر مفتاحاً تجفيرياً وحيداً. هذا ولا يزال دعم تدفقات الوسائط متعددة التوزيع أو تدفقات النقاط المتعددة أحادية التوزيع بحاجة لمزيد من الدراسة.

1.4 نقل المعلمات SRTP

يتكون توصيل الوسائط SRTP بأسلوب مزدوج كامل من قناتين أحاديتي الاتجاه، واحدة في كل اتجاه. ويُنقل كل عرض تجفيري في رسالة منفصلة **OpenLogicalChannel** H.245.

1.1.4 نقل المعلمة SrtpKeys

تُنقل المعلمة **SrtpKeys** التي تتضمن بيانات المفتاح التجفيري SRTP في المجال **genericKeyMaterial** للمعلمة **secureSharedSecret (V3KeySyncMaterial)** الواردة ضمن الحاوي **h235Key** في المعلمة **encryptionSync** للرسائل **OpenLogicalChannel** H.245.

ينبغي تعريف محتوى المفتاح التجفيري SRTP الوارد في الحاوي **genericKeyMaterial** بواسطة قيمة معرف الغرض H.235.8 (انظر الجدول 1) في المجال **standard** الوارد في **capabilityIdentifier** ضمن المجال **genericH235SecurityCapability** الوارد في **encryptionAuthenticationAndIntegrity** وفي **h235Media** للمعلمة **dataType** في الرسالة OLC.

كما يمكن لاقتراحات **OpenLogicalChannel** بديلة للقناة نفسها التي تحتوي على القيمة نفسها **sessionID** في المعلمات **H2250LogicalChannelParameters** أن تستخدم العرض التجفيري نفسه. وبما أنه سيتم قبول دورة بديلة واحدة فقط، فستكون أحادية المفتاح مضمونة.

2.1.4 نقل المعلمة SrtpCryptoCapability

تُنقل المعلمة **SrtpCryptoCapability** في المجال **genericH235SecurityCapability** ضمن المجال **encryptionAuthenticationAndIntegrity** في **h235Media** للمعلمة **dataType** للرسائل **OpenLogicalChannel**.

يمكن أن تتضمن الرسالة **TerminalCapabilitySet** مدخلاً واحداً أو عدة مدخلات **h235SecurityCapability** في الجدول **capabilityTable**. وللإشارة إلى دعم هذه الإجراءات، ينبغي ضبط النقطة الطرفية H.323 **genericH235SecurityCapability** ضمن **encryptionAuthenticationAndIntegrity** في مدخل **h235SecurityCapability** كما يلي:

- يتضمن المجال **capabilityIdentifier** معرف الغرض H.235.8 (انظر الجدول 1) في المجال **standard**؛
- تبقى المجالات **maxbitRate** و**collapsing** و**nonCollapsing** و**transport** غير مستعملة؛
- يتضمن المجال **nonCollapsingRaw** المعلمة **SrtpCryptoCapability**.

الجدول H.235.8/1 – معرف الغرض H.235.8

قيمة معرف الغرض
{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 90 }

2.4 وصف المعلمة SrtpCryptoCapability

يمكن أن تحتوي المعلمة **SrtpCryptoCapability** على معلمة واحدة أو أكثر **SrtpCryptoInfo** يمكن أن تُستخدم في تحديد قدرات دورة بروتوكول SRTP. وتُفسّر العناصر **BOOLEAN OPTIONAL** كما يلي:

1) إذا كان العنصر يساوي FALSE، لا توفَّر القدرة؛

2) إذا كان العنصر يساوي TRUE، تُوفَّر القدرة وتكون مطلوبة؛

3) إذا كان العنصر غائباً، توفر القدرة غير أنها لا تكون مطلوبة.

عند استخدام المعلمة **SrtpCryptoCapability** أثناء تبادل القدرات، من الممكن الإشارة إلى كافة الخيارات المقبولة داخل مقدرة تنوعيه وحيدة. وفي هذه الحالة، يشير حذف العنصر **BOOLEAN OPTIONAL** إلى أن القدرة متوفرة ولكنها غير مطلوبة.

عند استخدام هذه المعلمة في عبارة **dataType** من الرسالة OLC، يمكن استخدام خيار واحد. ولهذه الغاية، ينبغي مراعاة القواعد التالية:

- لا يجوز أن يحتوي العنصر **FecOrder** إلا على قيمة واحدة من القيم الاختيارية؛
- في **SrtpSessionParameters**، يجب أن تكون القيم **BOOLEAN OPTIONAL** إما TRUE أو FALSE؛
- ينبغي أن يحتوي العنصر **SrtpCryptoCapability** على عنصر واحداً **SrtpCryptoInfo**.

تتكون المعلمة **SrtpCryptoInfo** من المجال الإلزامي **cryptoSuite** ومن المجالين الاختياريين **sessionParams** و**allowMKI** الوارد وصفهما فيما يلي.

الجدول H.235.8/2 – معرفات الغرض للتسلسلات التجفيرية H.235.8

التسلسل التجفيري	قيمة معرف الغرض
AES_CM_128_HMAC_SHA1_80	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 91 }
AES_CM_128_HMAC_SHA1_32	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 92 }
F8_128_HMAC_SHA1_80	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 93 }

1.2.4 cryptoSuite

يحدد معرف الغرض (انظر الجدول 2) الوارد في المجال **cryptoSuite** خوارزميات التجفير والاستيقان الواجب استخدامها في دورة بروتوكول SRTP. وتتضمن مواصفة بروتوكول SRTP العديد من المعلمات المجمّعة في ثلاثة خيارات تسمى "متواليات تجفيرية". ويمكن توسيع هذه الخيارات بشكل يسمح بإضافة متواليات تجفيرية جديدة. والمتواليات التجفيرية الثلاث التي تم تحديدها هي التالية: AES_CM_128_HMAC_SHA1_80 وAES_CM_128_HMAC_SHA1_32 وF8_128_HMAC_SHA1_80. ويظهر الجدول 3 معلمات البروتوكول SRTP المصاحبة لكل متوالية من هذه المتواليات.

الجدول H.235.8/3 – القيم بالتغيب للمتواليات التجفيرية

المعلمة SRTP	AES_CM_128_ HMAC_SHA1_80	AES_CM_128_ HMAC_SHA1_32	F8_128_ HMAC_SHA1_80
طول المفتاح الرئيسي	128 بتة	128 بتة	128 بتة
قيمة الملح	112 بتة	112 بتة	112 بتة
مدة الحياة	2^31 رزمة	2^31 رزمة	2^31 رزمة
الشفرة	عداد AES	عداد AES	F8
مفتاح التجفير	128 بتة	128 بتة	128 بتة
شفرة استيقان الرسالة	HMAC-SHA1	HMAC-SHA1	HMAC-SHA1
طول علامة الاستيقان	80 بتة	32 بتة	80 بتة
طول مفتاح استيقان بروتوكول SRTP	160 بتة	160 بتة	160 بتة
طول مفتاح استيقان بروتوكول SRTCP	160 بتة	160 بتة	160 بتة

إن المجال **cryptoSuite** عبارة عن معلمة جرى التفاوض بشأنها.

2.2.4 sessionParams

يجوز لمعلمات الدورة أن تكون إما متفاوض عليها وإما إعلانية، ويشير تعريف معلمة محددة للدورة إلى ما إذا كانت متفاوض عليها أو إعلانية. وتنطبق المعلمات المتفاوض عليها، على البيانات المرسلة في الاتجاهين، في حين أن المعلمات الإعلانية لا تنطبق إلا على الوسائط التي أرسلها الكيان الذي ولّد وصف الدورة. وبالتالي، تنطبق المعلمة الإعلانية في عرضٍ ما على الوسائط التي يرسلها الكيان العارض، في حين تنطبق المعلمة الإعلانية في استجابة ما على الوسائط التي يرسلها الكيان المستجيب.

يتضمن المجال الاختياري **sessionParams** معلمات دورة بروتوكول SRTP.

1.2.2.4 kdr

تحدد المعلمة KDR معدل اشتقاق المفتاح، كما هو وارد في الفقرة 1.3.4 من المعيار RFC 3711. وينبغي أن تكون قيمة المعلمة عدداً صحيحاً في المجموعة {1, 2, ..., 24} يمثل القدرة للعدد 2 من 2^1 إلى 2^24 ضمناً. ويتحكم معدل اشتقاق مفتاح بروتوكول SRTP في مدى تواتر اشتقاق مفتاح جديد للدورة انطلاقاً من مفتاح رئيسي لبروتوكول SRTP (RFC 3711). وعندما لا يحدد معدل اشتقاق المفتاح (أي عندما تكون المعلمة KDR محذوفة)، يجرى اشتقاق أولي وحيد للمفتاح الرئيسي (RFC 3711). وتكون المعلمة KDR هو معلمة إعلانية.

2.2.2.4 unencryptedSrtp

هو عبارة عن مجال بوليّ اختياري، وإذا كان موجوداً فإنه يشير إلى أن الحمولات المفيدة رزم بروتوكول SRTCP غير مجفرة. وهو معلمة متفاوض عليها.

3.2.2.4 unencryptedSrtcp

هو عبارة عن مجال بوليّ اختياري، وإذا كان موجوداً فإنه يشير إلى أن الحمولات المفيدة للرزم SRTP غير مجفرة. وهو معلمة متفاوض عليها.

4.2.2.4 unauthenticatedSrtp

تستيقن الحمولات المفيدة للرزم SRTP وSRTCP بالتغيب. والمجال unauthenticatedSrtp هو مجال بوليّ اختياري. وإذا كان موجوداً، فإنه يشير إلى أن الحمولات النافعة للرزم SRTP غير مستيقنة. وتتطلب مواصفة البروتوكول SRTP، استعمال استيقان الرسائل بالنسبة لبروتوكول SRTCP ولكن ليس بالنسبة لبروتوكول SRTP (RFC 3711). وهو معلمة متفاوض عليها.

fecOrder 5.2.2.4

تشير المعلمة **fecOrder** إلى ترتيب معالجة التصحيح الأمامي للأخطاء (FEC) للرزم RTP (RFC 3550، RFC 2733) بالنسبة لتجفير SRTP عند مستوى المرسِل. وتشير القيمة **fecBeforeSrtp** للمعلمة **fecOrder** إلى أن الوظيفة FEC تنطبق قبل المعالجة SRTP التي يجريها مرسل وسائط SRTP وبعد معالجة SRTP التي يجريها مستقبِل وسائط البروتوكول SRTP. فإن **fecBeforeSrtp** هي القيمة بالتغيّب. وتشير **fecAfterSrtp** إلى الترتيب المعكوس للمعالجة. **FecOrder** هو معلمة إعلانية.

windowSizeHint 6.2.2.4

يحدد البروتوكول SRTP المعلمة SRTP-WINDOW-SIZE (RFC 3711، القسم 2.3.3) اللازمة للحماية من الهجمات بإعادة التنفيذ. وتساوي القيمة الدنيا 64 (RFC 3711)، إلا أنه يمكن اعتبار هذه القيمة منخفضة للغاية بالنسبة لبعض التطبيقات، مثلاً الفيديو.

توفر معلمة الدورة المتمثلة في بيان حجم النافذة (WSH)، بشكل دلالي، الحجم المناسب الذي ينبغي أن تكون عليه النافذة لكي تعمل بطريقة مرضية (مثلاً، على أساس عدد الرزم في الثانية الذي يعرفه المرسل). إلا أن البيانات التي تقدمها الأجهزة الواصفة المعنية بترزيم الوسائط قد تكون كافية بالنسبة للمستقبِل لاشتقاق المعلمة بشكل مرضٍ. وبالتالي، تعتبر هذه القيمة سوى دلالة للمستقبل الذي يمكنه أن يتجاهل القيمة المقدمة.

WindowSizeHint هو معلمة إعلانية.

7.2.2.4 تحديد معلمات جديدة للدورة SRTP

تكون المعلمات الجديدة لدورة البروتوكول SRTP إلزامية بالتغيّب. ويُستخدم المجال **newParameter** كآلية تمديد لمعلمات الدورة الجديدة. وإذا تلقت نقطة طرفية قديمة H.323 المعلمة **SrtpCryptoInfo** مع معلمة غير معروفة للدورة في المجال **newParameter**، سوف تعتبر المعلمة الجديدة **SrtpCryptoInfo** هذه غير صالحة.

3.4 وصف معلمات المجال SrtpKeys

يحتوي المجال **SrtpKeys** على معلمة مفتاحية أو أكثر **SrtpKeyParameter** ينبغي استخدامها لدورة البروتوكول SRTP. وتتضمن كل معلمة **SrtpKeyParameter** بيانات مفتاحية (المفتاح الرئيسي والملح) وكافة السياسات المتعلقة بالمفتاح الرئيسي، بما في ذلك المدة التي يمكن خلالها استخدام هذا المفتاح (فترة العمر) وما إذا كانت تستخدم أو لا تستخدم معرف المفتاح الرئيسي (MKI) لربط رزمة SRTP داخلة مع مفتاح رئيسي محدد. وتمثل التطبيقات الملائمة للسياسات المصاحبة للمفتاح الرئيسي ولن تقبل الرزم الداخلة التي تنتهك السياسة العامة (مثلاً، بعد انتهاء فترة عمر المفتاح الرئيسي).

masterKey 1.3.4

هو عبارة عن مفتاح رئيسي تجفيري يستخدم للدورة SRTP. ويتم تحديد طول هذا المفتاح من جانب المتوالية التجفيرية التي ينطبق عليها المفتاح. وإذا لم يطابق الطول ذلك المحدد للمتوالية التجفيرية، تُعتبر المعلمة "crypto" المعنية غير صالحة. وعلى كل مفتاح رئيسي أن يمثل عدداً عشوائياً على الصعيد التجفيري وينبغي أن يكون وحيداً لكل التدفق المقترح للوسائط.

masterSalt 2.3.4

هو عبارة عن ملح رئيسي تجفيري يُستخدم للدورة SRTP. ويتم تحديد طول هذا المفتاح من جانب المتوالية التجفيرية التي ينطبق عليها المفتاح. وإذا لم يطابق الطول ذلك المحدد للمتوالية التجفيرية، تُعتبر المعلمة "crypto" المعنية غير صالحة. وعلى كل ملح رئيسي أن يمثل عدداً عشوائياً على الصعيد التجفيري وينبغي أن يكون وحيداً لكل التدفق المقترح للوسائط.

lifetime 3.3.4

يمثل هذا المجال فترة العمر الاختيارية للمفتاح الرئيسي التي تقاس من خلال العدد الأقصى للرزم SRTP أو SRTCP التي تستخدم هذا المفتاح الرئيسي (ينبغي أن يكون عدد الرزم SRTP وعدد الرزم SRTCP أدنى من فترة العمر). كما يمكن الإشارة إلى قيمة مدة الحياة بشكل عدد صحيح إيجابي غير معدوم أو قدرة للعدد 2. ولا ينبغي أن تتجاوز قيمة "فترة العمر"

القيمة القصوى للرزم بالنسبة للمتوالية التجفيرية. وإذا كانت "فترة العمر" طويلة جداً أو غير صالحة، تُعتبر المعلمة "crypto" بكاملها غير صالحة. وفي غياب المجال lifetime، تُستخدم قيمة فترة العمر بالتغيّب. ويكون ذلك عملياً عندما تكون قيمة فترة العمر للمفتاح التجفيري SRTP هي قيمة بالتغيّب.

4.3.4 masterKeyId

يشير هذا المجال الاختياري إلى السياسة المتعلقة بالطريقة التي ينبغي أن تحدد المفاتيح بالنسبة لدورة SRTP. المعرف MKI هو معرف المفتاح الرئيسي لبروتوكول SRTP. وإذا تم التزويد بالمعرف MKI، يجب كذلك التزويد بطوله. وطول المعرف MKI هو حجم المجال MKI المحدد بالأثمونات في الرزمة SRTP. وإذا لم يقدَّم طول المعرّف أو إذا تجاوزت قيمته 128 (أثموناً)، لتعتبر المعلمة "crypto" بكاملها غير صالحة.

كما ذكر أعلاه، يمكن أن تحتوي معلمة المفتاح مفتاحاً رئيسياً أو أكثر. وفي حال تضمنت المعلمة أكثر من مفتاح رئيسي، على كافة المفاتيح الرئيسية في معلمة المفتاح هذه أن تدرج قيمة MKI. وفي حال استخدام المعرف MKI، ينبغي أن يكون طوله هو نفس طول كافة المفاتيح التي تتضمنها معلمة crypto معينة.

4.4 تدميث السياق التجفيري SRTP

بالإضافة إلى معلمات بروتوكول SRTP المحددة أعلاه، هناك ثلاث معلومات أساسية لتشغيل الأعداد SRTP بالتغيب:

- SSRC: مصدر التزامن
- ROC: عدّاد الدورات الكاملة لمصدر SSRC معيّن
- SEQ: رقم التتابع بالنسبة لمصدر SSRC معيّن

في دورة أحادية التوزيع، حسبما هو وارد في هذه التوصية، هناك ثلاثة قيود على هذه القيم. القيد الأول، هو على المصدر SSRC، ينبغي أن يكون تدفق المفتاح SRTP وحيداً لكل مشارك. وكما هو مشروح في البروتوكول SRTP، ينبغي عدم إعادة استعمال تدفق المفتاح على نصين أو أكثر من النصوص المختلفة العادية.

إن إعادة استخدام تدفق المفتاح يجعل النص المحفر عرضة للهجوم من جانب التحليل التجفيري. وتتمثل أحدى نقط الضعف في أن مجالات النصوص العادية المعروفة في تدفق ما يمكن أن تكشف أجزاء من تدفق المفتاح المعاد استخدامه، مما قد يكشف عن المزيد من النصوص العادية الواردة في تدفقات أخرى. وبما أن كافة آليات التجفير SRTP الحالية تستخدم تدفقات المفتاح، يشكل تقاسم المفتاح مشكلة عامة (RFC 3711). يحد البروتوكول SRTP من هذه المشكلة بإدراج مصدر تدفق المفتاح SSRC المرسل في تدفق المفتاح. ولكن البروتوكول SRTP لا يحل هذه المشكلة بكاملها لأن بروتوكول النقل بالوقت الفعلي يتسبب في تصادمات SSRC وهي نادرة جداً (RFC 3550) ولكنها ممكنة تماماً. وخلال التصادم، يتمتع مصدران أو أكثر من مصادر SSRC التي تتقاسم مفتاحاً رئيسياً بتدفقات مفتاح مماثلة لأجزاء تتراكب فيما بينها في فسحة رقم التتابع RTP. ويتحاشى وصف أمن بروتوكول SRTP إعادة استعمال تدفقات المفتاح من خلال فرض مفاتيح رئيسية وحيدة لمرسل هذا الوصف ومستقبله. وهكذا، تتم الاستجابة إلى القيد الأول.

وتجدر الإشارة كذلك إلى أن تصادمات المصادر SSRC تشكل مشكلة ثانية: يُستخدم المصدر SSRC لتحديد السياق التجفيري وبالتالي الشفرة والمفتاح والعداد، الخ...، لمعالجة الرزم الداخلة. وفي حال وقوع تصادم بين المصادر SSRC، يصبح التعرف على السياق التجفيري غامضاً، وقد لا تحدث المعالجة الصحيحة للرزم. ومن ناحية أخرى، إذا توجب إرسال رزمة BYE RTCP لمصدر SSRC متصادم، فمن الضروري أيضاً تأمين هذه الرزمة.

يتمثل القيد الثاني في وضع العداد ROC عند الصفر عندما يبدأ كل مصدر SSRC بإرسال الرزم. وبالتالي، لا وجود لمفهوم "المشارك المتأخر" في مواصفات أمن بروتوكول SRTP، لأن التدفقات أحادية التوزيع بين الكيانين. ويشكل العداد ROC والرقم SEQ "مؤشر الرزمة" في التغيرات SRTP بالتغيب، مع ضبط العداد ROC تلقائياً عند الصفر في بداية الدورة، وفقاً لهذه التوصية.

ويتمثل القيد الثالث في اختيار القيمة الأولية للرقم SEQ في الفاصل 1 – 15^2..0، ويسمح ذلك بتجنب أي غموض عند ضياع الرزم في بداية الدورة. في بداية الدورة، إذا اختار المصدر SSRC عشوائياً قيمة مرتفعة لرقم التتابع، ووضع المستقبل في حالة من الغموض وإذا ضاعت الرزم الأولية العابرة حتى دورة جديدة لرقم التتابع (أي إذا تجاوز رقم التتابع 1 – 16^2)، فإن المستقبل قد لا يتمكن عندئذ من إدراك أن العداد ROC الخاص به يحتاج إلى زيادة. وبتقييد القيمة الأولية SEQ بالمدى 1 – 15^2..0، فإن تحديد مؤشر الرزمة SRTP سيجد القيمة الصحيحة للعداد ROC، إلا في حالة ضياع إجمالي الرزم الأولى 15^2 (الذي يبدو بعيد المنال إن لم يكن مستحيلاً). انظر الفقرة1.3.3 من مواصفة البروتوكول SRTP فيما يتعلق بتحديد مؤشر الرزمة (RFC 3771).

1.4.4 ربط متأخر للمصادر SSRC بسياق تجفيري

يعتمد مؤشر الرزمة بالتالي على المصدر SSRC والرقم SEQ للرزمة الداخلة والعداد ROC الذي يمثل متغيرة للسياق التجفيري SRTP. وهكذا، يعتمد البروتوكول SRTP بشكل كبير على أحادية المصدر SSRC فيما يتعلق بالأمن. ومع الأخذ بالاعتبار القيود المشار إليها أعلاه، من الممكن إنشاء سياقات تجفيرية SRTP أحادية التوزيع من دون الحاجة إلى التفاوض بشأن القيم SSRC في مواصفة الأمن SRTP. وتوصي هذه التوصية بدلاً من ذلك باتباع نهج يسمى "الربط المتأخر". وعندما تصل رزمة، يمكن ربط المصدر SSRC الذي تحتويه الرزمة بالسياق التجفيري في وقت بداية الدورة (أي عند وصول الرزمة SRTP) بدلاً من وقت تشوير الدورة (أي عند استلام رسالة H.245). ومع وصول الرزمة التي تحتوي على المصدر SSRC، يقوم المستقبل بمعالجة كافة البيانات الضرورية للسياق التجفيري SRTP (مع الإشارة إلى أن قيمة العداد ROC تحديداً تساوي صفراً، وفي حال توفير قيم غير معدومة، سيلزم تشوير إضافي). بمعنى آخر، أن الرسالة H.245 تتعرف بشكل أولي على السياق التجفيري المصاحب لدورة RTP مؤمَّنة تستعمل الربط المتأخر وذلك بالشكل التالي:

<*, address, port>

حيث '*' هي بطاقة نوعية SSRC و"address" هو عنوان الاستقبال المحلي المتأتي من **mediaChannel** و"port" هو مرفأ الاستقبال المحلي المتأتي من **portNumber**. عند وصول الرزمة الأولى التي تحتوي ssrcX في المجال SSRC الخاص بها، يكون السياق التجفيري

<ssrcX, address, port>

مشروحاً مع مراعاة القيود التالية:

- يتم استيقان رزم الوسائط: يجب أن تنجح هذه العملية وإلا لا يستطبق السياق التجفيري؛
- لا يتم استيقان رزم الوسائط: يتم استطباق السياق التجفيري أوتوماتياً.

تجدر الإشارة إلى أنه لا يوصى باستخدام الربط المتأخر في غياب استيقان رزم الوسائط SRTP بسبب الأخطار العديدة التي تهدد أمنه (وبالطبع ينطبق ذلك على بروتوكول SRTP غير المستيقن عموماً).

ويشار أيضاً إلى أن استخدام الربط المخالف من دون استيقان يؤدي إلى إنشاء وضع محلي عند استقبال الرزمة المتأتية من أي مصدر SSRC غير معروف. وبالتالي لا يوصى بعدم استيقان SRTP إذ إنها تسهل الهجمات برفض الخدمة وعلى خلاف ذلك لا يعاني الربط المتأخر مع الاستيقان من هذا الضعف.

2.4.4 تقاسم السياقات التجفيرية بين الدورات أو موارد SSRC

بالنظر إلى القيود والإجراءات الواردة أعلاه، ليس من الضروري الإشارة بوضوح إلى المصدر SSRC والعداد ROC والرقم SEQ بالنسبة لدورة RTP أحادية التوزيع. وبذلك، لا توجد معلمات"crypto" لتشوير هذه العناصر. وبالتالي، في حالة استعمال الربط المتأخر، تتقاسم عدة مصادر SSRC تابعة للكيان نفسه المعلمات التجفيرية SRTP. وتنشأ مصادر متعددة SSRC من الكيان ذاته إما لوجود مصادر متعددة (ميكروفونات وآلات تصوير، إلخ) وإما لأن الحمولات النافعة RTP تحتاج إلى تعدد إرسال المصادر SSRC داخل هذه الدورة نفسها.

يسمح البروتوكول H.245 بتحديد عدة دورات RTP في نفس مواصفة الوسائط. وتتقاسم دورات RTP هذه المعلمات التجفيرية SRTP. ويتقاسم التطبيق الذي يستخدم المعلمة التجفيرية SRTP بهذه الطريقة مفتاحاً رئيسياً بين مختلف الدورات RTP أو المصادر SSRC وسيحل محل المفتاح الرئيسي عندما يوازي العدد الإجمالي للرزم لكافة المصادر SSRC 2^31 رزمة. ويكون كل مصدر من المصادر SSRC التي تتقاسم مفتاحاً رئيسياً مصدراً وحيداً.

ويحدد فترة عمر المفتاح الرئيسي فترات عمر جميع المفاتيح المشتقة من المفتاح الرئيسي. وبذلك، إذا كانت فترة عمر المفتاح الرئيسي تساوي 2^31 رزمة أُرسل مفتاح مشتق رزماً y – 2^31، لا يمكن إرسال إلا الرزم y بواسطة أي مفتاح مشتق من المفتاح الرئيسي. ويعود ذلك إلى أن فترة العمر تستند إلى القصور الحراري أو الطابع العشوائي في المفتاح كما لا يتم إدراج الطابع العشوائي من خلال اشتقاق مفتاح انطلاقاً من مفتاح رئيسي، نظراً لأن الطابع العشوائي أو القصور الحراري هما معلمتان ملازمتان للمفتاح.

3.4.4 حذف السياقات التجفيرية

تتناول الآلية المحددة أعلاه مسألة باستحداث السياقات التجفيرية. إلا أنه من الناحية العملية، قد يبدي المشاركون في الدورة رغبتهم في حذف السياقات التجفيرية قبل نهاية الدورة. فنظراً لأن السياق التجفيري يتضمن معلومات لا يمكن استعادتها أوتوماتياً (مثلاً، العداد ROC)، من المهم أن يتفق المرسل والمستقبل على متى يمكن حذف السياق التجفيري وربما وهو الأهم من ذلك على متى لا يمكن حذفه.

وحتى عندما يُستخدم الربط المتأخر لتدفق أحادي التوزيع، يضيع العداد ROC ولا يمكن استعادته أوتوماتياً (إلا إذا وضع عند الصفر) بمجرد حذف السياق التجفيري.

يجب حذف السياقات التجفيرية عند استلام رسالة **CloseLogicalChannel.** من ناحية أخرى، يخضع هذا الحذف للقواعد نفسها التي تدير حذف المصادر SSRC من جدول الأعضاء (RFC 3711)، وتجدر الإشارة إلى أن ذلك قد يحدث نتيجة لرزمة BYE SRTCP أو انتهاء بسيط بسبب الخمول. وينبغي على المشاركين الخاملين في الدورة الذين يرغبون في ضمان منع انتهاء التوقيت المصاحب لسياقاتهم التجفيرية أن يرسلوا الرزم SRTCP بفواصل زمنية منتظمة.

5 الإجراءات

ينبغي ألا تستخدم الإجراءات SRTP أدناه إلا للتفاوض بشأن أمن تدفقات الوسائط أحادية التوزيع بين كيانين في الحالات التي تكون فيها قناة التشوير H.245 محمية من جانب بروتوكول كبسلة أمن البيانات مثلاً IPsec (RFC 2401) و(RFC 2246) TLS. ويكفل تبادل المعلمات التجفيرية SRTP بواسطة الرسائل H.245 تحقيق الوظائف التالية:

1) تبادل مقدرات تجفير وتكاملية وسائط بروتوكول SRTP والتفاوض بشأنها؛
2) التفاوض بشأن التشفير لخوارزميات الأولية وإنشائها، والمفاتيح ومعلمات الدورة الواجب استخدامها بالنسبة للتدفقات SRTP في كل اتجاه؛
3) تعديل التشفير والخوارزميات والمفاتيح ومعلمات الدورة في أي وقت خلال دورة بروتوكول SRTP.

1.5 تبادل مقدرات الأمن

يحدد العنصر **SrtpCryptoCapability** المتواليات التجفيرية SRTP وخوارزميات التجفير والتكاملية التي يمكن لنقطة طرفية H.323 أن توفرها.

ويتم تحقيق تبادل مقدرات الأمن من خلال تبادل المقدرات بين المطاريف التي تستعمل مدخلاً واحداً أو **h235SecurityCapability** أو أكثر في الجدول **capabilityTable** للرسالة **TerminalCapabilitySet** H.245.

ويُستخدم المجال **mediaCapability** في المدخل **h235SecurityCapability** للجدول **capabilityTable** لربط مقدرة الأمن مع مدخل محدد مقدرة الوسائط في الجدول **capabilityTable**.

يحتوي المجال **encryptionAuthenticationAndIntegrity** في المدخل **h235SecurityCapability** على المجال **genericH235SecurityCapability** الذي يحدد المتواليات التجفيرية SRTP التي تحددها معرفات الغرض H.235.8. إذا كان المجال **standard** للعنصر **capabilityIdentifier** في المجال **genericH235SecurityCapability** يتضمن معرف الغرض H.235.8 (انظر الجدول 1)، فإن المجال **SrtpCryptoCapability** سيحتوي على معلمة واحدة **SrtpCryptoInfo** أو أكثر تمثل المتواليات التجفيرية التي توفرها النقطة الطرفية H.323. كما يحتوي المجال **cryptoSuite** في المجال **SrtpCryptoInfo** على معرف غرض كما هو محدد في الجدول 2 الذي يحدد متوالية تجفيرية معينةً. وداخل المجال **SrtpCryptoInfo**، يحدد المجال **sessionParams** معلمات الدورة ويشير مجال **allowMKI** إلى ما إذا كانت النقطة الطرفية H.323 توفر المعرف MKI.

2.5 التفاوض الأولي

1.2.5 العرض التجفيري الأولي

يُنقل كل عرض تجفيري في رسالة **OpenLogicalChannel** منفصلة ويجب أن يتضمن هيكلية **SrtpCryptoInfo** واحدة في المجال **SrtpCryptoCapability** وهيكلية واحدة **SrtpKeyParameters** أو أكثر في المجال **SrtpKeys**.

وفي حال الإجراءات العادية H.245 (وهي ليست إجراءات توصيل سريع)، ينبغي أن تدمج النقطة الطرفية H.323 العرض التجفيري كما هو وارد في الهيكلين **SrtpCryptoInfo** و**SrtpKeyParameters** في الرسالة **OpenLogicalChannel** H.245 باتجاه الذهاب (من النقطة الطرفية H.323 العارضة إلى النقطة الطرفية H.323 المستجيبة). وينبغي على النقطة الطرفية H.323 أن توفر، من بين قدرات الأمن التي توفرها، المقدرة المشار إليها خلال تبادل القدرات بين المطاريف باعتبارها قدرة الأمن المفضلة للرئيسي.

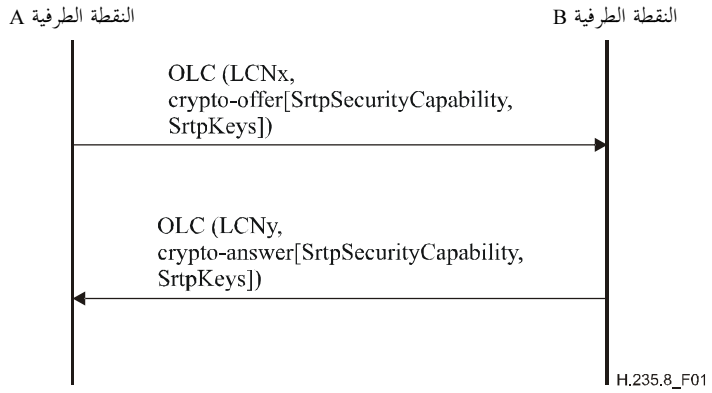
وفي حال إجراءات التوصيل السريع، ترسل النقطة الطرفية العارضة كل عرض تجفيري وارد وصفه في الهيكلين **SrtpCryptoInfo** و**SrtpKeyParameters** و**OpenLogicalChannel** H.245 في رسائل H.245 منفصلة باتجاه الإياب (بين النقطة الطرفية H.323 العارضة والنقطة الطرفية H.323 المستجيبة).

ينبغي إدراج الرسائل **OpenLogicalChannel** المعروفة حسب الترتيب التفضيلي بحيث تدرج أولاً أفضل المتواليات التجفيرية. وبشكل عام، على الصعيد التجفيري، يجب أن تكون المتواليات التجفيرية المفضلة أقوى من المتواليات التجفيرية الأقل تفضيلاً.

عندما يرسل الكيان العارض عرضاً تجفيرياً، ينبغي أن تكون مستعداً لتوفير أمن الوسائط وفقاً لأي من المعلمات التجفيرية المعروضة، وهناك مشكلتان مرتبطتان بذلك هما: أولاً، أن الكيان العارض لا يعرف المفتاح الذي سوف يستخدمه الكيان المستجيب للوسائط المرسلة إلى العارض. وبما أن وسائط الاتصال يمكن أن تصل قبل الاستجابة التجفيرية يمكن أن يحدث تأخير أو وإذا لم يكن هذا مقبولاً من الكيان العارض ينبغي له أن يستعمل آلية مثل إجراء إنشاء النداء المؤجل H.460.11 لمنع حدوث المشكلة المشار إليها أعلاه.

وفي حال تعدد العروض، يمكن أن تظهر مشكلة أخرى: إذ لا يستطيع الكيان العارض أن يحدد أي عرض قبله الكيان المستجيب إلى أن يتم الحصول على الاستجابة التجفيرية ومع ذلك يمكن للوسائط أن تصل قبل الاستجابة التجفيرية. وإذا لم يتقبل هذا الوضع، فإنه يمكن أما ألا يرسل أكثر من عرض واحد وإما أن يستعمل آلية مثل إجراءات إنشاء النداء المؤجل H.460.11 لمنع حدوث المشكلة المشار إليها أعلاه.

يمكن أن يتضمن الهيكل **SrtpCryptoInfo** معلمات الدورة.



الشكل H.235.8/1 – تبادل العرض–الإجابة في حالة توصيل سريع

1.1.2.5 الإجابة التجفيرية الأولية

1.1.1.2.5 اعتبارات عامة

تنطبق هذه الإجراءات على إجراءات التوصيل السريع وعلى الإجراءات H.245 العادية على حد سواء. وينبغي أن تتضمن الإجابة التجفيرية هيكلاً **SrtpCryptoInfo** في العنصر **SrtpCryptoCapability** بالإضافة إلى هيكل واحد أو أكثر من الهياكل **SrtpKeyParameters** في العنصر **SrtpKeys**.

وينبغي أن تطبق النقطة الطرفية H.323 المجيبة المتوالية التجفيرية المختارة من عرض تجفيري مرسل إلى القناة SRTP المناسبة أحادية الاتجاه في اتجاه العودة، ولأن تنتج المفتاح (أو المفاتيح) الواجب استخدامها لهذه القناة SRTP في اتجاه العودة.

إضافة إلى ذلك، تدرج النقطة الطرفية H.323 المجيبة مفتاحاً واحداً أو أكثر في العنصر **SrtpKeys** لاستخدامها للتدفق SRTP بين النقطة الطرفية H.323 المجيبة والنقطة الطرفية H.323 العارضة. ويمكن للنقطة الطرفية H.323 المجيبة أن تدرج أيضاً أي معلمات دورة متأتية من العرض التجفيري ترغب في التفاوض بشأنها.

لا تُقبل إلا المعلمات الصحيحة وهي لا تنتهك أي قواعد عامة محددة لمواصفات الأمن أو أي قاعدة محددة لطريقة النقل والمفتاح المعنية.

بالنسبة إلى التوصيل السريع، ينبغي للكيان المجيب، عند اختيار إحدى العروض التجفيرية الصالحة، أن يختار أفضل العروض التجفيرية التي يمكن توفيرها، أي المعلمة الأولى المدعومة الصالحة في القائمة، مع الأخذ بالاعتبار قدرات الكيان المجيب وسياسات الأمن المطبقة. وفي حال عدم صلاحية أي عرض من العروض، أو عدم توفير أي عرض من العروض الصالحة، ينبغي نبذ تدفق الوسائط المعروض.

عند قبول غرض تجفيري، ينبغي أن تتضمن الإجابة التجفيرية المفتاح (أو المفاتيح) التي سيستخدمها الكيان المجيب بالنسبة للوسائط المرسلة إلى الكيان العارض. وتجدر الإشارة إلى أنه ينبغي توفير مفتاح بغض النظر عن أي معلمات للاتجاه يتضمنها العرض أو الإجابة.

من جهة أخرى، ينبغي إدراج أية معلمة دورة متفاوض عليها في الإجابة التجفيرية. ولا تدرج معلمات الدورة الإعلانية التي يوفرها الكيان العارض في الإجابة التجفيرية، ولكن يمكن للكيان المجيب أن يوفر مجموعة خاصة من معلمات الدورة الإعلانية.

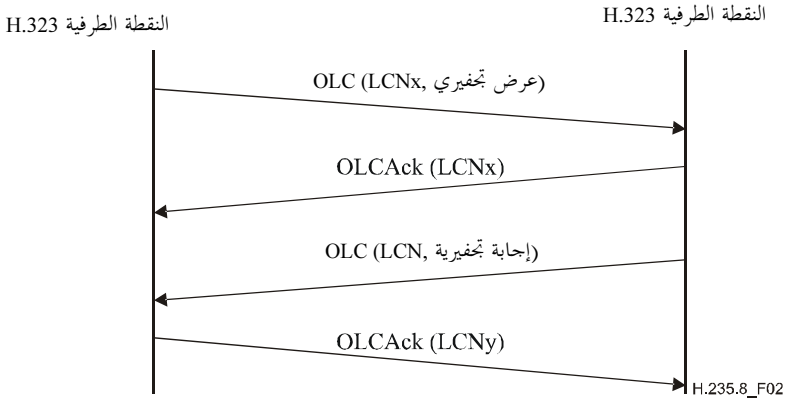
وما إن يستلم الكيان المجيب إحدى المعلمات التجفيرية المعروضة، يمكن لهذا الكيان أن يبدأ بإرسال الوسائط إلى الكيان الذي تقدم بالعرض وفقاً للعرض التجفيري المختار. إلا أنه تجدر الإشارة أيضاً إلى أنه لا يمكن للكيان الذي تقدم بالعرض أن يعالج بشكل صحيح رزم الوسائط هذه طالما أن الإجابة التجفيرية لم تُستلم بعد.

2.1.1.2.5 إجراءات التوصيل السريع

في حال إجراءات التوصيل السريع، ينبغي للنقطة الطرفية H.323 المستقبلة التي تتسلّم العروض التجفيرية في رسالة واحدة أو أكثر من الرسائل **OpenLogicalChannel** H.245 أن تجيب بقبولها أحد العروض من خلال إرسال الرسالة **OpenLogicalChannel** H.245 التي تتضمن إجابة تجفيرية كما هو وارد في الشكل 1، أو من خلال رفض كافة العروض التجفيرية عن طريق إرسال الرسالة **ReleaseComplete** مع العنصر **ReleaseCompleteReason** المضبوط عند **securityDenied**، أو من خلال إرسال العنصر **FastConnectRefused** في رسالة H.225.0. وإذا لم تدعم النقطة الطرفية H.323 المجيبة هذه التوصية أو أي مقترح من المقترحات التي يتضمنها العرض التجفيري ينبغي رفض العرض التجفيري بإرسال رسالة **ReleaseComplete** مع العنصر **ReleaseCompleteReason** مضبوطاً على **securityDenied** أو من خلاله بإرسال العنصر **FastConnectRefused** في رسالة H.225.0.

3.1.1.2.5 الإجراءات H.245 العادية

بالنسبة للإجراءات H.245 العادية (وهي ليست إجراءات توصيل سريع)، تُطبق الطريقة التالية. وإذا لم تكن النقطة الطرفية H.323 قد أرسلت فعليات رسالة **OpenLogicalChannel** تتضمن عرضاً تجفيرياً قبل تسلمها رسالة **OpenLogicalChannel** تتضمن عرضاً تجفيرياً، ينبغي لها إرسال رسالة **OpenLogicalChannelAck** تتضمن الرد التجفيري على النحو المبين في الشكل 2.



الشكل H.235.8/2 – تبادل العرض–الإجابة

إذا أرسلت النقطة الطرفية H.323 فعلياً رسالة **OpenLogicalChannel** تتضمن عرضاً تجفيرياً قبل استلامها رسالة **OpenLogicalChannel**، تتضمن عرضاً تجفيرياً يكون الإجراء الذي تتخذه النقطتان الطرفيتان H.323 للرئيسي والتابع كما يلي:

1) ينبغي للنقطة الطرفية H.323 الرئيسية أن تعالج العرض التجفيري المستلم، وإذا كان العرض موائماً للعرض التجفيري الذي أرسلته فعلياً، عليها أن تقبل العرض التجفيري المستلم باعتباره إجابة تجفيرية وذلك بإرسال رسالة **OpenLogicalChannelAck**، على النحو المبين في الشكل 3. وإذا لم يكن العرض التجفيري المستلم موائماً للعرض التجفيري الذي أرسلته النقطة الطرفية فعلياً،، عليها أن ترفض العرض التجفيري المستلم من خلال إرسال رسالة **OpenLogicalChannelReject** مع القيمة **cause** للعنصر **securityDenied**، على النحو المبين في الشكل 4. ويعني المصطلح "موائم" أنه ينبغي للمعلمات المتتالية في العرض التجفيري أن تتطابق مع المعلمات المتضمنة في الإجابة التجفيرية: **cryptoSuite** ومعلمات الدورة المتفاوض عليها؛

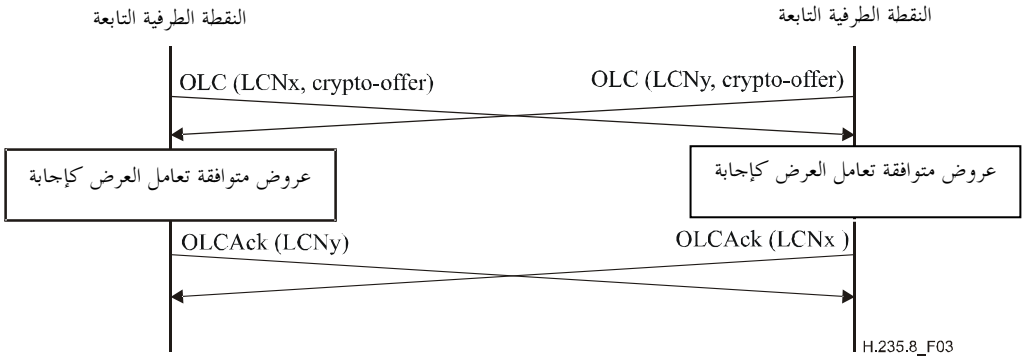
2) تعالج النقطة الطرفية H.323 التابعة العرض التجفيري المستلم، وإذا كان العرض موائماً مع العرض التجفيري الذي أرسلته فعلياً، أن تقبل العرض التجفيري المستلم باعتباره إجابة تجفيرية وذلك بإرسال رسالة **OpenLogicalChannelAck**، على النحو المبين في الشكل 3. وإذا لم يكن العرض التجفيري المستلم موائماً مع العرض الذي سبق وأرسلته فعلياً وإذا كانت ترغب في قبوله، يجب أن تقوم بذلك بإرسال الرسائل المتتالية المشار إليها في الشكل 4.

أ) **OpenLogicalChannelAck** لقبول العرض التجفيري الأولي من جانب العنصر الرئيسي.

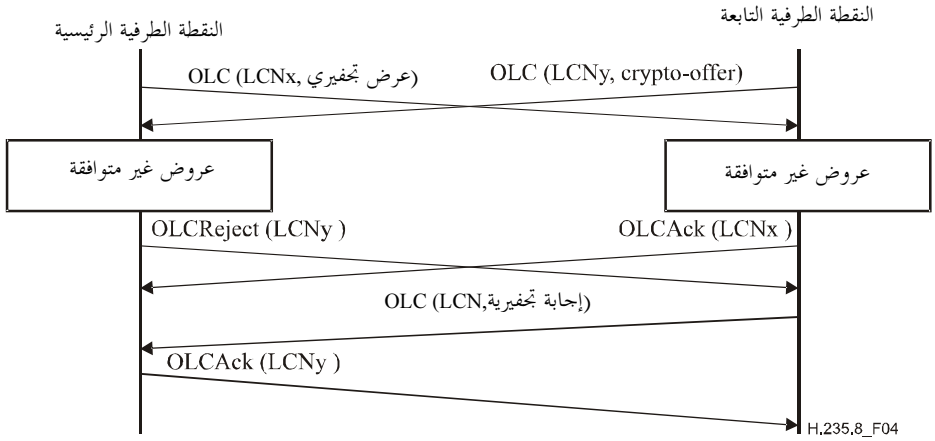
ب) **CloseLogicalChannel** لوضع حد لعرضه التجفيري الأولي إذا لم يستلم الرئيس الرسالة **OpenLogicalChannelReject**.

ج) **OpenLogicalChannel** مع إجابة تجفيرية مطابقة للعرض التجفيري الذي أرسله العنصر الرئيسي.

إذا لم تدعم النقطة الطرفية H.323 التابعة الاقتراح الذي يتضمنه العرض أو إذا لم ترغب في قبول العرض التجفيري، عليها أن تنبذ العرض بإرسال رسالة **OpenLogicalChannelReject** مع القيمة **cause** مضبوطة على **securityDenied**.



الشكل H.235.8/3 – تبادل متزامن لعرض–إجابة متوافقين



الشكل H.235.8/4– تبادل متزامن لعرض–إجابة غير متوافقين

2.1.2.5 معالجة الكيان العارض للإجابة الأولية

عندما يستلم الكيان العارض الإجابة التجفيرية، عليه أن يتحقق من قبول أحد العروض التجفيرية الأولية والإشارة إليه في الإجابة التجفيرية. من كذلك ينبغي أن تتضمن الإجابة التجفيرية مفتاحاً واحداً أو أكثر سوف تُستخدم للوسائط التي أرسلها الكيان المجيب إلى الكيان العارض.

وعلى الكيان العارض أن يتحقق من أن المفاتيح التي تتضمنها الإجابة التجفيرية لا تقابل أي مفتاح من المفاتيح التي يتضمنها العرض التجفيري. يتضمن العرض التجفيري معلمات دورة إلزامية متفاوض عليها، على الكيان العارض أن يتحقق من أن المعلمات المذكورة مدرجة في الإجابة التجفيرية وتقابل المعلمات المناظرة في العرض التجفيري. وإذا كانت الإجابة التجفيرية تحتوي على معلمات دورة إعلانية وإلزامية، ينبغي أن يكون الكيان العارض قادراً على توفيرها.

وفي حال فشل إحدى الأعمال الواردة أعلاه، ينبغي اعتبار عملية التفاوض فاشلة.

3.5 تعديل الدورة

ما إن يتم إنشاء تدفق وسائط بروتوكول SRTP، فإنه يمكن تعديله في أي وقت باستعمال تبادلات جديدة عرض-إجابة بهدف أداء إعادة حساب المفتاح أو تغيير المتوالية التجفيرية. ويجب نقل العرض التجفيري والإجابة التجفيرية الجديدين إلى المعلمتين **SrtpCryptoCapability** و**SrtpKeys** لرسالة **OpenLogicalChannel** H.245 على نحو يسمح بفتح قناة منطقية جديدة تحل محل القناة الموجودة وذلك باستعمال الإجراءات **replacementFor**. وينبغي للنقطة الطرفية H.323 العارضة أن تدرج العروض التجفيرية في رسالة أو أكثر من رسائل **OpenLogicalChannel** H.245 داخل الرسالة H.225.0.

ينبغي للنقطة الطرفية H.323 المجيبة والتي تستلم العروض التجفيرية أن تجيب بقبول أحد العروض من خلال إرسال رسالة **OpenLogicalChannel** H.245 في رسالة H.225.0 أو رفض العروض من خلال رسالة **OpenLogicalChannelReject** مع ضبط القيمة **cause** على **securityDenied**. وإذا تم رفض العرض التجفيري، تبقى المعلمات التجفيرية القديمة مكانها.

عند إنشاء مفتاح رئيسي جديد، يتوقع وجود نافذة زمنية ينبغي من خلالها للنقطة الطرفية H.323 أن تستلم وسائط مجفرة وفقاً للتبادل "عرض-إجابة" القديم والجديد. وينبغي استعمال المعرف MKI المتأتى من رزمة بروتوكول SRTP الداخلة سواء لربط هذه الرزمة مع المفتاح الرئيسي القديم أو الجديد. لهذا السبب، إذا كان من المتوقع تعديل المفاتيح خلال دورة لا تغير عناوين ومنافذ المصدر/المقصد، يكون استخدام المعرف MKI إلزامياً للسماح للمستقبل بالتعرف على البيانات المصاحبة للمفاتيح أثناء تغيير المفاتيح.

4.5 عدم التفاوض

في حال عدم التفاوض بشأن معلمات المتوالية التجفيرية أو المفتاح التجفيري أو الدورة، يحدد المرسل معلمات الأمن المتعلقة بالتدفق المعني. وفي غياب آلية تفاوض، على المرسل أن يدرج بشكل دقيق عرضاً تجفيرياً وعلى المستقبل أن يقبله أو أن يرفضه بإرسال رسالة **ReleaseComplete** مع العنصر **ReleaseCompleteReason** مضبوطاً على **securityDenied** أو رسالة **OpenLogicalChannelReject** مع القيمة **cause** مضبوطة على **securityDenied**. ويختار المرسل المواصفة الأمنية التي يعتبرها الأكثر أمناً لتحقيق غاياته.

5.5 التصحيح الأمامي للأخطاء

يجب تحديد مفتاح رئيسي مختلف لحماية التدفق FEC المرسل إلى عنوان IP و/أو زوج منافذ مختلفة عن تدفق الوسائط SRTP التي ينطبق عليها، على النحو المبين في القسم 1.11 من المعيار RFC 2733. وينبغي إنشاء هذا التدفق من خلال رسالة **OpenLogicalChannel** H.245 منفصلة مع العنصر **dataType** الموضوع عند fec. ويجب نقل المفتاح الرئيسي المصاحب للتدفق FEC في المجال **genericKeyMaterial** للمعلمة **secureSharedSecret (V3KeySyncMaterial)** المتضمنة في

الحاوي h235Key من المعلمة **encryptionSync** للرسالة **OpenLogicalChannel** H.245. وينبغي أن يكون المفتاح الرئيسي مختلفاً عن جميع المفاتيح الرئيسية الأخرى التي يعرضها تدفق الوسائط المصاحب.

6 تجفير بمفتاح عمومي لحماية تبادل المفاتيح في البروتوكول SRTP

يمكن تطبيق إجراءات تجفير إضافية بمفتاح عمومي لضمان السرية من طرف إلى طرف واستيقان بيانات مفتاح الدورة SRTP المتبادلة بين نقطتين طرفيتين H.323 من خلال تجفير تلك البيانات ثم توقيعها. ويمكن استخدام التجفير بمفتاح عمومي عندما ينتهي بروتوكول أمن الكبسلة (مثلاً، IPsec، TLS) على جهاز وسيط وبالتالي، لا يكفل الأمن من طرف إلى طرف.

ويجفر مفتاح الدورة SRTP الذي يجفر الوسائط SRTP من النقطة الطرفية الطالبة إلى النقطة الطرفية المطلوبة باستعمال المفتاح العمومي للنقطة الطرفية المطلوبة والموقع بالمفتاح الخاص للنقطة الطرفية الطالبة. وبالطريقة نفسها، مفتاح آخر للدورة SRTP) يجفر الوسائط SRTP من النقطة الطرفية المطلوبة إلى النقطة الطرفية الطالبة باستعمال المفتاح العمومي للنقطة الطرفية الطالبة والموقع بالمفتاح الخصوصي للنقطة الطرفية المطلوبة. ويمكن تطبيق الإجراء الوارد وصفه في هذه الفقرة على بوابة أو حارس بوابة أو نقطة طرفية.

ويجب نقل مفتاح الدورة SRTP باستعمال أجسام تركيب الرسالة المجفرة (CMS) في الرسائل H.245. ويُستخدم التركيب CMS في توقيع محتوى رسالة اعتباطية مجفرة بشكل رقمي. ويسمح التركيب CMS بعمليات كبسلة متعددة وبالتالي يسمح بتراكب أغلفة الكبسلة بعضها على بعض. وبوجه خاص، يجب نقل بيانات مفتاح الدورة SRTP في جسم التركيب CMS **EnvelopedData** الموقع باستعمال جسم التركيب **SignedData**.

1.6 التعرف على النقاط الطرفية

تُستخدم العناصر التالية للتعرف على نقطة طرفية أو بوابة أو حارس بوابة في شهادة المفتاح العمومي:

- H.323 URL؛
- UR مقيس غير H.323 (مثلاً، *tel*)؛
- تعرف/شهادة الجهاز (بحاجة لمزيد من الدراسة).

ينبغي استخدام شهادة المفتاح العمومي لإعلان تصاحب هوية النقطة الطرفية مع مفتاحها العمومي. وينبغي تخزين H.323 URL أو URL مقيس غير H.323 في المجال **subjectAltName** للشهادة.

يمكن للنقاط الطرفية أن تدير ذاكرة مفتاح محلي تحتوي على شهادات المفتاح العمومي لنقاط طرفية أخرى التي ترغب في إقامة اتصالات مأمونة معها من طرف إلى طرف. وينبغي النقطة الطرفية التي ترسل محتوى موقّعاً لتحقيق الاستيقان من طرف إلى طرف أن تدرج شهادة المفتاح العمومي التي تتضمن المفتاح العمومي الضروري للتحقق من التوقيع. على النقطة الطرفية المستقبلة أن:

أ) تتأكد من أن سلطة ترخيص معترف بها وقعت شهادة المرسل؛

ب) تثق بتأكيد أمني متعلق بالشهادة يقدمه طرف ثالث. ويجب توقيع هذا التأكيد بواسطة بيانات المفتاح القابلة للتحقق بشكل عام.

ملاحظة– يمكن أن يكون ذلك مفيداً في سيناريوهات لا تكون فيها البنية PKI الشاملة متيسرة للمستعملين وتستعمل شهادات فيها موقعة ذاتياً أو شهادات للأجهزة.

2.6 إجراءات تبادل مفتاح البروتوكول SRTP

ترغب النقطتان الطرفيتان الطالبة والمطلوبة في ضمان السرية من طرف إلى طرف واستيقان بيانات مفتاح دورته SRTP عندما يجتاز النداء عند إنشائه جهاز تشوير وسيط أو أكثر، ينبغي لهما استعمال تجفير المفتاح العمومي وX 509 (RFC 3280) وتبادل شهادات المفتاح العمومي.

وتظل إجراءات العرض–الإجابة الواردة في الفقرات السابقة من هذه التوصية كما هي، باستثناء النقاط المشار إليها فيما يلي.

1.2.6 تبادل المقدرات

للتفاوض بشأن استعمال شهادات المفتاح العمومي لتبادل مفاتيح بروتوكول SRTP، تحدد النقطة الطرفية H.323 المجال **genericH235SecurityCapability** في المجال **encryptionAuthenticationAndIntegrity** للمدخل **encryptionAuthenticationAndIntegrity** في الجدول **capabilityTable** لرسالة **TerminalCapabilitySet** H.245 على الشكل التالي:

- ينبغي للمجال **capabilityIdentifier** أن يحتوي على معرف الغرض CMS H.235.8 (انظر الجدول 4) الوارد في المجال **standard**؛
- ينبغي ألا تُستخدم المجالات **maxbitRate** و**collapsing** و**nonCollapsing** و**transport**؛
- ينبغي أن يحتوي المجال **nonCollapsingRaw** على المعلمة **SrtpCryptoCapability.**

2.2.6 تبادل المفاتيح

إذا تعين تجفير مفتاح الدورة SRTP باستخدام مفاتيح عمومية، يُنقل مفتاح الدورة SRTP المجفر ضمن أجسام تركيب الرسالة المجفرة CMS في الرسائل H.245. ويُنقل الجسمان **EnvelopedData** و**SignedData** بدلاً من **SrtpKeys** في المجال **genericKeyMaterial** للمعلمة (**V3KeySyncMaterial**) **secureSharedSecret** المتضمنة في الحاوي **h235Key** في المعلمة **encryptionSync** للرسائل **OpenLogicalChannel** H.245. وينبغي وضع الجسم **EnvelopedData** CMS في المجال **genericKeyMaterial** الذي يتبعه مباشرة الجسم **SignedData** CMS.

وينبغي أن يجفر الهيكل **SrtpKeys** باستخدام مفتاح تجفير المحتوى (CEK) CMS وتُنقل في الهيكل **EncryptedContentInfo** لجسم **EnvelopedData** CMS.

وينبغي تحديد وجود الجسم CMS الذي يحتوي بيانات مفتاح الدورة SRTP في الحاوي **genericKeyMaterial** باستعمال قيمة معرف الغرض CMS H.235.8 (انظر الجدول 4) في المجال **standard** للعنصر **capabilityIdentifier** ضمن المجال **genericH235SecurityCapability** للعنصر **encryptionAuthenticationAndIntegrity** في **h235Media** للنمط **dataType** للرسالة OLC.

الجدول H.235.8/4 – معرف الغرض CMS H.235.8

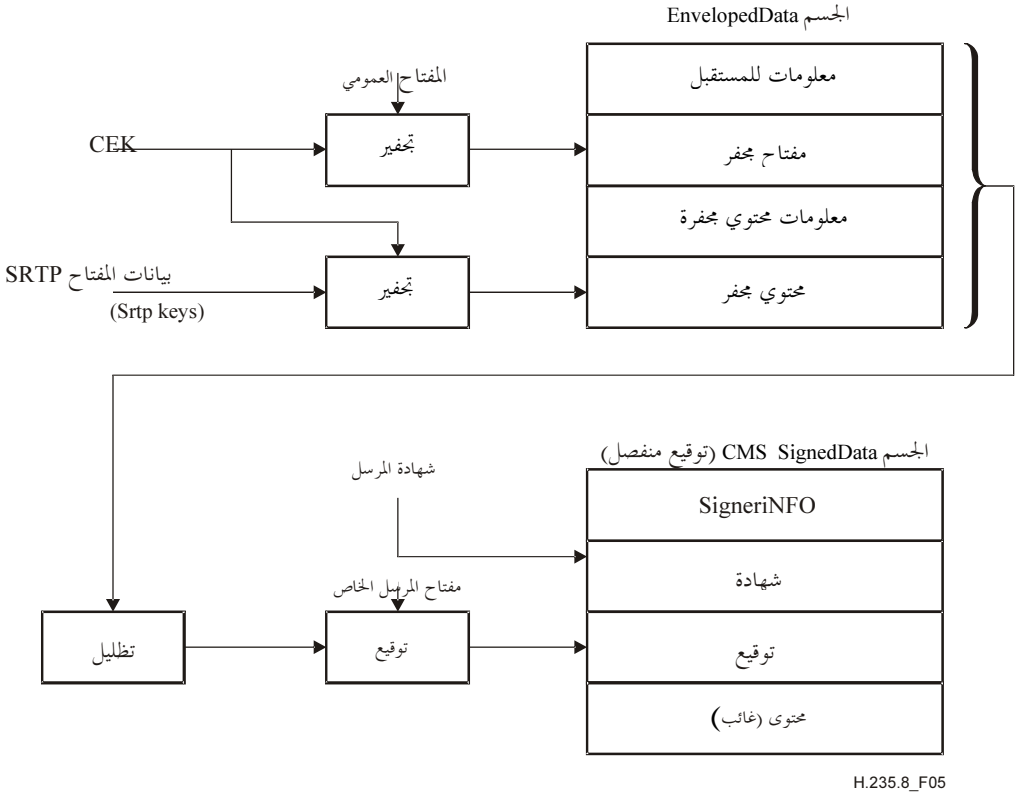
قيمة معرف الغرض
{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 94 }

3.6 استخدام الجسم CMS

ينبغي للنقطة الطرفية التي تنتج بيانات مفتاح الدورة SRTP **SrtpKeys** أي النقطة الطرفية المرسلة، أن تجفر هذه البيانات بواسطة مفتاح التجفير للمحتوى (CEK) CMS، ويكون هذا المفتاح مجفراً من قبل المفتاح العمومي للنقطة الطرفية الأخرى، أي النقطة الطرفية المستقبلة، وعليها أن تضع بيانات مفتاح الدورة SRTP المجفرة في جسم **EnvelopedData** CMS. وعلى النقطة الطرفية المرسلة بعدئذٍ أن توقع رقمياً الجسم **EnvelopedData** بواسطة مفتاحها الخاص وأن

تستحدث "توقيعاً منفصلاً" جسماً **SignedData** CMS. وأخيراً، يجب أن تدرج الشهادة والمفتاح الخاص بها في الجسم **CMS SignedData** وأن ترسل الجسم **EnvelopedData** مع الجسم **SignedData** "توقيع منفصل" إلى النقطة الطرفية المستقبلة. يرد وصف أكثر تفصيلاً في الفقرات التالية لاستحداث الجسمين **EnvelopedData** و**SignedData**.

يظهر في الشكل 5 الجسمان **EnvelopedData** و**SignedData** "توقيع منفصل".



الشكل H.235.8/5 – الجسمان CMS EnvelopedData وSignedData

1.3.6 إجراءات تطبّق على النقطة الطرفية المرسلة

ينبغي للنقطة الطرفية المرسلة أن تطبق الإجراءات التالية بهدف إنتاج بيانات مفتاح الدورة SRTP وتجفيرها وتوقيعها.

1.1.3.6 الجسم EnvelopedData

ينبغي للنقطة الطرفية المرسلة أن تنشئ الجسم **EnvelopedData** كما يلي:

1) إنتاج بيانات مفتاح الدورة SRTP **SrtpKeys** للمتوالية التجفيرية؛

2) إنتاج مفتاح عشوائي لتجفير المحتوى (CEK)؛

3) تجفير المفتاح CEK بواسطة المفتاح العمومي للنقطة الطرفية المستقبلة. ويفترض أن يكون لدى النقطة الطرفية المرسلة مفتاح عمومي وشهادة النقطة الطرفية المستقبلة. وضع معرف الخوارزمية المستخدم لتجفير المفتاح CEK في المجال **keyEncryptionAlgorithm** للهيكل **RecipientInfo.ktri**؛

4) وضع المفتاح CEK المجفر في المجال **encryptedKey** للهيكل **RecipientInfo** لجسم **EnvelopedData**. ويُستخدم المجال **rid** للهيكل **RecipientInfo.ktri** للتعرف على شهادة النقطة الطرفية المستقبلة والمفتاح العمومي الخاص بها المستخدم لتجفير المفتاح CEK؛

5) تجفير معطيات المفتاح **SrtpKeys** SRTP بواسطة المفتاح CEK ووضع معرف الخوارزمية المستخدمة للتجفير في المجال **contentEncryptionAlgorithm** للهيكل **EncryptedContentInfo**.

6) وضع بيانات المفتاح SRTP المجفرة في المجال **encryptedContent** للهيكل **EncryptedContentInfo**.

2.1.3.6 الجسم SignedData

ينبغي للنقطة الطرفية المرسلة أن تنشئ الجسم **SignedData** "توقيع منفصل" على الشكل التالي:

1) حساب ملخص الرسالة أو قيمة التظليل على الجسم **EnvelopedData**. ووضع معرف خوارزمية ملخص الرسالة في المجال **digestAlgorithm** للهيكل **SignerInfo**؛

2) توقيع ملخص الرسالة بواسطة المفتاح الخاص للنقطة الطرفية المرسلة ووضع قيمة التوقيع في المجال **signature** للهيكل **SignerInfo**. ووضع معرف خوارزمية التوقيع في المجال **signatureAlgorithm** للهيكل **SignerInfo**؛

3) وضع الشهادة التي تتضمن المفتاح العمومي للنقطة الطرفية المرسلة في هيكل **certificates** للهيكل **SignerData**. وينبغي ضبط المجال **sid** للهيكل **SignerInfo** أن للتعرف على الشهادة إما بواسطة اسم مميز للمرسل والرقم المسلسل للشهادة، أو قيمة التمديد X.509 subjectKeyIdentifier؛

4) ينبغي للمجال **eContentType** في الهيكل **encapContentInfo** في الجسم **SignedData** أن يتضمن معرف الغرض id-envelopedData. وينبغي للمجال **eContent** للهيكل **encapContentInfo** في الجسم **SignedData** أن يكون غائباً، بما أن ذلك توقيع منفصل وأن المحتوى الفعلي الموقّع هو الجسم **EnvelopedData**.

2.3.6 الإجراءات المطبقة على النقطة الطرفية المستقبلة

ينبغي للنقطة الطرفية المستقبلة أن تنفذ الإجراءات التالية بهدف التحقق من بيانات مفتاح الدورة SRTP وتجفيرها.

إذا لم تتمكن النقطة الطرفية المستقبلة من التصديق على بعض البيانات في الإجراءات الواردة أدناه، يتم رفض النداء بإرسال رسالة **ReleaseComplete** مع ضبط العنصر **ReleaseCompleteReason** على **securityDenied** أو إرسال العنصر **FastConnectRefused** في رسالة H.225.0.

1.2.3.6 الجسم SignedData

ينبغي للنقطة الطرفية المستقبلة أن تتحقق من الجسم **SignedData** "توقيع منفصل" المستقبل على النحو التالي:

1) الحصول على شهادة النقطة الطرفية المرسلة من الهيكل **certificates** للهيكل **SignerData**؛

2) التصديق على شهادة النقطة الطرفية المرسلة. ولا تندرج التفاصيل المتعلقة بالتثبت من صلاحية مسير الشهادة في إطار هذه التوصية. وإذا لم يستطع المستقبِل استيقان النقطة الطرفية المرسلة، فيمكنه رفض النداء؛

3) يمكن للنقطة الطرفية المستقبلة عندئذ أن تضيف الشهادة المصدق عليها إلى ذاكرتها المفتاحية؛

4) التأكد من قيمة التوقيع في المجال **signature** للهيكل **SignerInfo** بواسطة المفتاح العمومي للنقطة الطرفية المرسلة من الشهادة المصدق عليها، ثم استخدام خوارزمية التوقيع المحددة في المجال **signatureAlgorithm** للهيكل **SignerInfo**. وتشكّل نتيجة فك التجفير ملخص الرسالة الذي تحسبه النقطة الطرفية المرسلة على الجسم **EnvelopedData**؛

5) حساب ملخص الرسالة على الجسم **EnvelopedData** المستقبل باستخدام معرف خوارزمية ملخص الرسالة المحدد في المجال **digestAlgorithm** للهيكل **SignerInfo**؛

6) مقارنة قيمة ملخص الرسالة المجفرة بقيمة ملخص الرسالة المحسوبة. وإذا تقابل الملخصان، يمكن عندئذ معالجة الجسم **EnvelopedData**. وفي عكس ذلك، ترفض النقطة الطرفية المستقبلة النداء.

2.2.3.6 الجسم EnvelopedData

ينبغي للنقطة الطرفية المستقبلة أن تستخرج بيانات مفتاح الدورة SRTP للجسم **EnvelopedData** كما يلي:

1) استخدام المجال **rid** للهيكل **RecipientInfo** لتحديد الشهادة والمفتاح الخاص المقابل للنقطة الطرفية المستقبلة في ذاكرة مفتاح هذه النقطة. وإذا استلمت النقطة الطرفية المستقبلة جسماً **EnvelopedData** مجفراً بواسطة مفتاح عمومي غير معروف لها، تقوم النقطة برفض النداء؛

2) استخراج المفتاح CEK المجفر من مجال **encryptedKey** للهيكل **RecipientInfo.ktri** للجسم **EnvelopedData**؛

3) فك تجفير المفتاح CEK المجفر بواسطة المفتاح الخصوصي للنقطة الطرفية المستقبلة والخوارزمية المحددة في المجال **keyEncryptionAlgorithm** للهيكل **RecipientInfo.ktri**؛

4) استخراج بيانات مفتاح دورة SRTP المجفرة من بيانات مفتاح الدورة **(strp)** المجفرة في مجال **encryptedContent** للهيكل **EncryptedContentInfo**؛

5) فك تجفير بيانات مفتاح الدورة SRTP المجفرة بواسطة المفتاح CEK والخوارزمية المحددة في المجال **contentEncryptionAlgorithm** للهيكل **EncryptedContentInfo**.

7 التركيب المتعلق بمواصفات أمن H.235 SRTP

التركيب ASN.1 محدد فيما يلي.

```
H235-SRTP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
GenericData
FROM H323-MESSAGES;


  SrtpCryptoCapability ::= SEQUENCE OF SrtpCryptoInfo -- used in H.245
  genericH235SecurityCapability


  SrtpCryptoInfo ::= SEQUENCE
  {
     cryptoSuite                    OBJECT IDENTIFIER OPTIONAL ,
     sessionParams                  SrtpSessionParameters OPTIONAL,
     allowMKI                       BOOLEAN OPTIONAL,
     ...
  }

  SrtpKeys ::= SEQUENCE OF SrtpKeyParameters  -- used in H.235 V3KeySyncMaterial

  SrtpKeyParameters ::= SEQUENCE
  {
     masterKey                      OCTET STRING,
     masterSalt                     OCTET STRING,
     lifetime                       CHOICE
     {
     powerOfTwo                     INTEGER,
     specific                       INTEGER,
     …
     } OPTIONAL,
     mki                            SEQUENCE
     {
     length                         INTEGER(1..128),
     value OCTET STRING,
```

```
    ...
    } OPTIONAL,
    ...
}


SrtpSessionParameters ::= SEQUENCE
{
    kdr                             INTEGER(0..24) OPTIONAL, -- power of 2
    unencryptedSrtp                 BOOLEAN OPTIONAL,
    unencryptedSrtcp                BOOLEAN OPTIONAL,
    unauthenticatedSrtp             BOOLEAN OPTIONAL,
    fecOrder                        FecOrder OPTIONAL,
    windowSizeHint                  INTEGER(64..65535) OPTIONAL,
    newParameter                    SEQUENCE OF GenericData  OPTIONAL,
    ...
}

FecOrder ::= SEQUENCE
{
    fecBeforeSrtp                   NULL OPTIONAL,
    fecAfterSrtp                    NULL OPTIONAL,
    ...
}

END
```

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

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

طبعت في سويسرا

جنيف، 2006