الاتحـــــــــــاد الـــدولـــــــــي للاتصـــــــــالات

ITU-T

H.235.6

(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: مواصفة التجفير الصوتي مع إدارة مفاتيح H.235/H.245 الأصلية

التوصيـــة ITU-T H.235.6

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

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

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

التوصيـــة ITU-T H.235.6

إطار الأمن H.323: مواصفة التجفير الصوتي مع إدارة مفاتيح H.235/H.245 الأصلية

ملخص

تتضمن هذه التوصية إجراءات الأمن الخاصة بمواصفة التجفير الصوتي (واردة سابقاً في الملحق D/H.235) بما في ذلك ما يصاحبها من إدارة المفاتيح H.235/H.245 الأصلية.

وفي طبعات سابقة من السلسلة الفرعية H.235، كانت هذه المواصفة متضمنة في المتن الرئيسي لـــH.235 وفي ملحقها D. وتعرض التذييلات IV وV وVI للتوصية H.235.0 التقابل التام للفقرات والأشكال والجداول الخاصة بالطبعتين 3 و4 من التوصية ITU-T H.235.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 13 سبتمبر 2005 على التوصية ITU-T H.235.6 بموجب الإجراء المحدد في التوصية A.8.

كلمات رئيسية

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

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

جدول المحتويات

الصفحة

الصفحة

إطار الأمن H.323: مواصفة التجفير الصوتي مع إدارة مفاتيح H.235/H.245 الأصلية

1 مجال التطبيق

تحدد هذه التوصية مواصفة أمن خاصة بالتجفير الصوتي الذي يستعمل إدارة المفاتيح H.235/H.245 الأصلية. وتُحدَّد ضمن هذه التوصية الإجراءات الخاصة بالتجفير الصوتي، وبإدارة مفاتيح H.245 الأصلية المتعلقة به، على السواء

2 المراجع

1.2 المراجع المعيارية

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

- التوصية ITU-T H.225.0 (2003)، *بروتوكولات تشوير النداء ووضع قطار متعدد الوسائط في الرزم لأغراض أنظمة الوسائط المتعددة العاملة بأسلوب الرزم.*
- التوصية ITU-T H.235 الطبعة 1 (1998)، *أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235 الطبعة 2 (2000)، *أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235 الطبعة 3 (2003)، أمن وتجفير المطاريف متعددة الوسائط للسلسلة H *(المطاريف H.323 وغيرها من النمط H.245)* + التصويب 1 (2005)
- التوصية ITU-T H.235.0 (2005)، *إطار الأمن H.323: إطار أمن للأنظمة المتعددة الوسائط من السلسلة H (الأنظمة H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.1 (2005)، *أمن .H323: مواصفة الأمن الأساسي.*
- التوصية ITU-T H.235.2 (2005)، *أمن .H323: مواصفة الأمن بالتواقيع.*
- التوصية ITU-T H.235.3 (2005)، *أمن .H323: مواصفة الأمن الهجينة.*
- 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 H.323 الملحق F (1999)، *أنواع الأجهزة الطرفية البسيطة.*
- التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.*

- المعيار ISO 7498-2: 1989، *أنظمة معالجة المعلومات – التوصيل البيني في الأنظمة المفتوحة – نموذج مرجعي أساسي – الجزء 2: هيكلية الأمن.*
- التوصية | المعيار ITU-T X.803 (1994) ISO/IEC 10745: 1995، *تكنولوجيا المعلومات– التوصيل البيني للأنظمة المفتوحة – نموذج الأمن في الطبقات العليا.*
- التوصية | المعيار ITU-T X.810 (1995) ISO/IEC 10181-1: 1996، *تكنولوجيا المعلومات – التوصيل البيني في الأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: لمحة عامة.*
- التوصية ITU-T X.811 (1995)| المعيار ISO/IEC 10181-2: 1996، *تكنولوجيا المعلومات – التوصيل البيني في الأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار الاستيقان.*
- المعيار IETF RFC 2198 (1997)، *RTP Payload for Redundant Audio Data*
- المعيار IETF RFC 2246 (1999)، *The TLS Protocol Version 1.0*
- المعيار IETF RFC 2401 (1998)، *Security Architecture for the Internet Protocol*
- المعيار IETF RFC 2833 (2000)، *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
- المعيار IETF RFC 3546 (2003)، *Transport Layer Security Protocol (TLS) Extensions*
- US National Institute of Standards, "Advanced Encryption Algorithm (AES)", *Federal Information Processing Standard, (FIPS)* Publication 197, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- المعيار ISO/IEC 9797-1: 1999، *تكنولوجيا المعلومات – تقنيات الأمن – شفرات استيقان الرسالة (MAC) – الجزء 1: آليات استخدام شفرة فدرة.*
- المعيار ISO/IEC 9797-2: 2002، *تكنولوجيا المعلومات – تقنيات الأمن – شفرات استيقان الرسالة (MAC) – الجزء 2: آليات استخدام دالة التقطيع.*
- المعيار ISO/IEC 10118-3: 2004، *تكنولوجيا المعلومات – تقنيات الأمن – الجزء 3: دالات التقطيع المهداة.*
- المعيار ISO/IEC 10116: 2006، *تكنولوجيا المعلومات – تقنيات الأمن – أساليب التشغيل الخاصة بتشفير فدر بعدد بتات n.*

2.2 المراجع البحثية

[DES FIPS-46-2] US National Institute of Standards, Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 46-2, December 1993, http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[DES FIPS-74] US National Institute of Standards, Guidelines for Implementing and Using the Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 74, April 1981, http://www.itl.nist.gov/div897/pubs/fip74.htm.

[DES FIPS-81] US National Institute of Standards, DES Modes of Operation, *Federal Information Processing Standard*, (FIPS) Publication 81, December 1980, http://www.itl.nist.gov/fipspubs/fip81.htm.

[FIPS PUB 180-1] NIST, FIPS PUB 180-1: *Secure Hash Standard*, April 1995 http://csrc.nist.gov/fips/fip180-1.ps.

[LI] ETSI TR 101 772 V1.1.2, Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Lawful interception – top level requirements.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2268] IETF RFC 2268 (1998), *A Description of the RC2(r) Encryption Algorithm*.

[RFC2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

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

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[IKE] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[ISAKMP] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

[J.170] ITU-T Recommendation J.170 (2005), *IPCablecom security specification.*

[RTP] IETF RFC 3550 (2003), *RTP: A transport Protocol for Real-Time Applications*.

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

[SRTP] IETF RFC 3711 (2004), *The Secure Real-Time Transport Protocol*.

3 المصطلحات والتعاريف

تطبق التعاريف الواردة في الفقرات 3/H.323 و3/H.225.0 و3/H.245 لأغراض هذه التوصية. وبعض المصطلحات المستخدمة في هذه التوصية معرَّفة أيضاً في التوصيات X.800 | ISO 7498-2 وX.803 | ISO/IEC 10745 وX.810 | ISO/IEC 10181-1 وX.811 | ISO/IEC 10181-2.

ويولّد المفتاح العمومي، من ناحية أخرى، **مفتاح الدورة (Session Key)** اللازم لتجفير قطارات الوسائط من أجل دورة لبروتوكول النقل بالوقت الفعلي (RTP) (على قناة منطقية مفتوحة (OLC))، على أطول مستوى لنداء واحد. ويجفَّر مفتاح الدورة المتولدة بمفتاح يُشتق من **السر المتقاسم** Diffie-Hellman المتفق عليه الذي قامت كلتا النقطتين الطرفيتين، على السواء، بحسابه. وفي هذه الحالة، يعمل السر المتقاسم–DH كمفتاح عمومي لحماية مفتاح (مفاتيح) الدورة.

4 الرموز والاختصارات

تستعمل هذه التوصية الاختصارات التالية:

3DES معيار التوقيع الرقمي مضاعف ثلاث مرات *(Triple DES)*

AES خوارزمية تجفير متطورة *(Advanced Encryption Algorithm)*

ASN.1 ترميز علم النحو المجرد رقم 1 *(Abstract Syntax Notation One)*

CBC سلسلة فدر التجفير *(Cipher Block Chaining)*

CFB	أسلوب التجفير بالتغذية الراجعة *(Cipher Feedback)*
DES	معيار تجفير المعطيات *(Data Encryption Standard)*
DH	"ديفي هيلمان" *(Diffie-Hellman)*
DTMF	تردد متعدد بنغمة مزدوجة *(Dual Tone Multiple Frequency)*
ECB	أسلوب كتاب الشفرة الإلكتروني *(Electronic Code Book)*
EOFB	أسلوب OFB المحسّن *(Enhanced Output Feedback Mode)*
EP	نقطة طرفية *(Endpoint)*
FEC	تصحيح الخطأ الأمامي *(Forward Error Correction)*
GK	حارس بوابي *(Gatekeeper)*
HMAC	شفرة استيقان الرسائل المظللة *(Hashed Message Authentication Code)*
IPsec	أمن بروتوكول الإنترنت *(Internet Protocol Security)*
ITU	الاتحاد الدولي للاتصالات *(International Telecommunication Union)*
IV	متجه التدميث *(Initialization Vector)*
KS	مفتاح تمليح بأسلوب OFB المحسّن *(Salting Key in EOFB mode)*
MAC	شفرة استيقان الرسالة *(Message Authentication Code)*
MC	كيان تحكم متعدد النقاط *(Multipoint Controller)*
MCU	وحدة التحكم متعددة النقاط *(Multipoint Control Unit)*
MPS	تدفق الحمولة النافعة متعددة الوسائط *(Multiple Payload Stream)*
OFB	أسلوب الخرج بالتغذية الراجعة *(Output Feedback Mode)*
OID	معرف هوية غرض *(Object Identifier)*
OLC	قناة منطقية مفتوحة *(Open Logical Channel)*
RAS	القبول والتسجيل والوضع القانوني *(Registration, Admission and Status)*
RC	شفرة Rivest *(Rivest Cipher)*
ROC	عدّاد دورات كاملة *(Roll-over Counter)*
RSA	خوارزمية ريفست وشامير وأدلمان بالمفتاح العمومي *(Rivest, Shamir and Adleman)*
RTP	بروتوكول النقل بالوقت الفعلي *(Real-Time Protocol)*
RTCP	بروتوكول التحكم في النقل بالوقت الفعلي *(Real-Time Control Protocol)*
SDU	وحدة معطيات الخدمة *(Service Data Unit)*
SEQ	رقم تتابعي *(Sequence number)*
SHA	خوارزمية تظليل أمين *(Secure Hash Algorithm)*
TCP	بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*
TLS	أمن طبقة النقل *(Transport Layer Security)*
TSAP	نقطة نفاذ إلى خدمة النقل *(Transport Service Access Point)*
UDP	بروتوكول داتا غرام للمستعمل *(User Datagram Protocol)*

XOR أو حصراً *(Exclusive OR)*

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

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

عند استعمال تجفير الوسائط بالاقتران مع تحشية الحمولة النافعة، فإن النص أحياناً يشير إلى "إن قيمة الموهن ينبغي أن تحددها الاصطلاحات العادية للخوارزمية المجفرة"؛ انظر مثلاً الفقرة 1.6.7، والفقرة 3.8، والشكل 7.I. ويعني هذا أن بعض الخوارزميات المجفرة (على سبيل المثال، المعيار DES) تسدي مشورة تطبيقية إضافية بشأن الكيفية التي يمكن بها للمرسِل أن يختار قيمة بايتة (بايتات) التحشية. ويمكن أن تكون الأمثلة قيم ملء عشوائية، وقيم سكونية أو متتابعات متولدة أخرى. وأي أسلوب يجري استخدامه لا يؤثر على قابلية التشغيل البيني ومع ذلك فإن نوعية الأمن يمكن أن تكون مختلفة تماماً. ويُعتبر هذا مسألة تنفيذ ومن ثم فلن تعالَج أكثر من ذلك في هذه التوصية.

6 لمحة عامة عن النظام

1.6 مواصفة الأمن بالتجفير الصوتي

مواصفة الأمن بالتجفير الصوتي ليست مستقلة كما هو الحال بالنسبة إلى مواصفة الأمن الأساسي؛ بل هي خيار من مواصفة الأمن المذكورة أعلاه التي يمكن استعمالها مع الأمن الأساسي. ويعتمد الأمن بالتجفير الصوتي أيضاً على بعض خدمات الأمن ضمن إطار تشوير النداء وإجراءات إنشاء التوصيل مثل توافق مفاتيح ديفي–هيلمان وغيرها من وظائف إدارة المفاتيح.

وتستطيع الكيانات H.323 تطبيق التجفير الصوتي للحصول على السرية الصوتية. وهناك أربع خوارزميات للتجفير هي: نظام التجفير بواسطة المعيار المتوائم RC2 أو المعيار DES أو triple-DES على أساس النموذج التجاري واحتياجات التصدير. وإضافة إلى أسلوب التجفير CBC، بإمكان الكيانات H.323 تطبيق أسلوب تجفير التدفق EOFB. وقد لا تتطلب بعض البيئات التي توفر درجة ما من السرية اللجوء إلى التجفير الصوتي. وفي هذه الحالة لا حاجة لإجراء توافق مفاتيح ديفي–هيلمان وغيرها من إجراءات إدارة المفاتيح.

وبالنسبة لخيار السرِّية الصوتية، فإن النظام المقترح هو التجفير باستعمال المعيار AES-128، والمعيار المتوائم RC2، أو DES أو triple-DES على أساس النموذج التجاري واحتياجات التصدير. وقد لا تتطلب بعض البيئات التي توفّر درجة ما من السرِّية اللجوء إلى التجفير الصوتي. وفي هذه الحالة، لا حاجة لإجراء توافق مفاتيح ديفي–هيلمان وغيرها من إجراءات إدارة المفاتيح أيضاً.

وتتضمن المواصفة التي تتناولها هذه التوصية أيضاً قائمة بخوارزميات التجفير الصوتي المرشَّح التي اقترحت في الملحق D من الطبعة 2 من التوصية ITU-T H.235 والملحق D بالطبعة 3 للتوصية ITU-T H.235.

الملاحظة 1 – وهذه المواصفة الجديدة لخوارزميات التجفير تأخذ في الاعتبار التطورات المعروفة في مجال تحليل التجفير ونتائج الأمن بشأن شدة خوارزميات التجفير والتغيُّر في سياسات التصدير التجفيري. وبوجه خاص، تأخذ مواصفة خوارزميات التجفير في هذه التوصية في الاعتبار متطلبات التشغيل البيني مع الأنظمة التي تمتثل للطبعة 2 أو 3 من التوصية H.235.

وينبغي لكيانات H.323 التي تنفذ هذه التوصية مع الطبعة 4 من التوصية H.235 أو طبعة لاحقة لها أن تقترح خوارزمية تجفير متطورة (AES) بطول 128 بتة باعتبارها خوارزمية التجفير الصوتي المفضَّلة في المقدرات الأمنية التي تتيحها لتحقيق أعلى أداء وأفضل أمن. ويمكن لكيانات H.323 تلك بالإضافة إلى ذلك وعلى نحو خياري أن تقترح أيضاً خوارزمية Triple-DES بطول 168 بتة كخوارزمية تجفير صوتي لتحقيق درجة أعلى من قابلية التشغيل البيني مع أنظمة التوصية H.323 التي نفَّذت

سمات التجفير الصوتي في الملحق H.235/D الطبعتين 2 و3. وحيث أن خوارزميات التجفير المتوافقة (القابلة للتصدير) 56 بتة DES و56 بتة RC2 لم تعد تُعتبر آمنة بما فيه الكفاية بأي حال من الأحوال، فإن الكيانات H.323 يجب ألاّ تتيح خوارزميات التجفير الضعيفة إلى حد كبير تلك ما لم تكن هناك حاجة خاصة إلى ذلك من مثل تحقيق قابلية التشغيل البيني مع أنظمة التجفير الصوتي الواردة في الملحق D/H.235 الطبعتين 2 و3.

وينبغي لكيانات H.323 التي تطبق هذه التوصية مع الطبعة 4 من التوصية ITU-T H.235 أن تفضِّل قبول خوارزمية تجفير متطورة (AES) بطول 128 بتة إذا كانت سياستها الأمنية تتيح ذلك. ويجب للكيانات H.323 تلك أن تقبل بالإضافة إلى ذلك المعيار Triple-DES بطول 168 بتة إذا لم تقدَّم له الخوارزمية AES أو لم تسمح له بذلك سياساتها الأمنية. وينبغي لتلك الكيانات H.323 ألاّ تقبل المعيار DES بطول 56 بتة أو المعيار RC2 بطول 56 بتة المتوائم لأسباب أمنية ما لم تتيح سياساتها الأمنية صراحة خوارزميات التجفير غير الآمنة هذه أو ما لم تتطلب احتياجات القابلية للتصدير هذه الخوارزميات، وما لم تُعرض بدائل أكثر أمناً من مثل الخوارزمية AES بطول 128 بتة أو المعيار Triple-DES بطول 168 بتة.

ولا يرد وصف واضح لوسائل التحكم في النفاذ؛ ويمكن تطبيق هذه الوسائل محلياً استناداً إلى المعلومات الواردة في مجالات التجفير H.235 (ClearToken، CryptoToken).

ولا تصف هذه التوصية الإجراءات الخاصة بإسناد كلمات السر/أو المفاتيح السرية عند الاشتراك ولا إجراءات الإدارة والشؤون الإدارية المرتبطة بها. فهذه الإجراءات يمكن أن تحدث بوسائل تتجاوز نطاق تناول هذه التوصية.

وتستطيع كيانات الاتصال المعنية أن تحدد ضمنياً أي مواصفة أمن أساسية وأي مواصفة أمن مع التوقيع هي التي يتعين استعمالها بتقييم معرِّفات أغراض الأمن المشوَّرة في الرسائل (**tokenOID** و**algorithmOID**؛ انظر أيضاً الفقرة 11).

ويلخص الجدول 1 سمات الأمن لمواصفة التجفير الصوتي. ومواصفة التجفير الصوتي هذه محددة في الفقرات 7 و8 و9.

الجدول H.235.6/1 – مواصفة التجفير الصوتي

خدمات الأمن	وظائف النداء			
	RAS	H.225.0	H.245	RTP
الاستيقان والتكامل				
عدم النكران				
السرية				128-bit AES / 168-bit triple-DES / 56-bit RC2-متوائمة / 56-bit DES أسلوب CBC أو أسلوب EOFB
التحكم بالنفاذ				
إدارة المفاتيح		تبادل مفاتيح ديفي هيلمان بعد الاستيقان	إدارة مفاتيح H.235 متكاملة (تبادل مفاتيح ديفي هيلمان بعد الاستيقان)	

يقيم الإجراء العام سراً مشتركاً (تبادل ديفي–هيلمان) بين طرفي الاتصال عند إطلاق التوصيل. ويستعمل هذا السر المشترك بعد ذلك في حماية (مجموعة من) مفاتيح الوسيط المستخدمة لتجفير دورات الوسائط (RTP).

ومواصفة الأمن بالتجفير الصوتي تحسين خياري لمواصفة الأمن الأساسية ومواصفة الأمن بالتوقيع؛ ويمكن التفاوض بشأن استعمالها في سياق التفاوض بشأن مقدرة أمن المطراف. وفي البيئات التي تكون فيها السرية الصوتية مضمونة بواسطة وسائل أخرى، من غير الضروري تطبيق تجفير الوسيط وإجراءات إدارة المفاتيح المتصلة به (توافق المفاتيح ديفي–هيلمان وتحديثها وتزامنها).

وخوارزميات التجفير المستخدمة هنا هي: AES وRC2 المتوائمة وDES وtriple-DES .

ملاحظة – نظراً إلى إمكانية استخدام الخوارزمية DES للمعيار triple-DES ينجم عن ذلك تطبيق متماسك.

وبمعزل عن اختيار خوارزمية تجفير الوسيط المحدد ينبغي اتباع الخيارات التالية بوضوح:

- توليد متجه التدميث (IV) حسب الاقتضاء، وهو محدد في الفقرة 1.3.9؛
- القيام بعملية الملء حسب الاقتضاء، كما هو محدد في الفقرة 2.3.9.

وينبغي تجفير الحمولة النافعة السمعية بواسطة خوارزمية التجفير التي تم التفاوض بشأنها ("X" أو "Y" أو "Z3" أو "Z") طبقاً للإجراءات الوارد وصفها في الفقرة 9 و3.9 ولطرائق التجفير بالحشو الواردة في I.1. ويمكن تجفير الحمولة النافعة السمعية باستعمال خوارزمية التجفير بالتفاوض ("X1" أو "Y1" أو "Z1" أو "Z2") العاملة بأسلوب تجفير التدفق (EOFB).

7 تشوير وإجراءات التوصية H.245

بصورة عامة يجري التحكم في أوجه الجوانب المتعلقة بالخصوصية بالطريقة نفسها التي يجري التحكم فيها بأية معلمة تشفير أخرى، ويشير أي مطراف إلى مقدراته وينتقي مصدر المعطيات للاستعمال ويعطي المستقبل إشعاراً باستقبال الأسلوب أو برفضه. فيشار إلى جميع أوجه الآلية المستقلة عن النقل مثل انتقاء الخوارزمية بواسطة عناصر تنوعية للقناة المنطقية. وتنقل خصائص النقل مثل تزامن خوارزمية المفتاح/التجفير في البنى الخاصة بالنقل.

1.7 تشغيل آمن للقناة H.245

يجب أن يتم الحوار الذي جرى التفاوض بشأنه والاستيقان للقناة المنطقية H.245 قبل تبادل أية رسائل H.245 أخرى افتراضاً أن إجراءات التوصيل في الفقرة السابقة (إجراءات إقامة التوصيل) تشير إلى أسلوب تشغيل آخر. ويجب أن يجري كل تبادل للشهادات باستعمال أية آلية ملائمة لمطراف (مطاريف) السلسلة H إذا ما جرى التفاوض بشأنه. وبعد توفير أمن القناة H.245 تستعمل المطاريف البروتوكول H.245 بالطريقة نفسها التي تستعمله في أسلوب غير آمن.

2.7 تشغيل قناة التوصية H.245 غير الآمن

كما يمكن لقناة التوصية H.245 أن تعمل بطريقة غير آمنة يمكن للكيانين أن يفتحا قناة منطقية آمنة يمكن إجراء الاستيقان و/أو اشتقاق السر المشترك بواسطتها. فيمكن مثلاً أن يستعمل الأمر TLS أو IPsec عن طريق فتح قناة منطقية مع المجال **dataType** الذي يتضمن قيمة للمعلمة **h235Control**. وبعد ذلك يمكن استعمال تلك القناة لاشتقاق سر مشترك يحمي أية مفاتيح دورة وسيطة أو لنقل **EncryptionSync**.

3.7 تبادل المقدرات

عملاً بالإجراءات التي تنص عليها الفقرة 2.5 من التوصية H.245 (إجراءات تبادل المقدرات) وتوصية نظام السلسلة H الملائمة تتبادل النقاط الطرفية المقدرات باستعمال رسائل التوصية H.245. ومن الممكن أن تتضمن الآن مجموعات المقدرات هذه تعاريف تشير إلى المعلمات الأمنية والتجفيرية. فقد تشير نقطة طرفية مثلاً إلى مقدرات إرسال معطيات فيديوية H.261 عادية أو مجفرة واستقبالها.

وتنطوي كل خوارزمية تجفير تستعمل مع مفكك تشفير الوسائط على تعريف جديد للمقدرة. وكما هو الحال مع المقدرة الأخرى فمن الممكن أن تزود النقاط الطرفية مفككات تشفير مجفرة مستقلة وتابعة في تبادلها. ويسمح هذا للنقاط الطرفية بتدريج مقدراتها الأمنية على أساس الرأسية والموارد المتيسرة.

وبعد استكمال تبادل المقدرات من الممكن فتح قنوات منطقية آمنة للوسيط بالطريقة نفسها التي قد تفعل بطريقة غير آمنة.

4.7 الدور الرئيسي

تستعمل علاقة الرئيس–التابع H.245 لإقامة الكيان الرئيسي من أجل تشغيل قناة ثنائية الاتجاه وحل نزاعات أخرى. ويستعمل هذا الدور الرئيسي أيضاً في الوسائل الأمنية. ومع أن المصدر يحدد الأسلوب الأمني (الأساليب الأمنية) لتدفق الوسائط (مراعاة لمقدرات المستقبل) يكون الرئيس هو النقطة الطرفية التي تولد مفتاح التجفير. ويحصل توليد مفتاح التجفير هذا بغض النظر عما إذا كان الرئيس مستقبل الوسائط المجفر أو مصدره. ولإتاحة تشغيل قنوات متعددة المقاصد مع مفاتيح مشتركة ينبغي أن تنتج الوحدة MCU (وهي أيضاً الرئيس) المفاتيح.

5.7 تشوير القناة المنطقية

تفتح النقاط الطرفية قنوات منطقية وسيطة آمنة بالطريقة نفسها التي تفتح بها القنوات المنطقية الوسيطة غير الآمنة. ومن الممكن أن تشتغل كل قناة بطريقة مستقلة تماماً عن قنوات أخرى – خاصة عندما يرتبط هذا بالأمن. ويجب تعريف الأسلوب المعين في المجال **OpenLogicalChannel dataType**. ويجب نقل مفتاح التجفير الأولي عبر المجال **OpenLogicalChannel** أو **OpenLogicalChannelAck** ويتوقف هذا على علاقة الرئيس/التابع للمرسل **OpenLogicalChannel**.

ويجب أن تكون الرسالة **OpenLogicalChannelAck** تأكيداً لأسلوب التجفير. وإذا كان الأمر **openLogicalChannel** غير مقبول للمستقبل يجب إعادة **dataTypeNotSupported** أو **dataTypeNotAvailable** (شرط مؤقت) في المجال سبب الرسالة **OpenLogicalChannelReject**.

خلال تبادل البروتوكول الذي يقيم القناة المنطقية يجب إرسال مفتاح التجفير من الرئيس إلى التابع (بغض النظر عن مرسل رسالة **OpenLogicalChannel**). وبالنسبة إلى القنوات الوسيطة التي تفتحها النقطة الطرفية (غير الرئيس) يجب أن يعيد الرئيس مفتاح التجفير الأولي ونقطة التزامن الأولية في **OpenLogicalChannelAck** (في المجال **encryptionSync**). أما بالنسبة إلى القنوات الوسيطة التي يفتحها الرئيس يجب أن تشمل رسالة **OpenLogicalChannel** مفتاح التجفير الأولي ونقطة التزامن في المجال **encryptionSync**.

6.7 الأمن بالتوصيل السريع

قد تطبق النقاط الطرفية إجراء توصيل سريع (انظر الفقرتين 7.1.8 و8.1.7.1/H.323) باستعمال عنصر الانطلاق السريع بهدف التمكن من تبادل عناصر هامة (المفتاح الرئيسي ومفتاح تجفير الدورة) بأمان تام. وتتيح الإجراءات المحددة في الفقرة 1.6.7 انطلاقاً سريعاً "بسيطاً" دون اللجوء إلى خوارزميات التجفير المتعددة المقترحة؛ وعلى العكس من ذلك تصف الفقرة 1.1.6.7 الحالة الخاصة للانطلاق السريع عندما يتم اقتراح عدة خوارزميات تجفير تساعد على تشفير مكثف للرسائل.

1.6.7 أمن أحادي الاتجاه بالانطلاق السريع

يصف هذا الإجراء كيفية إنشاء قناة منطقية أحادية الاتجاه للأمن (نصف مزدوجة) بين الطالب والمطلوب.

الإجراءات من جهة الطالب

يقدم الطالب (مصدر العملية SETUP) فيشته DH والبنى FastStart التي يوفرها في نفس الوقت. وتسير الفيشة DH في المعلمة ClearToken المدمجة في فيشة CryptoToken أو في شكل معلمة ClearToken منفصلة، انظر أيضاً الفقرة 8.7. وخلال الفترة المقضية بين SETUP وCONNECT ينبغي تبادل الفيشة ديفي هيلمان (DH) التي تعطي إلى النقطتين الطرفيتين سراً مشتركاً. وينبغي أن يضم المجال **ClearToken** من المجالات **CryptoToken** مفتاحاً **dhkey** يستعمل لإرسال المعلمات كما هو وارد

في هذه التوصية. ويضم المجال **halfkey** المفتاح العمومي العشوائي بجزء واحد ويضم المجال **modsize** DH-prime ويضم المجال **generator** DH-group. ويعرض الجدول 4 المعلمات DH الواجب استعمالها. ولمزيد من التفاصيل [راجع RFC2412، التذييل E2].

الملاحظة 1 – بما أن الرسائل H.225.0 تخضع للاستيقان (كما سبق وورد في الإجراء I) فإن التبادل DH تبادل مستيقن.

عندما تتوفر معلومة تعرف الهوية وفي كل اتجاه لرسالة تشوير نداء H.225.0 تسيِّر نصف مفتاح ديفي هيلمان، ينبغي على الطالب أو المطلوب في حال تسجيلهما أن يدرجا فيشة **ClearToken** من طرف إلى طرف مع معرف الهوية **sendersID** موضوعاً على قيمة معرف هوية النقطة الطرفية للمرسل ذي المعلمة **tokenOID** الموضوعة على "E". وينبغي أن ينقل كل كيان تشوير H.323 وسيط هذه الفيشة الخاصة من طرف إلى طرف دون تعديل.

وتبقي البنى FastStart على القنوات المنطقية مفتوحة مع مقدرات الأمن المقترحة. وينبغي اقتراح القناتين H235Cap وnonH235Cap. وتقدم النقاط الطرفية المداخل **H235SecurityCapability** للكودكات التي توفرها وذلك أثناء تبادل المقدرات H.245. ويتم جمع كل كودك مع مقدرة أمن H.235 فردية. وينبغي أن تشير هذه المقدرات وفقاً للجدول 6 إلى توفير المعيار AES-CBC بمعدل 128 بتة ("Z3"-OID) أو المعيار RC2-CBC المتوائم ("X" - OID) أو المعيار DES-CBC بمعدل 56 بتة ("Y" - OID). وبإمكانها أن تشير إلى توفير المعيار Triple-DES-CBC بمعدل 168 بتة ("Z" - OID) أو المعيار Triple-DES-EOFB بمعدل 168 بتة ("Z1" - OID) أو المعيار RC2-EOFB المتوائم ("X1" - OID) أو المعيار DES-EOFB ("Y1" - OID) أو المعيار AES-EOFB ("Z2" - OID).

تسيِّر الرسالة **OpenLogicalChannel** المعلمات **forwardLogicalChannelParameters** و**reverseLogicalChannelParameters** في نفس الوقت مع المعلمة **dataType** التي توفر **h235Media** مع **encryptionAuthenticationAndIntegrity** حيث ينبغي وجود خوارزمية واحدة **MediaEncryptionAlgorithm** كحد أقصى في المقدرة **encryptionCapability**.

ويكون المطلوب هو الرئيس مسبقاً لأغراض علاقات الأمن، انظر أيضاً الفقرة 4.7.

وعلى الطالب أن يضع العنصر **mediaWaitForConnect** على القيمة "true"، للتأكد من أن عناصر مفتاح الدورة متوفرة وأن الوسائط المشفرة قابلة لفك التشفير. وفي السيناريوهات التي ترغب في "وسيط دون انتظار" وهي طريقة يتمكن المطلوب فيها من إرسال وسائط مجفرة وغير مجفرة في نفس الوقت وإرسال رسالة الاستجابة وعناصر مفاتيح التجفير، ينبغي على الطالب مبدئياً أن يعرف عدم قدرته على تشفير المحتوى إلا في حال توفر عناصر المفاتيح لديه.

الملاحظة 2 – في هذه الحالة إذا أرسل المطلوب الوسيط المجفر إلى الطالب (الأمر الذي يستطيع نظرياً فعله باعتبار أنه يمتلك العناوين RTP/RTCP للطالب)، لن يكون الطالب قادراً على فك التشفير دون الحصول على السر المشترك الذي توفره الرسالة (Call Proceeding ،Alerting).

الإجراءات من جهة المطلوب

يقدم المطلوب فيشته DH (انظر أيضاً الفقرة 8.7) والبنى FastStart التي توفرها خلال طور الانطلاق السريع (FastStart). ويوصي المطلوب في حال تطبيق الإجراء ديفي هيلمان بأن يرسل فيشته DH في رسالة الاستجابة في أقرب وقت ممكن؛ أي في رسالة الاستجابة التي تلي مباشرة الرسالة SETUP. مما يتيح للطالب أن يحسب المفتاح الرئيسي استناداً إلى السر المشترك DH وأن يستعد لاستقبال مفتاح الدورة والوسيط المجفر.

الملاحظة 3 – في حال عدم توفر خوارزمية تجفير من الجهتين تماشياً مع سياسة الأمن، قد يبقى تدفق المعطيات دون تجفير أو قد ينقطع التوصيل.

يأخذ كل كيان البتات المناسبة الأقل دلالة الواردة من السر المشترك ديفي–هيلمان لمفتاح التجفير الرئيسي (المفتاح الرئيسي)؛ أي البتات الست والخمسين الأقل دلالة من السر ديفي–هيلمان للمعرّفات "X" OID أو "X1" OID أو "Y1" OID أو "Y" OID، والبتات المائة والثماني والستين الأقل دلالة الواردة من السر ديفي–هيلمان للمعرّفات "Z" OID أو "Z1" OID أو "Z2" OID، والبتات المائة والثماني والعشرين الأقل دلالة من السر ديفي–هيلمان للمعرّفات "Z3" OID أو "Z2" OID. انظر أيضاً الجدول 6.

ترسل الاستجابات **OpenLogicalChannel(Ack)** مع مفتاح الدورة (الرئيسي) المولَّد والمدرج في المجال **encryptionSync**. ويضم هذا المجال مفتاح الدورة للقناة المنطقية طالب ← مطلوب. ويحصل تسيير المفتاح طبقاً للإجراء الوارد وصفه في الفقرة 3.8 باستعمال العنصر **KeySyncMaterial** أو العنصر **V3KeySyncMaterial** (انظر الفقرة 1.3.8). وينبغي تجفير مفتاح الدورة بواسطة السر المشترك DH وباتباع الطريقة الواردة أدناه.

الملاحظة 4 – لا توجد طريقة إلزامية لإنتاج مفاتيح الدورة التي تستعمل في تجفير الوسائط. وإنتاج هذه القيم مسألة تنفيذ تتوقف على الموارد وسياسة التجفير وخوارزمية التجفير الواجب استعمالها. ويستحسن توخي الحذر لتجنب إنتاج مفاتيح ضعيفة.

ينبغي إرسال مفتاح الدورة المجفر في المجال **H.235Key/sharedSecret** لمجال **encryptionSync** بواسطة الإجراء المحدد في الفقرة 3.8. وينبغي إرسال مفتاح الدورة في المجال **keyMaterial** للرسالة **KeySyncMaterial**. وفي حال عدم توافق القد مع مضاعف عدد صحيح من الفدر ينبغي تكميله بالحشو حتى يصبح مضاعفاً لعدد صحيح من الفدر قبل التجفير. ويتحدد اتساع الحشو في الاصطلاح العادي لخوارزمية التجفير، ويكون العنصر **KeySyncMaterial** (الذي خضع لعملية الحشو) مجفراً باستعمال ما يلي:

- البتات الست والخمسين للسر المشترك بدءاً من البتات الأقل دلالة لسر ديفي–هيلمان للمعرّفات "X" OID أو "X1" OID أو "Y1" OID أو "Y" OID؛
- جميع بتات السر المشترك للمعرّفات "Z2" OID أو "Z" OID أو "Z1" OID، بدءاً من البتات الأقل دلالة للسر DH.

وكبديل مفضل، يستحسن استعمال آلية النقل بالمفتاح المحسَّن وفقاً للفقرة 1.3.8، بسبب نتيجة تطبيق إجراء الدلالة المحدد للطبعة 3 (انظر الفقرة 2.8).

وفي الحالة التي يتوجب فيها إنشاء قناة آمنة لوسيط مزدوج الإرسال متكامل، تؤخذ من بين قناتين أحاديتي الاتجاه باستعمال الإجراء fast start فإنه ينبغي للمطلوب أن يفتح قناة منطقية ثانية باتجاه الطالب. ويشار إلى هذه القناة المنطقية في عنصر fastStart منفصل. ويدخل المطلوب مفتاح دورة مختلف لأغراض هذه القناة المنطقية في المجال **encryptionSync** باستعمال السر المشترك DH المتوفر كمفتاح رئيسي.

1.1.6.7 استعمال خوارزميات التجفير المتعددة في الإجراء fast connect

يؤدي التفاوض بشأن تجفير الوسيط في إطار الإجراءات fast connect إلى توسيع غير مجد لعدد العناصر **OpenLogicalChannel** في العنصر **fastConnect** في رسالة SETUP. وذلك يحدث بسبب اشتراط وجود عنصر **OLC** (OpenLogicalChannel) مستقل لكل تجميعة كودكات (**dataType**) مع خوارزمية تجفير (بما في ذلك "لا شيء").

تتحدد خوارزمية التجفير الواجب تطبيقها على تدفق معطيات بإدراج المجال **dataType.h235Media.encryptionAuthenticationAndIntegrity.encryptionCapability dataType** في العنصر **OLC**. وتنطوي العملية المحددة في التوصية H.235v2 على عدم إدراج سوى عنصر واحد **MediaEncryptionAlgorithm** في العنصر **encryptionCapability** بالرغم من أن هذا العنصر الأخير محدد بأنه تتابع عناصر سابقة. ويتيح هذا الإجراء إدراج تتابع من مقدرات التجفير حسب ترتيب الأفضلية في كل قناة **OLC** مقترحة. وينبغي أن ينتقي مستقبل القناة **OLC** عندئذ خوارزمية واحدة من بين تلك المقترحة عليه وأن يعيد إرسال القناة **OLC** مع الخوارزمية الوحيدة المختارة والحاضرة (مع عناوين النقل المناسبة ومعطيات مفتاح التجفير).

ومن أجل الحصول على أقصى فعالية يقدم معرّف هوية الغرض "NULL-ENCR" (انظر الجدول 2) خوارزمية التجفير "لا شيء" (null) التي تعني وجوب عدم وجود أي عملية تجفير. ولا يتطلب استعمال هذه الطريقة الخاصة إلا قناة **OLC** واحدة للكودك الواحد والاتجاه الواحد.

الجدول H.235.6/2 – معرف هوية الغرض للتجفير NULL

مرجع معرف الغرض	قيمة معرف هوية الغرض	الوصف
"NULL-ENCR"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 26}	يدل على "خوارزمية التجفير NULL"

إجراء يطبق على الطالب (انظر الفقرة H.323/1.7.1.8)

إذا حدد عنصر **dataType** ما تجفيراً عبر الخيار **h235Media**، استطاع العنصر المدرج **encryptionAuthenticationAndIntegrity** إدخال عنصر **encryptionCapability** يحتوي على عدة خوارزميات تجفير (بما فيها الخوارزمية NULL). وينبغي استعمال هذه البنية بغية توفير خيار من بين الخوارزميات المحددة لأغراض تجفير مقدرة الوسيط المصاحبة.

إجراء يطبق على المطلوب (انظر الفقرة H.323/1.7.1.8)

في حال اقتراح عدة خوارزميات تجفير لقناة معينة، ينبغي أن تختار النقطة الطرفية المطلوبة واحدة منها وأن تغير العنصر **OpenLogicalChannel** بحيث تستبعد الخوارزميات الأخرى.

2.6.7 أمن التوصيل السريع ثنائي الاتجاه

يتطلب موضوع الأمن فيما يخص القنوات ثنائية الاتجاه للمعطيات T.120 مزيداً من الدراسة.

7.7 الإشارات H.245 DTMF المجفرة

يجوز للنقاط الطرفية إرسال إشارات DTMF مجفرة بهدف الحصول على بعض السرية. وتستطيع النقاط الطرفية بواسطة مفتاح تجفير الدورة أن تجفر الإشارات DTMF في المعلمة **UserInputIndication** على شكل:

- سلسلة عناصر مجفرة: **encryptedAlphanumeric**؛
- سلسلة iA5 مجفرة: **encryptedSignalType** في **signal**؛
- سلسلة عامة مجفرة **encryptedAlphanumeric** في **extendedAlphanumeric**.

الملاحظة 1 – لا يتم تجفير المعلمات الإضافية لأغراض البروتوكول RTP في السلسلة iA5 مع الساعة والتاريخ وأرقام القنوات المنطقية أو التحديثات التي تجرى على الإشارة مع مدة النغمات، نظراً إلى اعتبار أنها لا تنقل معلومات حساسة.

تعود المقدرة **secureDTMF** التي يتم التفاوض بشأنها إلى السلسلة iA5 المجفرة.

ينبغي تطبيق إدارة المفاتيح كما وردت في الفقرة 1.6 للحصول على مفتاح تجفير الدورة. وينبغي استعمال هذا المفتاح لتجفير الإشارات DTMF H.245 (RFC 2833).

الملاحظة 2 – لا ينطوي ذلك بالضرورة على استعمال مفتاح الدورة أيضاً لتجفير الحمولة النافعة RTP.

غير أنه عند استعمال الإشارات DTMF عن طريق البروتوكول RTP بوضع المؤشر **rtpPayloadIndication** يوصي بشدة توفير الأمن للحمولة النافعة RTP باستعمال مواصفة تجفير الصوت الوارد في الفقرة 1.6.

ويشير الجدول 3 إلى خوارزميات التجفير المتاحة (DES أو 3DES أو AES) التي من شأنها أن تطبق الأسلوب EOFB (المتضمن للأسلوب OFB كحالة خاصة. انظر الفقرة 4.8). ومن أجل تفادي احتمال حشو السمات DTMF (RFC 2833)، فإنه لا يوصي باستعمال الفدر CBC أو CFB أو غيرها من أساليب تسلسل الفدرة التي قد تجعل الحشو ضرورياً، لأغراض تجفير الإشارات DTMF (RFC 2833).

1.7.7 سلسلة مجفرة أساسية

في حال انتقاء المعلمة **encryptedBasicString** في المقدرة **UserInputCapability** ينبغي أن تشير المعلمة **encryptedAlphanumeric** إلى خوارزمية التجفير المطبقة في المعرف **algorithmOID** مع العلم أن العنصر **paramS** يضم القيمة الأولية لعملية التجفير. وينبغي وضع السلسلة الهجائية الرقمية في **encrypted**.

2.7.7 السلسلة المجفرة iA5

في حال انتقاء المعلمة **encryptedIA5String** في المقدرة **UserInputCapability** ينبغي أن تضم المعلمة **encryptedSignalType** النمط **ClearSignalType** المجفر الذي يحتوي فيه العنصر **sig** على السمة **signalType** لحروف عادية. وينبغي أن يضم **signalType** سمة "!" متخيلة على المرسل إليه أن يحذفها.

وينبغي أن يشير العنصر **algorithmOID** إلى خوارزمية التجفير المستعملة مع العلم أن **paramS** يحتوي على القيمة الأولية لعملية التجفير.

3.7.7 السلسلة المجفرة العامة

في حال انتقاء المعلمة **encryptedGeneralString** في المقدرة **UserInputCapability** ينبغي أن يشير العنصر **encryptedAlphanumeric** الموجود في **extendedAlphanumeric** إلى خوارزمية التجفير المستعملة في المعرّف **algorithmOID** بينما ينبغي أن يضم العنصر **alphanumeric** سلسلة فارغة ويضم العنصر **paramS** القيمة الأولية لعملية التجفير.

4.7.7 قائمة بمعرّفات هويات الأغراض

الجدول H.235.6/3 – معرفات هويات الأغراض في تجفير الإشارات H.245 DTMF

مرجع معرّف الغرض	قيمة معرّف هوية الغرض	الوصف
"DES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 12}	تجفير إشارات H.245 DTMF بالمعيار DES-56 بالأسلوب EOFB
"3DES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 13}	تجفير إشارات H.245 DTMF بالمعيار 3DES-168 بالأسلوب EOFB
"AES-EOFB-DTMF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 14}	تجفير إشارات H.245 DTMF بالمعيار AES-128 بالأسلوب EOFB

8.7 العمل بأسلوب ديفي–هيلمان

تستخدم هذه التوصية البروتوكول ديفي هيلمان لأغراض الاتفاق بشأن المفتاح من طرف إلى طرف. ويمكن أن يعمل المفتاح ديفي–هيلمان الذي تم التفاوض بشأنه كمفتاح رئيسي أو مفتاح دينامي للدورة تبعاً للحالة (التوصيات ITU-T H.235.3 وH.530).

ويتصف النظام ديفي–هيلمان بمعلمات النظام g وp، حيث p هو عدد أولي كبير وg هو مولد مجموعة مضاعفات المقاس p أو مجموعة فرعية للمقاس p. ويدل g^x للمقاس p على نصف مفتاح (عمومي) ديفي هيلمان للطالب بينما g^y للمقاس p على نصف مفتاح (عمومي) ديفي هيلمان للمطلوب. ويعطي المعيار RFC 2412 معلومات أخرى توضيحية ونصائح بشأن كيفية اختيار معلمات ديفي هيلمان المحصنة.

وتنقل التوصية ITU-T H.235.0 حالة ديفي–هيلمان (g، p، g^x) المشفرة مع فيشة **ClearToken** حيث **dhkey** تضم نصف المفتاح $g^x \bmod p$ **halfkey** ($g^y \bmod p$ على التوالي) للسر العشوائي x (y على التوالي) والعدد الأولي p في **modsize** **والمولد** g. وهناك حالة خاصة هي المجموعة الثلاثية (0، 0، 0) أو المفتاح **dhkey** الفارغ الذي لا يمثل حالة DH لكن ينبغي استعماله للدلالة على أن مظهر تجفير الصوت غير مستعمل.

غالباً ما تكون المعلمتان p وg من النظام DH ثابتتين فيما يخص مجموعة من تطبيقات مع قيم محددة وأنظمة طرفية قادرة أيضاً على اختيار مجموعة معلماتها الخاصة. وينبغي أن يعرف المطلوب أن المعلمات DH غير المعيارية تقدم سوية أمن أقل مما قد يبدو في المعلمات للوصلة الأولى؛ فمثلاً قد يختار المطلوب عدداً غير أولي أو أن g تولد مجرد مجموعة فرعية أصغر بينما لا يمكن إجراء اختبار شامل للمعلمات عملياً. وسياسة أمن المطلوب هي التي تحدد قبول أو رفض مثل هذه العروض.

فيما يخص المعلمات الثابتة للنظام DH قد يؤدي تمييز بسيط عن طريق معرف هوية الغرض إلى رسائل مشفرة أكثر كثافة من تلك التي تضم قيماً حرفية. ويمكن لفيشة **ClearToken** التي تنقل حالة DH للمعلمات الثابتة DH المعيارية أن تشير إلى الحالة DH مع معرف هوية DH-OID في المجال **tokenOID**، شريطة ألا يكون المعرف **tokenOID** مستخدم لأغراض أخرى (كما يرد في الفقرة H.235.1/7 لفيشة مميزة **CryptoToken**). وبمقدور المرسل أن يدرج أيضاً القيم DH الحرفية ولكن ذلك ليس ضرورياً.

وفي الحالة التي يتوجب فيها الدلالة على عدة حالات DH كل منها عبر معرف DH-OID، ينبغي أن ترسل المعلمات DH التي تظهر في الفيشة **CryptoToken** المميزة (التي تشغلها التوصية H.235.1) بدون المفتاح **dhkey** وينبغي أن تنقل جميع الحالات DH في فيش **ClearTokens** مستقلة حيث يضم المعرف **tokenOID** المعرف DH-OID ويجوز غياب **dhkey**؛ وينبغي عدم استعمال جميع المجالات الأخرى في هذه الفيشة **ClearToken**.

الملاحظة 1 – لا يستبعد ذلك إمكانية نقل حالة DH في فيشة **CryptoToken** مستقلة أو فيش أخرى **ClearTokens** متوفرة بإدراج قيم المعلمات DH حرفياً.

وفي الحالة التي يتوجب فيها عدم الإشارة إلى حالة DH غير معيارية، ينبغي استعمال المعرف DH-OID "DHdummy" ووضع معلمات المجموعة DH غير المعيارية في **ClearToken** بشكل صريح.

يستطيع الطالب أن يخضع فيشة واحدة أو أكثر من الفيش **ClearTokens** التي تنقل كل منها حالة ديفي–هيلمان مختلفة. ويشجع الطالب على توفير أكبر عدد ممكن من الحالات DH تسمح به سياسة أمنه. وبذلك يستطيع المطلوب اختيار الحالة الملائمة للاستجابة، وذلك يزيد من احتمال وجود مجموعة معلمات مشتركة قابلة للتطبيق.

وينبغي أن يختار المطلوب حالة DH واحدة (أو لا شيء) ويقبلها استناداً إلى مجموعة غير مرتبة من الحالات DH التي يقدمها الطالب في الرسالة SETUP. وفي الحالة التي يستطيع المطلوب فيها اختيار حالة DH تستوفي احتياجاته الأمنية الخاصة، فعليه ألا يغير في الحالة DH المقترحة أو أن يرسل حالة لم يكن الطالب قد سبق وأرسلها له. وينبغي أن تقابل قوة خوارزميات التجفير المتيسرة في النقطتين الطرفيتين أثناء النداء قوة الحالة DH المختارة والتي أعاد المطلوب إرسالها، انظر الجدول 4. وينبغي على المطلوب الإشارة إلى الحالة DH المختارة في رسالة الاستجابة.

وفي الحالة التي يرفض فيها المطلوب جميع الاقتراحات لأسباب أمنية أو بسبب نقص مقدرات المعالجة ينبغي ألا يضع المطلوب المعلمة **dhkey** في رسالة الاستجابة.

وعلى المطلوب إدراج فيشته DH في الاستجابة SETUP على CONNECT. ويجوز المطلوب أن يدرج فيشته DH في رسالة الاستجابة التي تلي مباشرة الرسالة SETUP أو في مرحلة لاحقة على ألا تتعدى مرحلة الرسالة CONNECT.

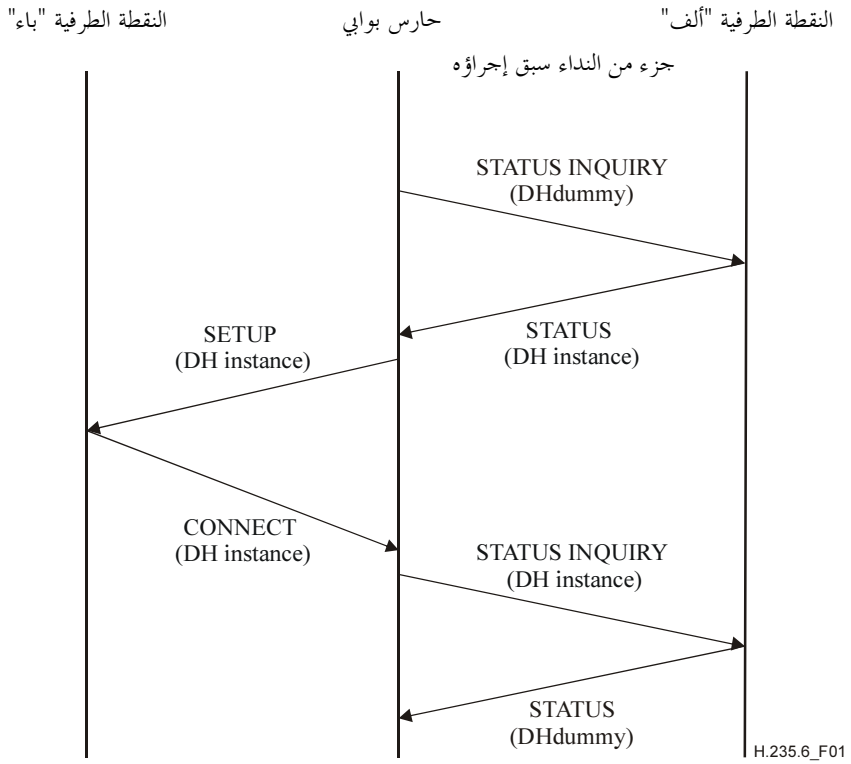
الملاحظة 2 – هناك عدة جوانب ينبغي مراعاتها فيما يتعلق باللحظة التي قد يدخل فيها المطلوب فيشة DH واحدة أو أكثر أثناء الإجابات SETUP على CONNECT وهي: وقت الاستجابة ورسم المعالجة الذي يتحمله المطلوب ومقدرة الوسيط دون انتظار وغيرها. وتعتبر هذه المسائل مستقلة عن التنفيذ.

غير أنه يمكن لبعض بوابات التسيير، لأسباب متفرقة، أن لا تسلّم جميع الاستجابات الحاصلة بين SETUP وCONNECT إلى الطالب. وهكذا يمكن استبعاد رسالة استجابة واحدة أو أكثر لتشوير النداء H.225.0 قد تضم فيشة DH، دون أن تصل إلى الطالب. ولن يكون بمقدور الطالب عندئذ حساب المفتاح الرئيسي DH ومفتاح أو مفاتيح دورة الوسيط. ومن أجل تفادي حصول ذلك ينبغي أن يدرج المطلوب دائماً نفس الفيشة DH في كل رسالة استجابة بين SETUP وCONNECT.

وفي الحالة التي يشير فيها المعرّف DH-OID إلى حالة DH مختلفة عن تلك المسيرة حالياً في **modsize** و**generator**، ينبغي أن تتمتع القيم الحرفية التي تنقلها المعلمتان **modsize** و**generator** بالأولوية على المعرف DH-OID في الفيشة. أما بالنسبة إلى الاستجابة، فينبغي أن يستعيض المطلوب عن المعرف DH-OID الذي يشكل مشكلة بالمعرف DH-OID الساكن كأن يكون "DH1024" الذي يقابل **modsize** وgenerator على سبيل المثال أو إن لم يوجد معرف DH-OID مقابل.

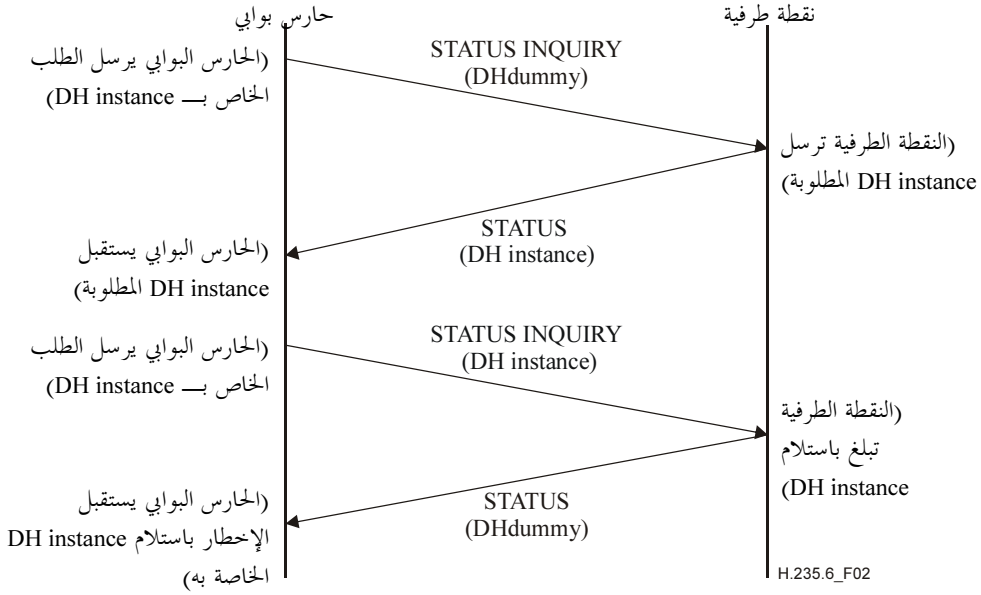
1.8.7 طلب إعادة التفاوض بشأن معلمات DH في وسط النداء

يمكن للحارس البوابي H.323 أن يطلب إعادة التفاوض بشأن المعلمات DH في وسط النداء باستعمال الإجراءات المحددة في هذه الفقرة. وقد يلزم إجراء إعادة التفاوض هذه لوضع اتفاق رئيسي DH بين نقطة طرفية موصولة فعلياً بالحارس البوابي ونقطة طرفية يتعين وصلها (انظر الشكل 1). ويلزم الإجراء الخاص بإعادة التفاوض بشأن معلمات ديفي–هيلمان من أجل دعم عدة خدمات إضافية. وينبغي ألاّ تؤدَّى جميع الإجراءات المحددة في هذه الفقرة إلا عندما تكون النقاط الطرفية لـــH.323 في حالة "توقف في جانب المرسِل"، وهي حالة محددة في الفقرة H.323/8.4.6.



الشكل H.235.6/1 – استعمال "طلب معلمات DH في وسط النداء" لأداء خدمات إضافية

من أجل طلب معلمات DH في وسط النداء، يرسل الكيان H.323 رسالة STATUS INQUIRY تضم مجال **ClearToken** مع معرّف DH-OID "DHdummy" في مجال **tokenOID** وتحذف باقي المجالات.



الشكل H.235.6/2 – طلب معلمات DH في وسط النداء

إذا تلقى كيان H.323 رسالة STATUS INQUIRY تحتوي على مجال **ClearToken** مع معرِّف هوية DH-OID "DHdummy" في مجال **tokenOID**، ينبغي للنقطة الطرفية H.323 أن تجيب برسالة STATUS تحتوي على المجموعة من حالات DH، انظر الشكل 2. وتحدَّد الحالات DH في هذه الرسالة STATUS تبعاً للقواعد المحددة في الفقرة 8.7 للرسالة SETUP.

الملاحظة 1 – يُفترض في الكيان H.323 الذي لا يستخدم هذا الإجراء أن يستجيب للرسالة STATUS INQUIRY برسالة STATUS بدون حالات DH.

ولإرسال حالة DH المقبولة في وسط النداء، ينبغي للكيان H.323 أن يرسل STATUS INQUIRY تحتوي على الحالة DH المقبولة، انظر الشكل 2. وتحدد الحالات DH في الرسالة STATUS INQUIRY هذه وفقاً للقواعد المحددة أعلاه في الفقرة 8.7 بالنسبة للاستجابة إلى الرسالة SETUP.

وإذا استقبلت نقطة طرفية H.323 رسالة STATUS INQUIRY من هذا القبيل تحتوي على مجال **ClearToken** مع حالة DH، ينبغي للنقطة الطرفية H.323 أن تستجيب برسالة STATUS تحتوي على مجال **ClearToken** مع معرِّف DH-OID "DHdummy" في المجال **tokenOID** ويُحذف باقي المجالات.

الملاحظة 2 – يُفترض في الكيان H.323 الذي لا يستخدم هذا الإجراء أن يستجيب للرسالة STATUS INQUIRY برسالة STATUS بدون حالات DH.

ينبغي للنقطة الطرفية H.323 التي تستقبل رسالة STATUS INQUIRY مع حالة DH أن تعيد حساب السر المشتَرك DH من حالة DH هذه وكذلك آخر مجموعة من الحالة (الحالات) DH التي أُرسلت بواسطة النقطة الطرفية H.323 هذه في النداء الخاص.

إذا استقبل حارس بوابي H.323 رسالة STATUS INQUIRY تحتوي على مجال **ClearToken** مع حالة DH أو مع معرِّف DH-OID "DHdummy" في المجال **tokenOID**، ينبغي عندئذ باستثناء الحالات العديدة المبينة أدناه توجيه الرسالة إلى الحالة الثانية من النداء التي تم استقبال الرسالة في سياقها.

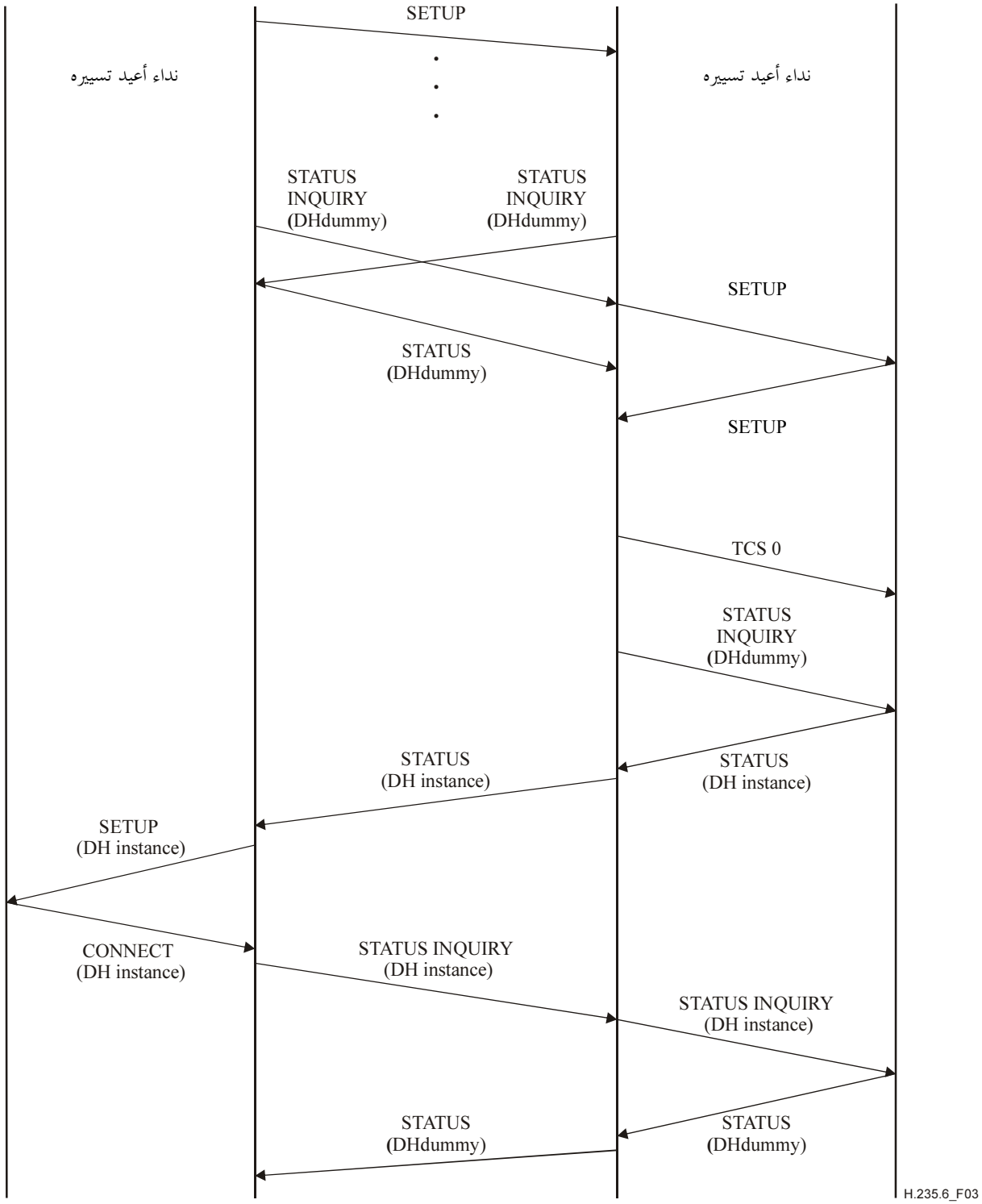
إذا استقبل حارس بوابي H.323 استجابة STATUS على رسالة STATUS INQUIRY أرسلها، ينبغي للحارس البوابي أن يعيد إرسال الرسالة STATUS إلى فرع النداء الذي تم استقبال الرسالة STATUS INQUIRY عليه.

إذا كان حارس بوابي H.323 ينتظر استجابة على الرسالة STATUS INQUIRY التي تحتوي على مجال **ClearToken** مع معرِّف DH-OID "DHdummy" في المجال **tokenOID** الذي أرسله، يستقبل رسالة STATUS INQUIRY تحتوي على

مجال **ClearToken** مع معرِّف DH-OID "DHdummy" في المجال **tokenOID** مع وضع علم CRV على القيمة 1، ينبغي عندئذ أن يستجيب الحارس البوابي برسالة STATUS تحتوي على مجال **ClearToken** مع معرِّف DH-OID "DHdummy" في المجال **tokenOID** (انظر الشكل 3).

إذا استقبل حارس بوابي H.323 رسالة STATUS INQUIRY تحتوي على مجال **ClearToken** مع حالة DH أو مع معرِّف DH-OID "DHdummy" في المجال **tokenOID** في الوقت الذي تكون فيه المرحلة الثانية من النداء لم تنشأ بعد، ينبغي للحارس البوابي أن ينتظر نشوء المرحلة الثانية من النداء وأن يرسل مقدرة فارغة توضع على هذه المرحلة من النداء، ثم يرسِل إليها الرسالة STATUS INQUIRY المستقبَلة (انظر الشكل 3).

ينبغي لأي حارس بوابي H.323 ألاّ يبدأ الإجراءات المحددة في هذه الفقرة بعد أن يكون قد أرسل رسالة STATUS تحتوي على حالة DH، وقبل أن يكون قد استقبَل الرسالة STATUS INQUIRY التي تحتوي على حالة DH.



الشكل H.235.6/3 – استعمال "معلمات DH طالبة في وسط النداء" من أجل إعادة التسيير المتزامنة للنداء بواسطة حارستي البوابة، على السواء

8 التشوير والإجراءات

يجب اتباع الإجراءات المذكورة في الفقرة H.323/8 (إجراءات تشوير النداء). يجب أن تتمكن النقاط الطرفية من تشفير وجود الشروط الأمنية (أو غيابها) المشار إليها في الرسائل H.225.0 والتعرف عليها (للقناة H.245).

في حالة وجوب ضمان أمن القناة H.225.0 ذاتها يجب اتباع الإجراءات نفسها الواردة في الفقرة H.323/8. والفارق في التشغيل هو أنه يجب أن تحصل الاتصالات فقط بعد التوصيل مع معرف هوية النقطة TSAP الآمنة وباستعمال الأساليب

الأمنية المحددة مسبقاً (مثل TLS (RFC 2246، RFC 3546)). ونظراً إلى أن رسائل التوصية H.225.0 هي الرسائل الأولى التي جرى تبادلها عند إقامة اتصالات التوصية H.323 لا يمكن أن تجري مفاوضات أمنية "داخل النطاق" لرسائل التوصية H.225.0. وبكلمات أخرى يجب أن يعرف الطرفان مسبقاً أنهما يستعملان أسلوباً أمنياً معيناً. وبالنسبة لتدفقات التوصية H.323 في البروتوكول IP يستعمل نفاذ بديل معروف (1300) للاتصالات الآمنة بالطريقة TLS (RFC 2246، RFC 3546).

تهدف تبادلات التوصية H.225.0 في ما يتعلق بأمن التدفقات H.323 إلى توفير آلية لإنشاء القناة الآمنة H.245. ومن الممكن اختيار أن يحصل الاستيقان خلال تبادل الرسائل H.225.0. ومن الممكن إجراء هذا الاستيقان بواسطة شهادة أو كلمة سر باستعمال التجفير و/أو التظليل (أي التوقيع). ويرد في الفقرات من 1.8 إلى H.235.0/3.2.8 عرض لخصائص أساليب التشغيل هذه.

يجب أن تجيب نقطة طرفية H.323 تستقبل رسالة إنشاء SETUP بواسطة المقدرة **h245SecurityCapability** المنشطة بالدلالة على الأسلوب **h245SecurityMode** الملائم والمقبول في رسالة التوصيل CONNECT. وفي حال غياب المقدرات المتداخلة من الممكن أن يرفض المطراف المطلوب التوصيل بإرسال رسالة **ReleaseComplete** مع شفرة السبب التي تضبط على ***SecurityDenied***. ويهدف هذا الخطأ إلى عدم نقل أية معلومات حول عدم المواءمة الأمنية ويكون على المطراف أن يحدد المشكلة بطريقة أخرى ما. وفي الحالات التي يستقبل فيها المطراف الطالب رسالة CONNECT بدون أسلوب أمني كافٍ أو مقبول من الممكن أن ينهي النداء بالرسالة **ReleaseComplete** برفقة شفرة السبب ***SecurityDenied***. وفي الحالات التي يستقبل فيها المطراف الطالب رسالة CONNECT بدون أية مقدرات أمنية يجوز لهذا المطراف أن ينهي النداء بإرسال رسالة **Release Complete** برفقة ***undefinedReason***.

إذا استقبل المطراف الطالب أسلوباً مقبولاً **h245Security** يجب أن يفتح القناة H.245 ويشغلها في الأسلوب الآمن المشار إليه. وينبغي اعتبار أن الفشل في إنشاء قناة التوصية H.245 في الأسلوب الآمن المحدد هنا خطأ بروتوكول وينبغي إنهاء التوصيل.

1.8 مواءمة المراجعة 1

يجب ألا تعيد نقطة طرفية ذات مقدرة أمنية أية مجالات أو دلالات أو حالة ترتبط بالأمن إلى النقطة الطرفية غير المزودة بمقدرة أمنية. وإذا استقبل الطالب رسالة SETUP لا تتضمن المقدرات الأمنية **H245Security** و/أو فيشة الاستيقان فمن الممكن أن يعيد هذا المستعمل إرسال رسالة **ReleaseComplete** لرفض التوصيل ولكن عليه أن يستعمل شفرة السبب ***undefinedReason*** في هذه الحالة. وبصورة مماثلة إذا استقبل الطالب رسالة CONNECT بدون **H245SecurityMode** و/أو فيشة استيقان بعد أن يكون قد أرسل رسالة SETUP مع **H245Security** و/أو فيشة استيقان يجوز لهذا المستعمل أيضاً أن ينهي التوصيل عن طريق إصدار رسالة **ReleaseComplete** مع شفرة سبب ***UndefinedReason***.

2.8 الدلالات الوظيفية في الطبعة 3

تقدم النقاط الطرفية في الطبعة 3 للتوصية ITU-T H.235 وفي الطبعات اللاحقة إجراءات أمن محسنة في مسار المعطيات لا توفرها الطبعتان 1 و2 من H.235. وإجراءات الأمن هذه هي التالية:

- تسيير محسّن للمفاتيح (**V3KeySyncMaterial**، انظر الفقرة 1.3.8)؛
- تحيين محسّن للمفاتيح، انظر الفقرة 2.6.8.

وبما أن النقاط الطرفية عموماً لا تعرف شيئاً عن موضوع توفيرها المتبادل لبعضها البعض في الطبعة 3 من التوصية ITU-T H.235 أو طبعة لاحقة تضاف إشارة علنية إلى الطبعة أثناء إنشاء النداء.

وينبغي أن تستعمل النقاط الطرفية الواردة في الطبعة 3 من التوصية ITU-T H.235 والطبعات اللاحقة دائماً الإجراء المذكور في هذه الفقرة بهدف تحديد وجود مقدرة الطبعة 3 (تسيير محسن للمفاتيح، تزامن محسن للتجفير). ويجوز للنقاط الطرفية

استعمال إجراءات (انظر الفقرة 3.8) تبعاً لنتيجة إجراء التشوير المنطقي وذلك بهدف تأمين المواءمة الرجعية مع النقاط الطرفية في الطبعتين 1 و2 للتوصية ITU-T H.235.

ومن أجل الدلالة على ضرورة استعمال الإجراءات المحسنة الواردة في الطبعة 3 من التوصية ITU-T H.235 ينبغي أن تدخل النقطتان الطرفيتان للطالب والمطلوب فيشة **ClearToken** إضافية تشير إلى مقدرة الطبعة 3 خلال تشوير النداء (SETUP، CONNECT، إلخ). ويدل غياب مثل هذه الفيشة على وجود الطبعة 1 أو 2 من التوصية ITU-T H.235 حصراً. وفي هذه الحالة ينبغي أن تستعمل النقطة الطرفية الإجراء الوارد في الفقرة 3.8. وفي الحالات الأخرى يجوز للنقاط الطرفية استعمال الإجراءات المحسنة كتلك الواردة في الفقرة 1.3.8. أو استعمال الإجراء الوارد في الفقرة 3.8 للطبعة 1 أو 2 من التوصية ITU-T H.235.

وينبغي أن تستعمل هذه الفيشة **ClearToken** معرف الهوية **tokenOID** موضوعاً على "V3" وأن تتخذ القيمة التالية:

« V3 »	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 24}	مؤشر مقدرة الطبعة 3 في الفيشة ClearToken أثناء تشوير النداء

وينبغي عدم استعمال جميع المجالات الأخرى في هذه الفيشة ما عدا إذا ما استخدمت لتسيير المعلمات DH.

3.8 تسيير المفتاح

ينتج الكيان الرئيسي عناصر مفتاح الدورة ويوزعها على الكيان الند الواحد أو أكثر. وهناك إجراءان لتسيير المفتاح:

- إجراء مصمم بشكل رئيسي لأغراض النقاط الطرفية للطبعتين 1 أو 2 من التوصية ITU-T H.235، ويرد وصفه في هذه الفقرة.
- إجراء محسّن لأغراض النقاط الطرفية للطبعة 3 والطبعات اللاحقة من التوصية ITU-T H.235 ويرد وصفه في الفقرة 1.3.8.

وتطبق النقاط الطرفية للطبعتين 1 أو 2 من التوصية ITU-T H.235 الإجراء التالي لتسيير مفتاح الدورة:

يضم العنصر **KeySyncMaterial** معرّف هوية النقطة الطرفية للكيان الرئيسي داخل المعلمة **generalID** ويسير عناصر مفتاح الدورة في **keyMaterial**. وينبغي إدراج قيمة **generalID** من أجل توفير سوية الحد الأدنى من استيقان مصدر مفتاح الدورة (انظر أيضاً الفقرة 6.8). وينبغي أن يتأكد المرسل إليه من صحة سمة المعرف **generalID** المستقبَل.

ملاحظة – يفترض في هذه التوصية أن كل نقطة طرفية مسجلة عند حارس بوابي ومزودة بمعرف هويات النقاط الطرفية الذي يمكن تسييره ضمن العنصر **generalID**. ولا تقدم هذه التوصية السيناريوهات بدون حارس بوابي التي تتطلب مزيداً من الدراسة.

ينبغي تجفير العنصر **KeySyncMaterial** باستعمال المفتاح الرئيسي الذي تم التفاوض بشأنه. وينبغي دائماً تكميل العنصر **KeySyncMaterial** بمعلومات الحشو من أجل جعل طوله مساوياً لمضاعف صحيح لطول الفدرة قبل التجفير التي ينبغي أن يضم آخر أثمون فيها عدد أثمونات الحشو (بما في ذلك الأثمون الأخير). وينبغي تحديد قيمة عناصر الملء باستعمال اصطلاح عادي لخوارزمية التجفير. وينبغي تخزين نتيجة التجفير في العنصر **sharedSecret** من المفتاح **H235Key**.

1.3.8 تسيير محسّن للمفتاح حسب الطبعة 3 من التوصية ITU-T H.235

تمت ملاحظة أن تعريف العنصر **KeySyncMaterial** بقواعد الترميز ASN.1 والطريقة التي طبقت فيها العملية ENCRYPTED{} على المعطيات في الطبعتين 1 و2 من التوصية ITU-T H.235 يظهر عدداً كبيراً من النصوص غير المشفرة (الواضحة) المعروفة أولها هو المعرف **generalID** للكيان الرئيسي، وكذلك أيضاً بعض بتات التشفير المعروفة لأغراض البنية. ويعرف المعرف **generalID** ولو كان مجفراً بواسطة الأجزاء الأخرى غير المجفرة من رسالة التشوير (مثل المعرف **senderID**). ويعتبر وجود مثل هذا النص الواضح المعروف خللاً كبيراً في مخطط الأمن وقد يؤدي إلى أن يتمكن المعتدي من "كسر" مفتاح الدورة بشكل أسهل وخاصة فيما يخص التجفير بالفدرة ذا القد الأقصر مثل التجفير DES-56 أو ما يتواءم مع RC2.

إضافة إلى ذلك ينبغي أن تكون الطبعة 3 من التوصية ITU-T H.235 قادرة على إتاحة تسيير عنصر المفتاح الإضافي أي:

- تسيير أمين لمفتاح التمليح باتجاه الكيان الند الواحد أو أكثر. ويتم إدراج مفتاح التمليح هذا لأغراض الأسلوب OFB المحسن؛ انظر الفقرة 4.8.

وتوسع الطبعة 3 من التوصية ITU-T H.235 المفتاح **H235Key** بإضافة **secureSharedSecret** المحتوية على العنصر **V3KeySyncMaterial** الذي يضم المعلمات التالية:

generalID، وتضم معرّف هوية النقطة الطرفية للمرسل إن توفرت وإلا يبقى هذا المجال دون استعمال.

algorithmOID، وتدل على خوارزمية التجفير المستعملة والأسلوب المتبع.

paramS وتضم قيمة التدميث المطبقة على تجفير المفتاح أو المفاتيح المسيرة.

الملاحظة 1 – ينبغي عدم تصميم متجه التدميث (IV) داخل المعلمة **paramS** مع المتجه IV رزمة الأسلوب RTP غير المشار إليه. ويضم العنصر **ClearSalt** خيارياً مفتاح تمليح غير مجفر لأغراض تجفير مفتاح الدورة (مثلاً: في حال الأسلوب EOFB).

encryptedSessionKey وتضم النص المجفر لمفتاح الدورة المجفر في حال وجوده.

encryptedSaltingKey وتضم النص المجفر لمفتاح تمليح المعطيات الأولية المجفرة إن وجدت. ومفتاح التمليح ضروري للأسلوب OFB المحسن.

clearSaltingKey وقد تضم مفتاح تمليح المعطيات الأولية غير المجفرة. وعند التطبيق ينبغي التأكد من عدم استعمال العنصرين **encryptedSaltingKey** و**clearSaltingKey** في نفس الوقت.

paramSsalt وتضم القيمة الأولية لتجفير مفتاح التمليح. ويضم العنصر **ClearSalt** خيارياً مفتاح تمليح غير مجفر لتجفير مفتاح التمليح (مثلاً: في حال الأسلوب EOFB).

الملاحظة 2 – ترسل المعلمات **generalID** و**algorithmOID** و**paramS** دائماً في نص واضح بينما تضم المعلمتان **encryptedSessionKey** و**encryptedSaltingKey** النص المجفر لعنصر المفتاح المجفر.

يولد الكيان الرئيسي المفتاح (أو المفاتيح) وفقاً لمقدرات المطراف التي يتم التفاوض بشأنها، ويرسل المفتاح (أو المفاتيح) باستعمال الرسالة **V3KeySyncMaterial** إلى النقاط الطرفية الندة. وهكذا ينبغي إعادة إرسال العنصر **V3KeySyncMaterial** دون تغيير عن طريق الحارسات البوابية الوسيطة إن توفرت.

وينبغي للنقاط الطرفية المطابقة للطبعة 3 أو الطبعات اللاحقة من التوصية ITU-T H.235 أن تستعمل دائماً العنصر **secureSharedSecret** في العنصر **H235Key** لكن بدلالة نتيجة إجراء التشوير المنطقي الوارد في الفقرة 2.8 وباستعمال الفيشة **ClearToken** حسب الطبعة 3، وتستطيع هذه النقاط استعمال العنصر **sharedSecret** لتأمين المواءمة الرجعية مع النقاط الطرفية المطابقة للطبعتين 1 و2 من التوصية ITU-T H.235.

4.8 الأسلوب OFB المحسّن

يعرّف الأسلوب OFB (المعيار ISO/IEC 10116) أسلوباً تشغيلياً يستخدم تجفير التدفقات بواسطة خوارزميات تجفير الفدرة. ويقدم الأسلوب OFB:

- أداء محسناً بفضل تقليص وقت معالجة التجفير؛
- معالجة أسهل وأقل تعقيداً للفدرات غير الكاملة؛
- مقاومة جيدة لأخطاء البتات.

والأسلوب OFB المحسّن هو أسلوب OFB معدّل قليلاً ويعرف هنا باسم EOFB ويقدم إضافة إلى خصائص الأسلوب OFB:

1) استعمال مفتاح تمليح KS يضاف إلى مفتاح التجفير KE؛

2) إدراج دليل ضمني للرزمة.

يضيف استعمال مفتاح تمليح إضافي تطبق عليه العملية المنطقية أو XOR مع المفعول الرجعي أمناً إضافياً بالنسبة إلى تحليل النص الواضح المعروف. وفي ذلك إفادة كبيرة من وجهة نظر الأمن لا يقدمها أي أسلوب تشغيل معياري (مثل CBC أو OFB أو غيرها). ويؤدي استعمال الأسلوب EOFB بالتالي إلى أمن أكبر بالنسبة إلى النص الواضح التكراري وكذلك إلى تحليل النص الواضح المعروف.

ويتحدد الأسلوب EOFB كما يلي: $C_i = P_i \oplus S_i$ مع $S_i = E_{KE}(KS \oplus S_{i-1})$ بالنسبة إلى $i = 1 \ldots n$ و$S_0 = IV$ حيث C_i هي فدرة نص التجفير وP_i هي فدرة النص الواضح قبل i؛ وS_i هي فدرة تدفق مفتاح i؛ وKE هو مفتاح التجفير و⊕ هو "أو" حصرية للبتات. ويوضح الشكل 6.I الأسلوب EOFB.

ويعمل الأسلوب EOFB أيضاً كأسلوب OFB معياري، مما يجعل من الأسلوب EOFB متوائماً رجعياً مع الأسلوب OFB. وعند الرغبة بالحصول على المواءمة الرجعية مع الأسلوب OFB المعياري ينبغي أن يتألف مفتاح التمليح KS من 0 فقط أو أن يترك المفتاح **encryptedSaltingKey** فارغاً في العنصر **V3KeySyncMaterial**. إلا أنه يوصي بشدة باستعمال مفتاح تمليح فعلي في الحالات التي تكون فيها الحمولات النافعة RTP للتجفير في تجفير الفدرة بقد فدرة أقصر مثل DES-56 أو المواءمة RC2.

بعد معالجة 2^{48} رزمة كحد أقصى ينبغي استعمال مفتاح تجفير دورة KE جديد ومفتاح تمليح KS جديد؛ وإلا فسيعاد استعمال تدفق المفاتيح مما يهدد الأمن.

يحدد البند 11 معرّفات هوية الأغراض في الأساليب DES-56-EOFB وRC2 المتوائم مع EOFB و3-DES-EOFB وAES-EOFB.

5.8 إدارة المفاتيح

ينبغي أن تستعمل النقاط الطرفية المطابقة لهذا الملحق إجراء التوصيل السريع وفقاً للفقرة 1.6.7. وفي حال عدم تطبيق الانطلاق السريع يجب استعمال تسيير نفقي من أجل ضمان أمن رسائل التحكم بالنداء H.245 تماشياً مع هذه التوصية. وتتيح إجراءات الانطلاق السريع إقامة قناة منطقية واحدة أو قناتين منطقيتين وحيدتي الاتجاه. وتدير إجراءات الانطلاق السريع التفاوض بشأن مقدرات الأمن وتوزيع الأسرار المشتركة المتقاسمة (السر DH المتقاسم) توزيعاً يعمل بمثابة مفتاح رئيسي وتوزيع مفاتيح التجفير.

ويحدد الجدول 4 المعرّفات OID الموزعة على عدة خوارزميات تجفير ويبين العلاقة بين هذه المعرّفات ومعرّفات المجموعة ديفي–هيلمان. ويعرف كل معرّف OID ثلاث مجموعات DH.

- "DHdummy": ينبغي تطبيق جزء من هذه المجموعة في حالة تصدير الأمن (512 بتة) أو استعمال مجموعة ما غير معرفة أو غير معيارية.

  الملاحظة 1 – لا توجد أي مجموعة DH خاصة معرفة؛ ويشير المعرف OID إلى كل مجموعة DH غير معيارية.
- ينبغي استعمال وحدة من المجموعة DH التي تحتوي على 512 بتة من أجل توليد مفتاح رئيسي لأغراض توزيع مفتاح دورة واحد أو أكثر على خوارزميات التجفير المتوائمة مع RC2 ("X") أو DES بطول 56 بتة ("Y").
- "DH1024": تستعمل هذه المجموعة DH لحالات الأمن بدرجة مرتفعة (1024 بتة). ويشير المعرف OID إلى مجموعة DH ثابتة ومعيارية وينبغي استعمال هذه المجموعة لإنتاج مفتاح رئيسي لأغراض توزيع مفتاح دورة واحد أو أكثر على خوارزميات التجفير 3-DES ("Z").
- "DH1536": تقترح هذه المجموعة كخيار لأغراض مواضيع الطبعة 3 مع احتياجات درجة أمن مرتفعة تتجاوز احتياجات المجموعة DH بطول 1024 بتة. ويشير المعرف OID إلى مجموعة DH ثابتة. وينبغي استعمال هذه المجموعة DH لإنتاج مفتاح رئيسي لأغراض توزيع مفتاح دورة واحد أو أكثر على إحدى خوارزميتي التجفير Triple-DES ("Z"، "Z1") أو AES-128 ("Z2"، "Z3").

ويوصى باستعمال المجموعة DH1024 والمجموعة DH1536 خيارياً ما عدا إذا ما تطلبت احتياجات أمن أخرى المعلمات ديفي–هيلمان. وإضافة إلى ذلك يوصى باستعمال المعرفات OID التي تعرف المجموعات DH (انظر الفقرة 8.7) غير أنه ينبغي إعداد التطبيقات لاستقبال معلمات المجموعة DH حرفياً دون الإشارة إلى المعرف OID علنياً. وفي هذه الحالة يجب التأكد في التطبيقات من تسيير المجموعة DH الصحيحة وفقاً للجدول 4.

ويجوز للنقاط الطرفية استعمال معلمات المجموعة DH غير المعيارية. وينبغي أن يدل المعرف OID "DHdummy" على هذه المجموعات غير المعيارية. ويعود للمطلوب أمر قبول أو رفض المجموعات DH من هذا النمط.

الملاحظة 2 – لا يلغي اختيار المجموعة DH ضرورة التفاوض بشأن خوارزمية تجفير الوسيط الفعلية. وينبغي إجراء هذا التفاوض باستعمال إجراء التفاوض بشأن مقدرة المطراف H.245.

الملاحظة 3 – خلال مرحلة إنشاء التوصيل (من SETUP إلى CONNECT) ينبغي عدم استعمال المعرفات OID في خوارزميات التجفير للإشارة إلى الحالة ديفي هيلمان.

الجدول H.235.6/4 – مجموعات ديفي–هيلمان

المعرف OID لخوارزمية التجفير	DH-OID	وصف المجموعة D-H
"X", "X1" (RC2-compatible), "Y", "Y1" (DES)	"DHdummy"	الأسلوب Mod-P، جميع البتات 512 الأولى المناسبة
"Z", "Z1" (triple-DES), "Z2", "Z3" (AES)	"DH1024"	الأسلوب Mod-P، 1024 بتة أولية أولي = $\{ [2^{894} \text{ pi}] + 129093 \} \times 2^{64} + 1 - 2^{960} - 2^{1024}$ = (179769313486231590770839156793787453197860296048756011706444 42368419718021615851936894783379586492554150218056548598050364644054819923910005079287700335581663922955313623907650873575991482257486257500742530207744771258955095793777842444242661733472762929938766870920560605027081084290769293201912819446762700 7)$_{10}$ مولد (الملاحظة) = 2
"Z", "Z1" (triple-DES), "Z2", "Z3" (AES)	"DH1536"	الأسلوب Mod-P، 1536 بتة أولية أولي = $\{ [2^{1406} \text{ pi}] + 741804 \} \times 2^{64} + 1 - 2^{1472} - 2^{1536}$ = (241031242692103258855207602219756607485695054850245994265411 69419581088316826122288900938582613416146732271414779040121965036489570505826319427307068050092230627347453410734066962460145893616597740410271692494532003787294341703258437786591981437631937768598695240889401955773461198435453015470437472077499697637500843089263392955599688824578724129938101291302945929999479263652640592846472097303849472116814344647144384885209401274598442888593365268963209196339197)$_{10}$ مولد (الملاحظة) = 2
الملاحظة – يُستعمَل المولد لإنتاج الفيشة DH.		

6.8 تحديث المفاتيح وتزامنها

فيما يخص عدد الفدر بطول 64 بتة، ينبغي أن توازي نسبة تحديث المفاتيح 2^{32} فدرة لكل مفتاح. ويستحسن أن تحدّث التطبيقات مفاتيحها قبل بلوغ 2^{30} فدرة مع نفس المفتاح (انظر الفقرة 1.9). وفيما يخص أرقام الفدر بطول 128 بتة، ينبغي أن تساوي نسبة تحديث المفاتيح أكثر من 2^{64} فدرة لكل مفتاح. ويستحسن أن تحدّث التطبيقات المفاتيح قبل بلوغ 2^{62} فدرة مع نفس المفتاح (انظر الفقرة 1.9). وللكيانين المعنيين حرية تغيير مفتاح دورة الوسيط بقدر ما يريدان من المرات مع مراعاة سياسة الأمن. فعلى سبيل المثال يستطيع الرئيس توزيع مفتاح دورة جديد بواسطة **encryptionUpdate** أو **encryptionUpdateCommand** من الرسالة **miscellaneousCommand**. ومن جهة أخرى يجوز للتابع أن يطلب من الرئيس مفتاحاً للدورة بغية تغييره بواسطة **encryptionUpdateRequest** من الرسالة **miscellaneousCommand**.

تضم الرسالة **MiscellaneousCommand** المعلمتين **encryptionUpdate** و**encryptionUpdateCommand** التي يوضع مجالها **encryptionSynch** على القيمتين التاليتين:

- **synchFlag**: الرقم الجديد للحمولة النافعة RTP الدينامية الذي يدل على تغيير المفتاح.
- **h235key**: يسير مفتاح الدورة الجديد المرقم. وهو مفتاح **H235Key** مشفر بالترميز ASN.1 يرسل كسلسلة من الأثمونات.

يستعمل المجال **sharedSecret** في البنية **H235Key** المجالات التالية:

- **algorithmOID**: موضوعاً على "X" أو "X1" للمعيار المتوائم RC2 بطول 56 بتة أو على "Y" و"Y1" للمعيار DES بطول 56 بتة. وعلى "Z" أو "Z1" للمعيار Triple-DES بطول 168 بتة وعلى "Z3" للمعيار AES بطول 128 بتة.

  الملاحظة 1 – خوارزمية تجفير مفتاح دورة هي نفس خوارزمية تجفير وسيط ثم التفاوض بشأنه.

- **paramS**: موضوعاً على القيمة الأولية. وبالنسبة إلى أعداد تدفقات الفدر بطول 64 بتة يضم المجال **iv8** تشكيلة بتات مؤلفة من فدرة بطول 64 بتة عشوائية ينتجها الكيان المبادر. أما بالنسبة إلى تدفقات الفدر بطول 128 بتة فإن المجال **iv16** يضم تشكيلة بتات مؤلفة من فدرة بطول 128 بتة عشوائية ينتجها البادئ. وينبغي عدم استعمال هذا المجال في الأسلوب CBC وقيمته NULL؛ مما يعني أنه ينبغي وضع القيمة CBC-IV لتجفير مفتاح الدورة على 0، ولا تستعمل إلا لتسيير المتجه IV في الأسلوب EOFB.
- **encryptedData**: ويوضع على النتيجة الحاصلة من **KeySyncMaterial** بالأرقام.

وكجزء من المجال **KeySyncMaterial**:

- **generalID**: معرف هوية المصدر الذي أعطى المفتاح.

  الملاحظة 2 – يفترض في هذه التوصية أن كل نقطة طرفية قد تسجلت في حارس بوابي وحصلت على معرّف هوية النقطة الطرفية الذي يمكن تسييره في المعرف **generalID**. ولا تتعرض هذه التوصية إلى السيناريوهات بدون حارس بوابي؛ وتستدعي هذه الحالة مزيداً من الدراسة.

- **keyMaterial**: موضوعاً على مفتاح الدورة الجديد. وهو مفتاح طوله 56 بتة بالنسبة إلى المعيار DES والمعيار المتوائم مع RC2، وطوله 168 بتة بالنسبة إلى المعيار Triple-DES، وطوله 128 بتة بالنسبة إلى المعيار AES. وينبغي أن ينتج الكيان الرئيسي مفتاح دورة جديد يستوفي معايير الأمن التالية كحد أدنى؛ ألا يكون مفتاح DES ضعيف أو نصف ضعيف وأن يستعمل مصدراً عشوائياً أميناً بقدر كافٍ.

وتضم الرسالة **MiscellaneousCommand** المجال **encryptionUpdateRequest** الذي يحوي **keyProtectionMethod** حيث العلم **sharedSecret** موضوع على TRUE.

الملاحظة 3 – بما أن تحديث المفاتيح وتزامنها مرتبطان بالرسائل H.245 التي لا تتراكم خلال التوصيل السريع، يجب استعمال تسيير نفقي H.245 للكيانات H.323 الأمينة.

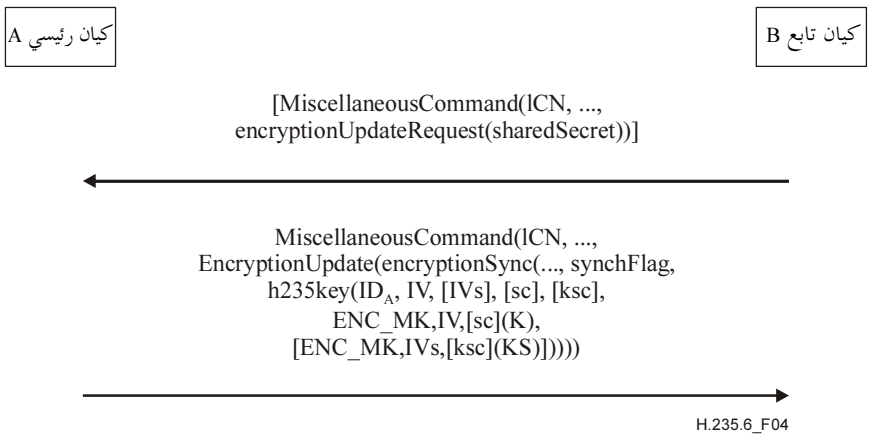
ولا تبقى مفاتيح دورة الوسيط على الدوام. فعند نقطة زمنية معينة ينتهي عمر مفتاح كل دورة. ومن ثم ينبغي استعمال مفتاح دورة جديد لحماية أمن دورة دائمة التطور. وفي سياق المؤتمرات، ينبغي تحديد وتوزيع مفتاح جديد للدورة الخاصة بمجموعة عندما ينضم أعضاء المجموعة إلى مؤتمر مؤمَّن أو يغادرونه، مما يؤدي بالتالي إلى منعهم من النفاذ إلى المعطيات الماضية أو المعطيات التي ترد في المستقبل.

- ويحدث تحديث وتزامن المفتاح القائم على نمط الحمولة النافعة، نمطاً جديداً للحمولة النافعة الدينامية لمفتاح الدورة الجديد هذا؛ انظر الفقرات 1.6.8 و2.6.8 و3.6.8.

ولتحديث المفتاح، تقدم هذه التوصية تنظيم اتصال بدون إشعار بالاستلام يطبَّق أيضاً بالنسبة للنقاط الطرفية في الطبقتين 1 و2 للتوصية H.235، وكذلك تنظيم اتصال قوي مع إشعار بالاستلام للنقاط الطرفية في الطبقة 3 للتوصية H.235 والتوصيات اللاحقة.

1.6.8 تحديث المفاتيح دون إشعار بالاستلام

يوضح الشكل 4 مرحلة الاتصال دون إشعار بالاستلام فيما يخص توزيع المفاتيح أو تحديث مفاتيح الدورة. وإذا رغب الكيان التابع بمفتاح دورة محدّث، باستطاعته أن يطلب مفتاح دورة جديداً من الكيان الرئيسي وذلك بإرسال طلب **encryptionUpdateRequest** إلى الكيان الرئيسي. ويرسل الكيان الرئيسي مفتاح دورة جديداً (مع أو بدون طلب **encryptionUpdateRequest** مسبق من الكيان التابع) إلى التابع في رسالة **EncryptionUpdate**.



الشكل H.235.6/4 – توزيع/تحديث مفاتيح الدورة من الكيان الرئيسي إلى الكيان (أو الكيانات) التابع (التابعة) دون إشعار بالاستلام

حيث:

ICN	رقم القناة المنطقية؛
SynchFlag	رقم الحمولة النافعة RTP الدينامية الجديدة؛
ID_A	المعرّف **generalID** للمصدر؛
IV	القيمة/المتجه الأولي لتجفير مفتاح الدورة؛
IVs	القيمة/المتجه الأولي لتجفير مفتاح التمليح؛
ENC_MK,IV,sc(K)	تجفير نص واضح *K* بواسطة *M* مع متجه أولي *IV* [ومفتاح تمليح *sc* في الأسلوب EOFB حصراً]
KS	مفتاح تمليح للمعطيات (في الأسلوب EOFB حصراً)؛
K	مفتاح الدورة بنص واضح؛
sc	مفتاح التمليح غير المجفر في حال استعمال الأسلوب EOFB لتجفير مفتاح الدورة؛
ksc	مفتاح التمليح غير المجفر في حال استعمال الأسلوب EOFB لتجفير مفتاح التمليح؛
s2M/m2S	مؤشر **الاتجاه** (الطبعة 3 من التوصية ITU-T H.235 v3 حصراً) بين (s2m = من التابع إلى الرئيس، m2s = من الرئيس إلى التابع)؛
[ ]	الجزء الخياري.

وقد تلجأ طرائق تحديث المفاتيح كما يرد وصفها في الفقرات التالية، إلى أسلوب التجفير EOFB من أجل حماية عناصر المفتاح المرسلة. ومن أجل إعمال الأسلوب EOFB لحماية عناصر المفتاح بنفس طريقة حماية الحمولة النافعة من المعطيات ينبغي استعمال مفتاح تمليح إضافي (sc أو ksc).

2.6.8 التحديث المحسّن للمفاتيح

ينبغي للنقاط الطرفية المطابقة للطبعة 3 والطبعات اللاحقة من التوصية ITU-T H.235 أن تنفذ الإجراء العلني/الضمني لتحديث المفاتيح مع إشعار بالاستلام. وذلك يعني الحصول على تقنيات تحديث موثوقة للمفاتيح تستند إلى طريقة تحديث المفاتيح دون إشعار بالاستلام كما هو وارد في الطبقات السابقة للطبعة 3 من التوصية المذكورة. وينبغي التفاوض بشأن مقدرات تنفيذ مثل هذا الإجراء بواسطة الدلالة الوظيفية للطبعة 3 وفقاً للفقرة 2.8.

يوضح الشكل 5 إجراءات تحديث المفاتيح في قناة منطقية يستعملها كيان تابع. وإذا رغب التابع بإطلاق عملية تحديث المفاتيح وطلب مفتاح دورة جديد من الرئيس، عليه أن يرسل إلى الرئيس الأمر **MiscellaneousCommand** وفيه العنصر **logicalChannelNumber** الذي يضم رقم القناة المنطقية (كما يحدده التابع) وينبغي وضع العنصر **sharedSecret** على "true"، ومؤشر **الاتجاه** على **slaveToMaster** وينبغي طلب الرقم الجديد للحمولة النافعة الدينامية في العنصر **synchFlag** ضمن طلب **EncryptionUpdateRequest**. وإذا أطلق الرئيس من ناحية أخرى عملية تحديث المفاتيح ينبغي عدم إرسال هذه الرسالة **EncryptionUpdateRequest**.

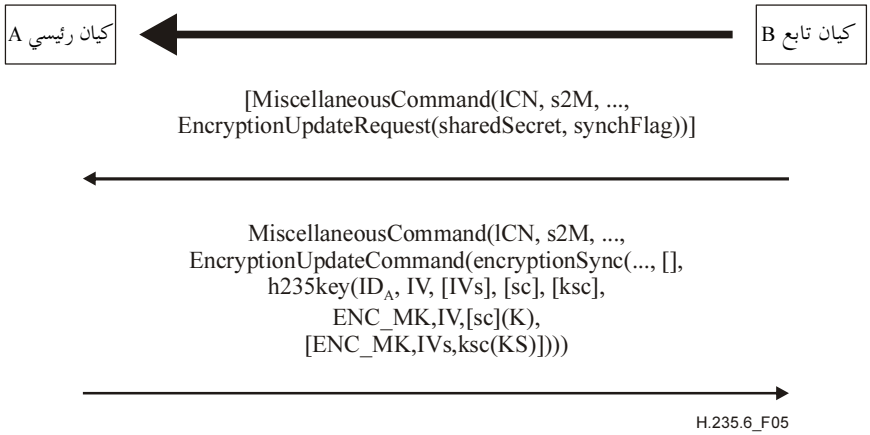
وينبغي على الرئيس – في حال استجاب لطلب التابع أو كانت المبادرة مبادرته – أن يرسل أمراً **EncryptionUpdateCommand** يضم فيه العنصر **logicalChannelNumber** رقم القناة المنطقية، وينبغي أن يوضع **الاتجاه** على **slaveToMaster** داخل **MiscellaneousCommand**، وأن يعكس العنصر **synchFlag** الموجود في **encryptionSync** الرقم الجديد للحمولة النافعة الدينامية.

وينبغي أن يسيّر العنصر **h235key** مفتاح الدورة. وينبغي أن يضم هذا العنصر **h235key** هوية الرئيس في المعلمة **generalID** والمتجه الأولي *IV* المستخدم في المعلمة **paramS**. وينبغي تسيير مفتاح دورة المعطيات المجفرة داخل المعلمة **encryptedSessionKey** التي تطبق فيها وظيفة التجفير على مفتاح دورة الكيان الرئيسي والقيمة الأولية الموجودة في **paramS** على مفتاح الدورة *K*. وفي الأسلوب EOFB يسيّر مفتاح تمليح غير مجفر في العنصر **ClearSalt** داخل المعلمة (*sc*) **paramS**. وينبغي أن يسير العنصر **encryptedSaltingKey** مفتاح تمليح المعطيات المجفرة الذي تطبق فيه وظيفة التجفير على مفتاح دورة الرئيس والقيمة الأولية **paramSsaltIV** على مفتاح تمليح المعطيات *KS*. وفي الأسلوب EOFB يسيّر مفتاح تمليح غير مجفر (*ksc*) في العنصر **ClearSalt** داخل المعلمة **paramSsalt**. وقد تضم المعلمة **clearSaltingKey** مفتاح تمليح معطيات غير مجفّر، وفي مثل هذه الحالة ينبغي أن يبقى المجال **encryptedSaltingKey** فارغاً والعكس بالعكس. ولا يرسل مفتاح تمليح غير مجفر إلا عند ضمان عدم إيذاء الأمن وإلا فيوصى بتجفير مفتاح تمليح المعطيات.

وعلى الكيان الرئيسي أن يكون مستعداً لاستقبال وسيط مجفر مع مفتاح دورة جديد فور إرسال الأمر **EncryptionUpdateCommand** ولكن عليه أن يستمر باستعمال مفتاح الدورة القديم إلى أن يستلم العنصر **EncryptionUpdateAck**. ويستطيع الرئيس أن يشرع بالدورة الجديدة التي تبدأ عند استلام رسالة **encryptionUpdateAck** بينما يستطيع التابع إطلاق مفتاح الدورة الجديد بعد استلام الأمر **EncryptionUpdateCommand**.

الملاحظة 1 – يمكن للرئيس اختيار أي قيمة للحمولة النافعة الدينامية للتابع لأن نمط الحمولة النافعة لا يتعلق إلا بمنفذ قناة الوسيط.

الملاحظة 2 – من غير الضروري للتابع أن يُشفر باستلامه للمفتاح الجديد علنياً. فبمقدور الرئيس أن يستنتج أن التابع قد استلم المفتاح المرسل عند استقباله للوسيط المجفر مع النمط الجديد للحمولة النافعة.

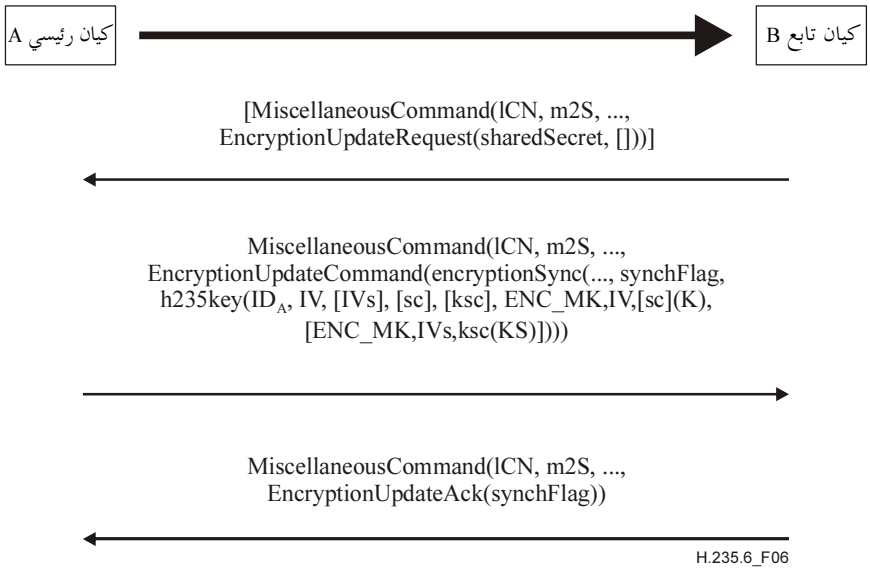


الشكل H.235.6/5 – تحديث مفتاح الدورة في القناة المنطقية للتابع

يبين الشكل 6 إجراءات تحديث مفاتيح القناة المنطقية التي يستعملها الرئيس. وفي حال شروع التابع بعملية تحديث المفاتيح وطلب مفتاح دورة جديد من الرئيس، عليه أن يرسل إلى الرئيس الأمر **MiscellaneousCommand** الذي يضم فيه العنصر **logicalChannelNumber** رقم القناة المنطقية (كما يحدده الرئيس)، وينبغي وضع **sharedSecret** على "true" ومؤشر **الاتجاه** على **masterToSlave**. أما إذا بدأ الرئيس بعملية تحديث المفتاح فينبغي عدم إرسال الرسالة **EncryptionUpdateRequest**.

وينبغي على الرئيس – في حال استجاب لطلب التابع أو إذا كانت المبادرة مبادرته – أن يرسل الأمر **EncryptionUpdateCommand** الذي يضم فيه العنصر **logicalChannelNumber** رقم القناة المنطقية على أن يوضع **الاتجاه** على **masterToSlave** وأن توفر المعلمة **encryptionSync** المؤشر **synchFlag** مع الرقم الجديد للحمولة النافعة الدينامية. ويسيّر العنصر **h235key** مفتاح الدورة الجديد وينبغي أن يحتوي على الكيان الرئيسي في **generalID** والمتجه الأولي *IV* المطبق في **paramS**. وينبغي تسيير مفتاح دورة الوسيط المجفر في المعلمة **encryptedSessionKey** التي ينبغي تطبيق وظيفة التجفير فيها على مفتاح الرئيس، وتطبيق القيمة الأولية في **paramS** على مفتاح الدورة *K*. وفي الأسلوب EOFB، يسير مفتاح تمليح غير مجفر في **ClearSalt** داخل المعلمة **paramS** (*sc*). وفي الأسلوب EOFB، ينبغي أن تسير المعلمة **encryptedSaltingKey** مفتاح تمليح الوسيط غير المجفر الذي تطبق فيه وظيفة التجفير على مفتاح دورة الرئيس والقيمة الأولية **paramSsaltIV** على مفتاح التمليح *KS*. وفي الأسلوب EOFB، يسير مفتاح التمليح غير المجفر (*ksc*) في العنصر **ClearSalt** داخل المعلمة **paramSsalt**. وقد يحتوي العنصر **clearSaltingKey** على مفتاح تمليح وسيط غير مجفر، وفي مثل هذه الحالة ينبغي أن يبقى المجال **encryptedSaltingKey** فارغاً والعكس بالعكس. ويتم إرسال مفتاح تمليح غير مجفر شريطة ألا يحل ذلك بالأمن، وإلا فيوصى بتجفير مفتاح التمليح.

على التابع أن يرسل إشعاراً باستلام مفتاح الدورة الجديد باستعمال الرسالة **MiscellaneousCommand** التي يحتوي فيها العنصر **logicalChannelNumber** على رقم القناة المنطقية وتعكس الرسالة **encryptionUpdateAck** الرقم الجديد للحمولة النافعة الدينامية في المعلمة **synchFlag**.



الشكل H.235.6/6 – تحديث مفتاح الدورة في القناة المنطقية للرئيس

3.6.8 تحديث المفتاح وتزامنه استناداً إلى نمط الحمولة النافعة

يقدم الرئيس مفتاح التجفير الأولي في نفس الوقت الذي يقدم فيه رقم مقدرة الحمولة النافعة الدينامية في **synchFlag** (بواسطة الرسالة **EncryptionSync** في قناة مطابقة للتوصية ITU-T H.245). وينبغي أن يبدأ مستقبل (أو مستقبلات) تدفق المعطيات باستعمال المفتاح فور استلام هذا الرقم للحمولة النافعة في الرأسية RTP.

وإذا كانت القناة المنطقية التي تم التفاوض بشأنها تسيّر نمطاً واحداً لا غير للحمولة النافعة أمكن أن تحل القيمة **synchFlag** محل نمط الحمولة النافعة التي تم التفاوض بشأنها في الرأسية RTP. أما إذا كانت القناة المنطقية التي تم التفاوض بشأنها قادرة على تسيير عدة أنماط للحمولة النافعة (حتى ولو كان ذلك في رزم RTP مستقلة)، فينبغي أن ترتب أنساق الرزم RTP كما هو مبين في المعيار RFC 2198 على أن تعمل المعلمة **synchFlag** كنمط الحمولة النافعة التي تحيط بنمط أو أنماط الحمولة النافعة الفعلية الموجودة في فدرة (أو فدر) الرأسية الإضافية كما هو محدد في المعيار RFC 2198.

ويمكن توزيع النقطة المطرافية الرئيسية لمفتاح جديد واحد أو أكثر في أي لحظة. وينبغي الإشارة إلى تزامن آخر مفتاح جديد مع تدفق المعطيات وذلك بواسطة انتقال نمط الحمولة النافعة إلى قيمة دينامية جديدة.

ملاحظة – يلاحظ أن القيم الخاصة تفقد أهميتها من اللحظة التي تغير فيها مفتاحاً جديداً عند كل توزيع.

7.8 التفاعلات غير المطرافية

1.7.8 البوابـــة

ينبغي اعتبار البوابة H.323 عنصراً موثوقاً به كما جاء في الفقرة H.235.0/6.6. ويشمل هذا البوابات الموجودة بين البروتوكولات (H.323–H.320 إلخ، ...) والبوابات الأمنية (مخدمات الذاكرة الوسيطة/حوائط الحماية). ويمكن ضمان سرية الاتصالات متعددة الوسائط بين النقطة الطرفية وتجهيز البوابة. ولكن ينبغي اعتبار ما يحصل بعد تجاوز البوابة على أنه مسبقاً غير آمن.

2.7.8 المفاتيح الجديدة

تُستكمل الإجراءات المبينة في الفقرة H.323/5.8 بمؤتمر متعدد النقاط (MC) لإخراج مشارك من مؤتمر. ويمكن للرئيس أن ينشئ مفاتيح تجفير جديدة للقنوات المنطقية (ولا يوزعها على الطرف الذي تم إخراجه)؛ ويمكن استعمال هذا الأسلوب للحيلولة دون الطرف الذي تم إخراجه ومراقبة تدفق المعطيات.

3.7.8 عناصر H.323 الموثوقة

تحظى وحدة (وحدات) المؤتمر متعددة النقاط MC(U)s، والبوابات والحارسات البوابية بوجه عام (إذا طبقت نموذج التسيير عبر الحارس البوابي) بالثقة فيما يتعلق بخصوصية قناة التحكم. وإذا تم تأمين قناة إنشاء التوصيلات (H.225.0) وتسييرها عبر الحارس البوابي، فينبغي الثقة فيها أيضاً. وإذا تعين على أي من هذه المكونات للتوصية H.323 العمل في تدفقات المعطيات (أي الخلط، وتحويل الشفرة، ينبغي إذن، بحكم تعريفها، أن تعتبر موثوقاً بها أيضاً فيما يتعلق بخصوصية الوسيط.

ويمكن أيضاً الثقة بالمخدمات الوسيطة لحائط الحماية (على الرغم من أنها لا تشكّل عناصر خاصة بالتوصية H.323) إذ أنها تنهي التوصيلات، وقد يتعين عليها معالجة الرسائل وتدفقات الوسائط.

8.8 الإجراءات متعددة النقاط

1.8.8 الاستيقان

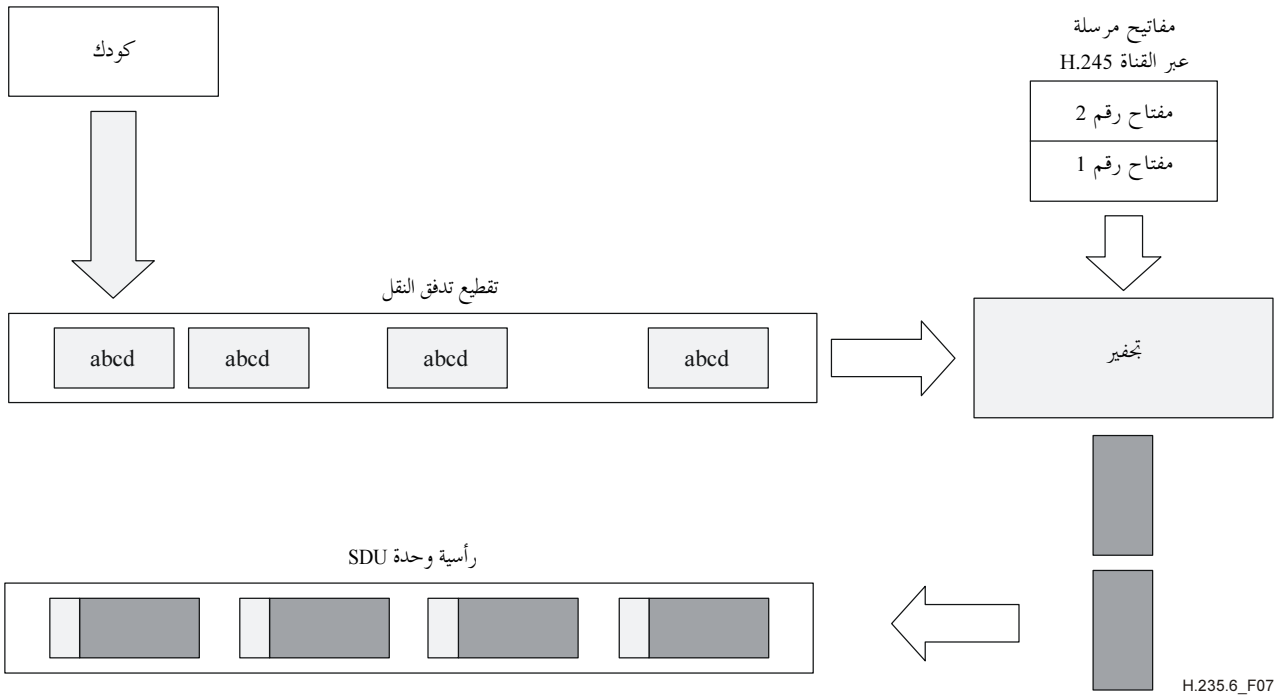
يجب أن يحصل الاستيقان بين النقطة الطرفية والوحدة MC(U) بنفس الطريقة المتبعة في مؤتمر من نقطة إلى نقطة. ويجب أن تحدد الوحدة MC(U) السياسة المتعلقة بمستوى الاستيقان وصلابته. وكما أشير في الفقرة H.235.0/6.6 ينبغي أن تكون الوحدة MC(U) موضع ثقة. ومن الممكن أن يحد مستوى الاستيقان الذي تستعمله الوحدة MC(U) من النقاط الطرفية الموجودة في مؤتمر. وتسمح الأوامر الجديدة **ConferenceRequest/ConferenceResponse** للنقاط الطرفية أن تحصل على شهادات من مشاركين آخرين في المؤتمر من الوحدة MC(U). وكما جاء في إجراءات التوصية H.245 من الممكن أن تطلب النقاط الطرفية في مؤتمر متعدد النقاط شهادات نقاط طرفية أخرى من MC ولكنها قد لا تتمكن من إجراء استيقان تجفيري ضمن القناة H.245.

2.8.8 الخصوصية

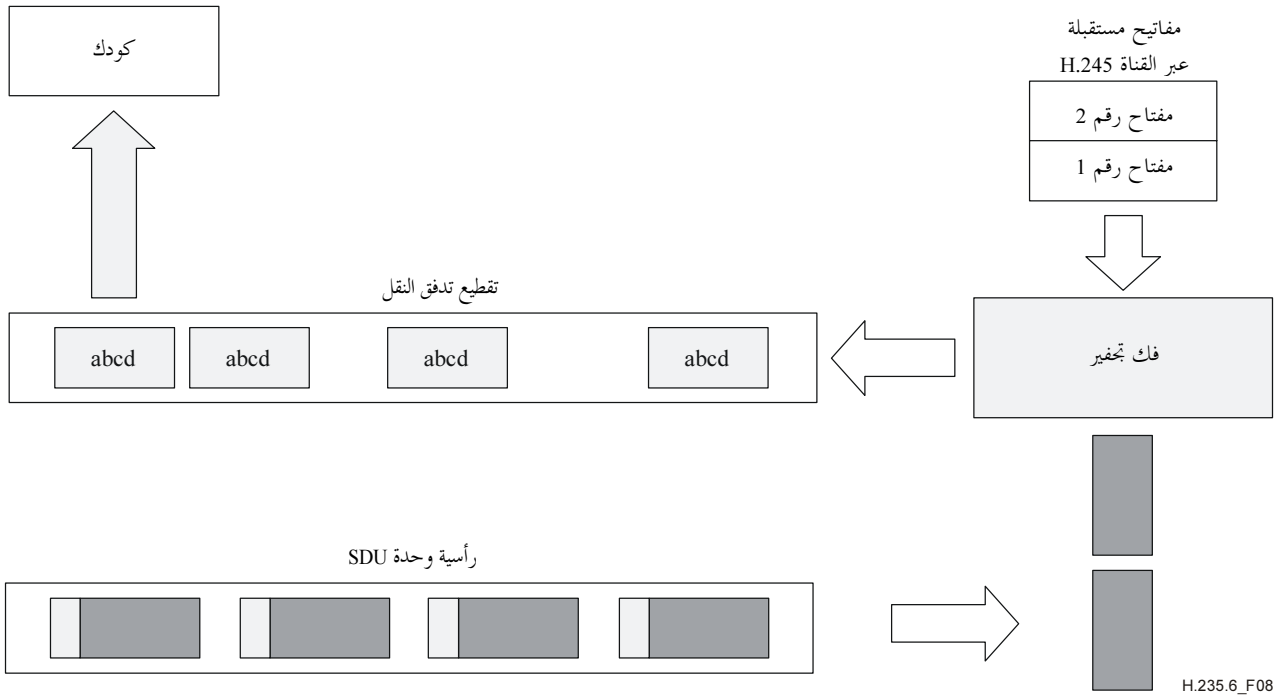
يجب أن تفوز وحدة التحكم MC(U) بجميع الاتصالات المتبادلة الرئيسية والتابعة ويجب على هذا الأساس توفير مفتاح (مفاتيح) التجفير إلى المشاركين في مؤتمر متعدد النقاط. ومن الممكن تحقيق خصوصية الاتصالات للمصادر الفردية ضمن دورة مشتركة (في حال تعدد المقاصد) باستعمال مفاتيح فردية أو مشتركة. ومن الممكن أن تختار الوحدة MC(U) هذين الأسلوبين بشكل اعتباطي ويجب ألا يخضعا لتحكم أية نقطة طرفية معينة ما عدا في الأساليب التي تسمح بها سياسة الوحدة MC(U). وبتعبير آخر من الممكن استعمال مفتاح مشترك عبر عدة قنوات منطقية مفتوحة من مصادر مختلفة.

9 إجراءات تجفير تدفقات الوسائط

يجب تشفير تدفقات الوسائط باستعمال الخوارزمية والمفتاح المتوفرين في القناة H.245. ويبين الشكلان 7 و8 التدفق العام. وتجدر الملاحظة أن رأسية النقل مرتبطة بوحدة SDU للنقل بعد تجفير هذه الوحدة وتدل القطع غير الشفافة على سرية الاتصالات. وبما أن المرسل يستقبل المفاتيح الجديدة ويستعملها في التجفير يجب أن تشير رأسية الوحدة SDU إلى المستقبل بطريقة ما أن المفتاح الجديد قيد الاستعمال الآن. وعلى سبيل المثال، في التوصية ITU-T H.323، تغير مثلاً رأسية البروتوكول RTP (SDU) نمط حمولتها النافعة للإشارة إلى بدالة المفتاح الجديد.



الشكل H.235.6/7 – تجفير الوسائط



الشكل H.235.6/8 – فك تجفير الوسائط

1.9 مفاتيح دورة الوسائط

تضم الرسالة **encryptionUpdate** (تحيين التجفير) المفتاح **h235Key** المشفر بالترميز ASN.1 ضمن سياق التفرع ASN.1 الوارد في التوصية ITU-T H.235 وينقل كسلسلة أثمونات غير شفافة في ما يتعلق بالتوصية H.245. ومن الممكن حماية المفتاح باستعمال إحدى الآليات الثلاث الممكنة عند نقلها بين نقطتين طرفيتين.

- إذا كانت القناة H.245 آمنة لا تطبق حماية إضافية على معلومات المفتاح. وينقل المفتاح "بوضوح" في ما يتعلق بهذا المجال ويستعمل خيار الترميز ASN.1 للقناة **secureChannel**.

- إذا أقيم مفتاح سري وخوارزمية خارج نطاق القناة H.245 ككل (أي خارج التوصية H.323 أو قناة منطقية **h235Control**) يستعمل السر المشترك لتجفير معلومات المفتاح ويدرج هنا المفتاح المشفر الناتج. وفي هذه الحالة يستعمل خيار الترميز ASN.1 للسر **sharedSecret** (سر مشترك).
- من الممكن استعمال الشهادات عندما لا تكون القناة H.245 آمنة ولكن يمكن استعمالها أيضاً فضلاً عن القناة H.245. وعندما تستعمل الشهادات تشفر معلومات المفتاح باستعمال مفتاح الشهادة العمومي وبنية الترميز ASN.1 **certProtectedKey**.

في أي وقت خلال المؤتمر من الممكن أن يطلب مستقبل (أو مرسل) مفتاحاً جديداً (بواسطة طلب من النمط **encrptionUpdateRequest**). وقد يكون السبب في ذلك أنه يشكل في أنه أضاع تزامن قناة منطقية. ويجب أن يولد الرئيس الذي يستقبل هذا الطلب مفتاحاً (أو مفاتيح) رداً على هذا الأمر. ومن الممكن أن يقرر الرئيس أيضاً بشكل لا تزامني توزيع مفتاح (أو مفاتيح) جديد (جديدة) وفي هذه الحالة يجب أن يستعمل رسالة **encryptionUpdate**.

وبعد استقبال **encryptionUpdateRequest**، يجب أن يرسل الرئيس **encryptionUpdate**. وإذا كان المؤتمر متعدد النقاط فينبغي أن يوزع التحكم MC (وهو أيضاً الرئيس) المفتاح الجديد على جميع المستقبلات قبل أن يعطي هذا المفتاح إلى المرسل. ويجب أن يستعمل مرسل المعطيات على القناة المنطقية في أقرب وقت ممكن بعد استقبال الرسالة.

ومن الممكن أيضاً أن يطلب المرسل (إذا افترضنا أنه ليس الرئيس) مفتاحاً جديداً. وإذا كان المرسل جزءاً من المؤتمر المتعدد النقاط يجب أن يكون الإجراء كما يلي:

- يجب أن يرسل المرسل **encryptionUpdateRequest** إلى التحكم MC (الرئيس).
- ينبغي أن يولد MC (الرئيس) مفتاحاً (مفاتيح) جديداً (جديدة) وأن يرسل رسالة **encryptionUpdate** إلى جميع المشاركين في المؤتمر باستثناء المرسل.
- بعد توزيع المفاتيح الجديدة على جميع المشاركين الآخرين يجب أن يرسل الرئيس **encryptionUpdate** إلى المرسل. وبعد ذلك يجب أن يستعمل المرسل المفتاح الجديد.

2.9 حماية الوسيط من الغرق

قد يرغب مستقبل تدفق معطيات البروتوكول RTP بمقاومة الاعتداءات التي تستهدف وظيفة رفض الخدمة واعتداءات الإغراق المحتملة عند نقاط النفاذ إلى الوحدات RTP/UDP. ويمكن للمستقبل عند تطبيق مقدرة الحماية من الغرق أن يحدد بسرعة ما إذا كانت رزمة RTP آتية من مصدر غير مسموح وأن يرفضها.

وفي حال تنشيط مقدرة الحماية من الغرق فإنها تشير إلى استعمال الآلية المناسبة:

- بالنسبة إلى معطيات "واضحة" دون تجفير (انظر الحالة 1 أدناه)؛
- بالنسبة إلى تجميعات مع معطيات وسائط مجفرة وعندما تضم المقدرة **EncryptionCapability** خوارزمية تجفير (انظر الحالة 2 أدناه).

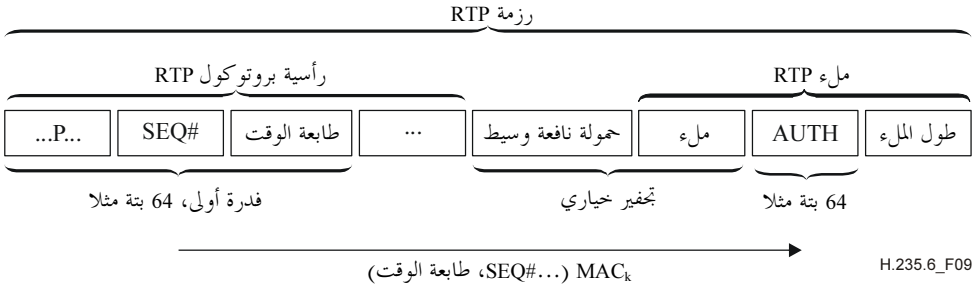
تقدم كلتا الإمكانيتين استيقاناً **RTP packet authentication** معدلاً للمجالات المختارة بواسطة شفرة تعرف هوية الرسائل المحسوبة (MAC). ويمكن حساب هذه الشفرة بواسطة معرفات هوية الأغراض المعرفة في الفقرة 1.2.9. ويتم الحصول على التجفير:

- باستعمال خوارزمية تجفير (مثل DES بالأسلوب MAC؛ انظر المعيارين ISO/IEC 9797-1 وISO/IEC 9797-2). ويشار إلى الشفرة DES-MAC بواسطة المؤشر OID "N" بينما يشار إلى الشفرة triple-DES-MAC بواسطة المؤشر OID "O"؛
- باستخدام وظيفة التجفير الاتجاهية (مثل SHA1). يستحسن استعمال المؤشر OID "M".

ويشار إلى الخوارزمية MAC في معرف هوية غرض الخوارزمية **antiSpamAlgorithm**. وإضافة إلى ذلك يشير المعرّف OID للخوارزمية ضمنياً إلى قد الشفرة MAC؛ مثال، 1 فدرة = 64 بتة بالنسبة إلى الشفرة DES-MAC. ومن أجل التوفير في عرض النطاق، يجوز بتر الشفرة MAC مقابل نقص طفيف بالأمن على نحو تتشكل فيه الشفرة MAC من 32 بتة مثلاً؛ مما يتطلب معرّف غرض مختلف وطريقة الحماية من الغرق مستقلة عن كل تجفير إضافي للحمولة النافعة (انظر الحالتين 1 و2 أدناه).

تستعمل الحماية من الغرق نسق الرزم RTP المبينة لاحقاً (انظر الشكل 9) عند تفسير تتابع الملء للبروتوكول RTP بالطريقة التالية (انظر الفقرة 5 في RFC 3550).

- ينبغي وضع البتة P لرأسية البروتوكول RTP على القيمة 1.
- ينبغي إضافة أثمونات الملء في نهاية الحمولة النافعة مع الدلالة التالية:



الشكل H.235.6/9 – نسق الرزم RTP للحماية من إغراق الوسيط

الملاحظة 1 – في حال عدم استعمال الحماية من الغرق لا يستعمل المجالان "AUTH" و"padlen" بدورهما ويطبق نسق الرزم RTP العادي.

1) *حالة الحماية من الغرق دون تجفير*

تطبق هذه الحالة عندما تكون معطيات الوسائط غير مجفرة ومجالات الملء فارغة. ويشتمل آخر أثمون ملء RTP عدد أثمونات الملء التي يستحسن تجاهلها في نهاية الرزمة RTP. وتسيّر أثمونات الملء الأخرى الشفرة MAC. وينبغي حساب هذه الشفرة استناداً إلى أول فدرة مجفرة للرأسية RTP التي تحتوي على طابعة الوقت ورقم التتابع المتغير الذي يستخدم الخوارزمية MAC التي يتم التفاوض بشأنها في المعلمة **antiSpamAlgorithm** والتي تطبق السر التناظري. ويجوز استخدام سر متقاسم ساكن أو مشكَّل يدوياً أو سر متقاسم k يتم التفاوض بشأنه دينامياً وفقاً للإجراءات التي تنص عليها التوصية ITU-T H.235.0. وفيما يخص قدود الفدر الأكبر (أكبر من 64 بتة)، يتوجب اتخاذ عدد كافٍ من البتات من الرأسية RTP، بل حتى من أول حمولة نافعة.

وفيما يخص حساب الشفرة MAC، يوصى باستعمال المفتاح الذي يتم الحصول عليه أثناء توزيع مفاتيح دورة الوسيط H.235، بالرغم من أن مفتاح الدورة المطبق لا يستعمل في تجفير الحمولة النافعة. ويمكن لأغراض إدارة المفاتيح استعمال التوصيل السريع الأمين مع مؤسسة المفاتيح (انظر الملحق H.323/J) أو الأسلوب اليدوي. ويقوم المرسل بحساب الشفرة MAC على النحو المبين أعلاه، ويدرج النتيجة في المجال MAC التابع لمجال الملء AUTH من البروتوكول RTP. ويعرف كل من المرسل والمرسل إليه قد المجال AUTH وطول الشفرة MAC من المعلمة **antiSpamAlgorithm**.

ينبغي القيام بالتحقق من الشفرة MAC جهة المرسل إليه في أسرع وقت ممكن ولربما في المجموعة RTP أو قبل تجفير الحمولة النافعة أو إزالة انضغاطها على أبعد تقدير. ويعيد المرسل إليه حساب الشفرة MAC أولاً بنفس طريقة المرسل ويقارن الشفرة MAC المحسوبة مع الشفرة MAC المعاد وضعها في مجال الملء RTP. وفي حال عدم توافق الشفرتين MAC، تكون رأسية الرزمة RTP قد تغيرت خلال النقل أو أن كياناً غير مرخص له ولا يمتلك مفتاحاً قد أرسلها. وبالتالي ينبغي تجاهل الرزم RTP التي يتعذر الاستيقان منها وتسجل الحادثة؛ إذ إن ذلك غالباً

ما يدل على محاولة اعتداء على وظيفة رفض الخدمة. وإلا فتستمر معالجة الرزمة RTP التي تم الاستيقان منها ويحذف مجال الملء RTP وترسل الحمولة النافعة في الكودك.

الملاحظة 2 – تتطلب العملية الإجمالية لحساب الشفرة MAC والتحقق منها مع التجفير DES عملية تجفير واحدة. وعلى العكس من ذلك يحسب التشفير SHA1 MAC استناداً إلى جزء بسيط من الرزم ذات الطول الثابت؛ وبالتالي فإن عمليات التجفير تستهلك حداً أدنى من موارد المعالجة.

2) *حالة طريقة الحماية من الغرق مع تجفير الحمولة النافعة*

تطبق هذه الحالة عند تجفير معطيات الوسائط وطلب طريقة الحماية من الغرق. وعندما لا تقابل الحمولة النافعة حدود فدر زوجية، ينبغي إضافة بعض أثمونات الملء الإضافية إلى الحمولة النافعة قبل الشفرة MAC. ويطابق تجفير الحمولة النافعة للوسيط الفقرة 9.

تعرِّف المعلمة **EncryptionCapability** خوارزمية تجفير الحمولة النافعة بينما تعرِّف المعلمة **antiSpamAlgorithm** طريقة الحماية من الغرق. ولأسباب أمنية ينبغي أن يستخدم تجفير الوسيط والشفرة MAC مفاتيح مختلفة للدورة. ويتم حساب المفتاح k للشفرة MAC بإدراج مفتاح التجفير K في وظيفة التظليل وحيدة الاتجاه الفريدة SHA1.

k = SHA1 (K)؛ ويستحسن أخذ عدد كافٍ من البتات من نتيجة التظليل، حسب ترتيب أثمونات الشبكة. وعندما تشير المعلمة إلى خوارزمية التجفير، ينبغي تحويل البتات التي تم جمعها إلى مفتاح تجفير صحيح؛ على سبيل المثال، بوضع بتات التعادلية للمعيار DES.

وعندما يجري المرسل إليه بنجاح التحقق من استيقان الرزمة RTP، يتم فك تجفير الحمولة النافعة وتستبعد أثمونات الملء RTP، ويطابق الإجراء العام الحالة 1 الواردة أعلاه.

1.2.9 قائمة بمعرّفات هوية الأغراض

يعدد الجدول 3 جميع معرّفات هوية الأغراض OID التي سبق ذكرها:

الجدول H.235.6/5 – معرفات هوية الأغراض المستعملة في الحماية من الغرق

معرّف هوية الغرض	قيمة معرّف هوية الغرض	الوصف
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 8}	حماية من الغرق تستعمل الشفرة HMAC-SHA1-96
"N"	{iso(1) identified-organization(3) oiw(14), secsig(3) algorithm(2) desMAC(10)}	حماية من الغرق تستعمل الشفرة MAC DES (56 بتة) (انظر المعيارين ISO/IEC 9797-1 وISO/IEC 9797-2) مع الشفرة MAC مع 64 بتة
"O"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	حماية من الغرق تستعمل الشفرة MAC DES مضاعفاً ثلاثاً (168 بتة) (انظر المعيارين ISO/IEC 9797-1 وISO/IEC 9797-2)

3.9 مصادر RTCP/RTP

يتبع استعمال التجفير في التدفق RTP المنهجية العامة التي توصي بها الوثيقة المشار إليها في [RTP]. ويجب أن يحصل التجفير رزمةً رزمةً بشكل مستقل.

ملاحظة – يتعين الإشارة إلى أنه إذا كان حجم رزمة RTP أكبر من حجم رزمة MTU، فإن من شأن الخسارة الجزئية (للجزء) أن تجعل رزمة RTP بأكملها غير قابلة لفك الشفرة.

ويجب ألا تجفّر الرأسية RTP. أما بالنسبة إلى الكودك السمعي/الفيديوي فإنه ينبغي تجفير مجمل الحمولة النافعة للكودك السمعي/الفيديوي بما في ذلك رأسيات الحمولة النافعة السمعية/الفيديوية التي قد تكون موجودة. ويقوم تزامن المفاتيح الجديدة والنص المجفر على نمط حمولة نافعة دينامي (انظر الفقرة 3.6.8).

وانطلاقاً من مبدأ عدم تطبيق التجفير إلا على الحمولة النافعة في كل رزمة RTP تبقى الرأسيات واضحة. ويفترض أن جميع الرزم RTP مشكلة من مضاعف عدد صحيح من الأثمونات. ولا تطرق هذه التوصية إلى دراسة كيفية تغليف الرزم RTP في طبقة النقل أو طبقة الشبكة. وعلى كل الأساليب أن تتوقع فقدان (أو تغيير تصنيف) الرزم وكذلك حشو الرزم لكي تحتوي على عدد صحيح مناسب من الأثمونات.

يجب أن يجري فك تجفير التدفق بدون أخذ الحالة بعين الاعتبار نظراً إلى إمكانية ضياع الرزمة؛ ويجب أن تكون الرزمة قابلة لفك التجفير بشكل منعزل. ويجب تطبيق شرطي أسلوب الخوارزمية للفدرة كما يلي:

1.3.9 متجهات التدميث

تنطوي معظم أساليب الفدرة على "تسلسل" ما وترتبط كل دورة تجفير بطريقة ما بدخل الدورة السابقة. وبالتالي يجب تزويد قيمة فدرة أولية ما في بداية الزمرة (تسمى عادة متجه التدميث (IV)) من أجل بدء عملية تجفير ما. وبغض النظر عن عدد أثمونات التدفق التي تعالج في كل دورة تجفير، فإن طول المتجه IV يساوي دائماً طول الفدرة. وتتطلب جميع الأساليب باستثناء أسلوب كتاب الشفرة الإلكتروني (ECB) المتجه IV.

1.1.3.9 متجهات التدميث CBC

يتطلب استعمال تجفير الفدر في الأسلوب CBC لتجفير الحمولات النافعة للرزم RTP متجه التدميث (IV). ويكون قد المتجه IV مساوياً لقد الفدرة في تجفير الفدرة. مثلاً يكون قد المتجه IV 64 بتة في المعيارين DES و3-DES بينما يساوي 128 بتة في المعيار AES.

فيما يخص حالات الأسلوب CBC (تسلسل فدر التجفير)، ينبغي تكوين متجه التدميث استناداً إلى B في الأثمونات الأولى (حيث B هو طول الفدرة) من التتابع (Seq# متسلسل + طابعة الوقت). مما يعطي التتابع *SSTTTT*، حيث *SS* هو Seq# RTP في أثمونين و*TTTT* هو الوقت والساعة RTP بأربعة أثمونات. وينبغي تكرار هذا النسق حتى إنتاج عدد كاف من الأثمونات بطول B أثموناً، مع البتر إن دعت الحاجة. ومثال على ذلك يحتوي متجها التدميث المكونان من 64 و128 بتة التابعين *SSTTTTSS* و*SSTTTTSSTTTTSSTT* على التوالي. وتجدر الإشارة إلى أن متجه التدميث المنتج بهذه الطريقة قد يظهر نسق مفتاح يعتبر "ضعيفاً" بالنسبة إلى خوارزمية معينة.

2.1.3.9 متجهات التدميث في الأسلوب EOFB

ينبغي حساب المتجه الأولي الوحيد IV لكل رزمة RTP في الأسلوب EOFB على النحو التالي:

يصاحب كل رزمة RTP دليل ضمني i من الرزم بطول 48 بتة، كما هو محدد في المعيار [SRTP] حيث $i = \text{SEQ} + \text{ROC} \times 2^{16}$، مع العلم بأن SEQ هو رقم التتابع المأخوذ من الرأسية RTP، وROC هو عدّاد الدورة الكاملة المكونة من 32 بتة الذي يعد عدد مرات دورة رقم التتابع (SEQ) مروراً بالرقم 65535.

وينبغي في البداية وضع عداد الدورة الكاملة ROC على الصفر. وفي كل مرة ينهي فيها رقم التتابع دورة بمقاس 2^{16}، ينبغي أن يزيد المرسل العداد ROC بمقاس 2^{32} واحد.

ويحسب المتجه IV بأنه ($i \parallel T \parallel i \parallel T \parallel \ldots$) مع دليل i طوله 48 بتة وطابعة وقت T طولها 32 بتة مأخوذة من الرأسية RTP المتسلسلة عدة مرات إلى أن يمتلئ قد الفدرة. ويعني الرمز || التسلسل.

ملاحظة – تتم صيانة وحساب عداد الدورة الكاملة والمتجه IV محلياً في كل جهة نظيرة دون إرسالهما.

وفي حال فقدان الرزم أو إعادة ترتيبها ينبغي الحساب على أساس الدليل i البالغ: $i = \text{SEQ} + v \times 2^{16}$ حيث تؤخذ v من المجموعة {ROC-1، ROC، ROC+1} بالمقاس 2^{32} على نحو تكون فيه v القيمة الأقرب (من جهة 2^{48}) من القيمة $s_l + \text{ROC} \times 2^{16}$ وحيث s_l هو رقم التابع جهة المستقبل. وبعد معالجة الرزمة باستعمال الدليل المقدّر على المستقبل تحديد ضرورة تحديث s_l وROC. وعلى سبيل المثال هناك طريقة بسيطة (لكنها معرضة للأخطاء) تنطوي على تثبيت s_l بالنسبة إلى

SEQ (إذا كان s_l < SEQ) وإذا استعملت القيمة v = ROC + 1، على تحديث ROC بالنسبة إلى v؛ لمزيد من المعلومات انظر أيضاً [SRTP القسم 1.2.3].

2.3.9 الحشو

يعالج الأسلوبان ECB وCBC تدفق الدخل فدرة فدرة دائماً وفي حين أن الأسلوبين CFB وOFB يستطيعان أن يعالجا أي عدد من أثمونات تدفق الدخل (N (≤ B)، يوصى بأن يكون $B = N$.

وهناك طريقتان لمعالجة الرزم التي لا تساوي حمولتها النافعة مضاعف عدد صحيح من الفدر:

1) استعارة نص تجفير في حالة الفدر الناقصة في الأسلوبين ECB وCBC وعدم الحشو في الأسلوبين CFB وEOFB.

2) الحشو بالطريقة التي يوصى بها [RTP]، القسم 1.5.

يصف البروتوكول [RTP، القسم 1.5] طريقة حشو تحشى بموجبها الحمولة النافعة حتى تبلغ مضاعف عدد صحيح من الفدرات. وينبغي أن يشير آخر أثمون إلى عدد أثمونات الحشو (بما في ذلك هذا الأثمون الأخير) وتدمث البتة P في الرأسية RTP. وينبغي تحديد قيمة الحشو بواسطة الصيغة العادية لخوارزمية التجفير.

يجب أن توفر جميع التطبيقات H.235 الطريقتين. ومن الممكن استنتاج الطريقة المستخدمة كما يلي: إذا كانت البتة P منشطة في الرأسية RTP تكون الرزمة محشوة وإذا لم تكن الرزمة مضاعف للطول B و لم تكن البتة P منشطة تطبق طريقة استعارة التجفير. وإلا تكون الرزمة مضاعف B ولا ينطبق الحشو.

3.3.9 حماية البروتوكول RTCP

يتطلب تطبيق تقنيات التجفير على عناصر بروتوكول التحكم بالوقت الفعلي (RTCP) مزيداً من الدراسة.

4.3.9 تدفق الحمولة النافعة الأمنية

تستخدم الشبكات H.323 عند استعمالها لإرسالات المودم بالبروتوكول IP مثلاً التشوير H.245 من أجل إنشاء قناة معطيات بالنطاق الصوتي والتفاوض بشأنها وتستخدم البروتوكول RTP من أجل وضع تدفق الحمولة النافعة المتعدد (MPS) في رزم.

فيما يخص قطار معطيات واحد مع نمط واحد من الحمولة النافعة أو التصحيح FEC لقناة أخرى، ينبغي أن يحل نمط الحمولة النافعة الدينامية في المعلمة **encryptionSync** محل نمط الحمولة النافعة بالتغيب.

وفيما يخص التدفقات المغلفة (أي التي تقدم التشفير بالإطناب أو مع تصحيح FEC مشفر طبقاً للمعيار RFC 2198)، ينبغي أن يحل نمط الحمولة النافعة في المعلمة **encryptionSync** محل نمط الحمولة النافعة المغلفة.

أما بالنسبة إلى تدفقات الحمولة النافعة المتعددة فينبغي تجاهل نمط الحمولة النافعة في العنصر **syncFlag** للمعلمة **encryptionSync** والاستعاضة عنها بأنماط الحمولة النافعة (الخيارية) الموجودة في العنصر (أو العناصر) **multiplePayloadStreamElement**.

وينبغي استعمال الأمر **EncryptionUpdateCommand** في إجراء تحديث المفتاح المحسّن لتوزيع عناصر مفتاح الدورة الجديد (انظر الفقرة 2.6.8). ولا تستعمل الرسالة **multiplePayloadStream** إلا عندما ينتظر تدفق الحمولة النافعة توزيع مفتاح جديد. وفي هذه الحالة يتم تجاهل نمط الحمولة النافعة الدينامية في **EncryptionSync**.

5.3.9 التشغيل البيني مع التوصية ITU-T J.170

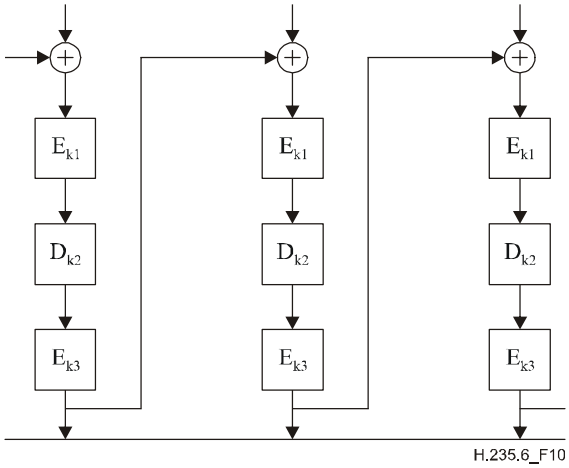
يحتاج هذا الموضوع إلى مزيد من الدراسة.

4.9 المعايير Triple-DES بالأسلوب CBC الخارجي

يستحسن في مواصفة الأمن هذه استعمال المعيار triple-DES بطول 168 بتة بالأسلوب CBC الخارجي المبين في الشكل 10. ويحيل كل دليل k_i في هذا الشكل إلى مفتاح بطول 56 بتة. ويجب استعمال مفتاح مختلف بطول 56 بتة لكل فدرة تجفير (E)

وفك تجفير (D). ومن غير المعروف أن أي مفتاح ضعيف طوله 64 بتة من المعيار DES يسبب ضعفاً في المعيار triple-DES. غير أنه ينبغي للتطبيقات المطابقة لهذه المواصفة أن ترفض المفتاح إذا كان من المعيار DES (انظر RFC 2405).

وهناك مزيد من المعلومات عن المعيار triple-DES في [Schneier] وفي [RFC 2405].



الشكل H.235.6/10 – التجفير Triple-DES بالأسلوب CBC الخارجي

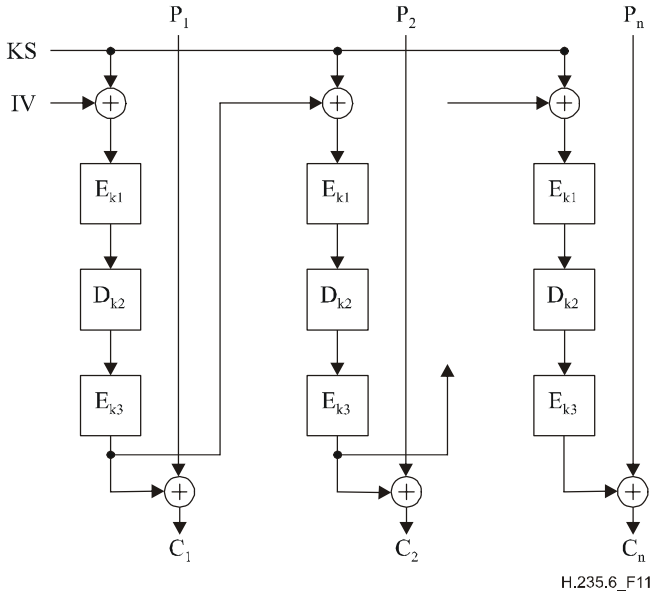
5.9 خوارزمية المعيار DES العاملة بالأسلوب EOFB

يمكن تجفير الصوت بواسطة خوارزمية المعيار DES العاملة في أسلوب تسلسل فدر تجفير التدفق EOFB. ويتيح الأسلوب EOFB استعمال التوازي في التطبيقات. وفي حال استعمال الأسلوب EOFB، يوصي لأسباب تتعلق بالأداء والأمن، بتطبيق مفعول رجعي على كامل فدرة التجفير (أي على البتات الأربع والستين بالنسبة إلى المعيار DES في حالة تكون فيها n مثلاً $n = j = 64$). غير أن الأسلوب EOFB قد يكون حساساً لاعتداءات معينة تتعلق بالخصائص الإحصائية لمعطيات الدخل بالنص الواضح، إذ إنه لا يؤمن تسلسل الفدر والبتات. وهكذا ينبغي تحديث المفاتيح (انظر الفقرة 6.8) بانتظام وكحد أدنى قبل البدء بدورة جديدة للقيمة الأولية. انظر الفقرة 2.1.3.9 فيما يتعلق بحساب القيمة الأولية.

6.9 تجفير المعيار Triple-DES العامل بالأسلوب EOFB الخارجي

يجوز في إطار هذه المواصفة استخدام التجفير triple-DES بطول 168 بتة في الأسلوب EOFB الخارجي الموضح في الشكل 11. ويشير كل عنصر k_i في هذا الشكل إلى مفتاح طوله 56 بتة. وينبغي استعمال مفتاح مختلف بطول 56 بتة لكل فدرة تجفير (E) وفك تجفير (D). ولم يسبب حسب علمنا أي من المفاتيح الضعيفة بطول 64 بتة من المعيار DES ضعفاً في المعيار triple-DES. غير أنه ينبغي لتطبيقات هذه المواصفة أن ترفض المفتاح عندما يكون مفتاح DES ضعيفاً [RFC 2405].

لمزيد من المعلومات عن المعيار triple-DES انظر [Schneier] و[RFC 2405].



الشكل H.235.6/11 – تجفير المعيار Triple-DES بالأسلوب EOFB الخارجي

10 الالتقاط القانوني

يبقي هذا الموضوع للدراسة (انظر [LI]).

11 قائمة معرّفات هوية الغرض

يعدد الجدول 6 الوارد أدناه جميع المعرّفات OID المذكورة (انظر أيضاً [OIW] و[WEBOID]). وهناك معرّفات هوية أغراض للبروتوكولين H.235v1 [التوصية ITU-T H.235v1] وH.235v2 [التوصية ITU-T H.235v2].

الجدول H.235.6/6 – معرّفات هوية الأغراض الواردة في الملحق D

تسمية المعرف	قيمة المعرف	الوصف
"DHdummy"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 40} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 40}	مجموعة DH غير معيارية تتوفر بوضوح.
"DH1024"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 43} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 43}	مجموعة DH طولها 1024 بتة
"DH1536"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 44}	مجموعة DH طولها 1536 بتة
"X"	{iso(1) member-body(2) us(840) rsadsi(113549) encryptionalgorithm(3) 2}	تجفير صوتي يستعمل خوارزمية متوائمة RC2 (56 بتة) أو RC2 متوائمة بأسلوب CBC ومجموعة DH طولها 512 بتة.
"X1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 27}	تجفير صوتي يستعمل خوارزمية متوائمة RC2 (56 بتة) أو RC2 متوائمة بأسلوب EOFB ومجموعة DH طولها 512 بتة.
"Y"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) descbc(7)}	تجفير صوتي يستعمل المعيار DES بطول (56 بتة) بأسلوب CBC ومجموعة DH طولها 512 بتة.
"Y1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 28}	تجفير صوتي يستعمل المعيار DES (56 بتة) بأسلوب EOFB خارجي وبطول 512 بتة ومجموعة DH طولها 64 بتة بمفعول رجعي.

الجدول H.235.6/6 – معرّفات هوية الأغراض الواردة في الملحق D

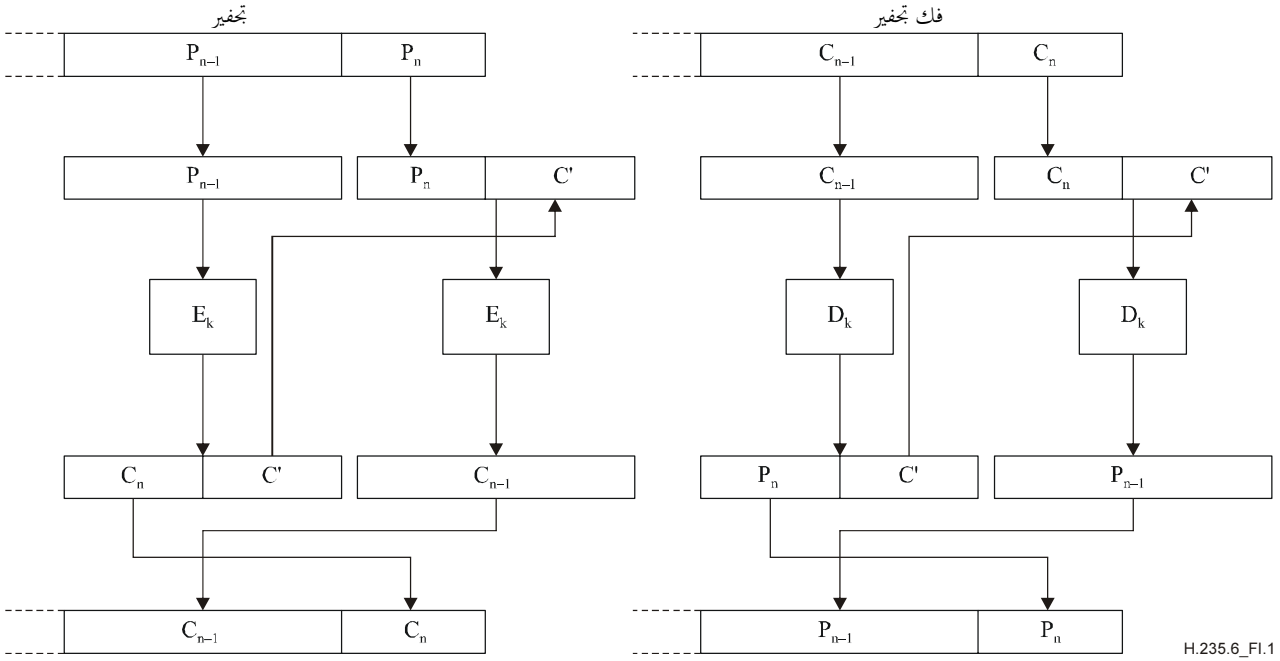
تسمية المعرف	قيمة المعرف	الوصف
"Z1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 29}	تجفير صوتي يستعمل المعيار Triple-DES بطول (168 بتة) بأسلوب EOFB خارجي ومجموعة DH طولها 1024 بتة بمفعول رجعي.
"Z2"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 30}	تجفير صوتي يستعمل المعيار AES بطول (128 بتة) بأسلوب EOFB ومجموعة DH طولها 1024 بتة.
"Z3"	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) 3 nistAlgorithm(4) aes(1) cbc(2)}	تجفير صوتي يستعمل المعيار AES بطول (128 بتة) بأسلوب CBC ومجموعة DH طولها 1024 بتة.
"Z"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	تجفير صوتي يستعمل المعيار Triple-DES (168 بتة) في أسلوب CBC خارجي ومجموعة DH طولها 1024 بتة.

التذييل I

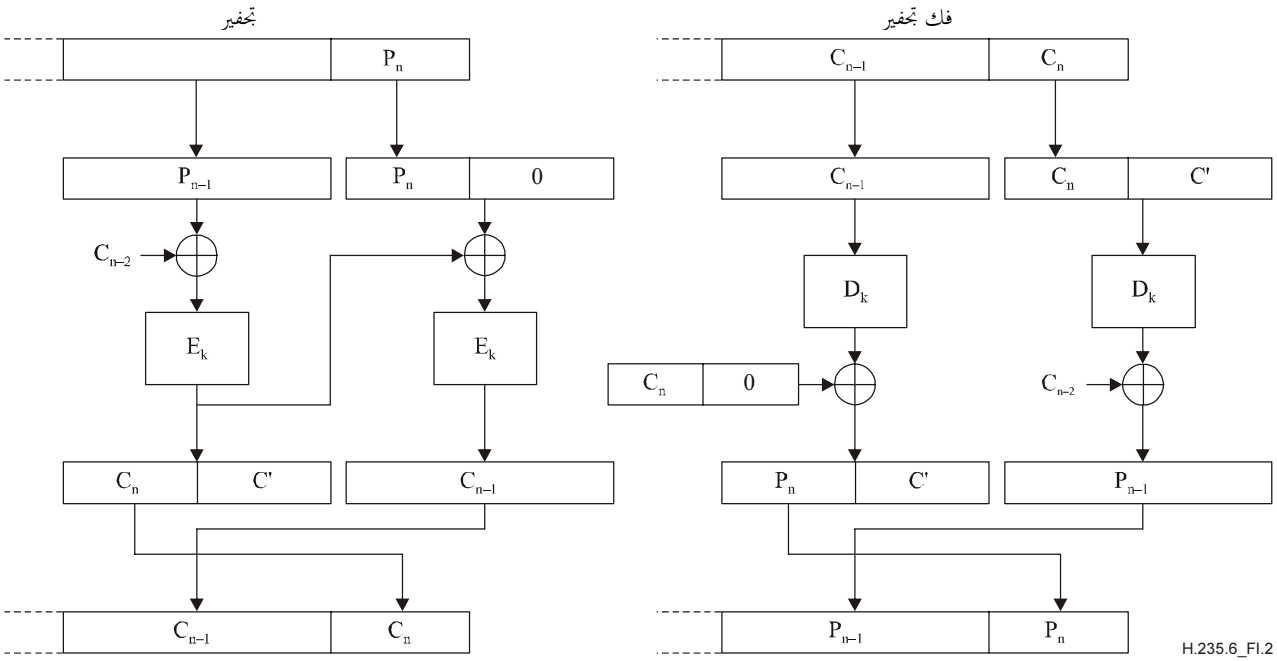
تفاصيل تطبيق التوصية ITU-T H.323

1.I طرائق حشو نص التجفير

يرد وصف سرقة نص التجفير في [Schneier] الصفحتان 191 و196. وتوضح الأشكال من 1.I إلى 5.I هذه التقنية.



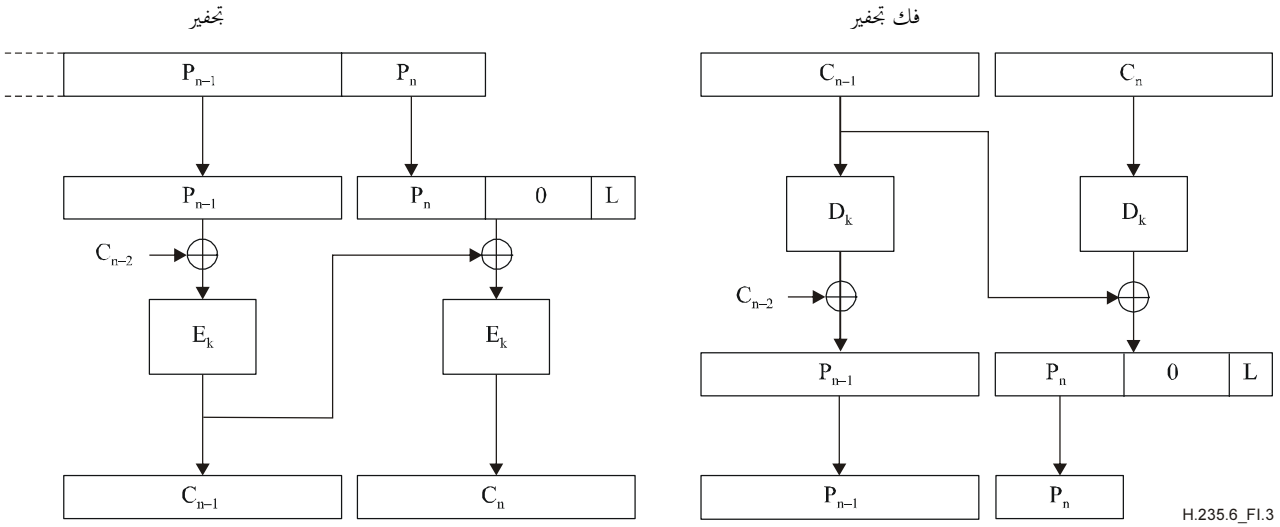
الشكل H.235.6/1.I – سرقة نص التجفير في الأسلوب ECB



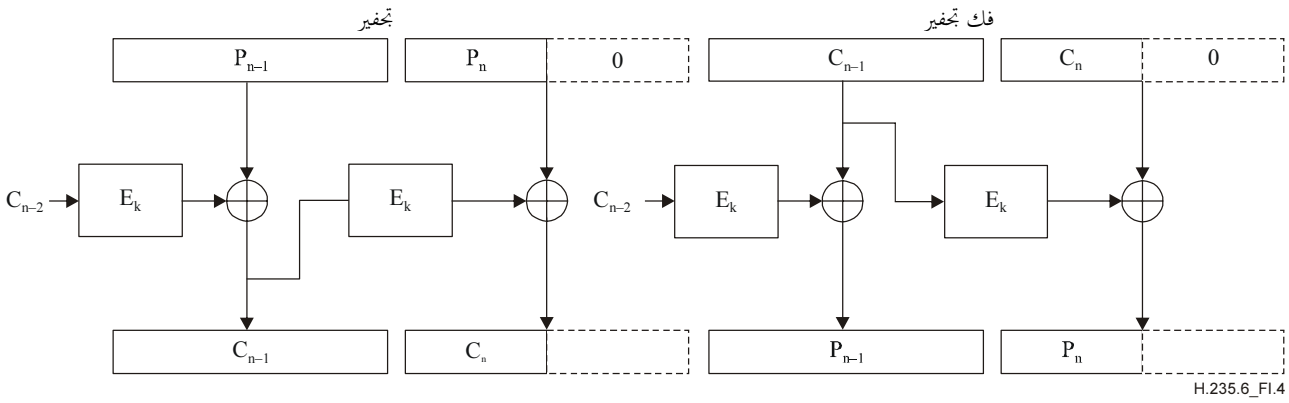
الشكل H.235.6/2.I – سرقة نص التجفير في الأسلوب CBC

ملاحظة – تتطلب سرقة نص التجفير في الأسلوبين ECB أو CBC أن تسيّر الحمولة النافعة فدرة كاملة كحد أدنى. وينبغي أن تتأكد التطبيقات التي تستعمل سرقة النصوص المجفرة في الأسلوبين ECB أو CBC من أن الحمولة النافعة تسير على الأقل فدرة مجفرة باختيار ملائم لوتيرة الاعتيان مثلاً أو باستعمال الرزم أو بالاختيار الملائم بخوارزمية التجفير.

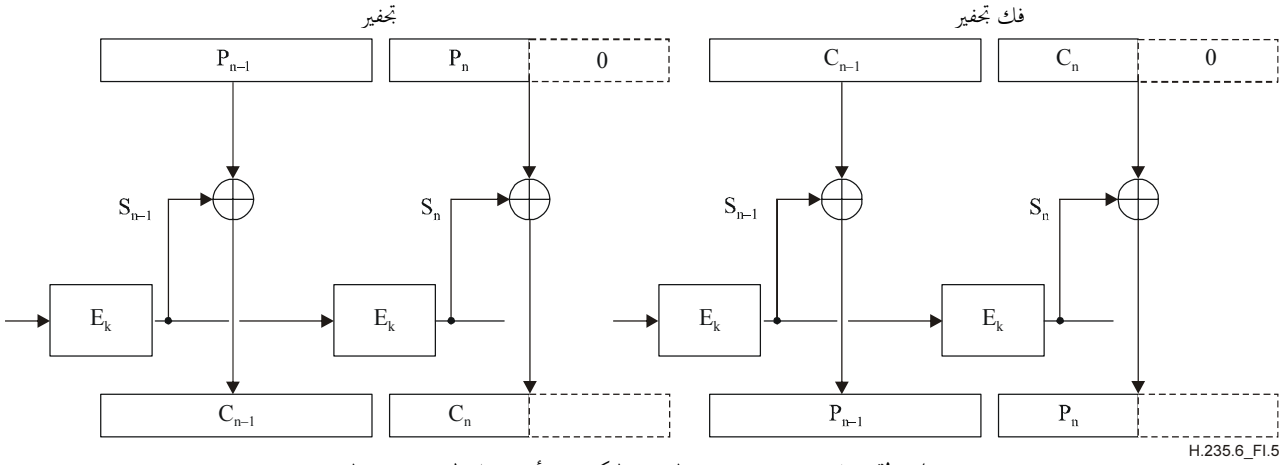
وفي الحالة التي تشغل فيها الحمولة النافعة أقل من فدرة، ينبغي استعمال متجه التدميث (IV) كفدرة نص مجفر سابق عند تطبيق أسلوب سرقة نص التجفير في الأسلوب CBC.



الشكل H.235.6/3.I – الحشو بالأصفار في الأسلوب CBC

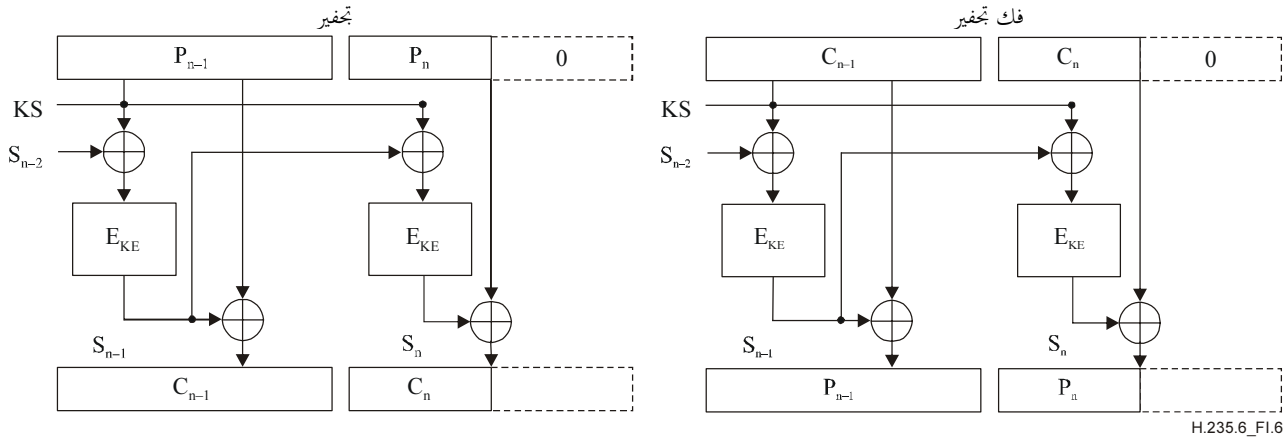


الشكل H.235.6/4.I – الحشو بالأصفار في الأسلوب CFB

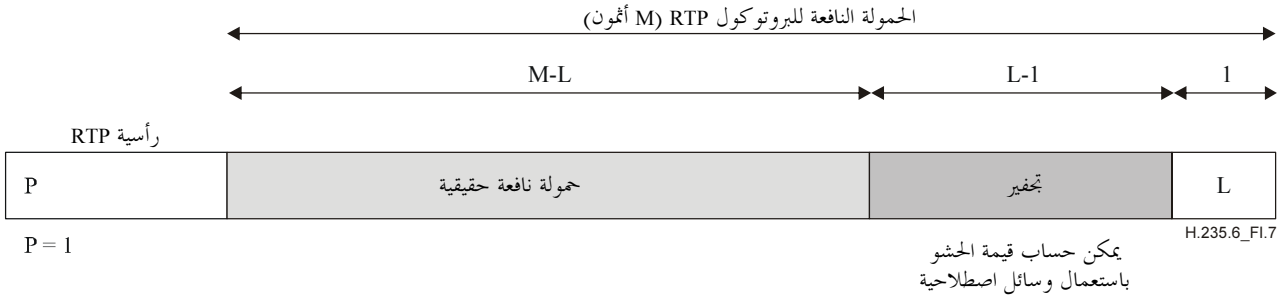


ملاحظة – الإشارة S_i هي نتيجة التجفير التكراري (أي تبديل المواقع) متجه التدميث.

الشكل H.235.6/5.I – الحشو بالأصفار في الأسلوب OFB



الشكل H.235.6/6.I – الأسلوب EOFB مع الحشو بالأصفار



الشكل H.235.6/7.I – الحشو كما يصفه البروتوكول RTP

2.I المفاتيح الجديدة

تطبق وحدة التحكم متعددة النقاط الإجراءات الواردة في الفقرة H.323/5.8 لإخراج مشارك من المؤتمر. ومن الممكن أن يولد الرئيس مفاتيح تجفير جديدة للقنوات المنطقية (وألا يوزعها على طرف مطرود)؛ ويمكن استعمال هذا لمنع الطرف المطرود من مراقبة التدفقات الوسيطة.

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