الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

H.235.0

(2014/01)

السلسلة H: الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

إطار الأمن H.323: إطار أمن للأنظمة متعددة الوسائط من السلسلة ITU-T H (الأنظمة ITU-T H.323 وغيرها من النمط ITU-T H.245)

التوصية ITU-T H.235.0

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية والأنظمة متعددة الوسائط

خصائص أنظمة الهاتف المرئي	H.100–H.199
البنية التحتية للخدمات السمعية المرئية	
اعتبارات عامة	H.200–H.219
تعدد الإرسال والتزامن في الإرسال	H.220–H.229
جوانب الأنظمة	**H.230–H.239**
إجراءات الاتصالات	H.240–H.259
تشفير الصور المتحركة الفيديوية	H.260–H.279
جوانب تتعلق بالأنظمة	H.280–H.299
الأنظمة والتجهيزات المطرافية للخدمات السمعية المرئية	H.300–H.349
معمارية خدمات الأدلة للخدمات السمعية المرئية والخدمات متعددة الوسائط	H.350–H.359
معمارية جودة الخدمات السمعية المرئية والخدمات متعددة الوسائط	H.360–H.369
خدمات إضافية في تعدد الوسائط	H.450–H.499
إجراءات التنقلية والتعاون	
لمحة عامة عن التنقلية والتعاون، تعاريف وبروتوكولات وإجراءات	H.500–H.509
التنقلية لأغراض الأنظمة والخدمات متعددة الوسائط في السلسلة H	H.510–H.519
تطبيقات وخدمات التعاون للوسائط المتعددة المتنقلة	H.520–H.529
الأمن في الأنظمة والخدمات المتنقلة متعددة الوسائط	H.530–H.539
الأمن في تطبيقات وخدمات التعاون للوسائط المتعددة المتنقلة	H.540–H.549
إجراءات التشغيل البيني في التنقلية	H.550–H.559
إجراءات التشغيل البيني للتعاون في الوسائط المتعددة المتنقلة	H.560–H.569
خدمات النطاق العريض والخدمات الثلاثية وخدمات الوسائط المتعددة المتقدمة	
خدمات متعددة الوسائط بالنطاق العريض على خط المشترك الرقمي فائق السرعة (VDSL)	H.610–H.619
تطبيقات وخدمات الوسائط المتعددة المتقدمة	H.620–H.629
تطبيقات شبكات المحاسيس الشمولية وإنترنت الأشياء	H.640–H.649
خدمات وتطبيقات تلفزيون بروتوكول الإنترنت متعددة الوسائط من أجل تلفزيون بروتوكول الإنترنت	
جوانب عامة	H.700–H.719
تلفزيون بروتوكول الإنترنت – الأجهزة المطرافية	H.720–H.729
تلفزيون بروتوكول الإنترنت – البرمجيات الوسيطة	H.730–H.739
تلفزيون بروتوكول الإنترنت – مناولة أحداث تطبيقات	H.740–H.749
تلفزيون بروتوكول الإنترنت – البيانات الشرحية	H.750–H.759
تلفزيون بروتوكول الإنترنت – أطر التطبيقات متعددة الوسائط	H.760–H.769
تلفزيون بروتوكول الإنترنت – اكتشاف الخدمة حتى الاستهلاك	H.770–H.779
اللافتات الرقمية	H.780–H.789
خدمات وتطبيقات الصحة الإلكترونية متعددة الوسائط	
اختبار الامتثال لقابلية التشغيل البيني لأنظمة الصحة الشخصية (HRN وPAN وLAN وWAN)	H.820–H.849
خدمات تبادل البيانات المتعلقة بالصحة الإلكترونية باستخدام الوسائط المتعددة	H.860–H.869

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

إطار الأمن H.323: إطار أمن للأنظمة متعددة الوسائط من السلسلة ITU-T H (الأنظمة ITU-T H.323 وغيرها من النمط ITU-T H.245)

ملخص

تصف التوصية ITU-T H.235.0 التحسينات التي أجريت ضمن إطار سلسلة التوصيات ITU-T H.3xx بهدف إدخال خدمات أمن مثل الاستيقان والخصوصية (تجفير المعطيات). وتُطبق الخطة المقترحة على المؤتمرات البسيطة من نقطة إلى نقطة والمؤتمرات من نقطة إلى نقاط متعددة على حد سواء انطلاقاً من أي من المطاريف التي تستعمل بروتوكول التحكم الوارد في التوصية ITU-T H.245؛ وعلى الأنظمة ITU-T H.323 التي تستعمل بروتوكول RAS و/أو بروتوكول تشوير النداء ITU-T H.225.0.

فعلى سبيل المثال، تعمل الأنظمة ITU-T H.323 في شبكات أسلوب الرزم التي لا تقدم نوعية خدمة مضمونة (QoS). ولنفس الأسباب التقنية التي تدعو الشبكة الأساسية إلى عدم تقديم جودة الأداء، فإن الشبكة لا توفر خدمة آمنة. وتثير عادة الاتصالات الأمنية في الوقت الحقيقي في شبكات لا توفر الأمن، الانشغال بأمرين رئيسيين هما: الاستيقان والخصوصية.

وتصف هذه التوصية البنية التحتية الأمنية والتقنيات الخاصة بسرية الاتصالات التي ينبغي أن تستعملها الأنظمة متعددة الوسائط المطابقة للسلسلة ITU-T H.3xx. وهي تتناول من جملة أمور أخرى المسائل المتعلقة بالمؤتمرات التفاعلية أي مسألتي الاستيقان والخصوصية، في جميع تدفقات الوسائط المتبادلة أثناء مؤتمر ما. وتقدم البروتوكولات والخوارزميات اللازمة بين الكيانات ITU-T H.323.

تستعمل هذه التوصية المقدرات العامة التي يرد وصفها في التوصية ITU-T H.245؛ وبالتالي فإن كل معيار تشغيل له صلة ببروتوكول التحكم هذا قادر على استخدام إطار الأمن موضوع الدراسة. ويتوقع أن مطاريف أخرى تعمل تبعاً للسلسلة ITU-T H. ستكون قدر الإمكان قادرة على التشغيل فيما بينها واستعمال الطرائق الواردة فيما بعد مباشرة، ولن توفر هذه التوصية في الوهلة الأولى تنفيذاً كاملاً في جميع المجالات. لكنها ستطور بشكل خاص الاستيقان من النقاط الطرفية وسرية الاتصالات متعددة الوسائط.

وتدرس هذه التوصية إمكانية التفاوض بين الخدمات والمقدرات بطريقة نوعية وإمكانية انتقاء تقنيات التجفير مقدراته المستعملة. وترتبط طريقة استعمالها بمقدرات الأنظمة ومتطلبات التطبيق والتقييدات الخاصة بسياسات الأمن. وتقدم هذه التوصية خوارزميات تجفير متعددة مع خيارات متعددة تتلاءم والأهداف المختلفة (مثل طول المفاتيح). وقد توزع بعض خوارزميات التجفير على خدمات أمن خاصة (مثل خوارزمية للتجفير السريع لتدفق الوسائط وخوارزمية أخرى لتشفير التشوير).

وتجدر الإشارة إلى أن بعض الخوارزميات وآليات التجفير المتاحة قد تكون محجوزة للتصدير أو لغايات أخرى وطنية (بمفاتيح مقيدة الطول مثلاً). وتقدم هذه التوصية تشوير الخوارزميات المعروفة إضافة إلى تشوير خوارزميات التجفير غير المعيارية أو الخاصة. ولا توجد أي خوارزمية ملزمة لكن ينصح بقوة أن توفر النقاط الطرفية أكبر قدر ممكن من الخوارزميات القابلة للتطبيق من أجل تحقيق قابلية التشغيل البيني. مما يتقارب من فكرة أن المطابقة مع التوصية ITU-T H.245 لا تضمن قابلية التشغيل البيني للكودكين في الكيان.

وتقسم الطبعة 4 من التوصية ITU-T H.235 الطبعة 3 من التوصية ITU-T H.235 إلى مجموعة من توصيات السلسلة الفرعية ITU-T H.235.x، وتقوم بإعادة هيكلتها. وأضيفت توصيتان جديدتان (ITU-T H.235.8 وITU-T H.235.9) إلى هذه المجموعة؛ ووُسعت سلسلة توصيات فرعية أخرى لتشمل خاصية وظيفية جديدة (ITU-T H.235.3 وITU-T H.235.5). وتضم التوصية ITU-T H.235.0 إطار الأمن ITU-T H.323 ونصاً مشتركاً ومعلومات عامة يُستفاد بها في جميع توصيات السلسلة الفرعية ITU-T H.235.x.

وتتيح التذييلات IV وV وVI تقابلاً بين نص وأشكال وجداول الطبعة 3 من التوصية ITU-T H.235 (2003)، بما في ذلك التصويب 1 والتعديلات اللاحقة على الهيكل الجديد.

وتعزز هذه الصيغة المراجعة للتوصية ITU-T H.235 الطبعة 4 لإضافة دعم لمواد المفاتيح ذات الأطوال التي تزيد عن 2048 بتة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T H.235.0	2005-09-13	16	11.1002/1000/8592-en
2.0	ITU-T H.235.0	2014-01-13	16	11.1002/1000/12058-en

مصطلحات أساسية

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

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). 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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

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

© ITU 2017

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

جدول المحتويات

الصفحة

الصفحة

إطار الأمن H.323: إطار أمن للأنظمة متعددة الوسائط من السلسلة ITU-T H (الأنظمة ITU-T H.323 وغيرها من النمط ITU-T H.245)

1 مجال التطبيق

تهدف التوصية ITU-T H.235.0 بشكل أساسي إلى توفير الاستيقان والسرية والتكامل ضمن إطار البروتوكول الحالي للسلسلة ITU-T H. ويوفر نص هذه التوصية تفاصيل عن التطبيق باستعمال [التوصية ITU-T H.323]. ومن المتوقع أن يعمل هذا الإطار مع بروتوكولات أخرى من السلسلة ITU-T H التي تستعمل بروتوكول التحكم الوارد في [التوصية ITU-T H.245] و/أو التي تستعمل بروتوكول RAS و/أو بروتوكول تشوير النداء H.225.0.

وتشمل الأهداف الإضافية لهذه التوصية ما يلي:

1) تطوير معمارية أمنية كإطار موسع ومرن يسمح بتطبيق نظام أمني للمطاريف التي تعمل وفقاً للسلسلة ITU-T H والأنظمة الأخرى من النمط ITU-T H.323. وينبغي توفير هذا الإطار من خلال مقدرات توفرها خدمات مرنة ومستقلة مثل إمكانية التفاوض والانتقاء في ما يتعلق بالتقنيات التجفيرية المستعملة وطريقة استعمالها.

2) توفير أمن جميع الاتصالات التي تحصل نتيجة لاستعمال بروتوكول التوصيات ITU-T H.3xx. ويشمل هذا أوجه إنشاء التوصيل والتحكم بالنداء وتبادل الوسائط بين جميع الكيانات. ويشمل هذا الشرط استعمال الاتصالات السرية (الخصوصية) ومن الممكن استغلال وظائف استيقان الند وكذلك حماية بيئة المستعمل من الاعتداءات.

3) ينبغي ألا تحول هذه التوصية دون إدماج وظائف أمنية أخرى في كيانات ITU-T H.3xx التي يمكن أن تحميها من اعتداءات متأتية من الشبكة.

4) ينبغي ألا تحد هذه التوصية من إمكانية أي من توصيات السلسلة ITU-T H.3xx من التوسع وفقاً للحاجة. وقد يشمل ذلك عدد المستعملين المحميين ومستويات الأمن المتاحة.

5) ينبغي عند الإمكان التزويد بجميع الآليات والتسهيلات بغض النظر عن طبقات أو طوبولوجيات النقل التحتية. وقد تتطلب مواجهة مثل هذه التهديدات وسائل أخرى تقع خارج نطاق هذه التوصية.

6) ينبغي اتخاذ تدابير احتياطية بخصوص التشغيل في بيئة مختلطة (كيانات محمية وغير محمية).

7) ينبغي أن توفر هذه التوصية إمكانية توزيع مفاتيح دورة تتلاءم والتجفير المستعمل (وهو ما لا يعني أن إدارة الشهادات القائمة على أساس المفاتيح العمومية يجب أن تكون جزءاً من هذه التوصية).

8) تقترح هذه التوصية مواصفتين للأمن تسهلان إمكانية التشغيل البيني؛ الأولى [ITU-T H.235.1] بسيطة وأكيدة، تقوم على كلمة السر ، والأخرى [ITU-T H.235.2] على التوقيع، وتستعمل التوقيعات الرقمية والشهادات وبنية تحتية بمفاتيح عمومية، ولا تخضع لتقييدات المواصفة [ITU-T H.235.1].

لا تفترض المعمارية الأمنية التي يرد وصفها في هذه التوصية أن المشاركين يعرفون بعضهم بعضاً. غير أنها تفترض أنه جرى اتخاذ تدابير وقائية لحماية النقاط الطرفية المطابقة للسلسلة ITU-T H. وبالتالي يتوقع أن يكون الخطر الأساسي الذي يهدد أمن الاتصالات هو استراق السمع على الشبكة أو طريقة أخرى ما لتحويل تدفقات المعطيات.

توفر التوصية [ITU-T H.323] وسيلة لعقد مؤتمر سمعي وفيديوي ومعطياتي بين طرفين أو أكثر غير أنها لا توفر الآلية التي تسمح لكل مشارك من استيقان هوية المشاركين الآخرين ولا توفر وسيلة تضمن سرية الاتصالات (أي تجفير التدفقات).

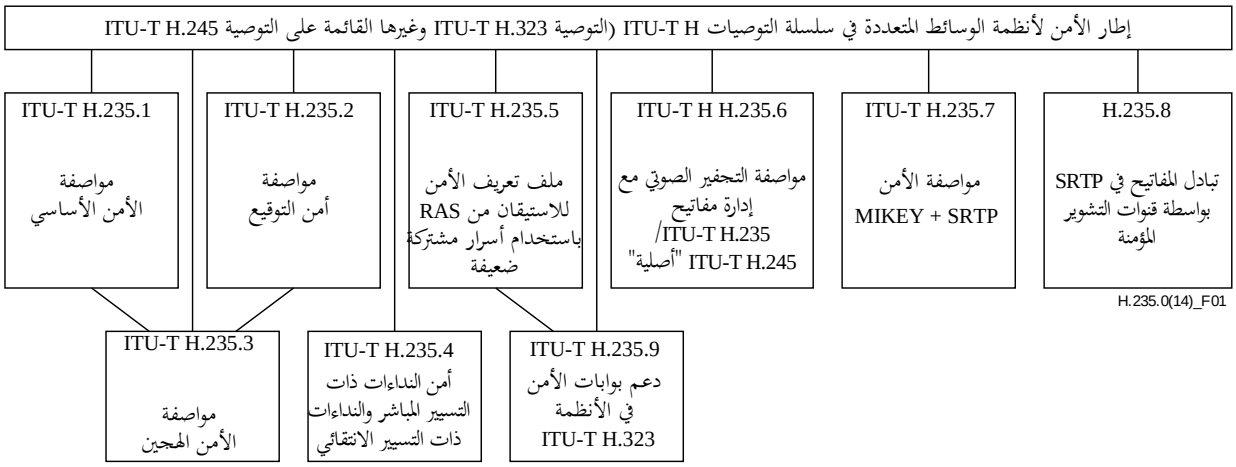
تستخدم المطاريف من نمط التوصيات [ITU-T H.323] و[ITU-T H.324] و[ITU-T H.310] إجراءات تشوير القناة المنطقية وفقاً للتوصية [ITU-T H.245]، التي تصف محتوى كل قناة منطقية عندما تفتح القناة. وهناك إجراءات للتعبير عن مقدرات

المستقبل والمرسل وتقتصر الإرسالات على ما تستطيع المستقبلات أن تفك تشفيره، ومن الممكن أن تطلب المستقبلات من المرسلات أسلوباً معيناً ترغب فيه. وترسل المقدرات الأمنية لكل نقطة طرفية بالطريقة نفسها التي ترسل فيها أية مقدرة اتصالات أخرى.

ومن الممكن استعمال بعض مطاريف السلسلة ITU-T H [ITU-T H.323] في تشكيلات متعددة النقاط. وتسمح الآلية الأمنية التي يرد وصفها في هذه التوصية بالتشغيل الآمن في هذه البيئات بما في ذلك تشغيل وحدة تحكم متعددة النقاط (MCU) مركزية وغير مركزية على حد سواء.

1.1 بنية توصيات السلسلة الفرعية ITU-T H.235.x

تشمل هذه التوصية المعنية بإطار الأمن البنية التالية ضمن توصيات السلسلة الفرعية ITU-T H.235.x على النحو الموضح الشكل 1. وتحتوي هذه التوصية على نص مشترك ومعلومات عامة يُستفاد بها في جميع توصيات السلسة الفرعية ITU-T H.235.x.



الشكل 1 – بنية توصيات السلسة الفرعية ITU-T H.235.x

تشير الخطوط الرأسية في الشكل 1 إلى التبعيات المباشرة بالنسبة إلى النص الرئيسي [ITU-T H.235.0]؛ وقد تكون هناك تبعيات غير مباشرة بالنسبة إلى توصيات أخرى ITU-T H.235.x. ويمكن استعمال عدة توصيات معاً وعلى نحو تكميلي (انظر الفقرة 9.6).

2 المراجع

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.

[ITU-T H.225.0] Recommendation ITU-T H.225.0 v7 (2009), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[ITU-T H.235] Recommendation ITU-T H.235 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

[ITU-T H.235.1] Recommendation ITU-T H.235.1 (2005), *H.323 security: Baseline security profile*.

[ITU-T H.235.2] Recommendation ITU-T H.235.2 (2005), *H.323 security: Signature security profile*.

[ITU-T H.235.3] Recommendation ITU-T H.235.3 (2005), *H.323 security: Hybrid security profile*.

[ITU-T H.235.4] Recommendation ITU-T H.235.4 (2005), *H.323 security: Direct and selective routed call security*.

[ITU-T H.235.5] Recommendation ITU-T H.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets*.

[ITU-T H.235.6] Recommendation ITU-T H.235.6 (2014), *H.323 security: Encryption profile with native ITU-T H.235/H.245 key management*.

[ITU-T H.235.7] Recommendation ITU-T H.235.7 (2005), *H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235*.

[ITU-T H.235.8] Recommendation ITU-T H.235.8 (2005), *H.323 security: Key exchange for SRTP using secure signalling channels*.

[ITU-T H.235.9] Recommendation ITU-T H.235.9 (2005), *H.323 security: Security gateway support for H.323*.

[ITU-T H.245] Recommendation ITU-T H.245 v16 (2011), *Control protocol for multimedia communication*.

[ITU-T H.323] Recommendation ITU-T H.323 v7 (2009), *Packet-based multimedia communications systems*.

[ITU-T H.324] Recommendation ITU-T H.324 (2009), *Terminal for low bit-rate multimedia communication*.

[ITU-T H.510] Recommendation ITU-T H.510 (2002), Mobility for H.323 multimedia systems and services.

[ITU-T H.530] Recommendation ITU-T H.530 (2002), *Symmetric security procedures for H.323 mobility in H.510*.

[ITU-T Q.931] Recommendation ITU-T Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control*.

[ITU-T X.800] Recommendation ITU-T X.800 (1991) | ISO/IEC 7498-2:1989, *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

[ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[IETF RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

[IETF RFC 2407] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*.

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

[IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

[IETF RFC 3546] IETF RFC 3546 (2003), Transport Layer Security (TLS) Extensions.

[IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

[ISO 7498-2] ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

[ISO/IEC 9798-2] ISO/IEC 9798-2:2008, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*.

[ISO/IEC 9798-3] ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

[ISO/IEC 9798-4] ISO/IEC 9798-4:1999, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*.

[ISO/IEC 14888-3] ISO/IEC 14888-3:2006, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.*

[ISO/IEC 15946-1] ISO/IEC 15946-1:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*.

[af-sec-0100.002] af-sec-0100.002 (2001), *ATM Security Specification Version 1.1*, ATM Forum.

3 المصطلحات والتعاريف

تنطبق التعاريف التي ترد في الفقرة 3 من التوصيات [ITU-T H.323] و[ITU-T H.225.0] و[ITU-T H.245] مع تلك التي ترد في الفقرة 1.3 لأغراض هذه التوصية. وتستعمل بعض المصطلحات التالية وفقاً للتعاريف التي ترد في التوصيات [ITU-T X.800] و[ITU-T X.803] و[ITU-T X.810] و[ITU-T X.811].

1.3 تعاريف معرّفة في أماكن أخرى

تستخدم هذه التوصية المصطلحات التالية المعرّفة في أماكن أخرى:

1.1.3 التحكم بالنفاذ [ITU-T X.800]: تدبير وقائي ضد الاستعمال غير المسموح به للموارد بما في ذلك استعمال الموارد بشكل غير مسموح به.

2.1.3 الاستيقان [ITU T X.811]: التأكد من الهوية التي يدعيها كيان ما.

3.1.3 إدارة المفاتيح [ITU-T X.800]: وهي توليد المفاتيح وتخزينها وتوزيعها ومحوها وتوثيقها وتطبيقها تماشياً مع السياسة الأمنية.

4.1.3 خوارزمية تجفير تناظرية (بمفتاح سري) [ITU-T X.810]: خوارزمية لأداء التجفير أو فك التجفير المقابل تتطلب نفس المفتاح للتجفير أو فكه.

5.1.3 التهديد [ITU-T X.800]: احتمال انتهاك الأمن.

2.3 المصطلحات المعرَّفة في هذه التوصية

تستعمل هذه التوصية المصطلحات التالية:

1.2.3 الترخيص: منح التخويل على أساس تعرف الهوية التي تم الاستيقان منها.

2.2.3 الاعتداء: الأنشطة المعتمدة للتحايل على أوجه العجز أو استغلالها في آليات أمن النظام. والاعتداء المباشر يستغل العجز في الخوارزميات أو المفاهيم أو الخصائص التي تستند إليها آلية الأمن. وتحصل اعتداءات غير مباشرة عند التحايل على الآلية أو عند استعمال الآلية بشكل غير صحيح.

3.2.3 الشهادة: مجموعة من المعطيات المرتبطة بالأمن تصدرها سلطة أمنية أو طرف ثالث موثوق به فضلاً عن معلومات أمنية تستعمل لتوفير خدمات التكامل واستيقان أصل المعطيات للمعطيات [ITU-T X.810]. وفي هذه التوصية يشير هذا المصطلح إلى شهادات "المفتاح العمومي" التي تكون قيماً تمثل المفتاح العمومي للمالك (وغيرها من المعلومات الخيارية) وقد تحققت بشأنها سلطة موثوق بها ووقعت عليها بشكل نسق لا يمكن تزويره.

4.2.3 الشفرة: خوارزمية تجفير أو متحولة رياضية.

5.2.3 السرية: الخاصية التي تمنع الكشف عن المعلومات إلى أفراد أو كيانات أو عمليات غير مرخص لها بذلك.

6.2.3 خوارزمية التجفير: وظيفة رياضية تحسب النتيجة استناداً إلى قيم دخل واحدة أو عدة.

7.2.3 EC-GDSA: توقيع رقمي لمنحنى إهليلجي مع تذييل تماثلي لخوارزمية التوقيع الرقمي (DSA) للمعهد الوطني للمعايير والتكنولوجيا (NIST)؛ انظر أيضاً الفقرة 6.6 من المرجع [ISO/IEC 14888-3].

8.2.3 نظام تجفيري لمنحنى إهليلجي: نظام تجفيري بمفتاح عمومي (انظر القسم 7.8 من المرجع [af-sec-0100.002]).

9.2.3 نظام توافق المفاتيح بالمنحنى الإهليلجي – ديفي–هيلمان: نظام توافق مفتاح ديفي–هليمان الذي يستعمل التجفير بمنحنى إهليلجي.

10.2.3 التجفير: العملية التي تجعل المعطيات غير مقروءة بالنسبة إلى كيانات غير مرخص لها وذلك عن طريق تطبيق خوارزمية تجفيرية (خوارزمية تجفير). وفك التجفير هو العملية المعاكسة التي تسمح بتحويل نص مجفّر إلى نص مقروء.

11.2.3 التكامل: خاصية المعطيات التي لم تعدل بشكل غير مسموح به.

12.2.3 تدفق الوسائط: التدفقات السمعية أو الفيديوية أو المعطياتية أو مركب من أي منها. وينقل تدفق الوسائط معطيات المستعمل أو التطبيق (الحمولة النافعة) ولكن لا ينقل معطيات تحكم.

13.2.3 عدم النكران: الحماية من نكران أحد الكيانات المشاركة في اتصال ما بأنه شارك في الاتصال بكامله أو في جزء منه.

14.2.3 الخصوصية: وهي أسلوب اتصال تستطيع بموجبه الأطراف المسموح لها وحدها بشكل صريح أن تفسر الاتصال. ويجري ذلك عادةً عن طريق التجفير وتقاسم المفتاح (المفاتيح) للنفاذ إلى الشفرة.

15.2.3 القناة الخاصة: القناة الخاصة ضمن سياق هذه التوصية قناة تنتج عن مفاوضات سابقة تجريها قناة آمنة يمكن استعمالها لمعالجة تدفقات الوسائط.

16.2.3 تجفير المفتاح العمومي: وهو نظام تجفير يستعمل مفاتيح لا تناظرية (للتجفير وفك التجفير) ذات علاقة رياضية بعضها مع بعض لا يمكن حسابها بشكل منطقي.

17.2.3 مواصفة للأمن: مجموعة (فرعية) متجانسة من الإجراءات والخصائص المتلائمة فيما بينها والتي تنص عليها التوصية [ITU-T H.235]، وهي مفيدة جداً للحفاظ على أمن الاتصالات متعددة الوسائط ITU-T H.323 بين الكيانات المعنية في سيناريو معين.

18.2.3 الإغراق: اعتداء يهدف إلى جعل نظام في حالة رفض الخدمة وذلك بإغراقه بعدد كبير من المعطيات غير المسموحة. وهناك حالة خاصة هي إغراق وسيط بإرسال رزم RTP إلى موانئ UDP. وفي هذه الحالات يتم إغراق النظام بالرزم التي تستهلك معالجتها موارد النظام الثمينة.

4 الاختصارات والمختصرات

تستعمل هذه التوصية الاختصارات والمختصرات التالية:

3DES معيار التوقيع الرقمي مضاعف ثلاث مرات *(Triple Date Encryption Standard algorithm)*

AES خوارزمية معيارية للتجفير المتقدم *(Advanced Encryption Standard algorithm)*

ALG بوابة طبقة التطبيق *(Application Layer Gateway)*

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

BES خدمة مخصصة *(Back-End Server)*

CA سلطة إصدار الشهادة *(Certificate Authority)*

CBC سلسلة فدر التجفير *(Cipher Block Chaining)*

CFB أسلوب التجفير بالتغذية الراجعة *(Cipher Feedback)*

CRL قائمة بالشهادات الملغاة *(Certificate Revocation List)*

DES معيار تجفير المعطيات *(Data Encryption Standard)*

DH ديفي-هيلمان *(Diffie-Hellman)*

DNS نظام تسمية المجال *(Domain Name System)*

DSS معيار التوقيع الرقمي *(Digital Signature Standard)*

DTMF تردد متعدد بنغمة مزدوجة *(Dual Tone Multi-Frequency)*

ECB أسلوب كتاب الشفرة الإلكتروني *(Electronic Code Book)*

ECC / EC نظام تجفير بمنحنى إهليلجي *(Elliptic Curve Cryptosystem)*

EC-GDSA توقيع رقمي بمنحنى إهليلجي مع تذييل مماثل بخوارزمية التوقيع الرقمي NIST (DSA)
(Elliptic Curve digital signature with appendix analogue of the NIST Digital Signature Algorithm)

ECKAS-DH نظام توافق المفاتيح بالمنحنى الإهليلجي – ديفي – هيلمان
(Elliptic Curve Key Agreement Scheme – Diffie-Hellman)

EOFB أسلوب OFB المحسّن *(Enhanced OFB mode)*

EP نقطة طرفية *(End Point)*

GK حارس بوابي *(Gatekeeper)*

GW بوابة *(Gateway)*

ICV قيمة التحقق من التكامل *(Integrity Check Value)*

ID معرف هوية *(Identifier)*

IPsec أمن بروتوكول الإنترنت *(Internet Protocol security)*

ISAKMP بروتوكول إدارة مفاتيح أمن الإنترنت *(Internet Security Association Key Management Protocol)*

IV متجه التدميث *(Initialization Vector)*

LDAP البروتوكول السريع للنفاذ إلى الدليل *(Lightweight Directory Access Protocol)*

MAC شفرة استيقان الرسالة *(Message Authentication Code)*

MC المتحكم في البث المتعدد *(Multipoint Controller)*

MCU وحدة التحكم متعددة النقاط *(Multipoint Control Unit)*

MPS تدفق الحمولة النافعة متعددة الوسائط *(Multiple Payload Stream)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

OCSP بروتوكول الوضع القانوني للشهادة على الخط *(Online Certificate Status Protocol)*

OFB أسلوب الخرج بالتغذية الراجعة *(Output Feedback Mode)*

OID معرف هوية غرض *(Object Identifier)*

PDU وحدة معطيات بروتوكولية *(Protocol Data Unit)*

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

POTS الخدمة الهاتفية التقليدية *(Plain Old Telephone Service)*

PRF وظيفة شبه عشوائية *(Pseudo-Random Function)*

Q&A سؤال وجواب *(Question and Answer)*

QoS نوعية الخدمة *(Quality of Service)*

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

RSA خوارزمية ريفست وشامير وأدلمان بالمفتاح العمومي
(Rivest, Shamir and Adleman (public-key algorithm))

RTCP بروتوكول التحكم في النقل بالوقت الفعلي *(Real-time Transport Control Protocol)*

RTP بروتوكول النقل بالوقت الفعلي *(Real-time Transport Protocol)*

SA اقتران أمني *(Security Association)*

SASET نمط طرفي سمعي بسيط أمين *(Secure Audio Simple End-point Type)*

SDU وحدة معطيات الخدمة *(Service Data Unit)*

SHA1 خوارزمية تظليل أمين رقم 1 *(Secure Hash Algorithm 1)*

SRTP بروتوكول نقل أمين بالوقت الفعلي *(Secure Real-Time Transport Protocol)*

SSL طبقة موصلة أمينة *(Secure Socket Layer)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TSAP نقطة نفاذ إلى خدمة النقل *(Transport Service Access Point)*

TTP طرف ثالث موثوق به *(Trusted Third Party)*

UDP بروتوكول بيانات المستعمل *(User Datagram Protocol)*

XOR, ○ أو حصراً *(Exclusive OR)*

X || Y سَلسَلة X و Y *(Concatenation of X and Y)*

5 المصطلحات

تستعمل هذه التوصية المصطلحات التالية:

- "**shall**" تشير إلى طلب إلزامي.
- "**should**" تشير إلى عمل مقترح ولكنه خياري.
- "**may**" تشير إلى عمل خياري وليس توصية بإجراء عمل ما.

تشير الفقرات والفقرات الفرعية والملحقات والتذييلات إلى تلك التي تتضمنها هذه التوصية إلا إذا ذكرت توصية أخرى صراحة. فتشير "4.1" مثلاً إلى الفقرة الفرعية 4.1 من هذه التوصية و"H.245/4.6" إلى الفقرة الفرعية 4.6 من التوصية [ITU-T H.245].

وتصف هذه التوصية استعمال أنماط رسالة مختلفة عدد "n": ITU-T H.245 وRAS وITU-T Q.931، إلخ. وللتمييز بين أنماط الرسالة المختلفة يجب اتباع الاصطلاح التالي. وتتألف الرسالة ITU-T H.245 وأسماء المعلمات من كلمات متسلسلة متعددة يجري التشديد عليها بكتابتها بالحرف الطباعي البارز (**maximumDelayJitter** ارتعاش المهلة القصوى). وتختصر ثلاثة أحرف **(ARQ)** أسماء الرسالة RAS. وتتألف أسماء الرسالة ITU-T Q.931 من كلمة أو كلمتين مع كتابة الحروف الأولى بالأحرف الاستهلالية (**Call Proceeding**).

وتستعمل هذه التوصية فكرة تقضي بوضع بنية معطيات ASN.1 مركبة عند NULL، على سبيل المثال "**ParamS** يحدد عند NULL" (راجع الفقرات 7 [ITU-T H.235.1] و8 [ITU-T H.235.1] و1.9 [ITU-T H.235.1] و2.9 [ITU-T H.235.1] و7 [ITU-T H.235.2] و9 [ITU-T H.235.2] و1.15 [ITU-T H.235.2] و2.15 [ITU-T H.235.2]). وهو ما يعني أن كل العناصر الاختيارية في التتابع المعني (أي **Params**) غير موجودة.

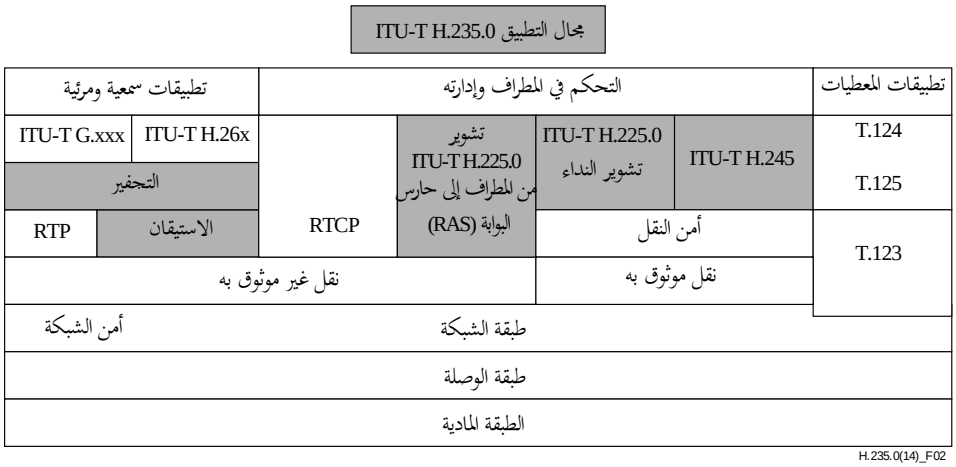
وتعرّف هذه التوصية عدة معرفات أغراض (OID) مختلفة للدلالة على مقدرات الأمن وإجراءات أو خوارزميات الأمن. وتتعلق هذه المعرفات بشجرة تراتبية من قيم مخصصة قد تتأتى من مصادر خارجية أو تشكل جزءاً من تفرع معرفات أغراض يديرها قطاع تقييس الاتصالات. وتتميز معرفات هويات الأغراض التابعة بالتوصية [ITU-T H.235] بالخصائص التالية:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**} حيث **V** ترمز إلى رقم عشري بسيط يحدد الطبعة المستخدمة من التوصية [ITU-T H.235]؛ مثال 1 أو 2 أو 3 أو 4. وترمز **N** إلى عدد يعرف بشكل لا لبس فيه حالة معرف هوية الغرض وبالتالي الإجراء المصاحب لخوارزمية الأمن أو مقدرة الأمن.

وبناءً عليه يتكوَّن معرف الغرض المشفر بالترميز ASN.1 من تتابع أرقام. وللتبسيط يستخدم كل معرف OID نص تذكيري مكثف في النص، مثال: "OID". وتعطى جداول تبين التقابل بين كل سلسلة OID وتتابع الأرقام ASN.1. وينبغي ألا تستعمل تطبيقات التوصيات [ITU-T H.235] إلا الأرقام المشفرة بالترميز ASN.1.

6 مدخل إلى النظام

يعطي الشكل 2 لمحة عامة عن مجال تطبيق هذه التوصية في إطار التوصية [ITU-T H.323].



الشكل 2 – لمحة عامة

بالنسبة إلى التوصية [ITU-T H.323]، ينبغي إجراء تشوير استعمال البروتوكول TLS ([IETF RFC 2246]، [IETF RFC 3546])، IPsec أو آلية خاصة على قناة التحكم ITU-T H.245 على القناة ITU-T H.225.0 المؤمنة وغير المؤمنة خلال التبادل الأولي للرسائل ITU-T Q.931.

1.6 الملخص

1) من الممكن تأمين قناة تشوير النداء باستعمال البروتوكول TLS ([IETF RFC 2246]، [IETF RFC 3546]) أو IPsec ([IETF RFC 2401]، [b-IETF RFC 2409]) في نفاذ معروف وآمن (التوصية [ITU-T H.225.0]).

2) يمكن استيقان المستعملين إما خلال توصيل النداء الأولي وإما خلال إجراء أمن القناة ITU-T H.245 و/أو عن طريق تبادل الشهادات على القناة ITU-T H.245.

3) تحدد تمديدات آلية التفاوض بشأن المقدرة الموجودة مقدرات تجفير القناة الوسيطة.

4) يجري التوزيع الأولي لمواد أساسية في الكيان الرئيسي من خلال رسائل **OpenLogicalChannel** أو **OpenLogicalChannelAck** للتوصية ITU-T H.245.

5) من الممكن تحقيق إعادة تعريف المفاتيح بواسطة أوامر التوصية ITU-T H.245: **EncryptionUpdateCommand** و**EncryptionUpdateRequest** و**EncryptionUpdate** و**EncryptionUpdateAck**.

6) تجري حماية توزيع المعطيات المتصلة بالمفتاح إما عن طريق تشغيل قناة التوصية ITU-T H.245 كقناة خاصة أو حماية المعطيات المتصلة بالمفتاح بشكل محدد باستعمال الشهادات المختارة المتبادلة.

7) البروتوكولات الأمنية المقدمة تكون مطابقة للمعايير ISO المنشورة أو المعايير IETF المقترحة.

2.6 الاستيقان

تتحقق عملية الاستيقان من أن المستجيبين هم بالفعل من يدعون. ومن الممكن إجراء الاستيقان في إطار تبادل الشهادات ذات المفتاح العمومي. ومن الممكن أيضاً تحقيق الاستيقان عن طريق تبادل يستعمل سراً تتقاسمه الكيانات المعنية. ويتخذ الاستيقان شكل كلمة سر سكونية أو معلومات ما أخرى.

وتصف هذه التوصية بروتوكول تبادل الشهادات ولكنها لا تحدد المعايير التي يجري التحقق منها وقبولها بواسطتها. وبصورة عامة تمنح الشهادات بعض الضمانات للمحقق تثبت صورة مقدم الشهادة. ويهدف تبادل الشهادة إلى استيقان *مستعمل* النقطة الطرفية وليس مجرد النقطة الطرفية المادية. ويثبت بروتوكول الاستيقان أن المستجيبين يملكون المفاتيح الخاصة التي تقابل المفاتيح العامة التي تتضمنها الشهادات وذلك باستعمال الشهادات الرقمية. ويحمي هذا الاستيقان من اعتداءات الوسطاء ولكنه لا يثبت هوية المستجيبين بصورة أوتوماتية. ويقضي القيام بذلك اعتماد سياسة ما تتعلق بمحتوى الشهادات الأخرى. وتتضمن الشهادة عادة تعريف هوية مزود الخدمة مثلاً لشهادات الترخيص فضلاً عن شكل ما لهوية حساب المستعمل التي يصفها مزود الخدمة.

ولا يعطي إطار الاستيقان في هذه التوصية تحديدات حول مضمون الشهادات (أي أنه لا يحدد سياسة الشهادة) أكثر من تلك التي يقضي بها بروتوكول الاستيقان. غير أن التطبيق الذي يستعمل هذا الإطار قد يفرض شروطاً سياسية رفيعة المستوى مثل تقديم الشهادة إلى المستعمل للحصول على موافقته. ومن الممكن إما أتمتة السياسة الرفيعة المستوى هذه ضمن التطبيق وإما طلب التفاعل الإنساني.

وفيما يخص الاستيقان الذي لا يستعمل الشهادات الرقمية تقدم هذه التوصية التشوير لإكمال سيناريوهات الاختبار/الاستجابة. وتقضي طريقة الاستيقان هذه بالتنسيق المسبق بواسطة الكيانات المتصلة للحصول على سر مشترك. وزبون خدمة قائمة على اشتراك مثال على ذلك.

وكخيار ثالث، يمكن إكمال الاستيقان ضمن سياق بروتوكول أمني منفصل مثل الأمن TLS ([IETF RFC 2246]، [IETF RFC 3546]) أو IKE [b-IETF RFC 2409].

وبإمكان الكيانات النظيرة توفير الاستيقان الثنائي والأحادي الاتجاه على حد سواء. ومن الممكن أن يحصل هذا الاستيقان على بعض قنوات الاتصالات أو كلها.

جميع آليات الاستيقان المحددة التي يرد وصفها في هذه التوصية مماثلة للخوارزميات التي وصفتها المنظمة ISO وفقاً للتحديد الذي جاء في الفقرتين 2 و3 من [ISO/IEC 9798] أو على أساس البروتوكولات IETF.

1.2.6 الشهادات

يقع تقييس الشهادات بما في ذلك توليدها وإدارتها وتوزيعها خارج نطاق هذه التوصية. ويجب أن تكون الشهادات المستعملة لإقامة قنوات آمنة (تشوير النداء و/أو التحكم بالنداء) مطابقة لتلك التي يوصي بها أي بروتوكول جرى التفاوض بشأنه لتوفير أمن هذه القنوات.

وينبغي الإشارة إلى أن النقاط الطرفية ضرورية للاستيقان الذي يستعمل شهادات مفتاح عمومي بهدف توفير التوقيعات الرقمية باستعمال قيمة مفتاح خصوصي مصاحب. ولا يشكل تبادل شهادات المفتاح العمومي بمفرده حماية من اعتداءات الوسائط. وتكون بروتوكولات التوصية ITU-T H.235 مطابقة لهذا الشرط.

3.6 أمن إقامة النداء

ثمة سببان على الأقل لحفز تأمين قناة إقامة النداء (مثلاً التوصية [ITU-T H.323] باستعمال التوصية [ITU-T Q.931]). السبب الأول هو الاستيقان البسيط قبل قبول النداء، والثاني السماح بتخويل النداء. وإذا كانت هذه الوظيفية مرغوبة في مطراف السلسلة ITU-T H ينبغي استعمال أسلوب اتصالات آمن (مثل TLS/IPsec للتوصية [ITU-T H.323]) قبل تبادل رسائل توصيل النداء. وإلا من الممكن أيضاً توفير التخويل على أساس استيقان خاص بالخدمة. وتقع التقييدات على سياسة التخويل الخاص بالخدمة خارج نطاق هذه التوصية.

4.6 أمن التحكم بالنداء (ITU-T H.245)

ينبغي أيضاً تأمين قناة التحكم بالنداء [ITU-T H.245] بشكل ما لتأمين خصوصية الوسائط اللاحقة. ويجب تأمين القناة ITU-T H.245 باستعمال أية آلية خصوصية جرى التفاوض بشأنها (ويشمل هذا الخيار "لا شيء"). وتستعمل رسائل التوصية ITU-T H.245 للإشارة إلى خوارزميات التجفير ومفاتيح التجفير في القنوات الوسيطة المتقاسمة والخاصة. وتسمح إمكانية القيام بهذا على أساس كل قناة منطقية على حدة بتجفير القنوات الوسيطة المختلفة عن طريق الآليات المختلفة. فيمكن مثلاً استعمال المفاتيح العامة في مؤتمرات مركزية متعددة النقاط للتدفقات على كل نقطة طرفية. ومن الممكن أن يسمح ذلك بجعل التدفقات الوسيطة خاصة لكل نقطة طرفية في المؤتمر. وبهدف استعمال رسائل التوصية ITU-T H.245 بطريقة آمنة ينبغي فتح القناة ITU-T H.245 (قناة منطقية 0) بطريقة آمنة يمكن التفاوض بشأنها.

وتعتمد الآلية التي تؤمَّن بها قناة ITU-T H.245 على مطاريف السلسلة ITU-T H المعنية. ويكون الشرط الوحيد المفروض على جميع الأنظمة التي تستعمل هذه البنية الأمنية أن يكون لكل منها طريقة للتفاوض و/أو الإشارة إلى أنه يجب تشغيل القناة ITU-T H.245 بطريقة معينة آمنة قبل تدميثها بشكل فعلي. وتستعمل التوصية ITU-T H.323 مثلاً رسائل تشوير توصيل التوصية ITU-T H.225.0 لإنجاز ذلك.

5.6 خصوصية الاتصالات في تدفقات الوسائط

تصف هذه التوصية خصوصية الاتصالات في تدفقات الوسائط التي تنقل بأسلوب الرزم. ويجوز أن تكون هذه القنوات أحادية الاتجاه ضمن إطار تعريف القنوات المنطقية ITU-T H.245. ولا يفرض أن تكون القنوات أحادية الاتجاه عند طبقة النقل أو الطبقة المادية.

وينبغي أن تكون الخطوة الأولى لتحقيق خصوصية الاتصالات تزويد قناة تحكم خاصة تمكن إقامة معدات لتوليد مفاتيح إبراق تجفيرية و/أو قنوات منطقية تنقل التدفقات الوسيطة المجفرة. ولذلك عند العمل في مؤتمر آمن من الممكن أن تستعمل أية نقاط طرفية مشاركة قناة مجفرة ITU-T H.245. وبهذه الطريقة يمكن حماية انتقاء خوارزمية التجفير ومفاتيح التجفير المرسلة من خلال أمر **OpenLogicalChannel** ITU-T H.245.

من الممكن تشغيل القناة الآمنة ITU-T H.245 مع خصائص تختلف عن تلك التي تكون في القناة (القنوات) الوسيطة الخاصة طالما أنها توفر مستوى مقبول من السرية للطرفين. ويسمح هذا للآليات الأمنية التي تحمي التدفقات الوسيطة وجميع قنوات التحكم أن تعمل بطريقة مستقلة بشكل كامل مع توفير مستويات مختلفة من القوة والتعقيد.

وإذا ما طلب تشغيل القناة ITU-T H.245 بشكل غير مجفر يمكن تجفير مفاتيح التجفير الوسيطة المحددة بشكل منفصل بالطريقة التي أشارت إليها الأطراف المشاركة ووافقت عليها. ويمكن استعمال قناة منطقية من النمط **h235Control** لتوفير مواد لحماية مفاتيح التجفير الوسيطة. ومن الممكن تشغيل هذه القناة المنطقية بأي أسلوب جرى التفاوض بشأنه بشكل ملائم.

ويجب أن تتخذ خصوصية (تجفير) المعطيات التي تنقلها القنوات المنطقية الشكل الذي تحدده القناة **OpenLogicalChannel**. ويجب ألا تجفر معلومات الرأسية الخاصة بالنقل. ويجب أن تقوم خصوصية المعطيات على التجفير من طرف إلى طرف.

6.6 عناصر موثوقة

تعرّف مطاريف قناة الاتصالات قاعدة الاستيقان (الثقة) والخصوصية. وبالنسبة إلى قناة إجراء التوصيل فمن الممكن أن يكون هذا بين الطالب ومكونة الشبكة المستضيفة. "فيتوقع" الهاتف مثلاً أن بدالة الشبكة توصله مع المركز الذي طلب رقمه. ولهذا السبب يجب اعتبار أن كياناً ينهي قناة تحكم مجفرة ITU-T H.245 أو أية قنوات منطقية من نمط **encryptedData** يكون عنصراً موثوقاً من التوصيل. ومن الممكن أن يشمل هذا الوحدات MC(U) والبوابات. وتكون نتيجة الوثوق بعنصر ما هي الثقة في الكشف عن آلية الخصوصية (الخوارزمية والمفتاح) لذلك العنصر.

ونظراً إلى ما ورد أعلاه ينبغي على المشاركين في مسار الاتصالات استيقان العناصر "الموثوقة" كلها. ويجري ذلك عادة عن طريق تبادل الشهادات كما قد يحصل للاستيقان "المعياري" من طرف إلى طرف. ولا تقتضي هذه التوصية أي مستوى معين من الاستيقان باستثناء اقتراح أنه من المقبول أن تستعمل جميع الكيانات العنصر الموثوق. وينبغي إكمال دراسة التفاصيل حول نموذج موثوق وسياسة الشهادات.

ومن الممكن ضمان الخصوصية بين نقطتين طرفيتين إذا ثبت أن التوصيلات بين العناصر الموثوقة محمية من اعتداءات الداخلين على الخط.

1.6.6 إيداع المفتاح

تتضمن هذه التوصية أحكاماً للكيانات التي تستعمل بروتوكول التوصية ITU-T H.235 لتوفير مقدرة "طرف ثالث موثوق" (TTP) ضمن عناصر التشوير مع أن التشغيل لا يقتضي ذلك.

ينبغي توفير مقدرة استرداد مفاتيح التجفير للوسائط الضائعة في المنشآت عند الحاجة أو عند الرغبة.

وإيداع المفتاح وظيفة غالباً ما يشار إليها بالمصطلح الطرف الثالث الموثوق (TTP). وينبغي إكمال دراسة هذه الوظيفة.

7.6 عدم النكران

يتطلب هذا الموضوع مزيداً من الدراسة.

8.6 الأمن في بيئة متنقلة

يجوز تشغيل أنظمة ITU-T H.323 في بيئة متنقلة طبقاً للتوصية [ITU-T H.510]. ويرد وصف إجراءات الأمن وبروتوكولاته المطبقة على هذه الأنظمة في التوصية [ITU-T H.530] التي تعد للعمل بروتوكولات وإجراءات مستمدة من هذا التوصية.

9.6 مواصفات الأمن

تحيل هذه التوصية على عدد من مواصفات الأمن ITU-T H.235 (ITU-T H.235.1 وITU-T H.235.2 وITU-T H.235.3 وITU-T H.235.4 وITU-T H.235.5 وITU-T H.235.6 وITU-T H.235.7 وITU-T H.235.8 وITU-T H.235.9). وتحدد

كل مواصفة أمن استخداماً خاصاً للوظائف أو الوظائف الفرعية H.235 التي تستجيب لاحتياجات بيئات محددة وتطبيقات واضحة المعالم.

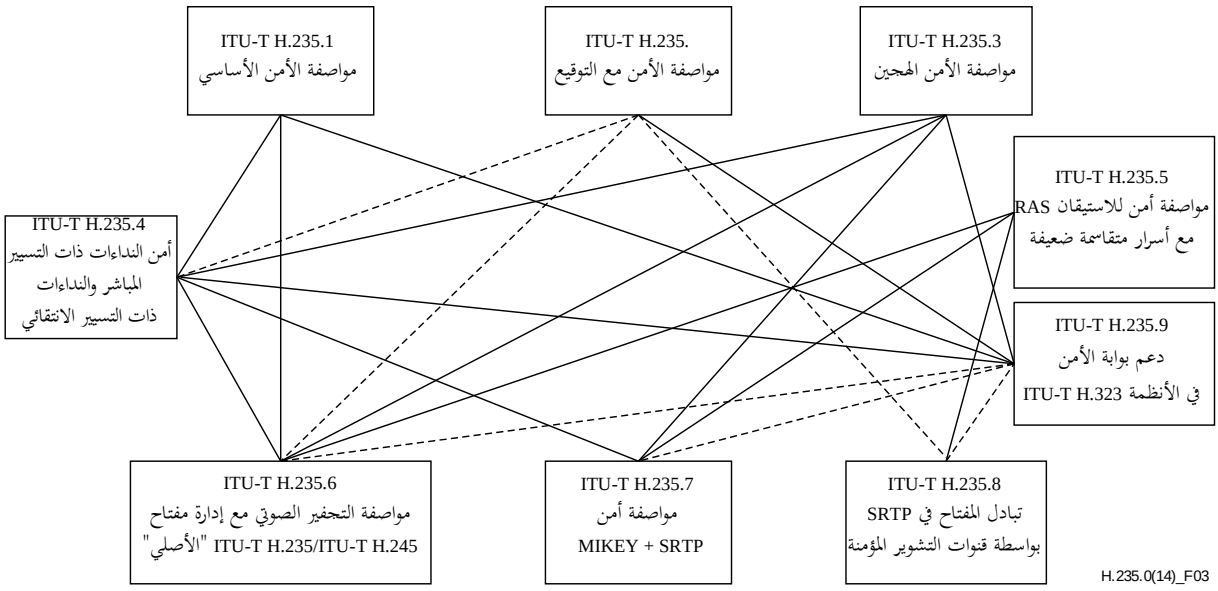
وتطبق مواصفات الأمن بكاملها أو بانتقاء أجزاء منها بحسب البيئة والتطبيق. ويشير عادة معرف هوية غرض رسائل التشوير في الأنظمة ITU-T H.235 إلى مواصفة الأمن المتبعة. ويتم اختيار مواصفة الأمن مبدئياً في هذه الأنظمة تبعاً للاحتياجات.

تستطيع النقاط الطرفية خيارياً أن تقترح عدة مواصفات أمن في الرسائل **RRQ/GRQ** وأن تترك للحارس البوابي أمر اختيار المواصفة الأكثر ملاءمة على أن يذكره في الاستجابة المتضمنة في الرسالة **RCF/GCF**. كما تستطيع العمليات **LRQ/LCF** التي تجري بين حراس البوابات أن تسيّر عدة مواصفات للأمن. وأثناء حساب التواقيع الرقمية أو قيم التظليل التي من شأنها ضمان تكامل الرسائل، ينبغي أولاً حساب قيم التظليل والتواقيع الرقمية التي لا تضمن تكامل الرسائل في المجموعات الفرعية للمجال وتدوينها في الرسالة، أما التواقيع الرقمية وقيم التظليل التي تضمن تكامل الرسائل فتتألف من "0" كاملة في الذاكرة الوسيطة للرسائل، ثم تحسب جميع التواقيع الرقمية وقيم التظليل باستعمال هذه الذاكرة الوسيطة وتوضع بعد ذلك في الرسالة.

وتحدد كل توصية من توصيات السلسلة الفرعية مواصفة أمن ITU-T H.235.0. وتتكون مواصفة الأمن عادة من استطباق من التوصية ITU-T H.235.0 خاص بأحد السيناريوهات و/أو يدرج مواصفة خصائص أمن خاصة أو مجموعة من آليات أمن/مواصفات أمنية.

كل مواصفات الأمن اختيارية في التوصية ITU-T H.235.0.

يوضح الشكل 3 بعض التركيبات النمطية والممكنة لمواصفات الأمن. ويشير الخط المستقيم إلى أن التركيب بين مواصفتين للأمن معرف وممكن. ويشير الخط المنقوط إلى أن التركيبة ممكنة عموماً ولكنها قد لا تكون مفيدة. ويدل عدم وجود خط إلى أن التركيبة لم تحدد بعد.



الشكل 3 – توضيح تركيبات مواصفات الأمن

10.6 عبور مؤمّن لتجهيزات NAT/جدار الحماية

تحدد التوصية [ITU-T H.235.9] إجراءات تسمح باكتشاف وجود بوابات أمن (مثل بوابات طبقة التطبيق (ALG)) في مسير التشوير ITU-T H.225.0 RAS بين كيانين ITU-T H.323 (حارس البوابة، نقطة طرفية) كما تسمح لحارس البوابة وبوابة الأمن بتبادل معلومات أمنية لحماية تكامل اتصالات معطيات التشوير وسريتها.

وتتيح التوصيات [ITU-T H.235.1] (الإجراء IA) و[ITU-T H.235.2] (إجراء استيقان فقط) إجراءات تكميلية محددة تسمح لاستيقان الرسائل القائم على أساس بروتوكولات ITU-T H.235 RAS وتشوير النداء ITU-T H.225.0 بعبور تجهيزات NAT/جدار الحماية.

7 عمليات إجراء التوصيل

كما أشير في فقرة المدخل إلى النظام، يجب أن تعمل قناة توصيل النداء (التوصية ITU-T H.225.0 للسلسلة ITU-T H.323) وقناة التحكم في النداء (التوصية ITU-T H.245) في الأسلوب الآمن أو غير الآمن الذي جرى التفاوض بشأنه خلال التبادل الأول للرسائل. وبالنسبة إلى قناة توصيل النداء فأسلوب الأمن محدد *بشكل مسبق* (بالنسبة إلى التوصية ITU-T H.323 يجب استعمال نقطة TSAP تؤمنها TLS (المنفذ 1300) للرسائل ITU-T Q.931). أما بالنسبة إلى قناة التحكم بالنداء فتحدد المعلومات التي تمر عبر بروتوكول إجراء التوصيل الأولي أسلوب الأمن المستعمل في مطراف السلسلة H.

وفي الحالات التي لا تكون فيها مقدرات أمنية متداخلة من الممكن أن يرفض المطراف المطلوب التوصيل. وينبغي ألا ينقل خطأ العودة أية معلومات حول عدم الملاءمة الأمنية ويكون على المطراف الطالب أن يحدد المشكلة بطريقة أخرى. وفي الحالات التي يستقبل فيها المطراف الطالب رسالة بدون مقدرات أمنية كافية ينبغي أن ينهي النداء.

إذا كان للمطاريف الطالبة والمطلوبة مقدرات أمنية ملائمة يجب أن يفترض الطرفان أنه يجب أن تعمل قناة التوصية ITU-T H.245 في الأسلوب الآمن الذي جرى التفاوض بشأنه. وينبغي أن يعتبر الفشل في إجراء قناة التوصية ITU-T H.245 في الأسلوب الآمن المحدد هنا خطأً بروتوكولياً وينبغي عند ذلك إنهاء التوصيل.

تصف التوصية [ITU-T H.235.6] إجراءات تكميلية لإنشاء توصيل الأمن بما في ذلك إدارة المفتاح (راجع الفقرة 7 و8 من التوصية [ITU-T H.235.6]).

8 تشوير الاستيقان وإجراءاته

يستند الاستيقان، عادة، إلى طريقة السر المتقاسم (تتيح معرفة هذا السر الاستيقان) أو إلى المفتاح العمومي مع شهادات (امتلاك مفتاح خاص هو إثبات هوية). ويتطلب السر المتقاسم والاستعمال الناتج عن ذلك للتجفير التناظري اتصالاً مسبقاً بين الكيانات التي تجري الاتصالات. ويجوز الاستعاضة عن اللقاء الشخصي المسبق أو الاتصال مع إجراءات الأمن بتبادل مفتاح المعلومات السري أو خلفه باستعمال طرائق التجفير بمفتاح عمومي كتبادل مفاتيح ديفي–هيلمان مثلاً. وفيما يتعلق بإنتاج المفتاح وتبادله ينبغي أن يتم الاستيقان من الأطراف المتواصلة، على سبيل المثال بواسطة الرسائل بتوقيع رقمي؛ وإذا تعذر ذلك، فإن الأطراف المتواصلة لا تعلم الجهة التي تتقاسم معها المعلومات السرية.

تقترح هذه التوصية طرائق استيقان على أساس الاشتراك الذي يشترط وجود اتصال مسبق من أجل تقاسم معلومة سرية، وطرائق استيقان تستعمل التجفير بالمفتاح العمومي مباشرة من أجل الاستيقان أو إنتاج سر متقاسم.

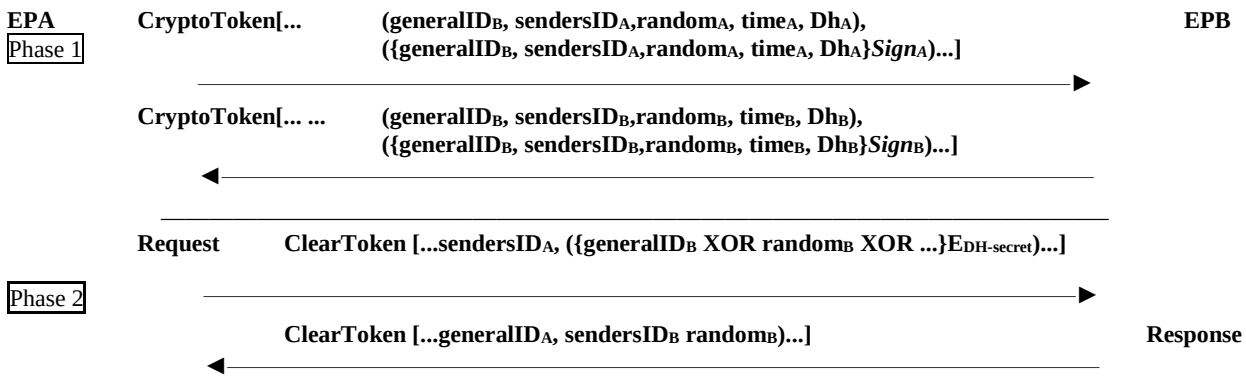
1.8 طريقة ديفي–هيلمان مع الاستيقان الخياري

لا تهدف هذه الطريقة إلى توفير استيقان مطلق على مستوى المستعمل. ولكنها توفر التشوير الكفيل بتوليد سر مشترك بين كيانين من الممكن أن يؤدي إلى معلومات حسابات المفاتيح للاتصالات الخاصة.

وفي نهاية هذا التبادل يكون للكيانين مفتاح سري مشترك فضلاً عن خوارزمية مختارة يمكن استعمال هذا المفتاح معها. ومن الممكن الآن استعمال هذا المفتاح السري المشترك في جميع تبادلات طلب/استجابة لاحقة. وينبغي الإشارة إلى أنه من الممكن أن يولد التبادل ديفي–هيلمان مفاتيح *ضعيفة* معروفة لخوارزميات معينة. وعندما يكون الأمر على هذا النحو ينبغي أن يفك كل كيان التوصيل أو يعيده لإقامة مجموعة مفتاح جديدة.

ويبين الطور الأول للشكل 4 المعطيات المتبادلة خلال الطريقة ديفي–هيلمان. ويسمح الطور الثاني باستيقان المستجيب لرسائل الطلب الخاصة بالتطبيق أو البروتوكول. وتجدر الملاحظة أنه يمكن إعادة قيمة عشوائية جديدة مع كل إجابة.

ملاحظة – في حال تبادل الرسائل في قناة غير أمنية، يجب استعمال التواقيع الرقمية (أو أي طريقة أخرى للاستيقان من المصدر) بهدف تعرف هوية الأطراف التي سيتم تقاسم المعلومة السرية بينها. كما يمكن أيضاً توفير عنصر توقيع خياري (المشار إليه أدناه ***بالأحرف المائلة***).



[... ...] تشير إلى تتابع من العلامات.

() تشير إلى علامة معينة قد تتضمن عناصر متعددة.

{}EDH-secret تشير إلى أن القيم الداخلية مجفرة باستعمال سر Diffie-Hellman.

EPB تعرف أي مفتاح سري مشترك ينبغي استعماله لفك تشفير معرف الهوية **generalIDB** عن طريق مقارنته مع **generalIDA** التي ينبغي نقلها أيضاً في الرسالة **sendersIDA**. تجدر الملاحظة أن القيمة المجفرة في الطور 2 تمر في حقل **generalID** في **clearToken** لتبسيط التشفير.

الشكل 4 – تبادل بأسلوب ديفي–هيلمان مع الاستيقان الخياري

2.8 استيقان قائم على الاشتراك

مع أن الإجراءات المعروضة هنا (وخوارزميات ISO التي تكون مشتقة منها) ثنائية الاتجاه في طبيعتها فإنه لا يمكن استعمالها إلا في اتجاه واحد إذا كان الاستيقان ضرورياً في ذلك الاتجاه فقط. وترد إجراءات المرور الثنائي والثلاثي. ويمكن إجراء الاستيقان المتبادل في ممرين في اتجاه واحد إذا لم يكن الاستيقان من رسائل الاتجاه المعاكس إلزامياً. وتفترض هذه التبادلات أن كل طرف يملك معرف هوية معروف (مثل معرف هوية النص) يتعرف عليه بشكل فريد من نوعه. وفي حالة الإجراء بممرين، يفترض، علاوةً على ذلك، وجود إشارة إلى الوقت يقبل بها الطرفان (تسمح بتحديد الطابعات الزمنية). وتكون فترة التخالف الزمني المقبولة مسألة تتعلق بالتطبيق المحلي. ويستخدم إجراء الممرات الثلاثة رقماً غير متوقع ينتج عشوائياً (ويمكن زيادة "بقيمة عشوائية" لعداد تتابعي) أي امتحان يقترحه المستيقن. ويخص هذا العدد العشوائي للحماية من الاعتداءات التكرارية. وعلى عكس إجراءات الممرين، لا تستيقن إجراءات الممرات الثلاثة من الرسالة الأولى (الأولية) التي تضم رقم امتحان المرسل.

هناك ثلاثة أنواع مختلفة يمكن تطبيقها وفقاً للشروط:

1) كلمة سر قائمة على التجفير التناظري؛

2) كلمة سر قائمة على التظليل؛

3) شهادة مع تواقيع.

في جميع الحالات تتضمن العلامة المعلومات وفقاً للوصف الذي يرد في الفقرات الفرعية التالية تبعاً للنوع المختار. ويلاحظ أنه يمكن معرفة **generalID** من خلال تفحص التشكيلة أو الدليل وليس من خلال تبادل البروتوكولات داخل النطاق. ومن أجل تسهيل عملية المعالجة جهة المرسل إليه ينبغي أن يدرج المرسل هويته في المعرّف **sendersID** ويضع المعرّف **generalID** على تعرف هوية المرسل.

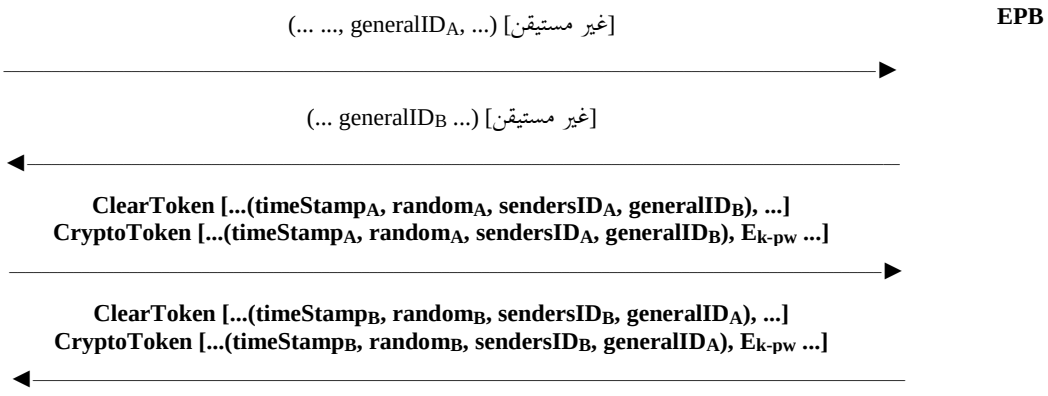
الملاحظة 1 – عند صنع طابعات التاريخ والساعة واعتمادها في إطار تبادل الأمن ينبغي أن يتخذ المصنع الاحتياطات التالية: ينبغي أن تكون درجة تحبيبة الطابعة دقيقة على نحو يضمن حصول الزيادة عند مرور كل رسالة جديدة. وفي غياب هذا الضمان تصبح الاعتداءات التكرارية ممكنة (مثال: في حال الطابعة لا تزيد إلا الدقائق يمكن لنقطة طرفية "C" محاولة إزعاج نقطة طرفية "A" أثناء الدقيقة التي تلي اللحظة التي ترسل فيها النقطة الطرفية "A" رسالة إلى النقطة الطرفية "B").

الملاحظة 2 – لا يمكن ضمان أمن الرسالة إذا تعدد إرسالها.

1.2.8 كلمة سر مع تشفير تناظري

يبين الشكلان 5 و6 نسق العلامة وتبادل الرسائل المطلوب لأداء هذا النمط من الاستيقان في ممرين وفي ثلاثة ممرات على التوالي. ويقوم هذا البروتوكول على الفقرة 1.2.5 (للممرين) والفقرة 2.2.5 (ثلاثة ممرات) من المعيار [ISO/IEC 9798-2]؛ ويفترض أنه يجري تبادل معرف الهوية وكلمة السر المصاحبة خلال الاشتراك. ويكون طول مفتاح التجفير عدد N من الأثمونات (كما تشير الخوارزمية AlgorithmID)، وتشكل كما يلي:

- إذا كان طول كلمة السر = N، مفتاح = كلمة السر؛
- إذا كان طول كلمة السر < N، المفتاح مليء بالأصفار؛
- إذا كان طول كلمة السر > N، توزع الأثمونات N الأولى على المفتاح وبعد ذلك يجمع M*th* + N أثمونة من كلمة السر إلى كلمة XOR'd أو حصراً مع Mmod(N)*th* أثمون (لجميع الأثمونات التي تكون بعد N) (أي يعاد طي جميع أثمونات كلمة السر "الإضافية" بشكل متكرر على المفتاح بواسطة الوظيفة XORing).



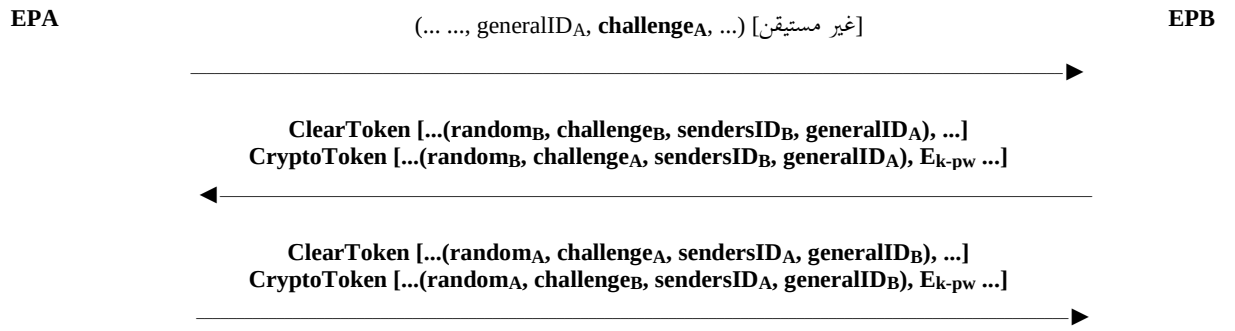
الملاحظة 1 – تكون علامة العودة من الطرف EPB خيارية وإذا أسقطت يجري إنجاز الاستيقان في اتجاه واحد.

الملاحظة 2 – يشير المتغير **E$_{k-pw}$** إلى القيم المجفرة باستعمال المفتاح "k" المشتق من كلمة السر "pw".

الملاحظة 3 – **random** هو عداد تدريجي وحيد الوتيرة يضفي طابع التفرد على الرسائل المتعددة باستعمال نفس طابعة الوقت والساعة.

الملاحظة 4 – تعطي النقطة EPA في الرسالة الثالثة علامة **ClearToken** مستقلة تعرف بواسطة نفس المعرف OID المستعمل في **CryptoToken**؛ وكذلك الأمر بالنسبة إلى الرسالة الرابعة وعكسها.

الشكل 5 – الاستيقان باستعمال كلمة سر بتجفير تناظري؛ ممرّان



الملاحظة 1 – الامتحان **challenge$_A$** والعلامة **CryptoToken** المجفرة والمرسلة في قناة الرجوع من B إلى A ليسا ضروريين في حالة الاستيقان باتجاه واحد.

الملاحظة 2 – يشير المتغير **E$_{k-pw}$** إلى وظيفة تجفير مجفرة بواسطة المفتاح "k" استناداً إلى كلمة السر "pw".

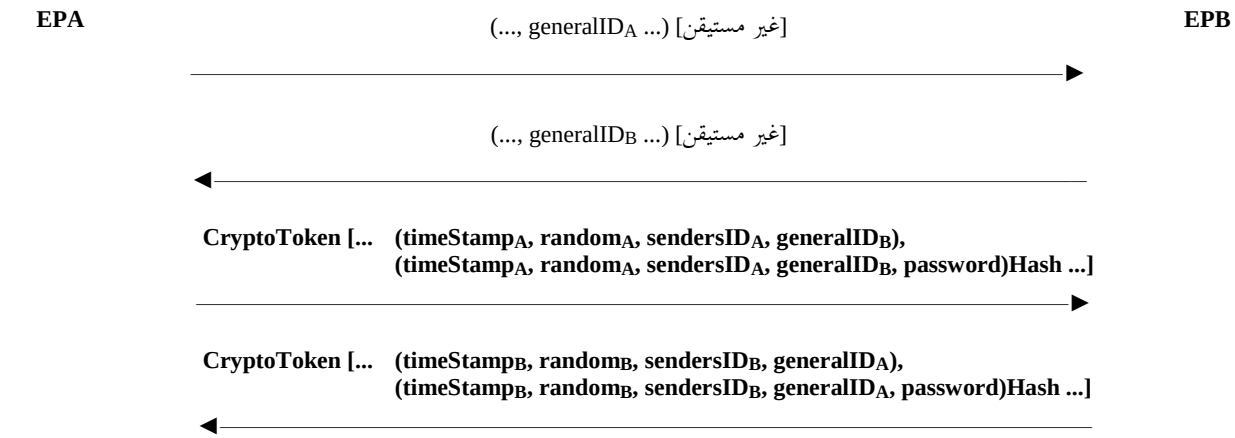
الملاحظة 3 – ترسل النقطة EPA في الرسالة الثالثة امتحاناً جديداً **challenge$_A$** واضحاً في علامة **ClearToken** مستقلة تعرف بواسطة نفس المعرف OID المستعمل في علامة **CryptoToken**. وترسل النقطة EPA أيضاً الامتحان **challenge$_B$** المجفر رداً على ذلك؛ وكذلك الأمر بالنسبة إلى الرسالة الثانية والعكس بالعكس.

الملاحظة 4 – في حال وجود عدة رسائل في الانتظار ينبغي أن يصبح الامتحان فريداً بواسطة الوظيفة **random** (أي العداد التدريجي وحيد الوتيرة).

الشكل 6 – الاستيقان باستعمال كلمة السر بتجفير تناظري؛ ثلاثة ممرات

2.2.8 كلمة السر مع التظليل

يبين الشكلان 7 و8 نسق العلامة وتبادل الرسائل المطلوب لإجراء هذا النوع من الاستيقان بممرين أو ثلاثة على التوالي. ويقوم هذا البروتوكول استناداً إلى الفقرتين 1.2.5 و2.2.5 من المعيار [ISO/IEC 9798-4]؛ ويفترض أن يجري تبادل معرف هوية وكلمة سر مصاحبة خلال الاشتراك. وتحتوي التوصية [ITU-T H.235.1] على وصف تفصيلي لإجراء التظليل بممرين.

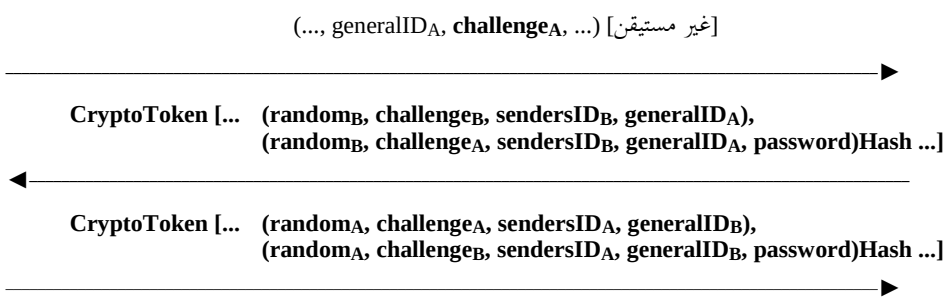


الملاحظة 1 – تكون علامة العودة من الطرف EPB خيارية وإذا أسقطت يجري إنجاز الاستيقان في اتجاه واحد.

الملاحظة 2 – يشير المتغير **Hash** إلى وظيفة التظليل التي تعمل على القيم الداخلية.

الملاحظة 3 – **random** هو عداد تدريجي وحيد الوتيرة يضفي الفرادة على الرسائل المتعددة باستعمال نفس طابعة الوقت والساعة.

الشكل 7 – استيقان باستعمال كلمة السر مع التظليل؛ ممران



الملاحظة 1 – تكون علامة العودة من الطرف EPB خيارية وإذا أسقطت يجري إنجاز الاستيقان في اتجاه واحد.

الملاحظة 2 – يشير المتغير **Hash** إلى وظيفة التظليل التي تعمل على القيم الداخلية.

الملاحظة 3 – ترسل النقطة EPA في الرسالة الثالثة امتحاناً جديداً **challenge$_A$** واضحاً في العلامة **ClearToken** المدرجة في **cryptoHashedToken**. ثم ترسل النقطة EPA امتحان **challenge$_B$** المظلل على سبيل الرد؛ وكذلك الأمر بالنسبة إلى الرسالة الثانية والعكس بالعكس.

الملاحظة 4 – في حال وجود عدة رسائل في الانتظار ينبغي أن يصبح الامتحان فريداً باستعمال **random** (عداد تدريجي وحيد الوتيرة).

الشكل 8 – كلمة السر مع التظليل؛ ثلاثة ممرات

الملاحظة 1 – تستعمل البنية cryptoHashedToken لنقل معلمات تستخدم في هذا التبادل. وتدرج في هذه البنية الصيغ "الواضحة" للمعلمات اللازمة لحساب القيمة المظللة. وينبغي أن يدخل المصنعون طابعة الوقت والساعة في المعلمات hashedVals *وعدم* إدراج كلمة السر (مثال، ينبغي أن يعرف المرسل إليه كلمة السر والمعرف 'generalID' *مسبقاً*؛ ويمكن إلغاء ما يقدمه).

الملاحظة 2 – ينبغي تطبيق وظيفة التظليل على البنية **EncodedGeneralToken** التي تضم المجالات ID وطابعة الوقت والساعة وكلمة السر كحد أدنى. وينبغي **عدم** تسيير قيمة كلمة السر في **ClearToken**.

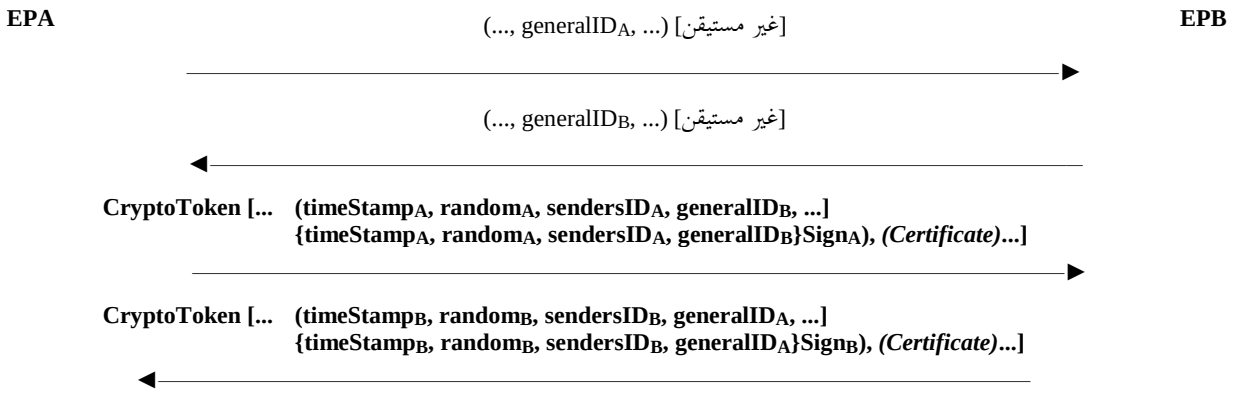
الملاحظة 3 – ينبغي أن يتأكد المصنعون من أن كلمات السر التي يدخلها المستعمل تشكل إنتروبيا كافية. فكلمات السر بالغة القصر أو شديدة الحساسية لاعتداءات المعاجم مرفوضة. وقد يكون من المفيد أحياناً تمرير كلمة السر جملة يدخلها المستعمل عبر وظيفة تظليل تجفيري ثم استعمال بتات الخروج.

3.2.8 استيقان بالشهادة مع تواقيع

يبين الشكلان 9 و10 نسق العلامة وتبادل الرسائل المطلوبة لإجراء هذا النوع من الاستيقان. ويقوم هذا البروتوكول على الفقرة 1.2.5 من المعيار [ISO/IEC 9798-3]؛ ويفترض أن يتم تبادل معرف الهوية والشهادة المصاحبة خلال الاشتراك. وتحتوي التوصية [ITU-T H.235.2] على وصف تفصيلي لإجراء التوقيع في ممرين.

الملاحظة 1 – يمكن أيضاً تزويد عنصر شهادة خياري الذي يبرز ***بالخط المائل*** أدناه.

الملاحظة 2 – في حال تعدد إرسال الرسالة ينبغي عدم إدراج معرّف هوية المقصد (**generalID$_B$** بالنسبة إلى الرسائل الواردة من A أو بالعكس) في العلامة **ClearToken**.



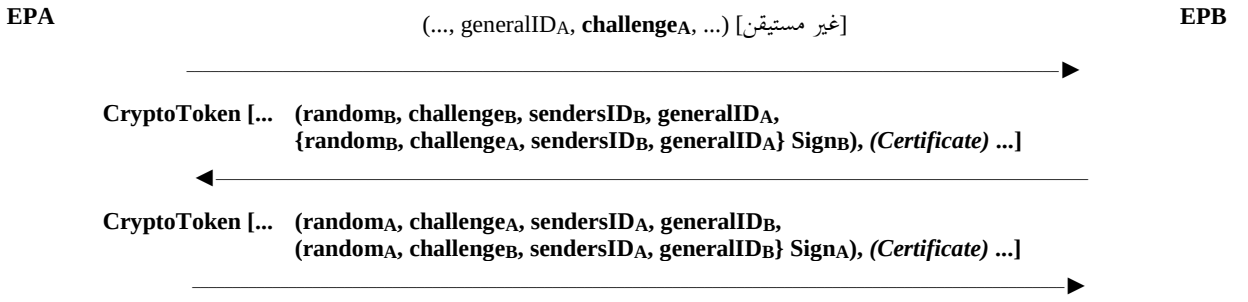
الملاحظة 1 – تكون علامة العودة من الطرف EPB خيارية وإذا أسقطت يجري إنجاز الاستيقان في اتجاه واحد.

الملاحظة 2 – من الممكن أن يختار المرسل الموجود في الطرف EPA إدراج شهادة من نوع "الدفع".

الملاحظة 3 – يشير المتغير **Sign** إلى وظيفة التوقيع (من الشهادة المصاحبة) التي تنفذ على القيم الداخلية.

الملاحظة 4 – **random** هو عداد تدريجي وحيد الوتيرة يضفي الفرادة على الرسائل المتعددة باستعمال نفس طابعة الوقت والساعة.

الشكل 9 – الاستيقان باستعمال شهادة بتوقيع؛ ممران



الملاحظة 1 – تكون علامة العودة من الطرف EPB خيارية وإذا أسقطت يجري إنجاز الاستيقان في اتجاه واحد.

الملاحظة 2 – يجوز للمرسل الموجود في النقطة EPA إدراج شهادة من نمط "الدفع" كإجراء خياري.

الملاحظة 3 – يشير المتغير **Sign** إلى وظيفة التوقيع (من الشهادة المصاحبة) التي تنفذ على القيم الداخلية.

الملاحظة 4 – ترسل النقطة EPA في الرسالة الثالثة امتحاناً جديداً **challenge$_A$** "واضحاً" مع العلامة **GeneralToken** المشفرة المدمجة. وترسل النقطة EPA أيضاً الامتحان **challenge$_B$** على سبيل الرد؛ وكذلك الأمر بالنسبة إلى الرسالة الثانية والعكس بالعكس.

الملاحظة 5 – **random** هو عداد تدريجي وحيد الوتيرة يضفي الفرادة على الرسائل المتعددة باستعمال نفس طابعة الوقت والساعة.

الشكل 10 – الاستيقان باستعمال شهادة بتوقيع؛ ثلاثة ممرات

4.2.8 استعمال السر المتقاسم وكلمات السر

تطبق في هذه التوصية بعض تقنيات التجفير التناظرية لأغراض الاستيقان والتكامل والسرية. ويستخدم هنا المصطلحان "كلمة السر" و"السر المتقاسم" مع التقنيات التناظرية. ويقصد بالمصطلح النوعي "السر المتقاسم" سلسلة بتات اعتباطية. ويمكن أن تخصص هذه السلسلة أو تشكيلها عند اشتراك المستعمل أو أن تشكل جزءاً من حساب الاستيقان من النمط ديفي–هيلمان مثلاً.

وقد تشبه كلمة السر سلسلة سمات هجائية رقمية يمكن للمستعملين حفظها. ومن البديهي أن استعمال كلمات السر يتطلب بعض الحذر. وحتى يتسنى توفير ضمانات أمن كافية، ينبغي اختيار كلمات السر بصفة عشوائية ضمن حيز شاسع، وينبغي لكلمات السر أن تكون لها أنتروبيا كافية بحيث لا يمكن الكشف عنها، وأخيراً ينبغي تغيير كلمات السر بانتظام. ولا تدخل قواعد خلق كلمات السر وتحديثها ضمن إطار هذه التوصية.

وهناك طريقة فعالة للإفادة من كلمات السر والأسرار المتقاسمة تكمن في تحويل سلسلة كلمة سر المستعمل إلى سلسلة بتات ثابتة تصبح بذلك سراً متقاسماً بواسطة وظيفة التظليل أحادي الجانب والمتين على صعيد التجفير.

وعلى سبيل المثال بالنسبة إلى مواصفة الأمن الوارد في التوصية [ITU-T H.235.1]، تنتج وظيفة التظليل SHA1 المطبقة على سلسلة كلمة السر سراً متقاسماً من 20 أثمونا. وتفيد عملية التظليل ليس بحجب كلمة السر بحد ذاتها وحسب بل في تحديد نسق سلسلة بتات بطول ثابت دون إلغاء الأنتروبيا فعلياً.

وبناءً عليه يكون:

السر المتقاسم = SHA1 (كلمة السر).

3.8 تشوير و إجراءات RAS للاستيقان

لا تنص هذه التوصية صراحة على أي شكل من سرية الرسالة بين الحارسات البوابية والنقاط الطرفية. وثمة نمطان من الاستيقان يمكن استعمالهما. يقوم النمط الأول على التجفير التناظري الذي لا يفرض اتصالاً سابقاً بين النقطة الطرفية والحارس البوابي. أما النمط الثاني فقائم على الاشتراك ويكون له شكلان: كلمة سر أو شهادة. وتشتق جميع هذه الأشكال من الإجراءات المبينة في الفقرات 8 و1.2.8 و2.2.8 و3.2.8. وفي هذه التوصية يمثل الوسمان (للنقطتين الطرفيتين EPA وEPB) في الفقرات الفرعية السابقة الذكر النقطة الطرفية والحارس البوابي على التوالي.

1.3.8 الاستيقان بين النقطة الطرفية والحارس البوابي (غير قائم على الاشتراك)

من الممكن أن توفر هذه الآلية للحارس البوابي وصلة تجفيرية تكون بموجبها النقطة الطرفية المعينة التي سجلت سابقاً هي الجهة التي تصدر رسائل RAS لاحقة. وتجدر الإشارة إلى أن هذه العملية قد لا توفر للنقطة الطرفية أي استيقان للحارس البوابي ما لم يدرج عنصر توقيع خياري. ويحصل إنشاء علاقة الهوية عندما يرسل المطراف الطلب **GRQ** وفقاً لما جاء في الفقرة 1.2.7 [ITU-T H.323]. ويجب أن يحصل تبادل ديفي–هيلمان مع الرسالتين **GRQ** و**GCF** كما هو مبين في المرحلة الأولى من الفقرة 8. ثم ينبغي استعمال هذا المفتاح السري المشترك من أجل كل طلب **PRQ/URQ** لاحق يرسله المطراف إلى الحارس البوابي. وإذا كان الحارس البوابي يعمل بهذا الأسلوب ويستقبل **GRQ** بدون علامة تتضمن *DHkey* أو *DHkeyExt* أو قيمة خوارزمية مقبولة يجب أن يعيد إرسال شفرة السبب **securityDential** أو أي شفرة خطأ في الأمن ملائمة أخرى في رسالة الرفض **DRJ** وفقاً لنص الفقرة 1.11.

من الممكن استعمال المفتاح السري المشترك المنتج بطريقة ديفي–هيلمان خلال التبادل **GRQ/GCF** لأغراض الاستيقان في رسائل **xRQ** لاحقة. ويجب استعمال الإجراءات التالية لاستكمال أسلوب الاستيقان هذا.

المطراف **(xRQ):**

1) يجب أن يوفر المطراف جميع المعلومات في الرسالة وفقاً للوصف الذي ورد في الفقرات ذات الصلة من التوصية [ITU-T H.225.0].

2) يجب أن يجفر المطراف المعرّف **GatekeeperIdentifier** (الذي أعيد في الرسالة **GCF**) باستعمال المفتاح السري المشترك الذي جرى التفاوض بشأنه. ويجب أن ينقل في علامة **clearToken** (انظر الفقرة 1.8) بكونه معرّف هوية عام **generalID**.

يجب أن تكون البتات الـ 16 من الرقم العشوائي **random** وبعد ذلك الرقم **requestSeqNum** مجمعة بواسطة XOR مع كل 16 بتة من المعرف **GatekeeperIdentifier**. وإذا لم ينته المعرّف **GatekeeperIdentifier** بحد زوجي في الموقع السادس عشر، يجب أن تكون البتات الثمانية الأخيرة للمعرّف **GatekeeperIdentifier** مجمعة بالعامل XOR مع أقل الأثمونات دلالة من القيمة العشوائية وبعد ذلك مع الرقم **requestSeqNum**. ويجب تجفير المعرّف **GatekeeperIdentifier** باستعمال الخوارزمية التي انتقيت في الرسالة (algorithmOID) **GCF** وباستعمال السر المشترك بكامله.

وتعطي الأمثلة التالية لمحة عامة عن هذا الإجراء:

RND16: قيمة تحوي 16 بتة من القيمة العشوائية

SQN16: قيمة تحوي 16 بتة من الرقم requestSeqNum

BMPX: السمة BMP العاشرة من المعرف GatekeeperIdentifier

(BMP1) XOR (RND16) XOR (SQN16) = BMP1'

(BMP2) XOR (RND16) XOR (SQN16) = BMP2'

(BMP3) XOR (RND16) XOR (SQN16) = BMP3'

(BMP4) XOR (RND16) XOR (SQN16) = BMP4'

(BMP5) XOR (RND16) XOR (SQN16) = BMP5'

:

:

(BMPn) XOR (RND16) XOR (SQN16) = BMPn'

بهدف ربط هذه الرسالة والرسائل اللاحقة بشكل تجفيري مع الكيان المسجل الأصلي في البداية (النقطة الطرفية التي أصدرت الطلب **RRQ**) يجب استعمال أحدث قيمة عشوائية **random** أعيدت (من الممكن أن تكون هذه القيمة أحدث من القيمة التي أعيدت في الرسالة **RCF** التي تلي رسالة لاحقة **xCF**).

الحارس البوابي (**xRJ/xCF**):

1) يجب أن يحفر الحارس البوابي معرّفه **GatekeeperIdentifier** (وفقاً للإجراء الذي يرد وصفه أعلاه) باستعمال مفتاح السر المشترك المصاحب لاسم النقطة الطرفية؛ ويقارنه مع القيمة الموجودة في الطلب **xRQ**.

2) يجب أن يعيد الحارس البوابي رسالة الرفض **xRJ** إذا لم تتوافق القيمتان المجفرتان.

3) إذا كان المعرّف **GatekeeperIdentifier** ملائماً يجب أن يطبق الحارس البوابي أي منطق محلي متوفر وأن يجيب بواسطة **xCF** أو **xRJ**.

4) إذا أرسل الحارس البوابي رسالة **xCF** ينبغي أن تتضمن المعرّف **EndpointIdentifier** الموزع وقيمة عشوائية جديدة في المجال **random** من المعلمة **clearToken**.

راجع الطور الثاني من الشكل 4 للاطلاع على تمثيل بياني لهذا التبادل. ويعرف الحارس البوابي المفتاح السري المشترك الواجب استعماله لتجفير معرّف هوية الحارس البوابي المشار إليه بواسطة الاسم المستعار في الرسالة.

2.3.8 الاستيقان بين النقطة الطرفية والحارس البوابي (القائم على الاشتراك)

ينبغي أن تتضمن جميع الرسائل RAS غير **GRQ/GCF** فيش الاستيقان التي يتطلبها أسلوب التشغيل الخاص. وثمة ثلاث صيغ مختلفة يمكن تطبيقها وفقاً للشروط والبيئة:

1) استيقان قائم على كلمة السر بالتجفير التناظري

2) استيقان قائم على كلمة السر مع التظليل

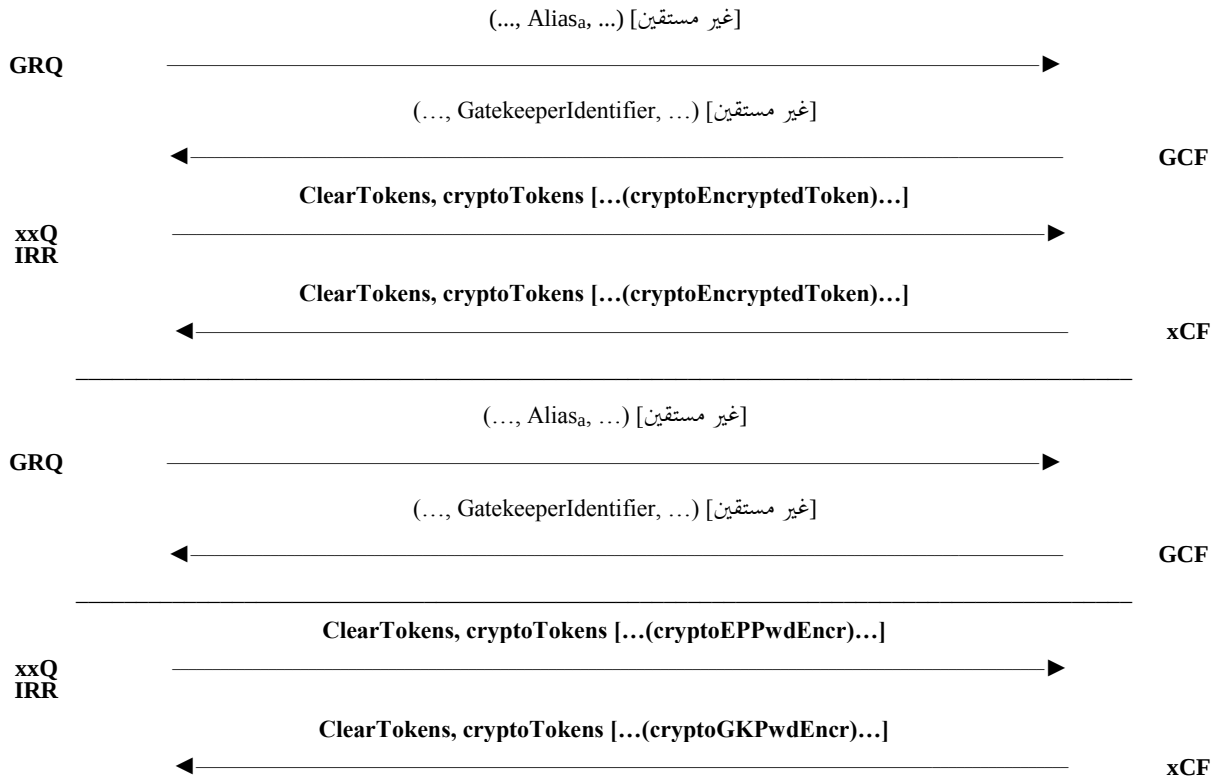
3) استيقان قائم على الشهادة مع التواقيع.

وفي جميع الحالات تتضمن العلامة المعلومات وفقاً للوصف الذي ورد في الفقرات الفرعية التالية ويتوقف هذا على الصيغة المختارة. وإذا كان الحارس البوابي بأسلوب آمن ويستقبل رسالة RAS بدون قيمة مقبولة للعلامة يجب أن يعيد إرسال شفرة

السبب **securityDenial** أو أي شفرة ملائمة أخرى تتعلق بخطأ الأمن طبقاً للفقرة 1.11 في رسالة الرفض. وفي جميع الحالات تكون العلامة التي يعيد الحارس البوابي إرسالها خيارية؛ وإذا أسقطت يمكن إنجاز الاستيقان في اتجاه واحد فقط.

1.2.3.8 كلمة السر بالتجفير التناظري

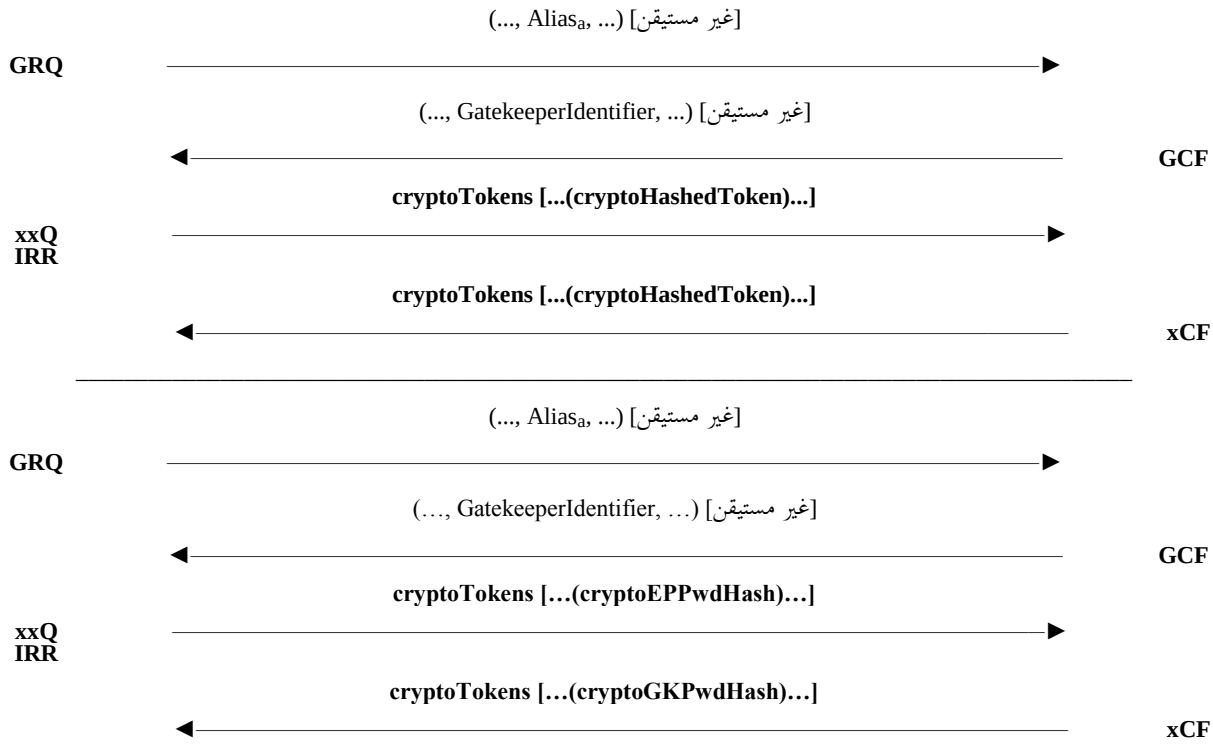
قد تفشل مرحلة الكشف التي يقوم بها الحارس البوابي (**GRQ** و**GCF** و**GRJ**) كما هو مبين في الشكل 11 أو قد تنجح باستعمال المعلمة **cryptoTokens**.



الشكل 11 – كلمة السر بالتجفير التناظري

2.2.3.8 كلمة السر مع التظليل

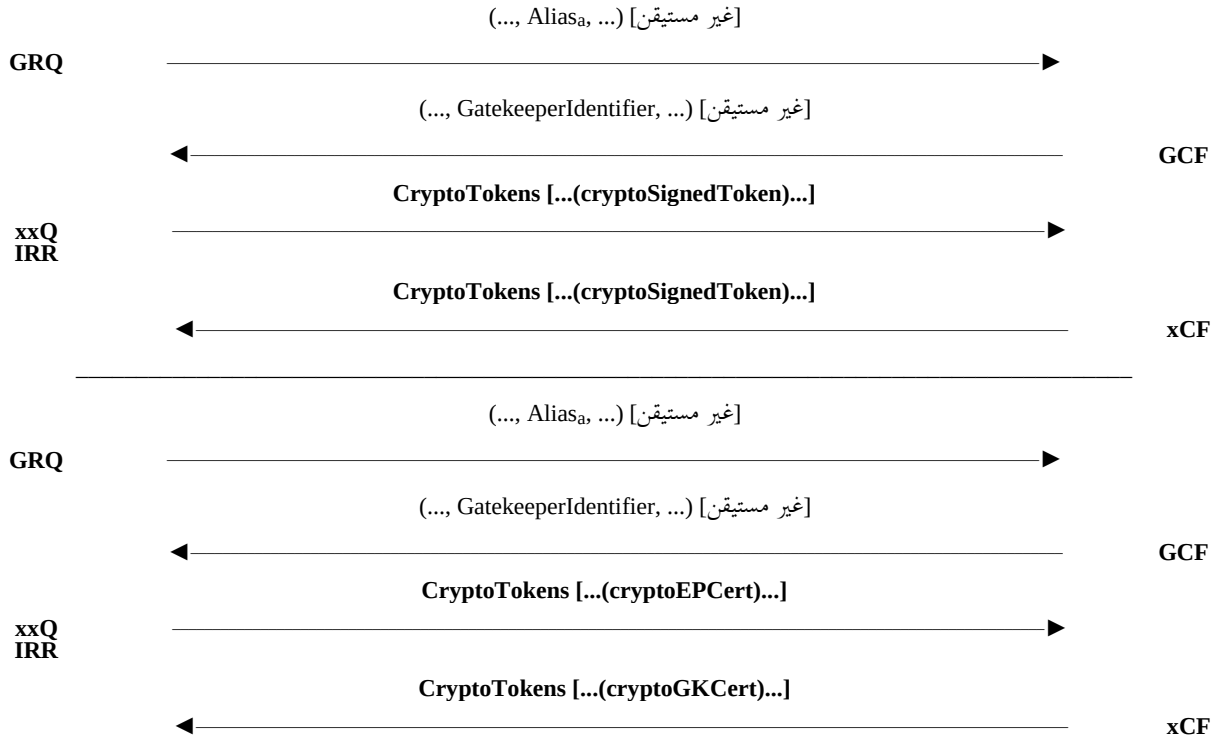
قد تفشل مرحلة الكشف التي يقوم بها الحارس البوابي (**GRQ** و**GCF** و**GRJ**) كما هو مبين في الشكل 12 أو على العكس قد تنجح هذه المرحلة باستعمال المعلمة **cryptoTokens** طبقاً للتوصية [ITU-T H.235.1].



الشكل 12 – كلمة السر مع التظليل

3.2.3.8 الاستيقان باستعمال الشهادة مع التواقيع

قد تفشل مرحلة الكشف التي يقوم بها الحارس البوابي (**GRQ** و**GCF** و**GRJ**) كما هو مبين في الشكل 13 أو على العكس قد تنجح باستعمال المعلمة **cryptoTokens** وفقاً للتوصية [ITU-T H.235.2].



الشكل 13 – الاستيقان باستعمال الشهادة مع التواقيع

4.8 إدارة المفاتيح في القناة RAS

يستحسن في بعض الحالات أن يوزع الحارس البوابي مفاتيح الدورة (RAS) على نقطة أو نقاط طرفية تابعة له، أو أن يتم توزيعها من نقطة طرفية إلى أخرى. وتفترض الآلية المقترحة أن الحارس البوابي والنقطة الطرفية يتقاسمان مفتاحاً سرياً موثوقاً أو أن كلاً منهما يعرف المفتاح العمومي الذي يمتلكه الآخر. وعلى سبيل المثال يمكن ذكر حالة حارس التسيير الذي يرسل مفتاح دورة إلى نقطة طرفية في رسالة RAS كالرسالة **RCF** أو **ACF** الواجب استعمالها في تجفير قناة تشوير يسيرها الحارس البوابي. مثال آخر هو حالة الحارس البوابي الذي يرسل مفتاح دورة ينبغي استعماله في تجفير الاتصالات RAS المتتالية (مثل **RRQ** أو **ARQ**).

وهذه الآلية مماثلة لتلك المستعملة في توزيع مفاتيح دورة الوسائط. ويمكن اللجوء إليها من أجل تفادي إجراء التفاوض بشأن المفتاح في بعض الحالات.

من أجل تسيير المفاتيح ينبغي استعمال المجال الخياري **h235Key** في **ClearToken** في الطبعة ITU-T H.235v3. وتتيح المرونة التي يقدمها العنصر **H235Key** تسيير عناصر مفتاح التجفير باستعمال:

- قناة أمنية (الخيار **secureChannel**) بافتراض أن قناة الاتصالات RAS أو قناة التشوير أمينتان بوسائل أخرى (SSL/IPsec، إلخ)؛
- سر تجفير مشترك في قناة واضحة (الخيار **sharedSecret**) وقد يكون الخيار **secureSharedSecret** أفضل؛
- تجفير وشهادة مفتاح عمومي في قناة واضحة (الخيار **certProtectedKey**).

استعمال مفاتيح دورة RAS متبادلة وتطبيقها على الاتصالات RAS ورسائل تشوير النداء و/أو قنوات النقل مواضيع تتطلب مزيداً من الدراسة.

9 الاستيقان اللا تناظري وتبادل المفاتيح بواسطة أنظمة التجفير بالمنحنى الإهليلجي

تقدم هذه التوصية تقنيات متطورة بالمنحنى الإهليلجي تطبق على التوقيع وإدارة المفاتيح والتجفير. وفيما يلي بعض المزايا الرئيسية بالنسبة إلى التقنيات اللاتناظرية "التقليدية" بالخوارزمية RSA:

- مفاتيح تجفير أقصر تضمن أمناً مماثلاً للأمن الذي تقدمه الخوارزمية RSA: عموماً يكون طول مفاتيح الأنظمة بالمنحنى الإهليلجي 160 بتة وهو مقدار مكافئ على صعيد الأمن لمفتاح RSA ذي 1024 بتة، ويستهلك المفتاح الأقصر قدراً أقل من ذاكرة التخزين ويجعل استعمال أنظمة التجفير بالمنحنى الإهليلجي مفيدة جداً في البطاقات المحوسبة وغيرها من الأجهزة القليلة الاستهلاك للذاكرة. وفي السياق ITU-T H.323 تكون النقاط الطرفية البسيطة الصوتية الأمنية (SASET) هي من النمط J/H.323 قليلة التكلفة وتتماشى كثيراً مع انتشار التقنيات بالمنحنى الإهليلجي؛
- السرعة الكبيرة في المعالجة على صعيد البرمجيات والمعدات على حد سواء: إذ إن المفاتيح الأقصر تزيد من سرعة المعالجة مما يسفر عن استجابة تفاعلية (للمستعمل) أسرع.

وترد جميع المعلومات العامة والشروحات وإجراءات معالجة التجفير الإهليلجي في القسم 7.8 من المرجع [af-sec-0100.002]. ويستحسن تشفير النقاط الإهليلجية في ترميزها الخاص غير المنضغط بدون طريقة نقطة الانضغاط وإزالة الانضغاط. وترد معلومات أخرى عن هذا الموضوع في المعيارين [ISO/IEC 15946-1] و[ISO/IEC 14888-3].

1.9 إدارة المفاتيح

أنظمة توافق مفاتيح النمط ديفي–هيلمان الإهليلجية مماثلة للحالة التقليدية mod-p التي يرد تعريفها في هذه التوصية. وهناك حالتان:

- منحنيات إهليلجية في مجال رئيسي: يحتوي المجال **eckasdhp** على المنحنى الإهليلجي والمعلمات ديفي–هيلمان؛
- منحنيات إهليلجية من الصنف 2: يحتوي المجال **eckasdh2** على المنحنى الإهليلجي والمعلمات ديفي–هيلمان.

وتوجد البنية ECKASDH في الحالتين. وترد بعض الأمثلة على المنحنيات الإهليلجية في المعيار [ISO/IEC 15946-1]. ويجوز استعمال أي منحنٍ إهليلجي آخر مناسب.

وبسبب البنية المنظمة التي توفرها العلامة **ClearToken** ينبغي ألا يحصل تشوير **dhkey** و**eckasdhkey** في نفس الوقت؛ ويتطلب تطبيق تبادل المفاتيح ديفي–هيلمان وجود واحد منهما فقط.

ملاحظة – ينبغي تمييز المعلمتين السريتين المختارتين اعتباطياً: ***a*** للجزء A و***b*** للجزء B، عن معاملي ويرستراس ***a*** و***b***.

2.9 التوقيع الرقمي

يحتوي المجال **ECGDSASignature** على القيمتين **r** و**s** من التوقيع الرقمي الإهليلجي المحسوب. ويضم القسم 3.7.8 من [af-sec-0100.002] والفصل 5 من المعيار [ISO/IEC 14888-3] معلومات أخرى عن المجال EC-GDSA من خوارزمية التوقيع.

وينبغي تشفير التوقيع الرقمي **ECGDSA** الإهليلجي بالترميز ASN.1 أولاً ثم وضعه في المجال **signature** في الماكرو **SIGNED** المذكورة في هذه التوصية. وفيما يخص التوقيع الرقمي ينبغي أن يدرج المرسل معرّف هوية الغرض في المعلمة **algorithmOID** التي من شأنها أن تمكن المرسل إليه من تحديد استعمال التوقيع الرقمي الإهليلجي.

10 الوظيفة شبه العشوائية (PRF)

يهدف تعريف الوظيفة شبه العشوائية (PRF) في هذه الفقرة إلى إنقاص المفاتيح الدينامية استناداً إلى عناصر مفتاح ساكن وقيمة عشوائية.

ملاحظة – هذه الوظيفة PRF مماثلة للوظيفة MIKEY PRF (انظر القسم 2.1.4 من المعيار [IETF RFC 3830]).

وتستخدم طريقة حساب المفتاح معلمات الدخل التالية:

- *inkey*: مفتاح دخول إلى وظيفة الاشتقاق.
- *inkey_len*: طول مفتاح الدخل بالبتات.
- *label*: واسم خاص يرتبط بنمط المفتاح الذي يجب الحصول عليه وبالقيمة العشوائية **challenge**.
- *outkey_len*: الطول المطلوب لمفتاح الخروج مقدراً بالبتات.

والوظيفة شبه العشوائية مزودة بالمخارج التالية:

- *outkey*: مفتاح خروج بالطول المطلوب.

ينبغي أن تستعمل الوظيفة PRF الوظيفة PRF المحددة في القسم 2.1.4 من المرجع [IETF RFC 3830].

11 استرداد الخطأ الأمني

لا تحدد هذه التوصية ولا توصي بأية طريقة تستطيع النقاط الطرفية بموجبها أن تراقب سرية اتصالاتها المطلقة. ولكنها توصي بتدابير تتخذ عندما يكشف عن فقدان السرية.

إذا كشفت أية نقطة طرفية عن انتهاك في أمن قناة توصيل النداء (مثلاً في القناة [ITU-T H.225.0] لتدفق تبعاً للتوصية [ITU-T H.323]) ينبغي إقفال التوصيل فوراً بعد إجراءات البروتوكول الملائمة للنقطة الطرفية المعنية (بالنسبة إلى الفقرة 5.8 [ITU-T H.323] باستثناء الخطوة 5-B).

إذا كشفت إحدى النقطتين الطرفيتين عن انتهاك في أمن القناة H.245 أو القناة المنطقية للمعطيات الآمنة **(h235Control)**، ينبغي إقفال التوصيل فوراً بعد إجراءات البروتوكول الملائمة للنقطة الطرفية المعنية (بالنسبة إلى الفقرة H.323/5.8 باستثناء الخطوة 5-B).

إذا كشفت أية نقطة طرفية عن فقدان الخصوصية على قناة منطقية ينبغي أن تطلب فوراً مفتاحاً جديداً **(encryptionUpdateRequest)** و/أو إقفال القناة المنطقية. ومن الممكن أن يتسبب فقدان الخصوصية على قناة منطقية في إغلاق جميع القنوات المنطقية الأخرى إذا قررت الوحدة MC(U) ذلك و/أو إعادة حساب مفاتيحها. يجب أن ترسل الوحدة MC(U) طلب تحيين **encryptionUpdateRequest**، ورسالة تحيين **encryptionUpdate** إلى جميع النقاط الطرفية المتأثرة.

من الممكن أن يتسبب خطأ أمني على قناة فردية في إغلاق التوصيل على جميع نقاط المؤتمر الطرفية مما يؤدي إلى إنهاء المؤتمر إذا ما قررت الوحدة MC(U) ذلك.

1.11 تشوير الخطأ

ينبغي أن يوفر الحارس البوابي المزود بمقدرات الأمن أو أي كيان ITU-T H.225.0 بأمن محسن دلالات عن الأخطاء. وتدل أخطاء الأمن أن كياناً ما لم يتمكن من معالجة الرسالة المستقبلة بشكل صحيح. وفي كل مرة يحصل ذلك ينبغي إعطاء شفرة أخطاء مفصلة.

- تشير الرسالة **securityWrongSyncTime** إلى أن المرسل واجه مشكلة أمنية مع طابعات وقت غير ملائمة. وقد يكون ذلك ناجماً عن مشكلة في المخدم الزمني أو فقدان التزامن أو عن تأخر مفرط في الانتشار في الشبكة.
- تشير الرسالة **securityReplay** إلى وجود اعتداء بواسطة إعادة الإرسال. وهذا يقع عندما يظهر نفس رقم التتابع أكثر من مرة في ساعة وتاريخ محددين.
- تشير الرسالة **securityWrongGeneralID** إلى عدم توافق في معرّف الهوية العام في الرسالة، وقد ينجم ذلك عن عنونة خاطئة.
- تشير الرسالة **securityWrongSendersID** إلى عدم توافق في معرّف هوية المرسل في الرسالة. وقد ينجم ذلك عن إدخال خاطئ يقوم به المستعمل.
- تشير الرسالة **securityIntegrityFailed** إلى فشل التحقق من التكامل/التوقيع. وقد ينجم ذلك في حالة التوصية [ITU-T H.235.1] عن كلمة سر خاطئة أو مدخلة بشكل خاطئ أثناء الطلب الأولي أو عن هجوم نشط. أما فيما يخص التوصيتين [ITU-T H.235.2] و[ITU-T H.235.3] فذلك يعني فشل التحقق من التوقيع الرقمي في الرسالة. وقد ينجم ذلك عن تطبيق مفتاح خصوصي/عمومي خاطئ أو عن هجوم نشط.
- تشير الرسالة **securityWrongOID** إلى كل عدم توافق في المعرّفات OID الموجودة في العلامة (واضحة كانت أم مجفرة) أو في المعرفات OID الموجودة في الخوارزمية. وذلك يعني أن عدة خوارزميات/مواصفات أمنية قد استخدمت.
- تشير الرسالة **securityDHmismatch** إلى كل عدم توافق بين المعلمات ديفي–هيلمان المتبادلة. وقد يشير ذلك إلى أن عدة مجموعات معلمات DH أو حتى عدة خوارزميات تجفير صوت قد استخدمت.
- تشير الرسالة **securityCertificateExpired** إلى انتهاء صلاحية الشهادة.
- تشير الرسالة **securityCertificateDateInvalid** إلى أن تاريخ صلاحية الشهادة لم يبدأ بعد.
- تشير الرسالة **securityCertificateRevoked** إلى ملاحظة أن الشهادة لاغية.
- تشير الرسالة **securityCertificateNotReadable** إلى عدم التمكن من فك تشفير الشهادة بالترميز ASN.1 بشكل صحيح أو إلى عدم صلاحية نسقها.
- تشير الرسالة **securityCertificateSignatureInvalid** إلى عدم صحة توقيع الشهادة.
- تشير الرسالة **securityCertificateMissing** إلى نقصان شهادة متوقعة أو إلى عدم إمكانية تحديد موقعها.
- تشير الرسالة **securityCertificateIncomplete** إلى عدم وجود بعض ملحقات بالشهادة كان يتوقع وصولها.
- تشير الرسالة **securityUnsupportedCertificateAlgOID** إلى عدم فهم أو عدم توفير بعض خوارزميات التجفير مثل خوارزمية التظليل أو التوقيع الرقمية المستخدمة في الشهادة. ويجوز للمرسل في الإجابة المعاد إرسالها أن يرسل قائمة بالشهادات المقبولة في فيش مختلفة بغية تسهيل انتقاء المرسل إليه للشهادة الملائمة.

- تشير الرسالة **securityUnknownCA** إلى عدم التمكن من إيجاد الشهادة CA/الجذر أو عدم إمكانية اتباعها بسلطة CA موثوقة.

في جميع حالات الفشل الأخرى لعمليات الأمن ITU-T H.235 ينبغي إعادة إرسال الرسالة **securityDenial** للرسالة ITU-T H.225.0 RAS (استجابة **securityDenied** لتشوير النداء ITU T H.225.0).

الملاحظة 1 – يجوز أن تقع الأخطاء securityWrongSyncTime وsecurityReplay وsecurityWrongGeneralID وsecurityWrongSendersID وSecurityIntegrityFailed وsecurityDHmismatch وsecurityWrongOID في مواصفات الأمن ITU-T H.235.1 أو ITU-T H.235.2 أو ITU-T H.235.3.

الملاحظة 2 – ويجوز أن تقع الأخطاء securityCertificateExpired وsecurityCertificateDateInvalid وsecurityCertificateRevoked وsecurityCertificateNotReadable وsecurityCertificateSignatureInvalid وsecurityCertificateMissing وsecurityCertificateIncomplete وsecurityUnsupportedCertificateAlgOID وsecurityUnknownCA في مواصفتي الأمن ITU-T H.235.2 أو ITU-T H.253.3.

الملحق ألف

ASN.1 ITU-T H.235

(هذا الملحق جزء لا يتجزأ من هذه التوصية)

```
H235-SECURITY-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- EXPORTS All

ChallengeString         ::= OCTET STRING (SIZE(8..128))
TimeStamp               ::= INTEGER(1..4294967295)     -- seconds since 00:00
                                                       -- 1/1/1970 UTC
RandomVal               ::= INTEGER -- 32-bit Integer
Password                ::= BMPString (SIZE (1..128))
Identifier              ::= BMPString (SIZE (1..128))
KeyMaterial             ::= BIT STRING(SIZE(1..2048))
KeyMaterialExt          ::= BIT STRING(SIZE(2049..65536))


NonStandardParameter ::= SEQUENCE
{
     nonStandardIdentifier   OBJECT IDENTIFIER,
     data                    OCTET STRING
}

-- if local octet representations of these bit strings are used they shall
-- utilize standard Network Octet ordering (e.g., Big Endian)
-- for keylengths up to 2048
DHset ::= SEQUENCE
{
     halfkey       BIT STRING (SIZE(0..2048)), -- = g^x mod n
     modSize       BIT STRING (SIZE(0..2048)), --  n
     generator     BIT STRING (SIZE(0..2048)), -- g
     ...
}

-- for keylengths exceeding 2048
DHsetExt ::= SEQUENCE
{
     halfkey       BIT STRING (SIZE(2049..65536)),           -- = g^x mod n
     modSize       BIT STRING (SIZE(2049..65536))  OPTIONAL, --  n
     generator     BIT STRING (SIZE(2049..65536))  OPTIONAL, -- g
     ...
}


ECpoint ::= SEQUENCE -- uncompressed (x, y) affine coordinate representation of
                     -- an elliptic curve point
{
     x         BIT STRING (SIZE(0..511)) OPTIONAL,
     y         BIT STRING (SIZE(0..511)) OPTIONAL,
     ...
}

ECKASDH::= CHOICE -- parameters for elliptic curve key agreement scheme Diffie-
Hellman
{
```

```
    eckasdhp SEQUENCE -- parameters for elliptic curves of prime field
    {
        public-key    ECpoint, -- This field contains representation of
            -- the ECKAS-DHp public key value. This field contains the
            -- initiator's ECKAS-DHp public key value (aP) when this
            -- information element is sent from originator to receiver. This
            -- field contains the responder's ECKAS-DHp public key value (bP)
            -- when this information element is sent back from receiver to
            -- originator.
        modulus       BIT STRING (SIZE(0..511)), -- This field contains
            -- representation of the ECKAS-DHp public modulus value (p).
        base          ECpoint, -- This field contains representation of the
            -- ECKAS-DHp public base (P).
        weierstrassA  BIT STRING (SIZE(0..511)), -- This field contains
            -- representation of the ECKAS-DHp Weierstrass coefficient (a).
        weierstrassB  BIT STRING (SIZE(0..511)) -- This field contains
            -- representation of the ECKAS-DHp Weierstrass coefficient (b).
    },

    eckasdh2 SEQUENCE -- parameters for elliptic curves of characteristic 2
    {
        public-key    ECpoint, -- This field contains representation of
            -- the ECKAS-DH2 public key value.
            -- This field contains the initiator's ECKAS-DH2 public key value
            -- (aP) when this information element is sent from originator to
            -- receiver. This field contains the responder's ECKAS-DH2 public
            -- key value (bP) when this information element is sent back from
            -- receiver to originator.
        fieldSize     BIT STRING (SIZE(0..511)), -- This field contains
            -- representation of the ECKAS-DH2 field size value (m).
        base          ECpoint, -- This field contains representation of the
            -- ECKAS-DH2 public base (P).
        weierstrassA  BIT STRING (SIZE(0..511)), -- This field contains
            -- representation of the ECKAS-DH2 Weierstrass coefficient (a).
        weierstrassB  BIT STRING (SIZE(0..511)) -- This field contains
            -- representation of the ECKAS-DH2 Weierstrass coefficient (b).
    },
    ...
}

ECGDSASignature::= SEQUENCE -- parameters for elliptic curve digital signature
            -- algorithm
{
    r         BIT STRING (SIZE(0..511)), -- This field contains the
            -- representation of the r component of the ECGDSA digital
            -- signature.
    s         BIT STRING (SIZE(0..511)) -- This field contains the
            -- representation of the s component of the ECGDSA digital
            -- signature.
}

TypedCertificate ::= SEQUENCE
{
    type          OBJECT IDENTIFIER,
    certificate   OCTET STRING,
    ...
}

AuthenticationBES ::= CHOICE
{
    default       NULL, -- encrypted ClearToken
    radius        NULL, -- RADIUS-challenge/response
    ...
}
```

```
AuthenticationMechanism  ::= CHOICE
{
     dhExch          NULL, -- Diffie-Hellman
     pwdSymEnc       NULL, -- password with symmetric encryption
     pwdHash         NULL, -- password with hashing
     certSign        NULL, -- Certificate with signature
     ipsec           NULL, -- IPSEC based connection
     tls             NULL,
     nonStandard     NonStandardParameter, -- something else.
     ...,
     authenticationBES  AuthenticationBES, -- user authentication for BES
     keyExch   OBJECT IDENTIFIER -- key exchange profile
}

ClearToken          ::= SEQUENCE  -- a "token" may contain multiple value types.
{
     tokenOID        OBJECT IDENTIFIER,
     timeStamp       TimeStamp OPTIONAL,
     password        Password OPTIONAL,
     dhkey           DHset OPTIONAL,   -- for keylengths up to 2048
     challenge       ChallengeString OPTIONAL,
     random          RandomVal OPTIONAL,
     certificate     TypedCertificate OPTIONAL,
     generalID       Identifier OPTIONAL,
     nonStandard     NonStandardParameter OPTIONAL,
     ...,
     eckasdhkey      ECKASDH OPTIONAL,  -- elliptic curve Key Agreement
                                        -- Scheme-Diffie Hellman Analogue
                                        -- (ECKAS-DH)
     sendersID       Identifier OPTIONAL,
     h235Key         H235Key OPTIONAL, -- central distributed key in V3
     profileInfo     SEQUENCE OF ProfileElement OPTIONAL,  -- profile-specific
     dhkeyext        DHsetExt OPTIONAL  -- for keylengths exceeding 2048

}

--   An object identifier should be placed in the tokenOID field when a
--   ClearToken is included directly in a message (as opposed to being
--   encrypted). In all other cases, an application should use the
--   object identifier { 0 0 } to indicate that the tokenOID value is not
--   present.
--   Start all the cryptographic parameterized types here...
--

ProfileElement      ::= SEQUENCE
{
     elementID       INTEGER (0..255), -- element identifier, as defined by
                                       -- profile
     paramS          Params OPTIONAL,  -- any element-specific parameters
     element         Element OPTIONAL, -- value in required form
     …
}

Element ::= CHOICE
{
     octets               OCTET STRING,
     integer              INTEGER,
     bits                 BIT STRING,
     name                 BMPString,
     flag                 BOOLEAN,
     …
}
```

```
SIGNED { ToBeSigned } ::= SEQUENCE {
     toBeSigned          ToBeSigned,
     algorithmOID        OBJECT IDENTIFIER,
     paramS              Params,   -- any "runtime" parameters
     signature           BIT STRING -- could be an RSA or an ASN.1 coded
ECGDSA Signature
} ( CONSTRAINED BY { -- Verify or Sign Certificate -- } )


ENCRYPTED { ToBeEncrypted } ::= SEQUENCE {
     algorithmOID        OBJECT IDENTIFIER,
     paramS              Params,   -- any "runtime" parameters
     encryptedData       OCTET STRING
} ( CONSTRAINED BY { -- Encrypt or Decrypt -- ToBeEncrypted } )

HASHED { ToBeHashed } ::= SEQUENCE {
     algorithmOID        OBJECT IDENTIFIER,
     paramS              Params,   -- any "runtime" parameters
     hash                BIT STRING
} ( CONSTRAINED BY { -- Hash -- ToBeHashed } )

IV8 ::= OCTET STRING (SIZE(8)) -- initial value for 64-bit block ciphers
IV16 ::= OCTET STRING (SIZE(16)) -- initial value for 128-bit block ciphers

-- signing algorithm used must select one of these types of parameters
-- needed by receiving end of signature.

Params ::= SEQUENCE {
     ranInt         INTEGER OPTIONAL, -- some integer value
     iv8            IV8 OPTIONAL, -- 8-octet initialization vector
     ...,
     iv16           IV16 OPTIONAL,-- 16-octet initialization vector
     iv             OCTET STRING OPTIONAL, -- arbitrary length initialization
     vector
     clearSalt      OCTET STRING OPTIONAL -- unencrypted salting key for
     encryption
}

EncodedGeneralToken ::= TYPE-IDENTIFIER.&Type (ClearToken -- general usage token
-- )
PwdCertToken ::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, generalID
PRESENT})
EncodedPwdCertToken ::= TYPE-IDENTIFIER.&Type (PwdCertToken)

CryptoToken::= CHOICE
{

     cryptoEncryptedToken SEQUENCE -- General purpose/application specific token
     {
          tokenOID       OBJECT IDENTIFIER,
          token          ENCRYPTED { EncodedGeneralToken }
     },
     cryptoSignedToken  SEQUENCE -- General purpose/application specific token
     {
          tokenOID       OBJECT IDENTIFIER,
          token          SIGNED { EncodedGeneralToken }
     },
     cryptoHashedToken SEQUENCE -- General purpose/application specific token
```

```
    {
        tokenOID            OBJECT IDENTIFIER,
        hashedVals          ClearToken,
        token HASHED { EncodedGeneralToken }
    },
    cryptoPwdEncr ENCRYPTED { EncodedPwdCertToken },
    ...
}

-- These allow the passing of session keys within the H.245 OLC structure.
-- They are encoded as standalone ASN.1 and based as an OCTET STRING within
-- H.245
H235Key  ::=CHOICE  -- This is used with the H.245 or ClearToken "h235Key"
field
{
    secureChannel           KeyMaterial, -- For keylengths up to 2048
    sharedSecret            ENCRYPTED {EncodedKeySyncMaterial},
    certProtectedKey        SIGNED {EncodedKeySignedMaterial },
    ...,
    secureSharedSecret      V3KeySyncMaterial, -- for H.235 V3 endpoints
    secureChannelExt        KeyMaterialExt  -- for keylengths exceeding 2048

}

KeySignedMaterial ::= SEQUENCE {
    generalId     Identifier, -- slave's alias
    mrandom       RandomVal, -- master's random value
    srandom       RandomVal OPTIONAL, -- slave's random value
    timeStamp     TimeStamp OPTIONAL, -- master's timestamp for unsolicited EU
    encrptval     ENCRYPTED { EncodedKeySyncMaterial }
}
EncodedKeySignedMaterial ::= TYPE-IDENTIFIER.&Type (KeySignedMaterial)

H235CertificateSignature    ::= SEQUENCE
{
    certificate             TypedCertificate,
    responseRandom          RandomVal,
    requesterRandom         RandomVal OPTIONAL,
    signature               SIGNED { EncodedReturnSig },
    ...
}

ReturnSig ::= SEQUENCE {
    generalId               Identifier, -- slave's alias
    responseRandom          RandomVal,
    requestRandom           RandomVal OPTIONAL,
    certificate             TypedCertificate OPTIONAL -- requested certificate
}

EncodedReturnSig ::= TYPE-IDENTIFIER.&Type (ReturnSig)
KeySyncMaterial    ::= SEQUENCE
{
    generalID     Identifier,
    keyMaterial   KeyMaterial,
    ...
}
EncodedKeySyncMaterial  ::=TYPE-IDENTIFIER.&Type (KeySyncMaterial)



V3KeySyncMaterial  ::= SEQUENCE
{
    generalID               Identifier OPTIONAL, -- peer terminal ID
    algorithmOID            OBJECT IDENTIFIER OPTIONAL, -- encryption algorithm
```

```
    paramS                  Params, -- IV
    encryptedSessionKey     OCTET STRING OPTIONAL, -- encrypted session key
    encryptedSaltingKey     OCTET STRING OPTIONAL, -- encrypted media salting
                                                   -- key
    clearSaltingKey         OCTET STRING OPTIONAL, -- unencrypted media salting
                                                   -- key
    paramSsalt              Params OPTIONAL, -- IV (and clear salt) for salting
                                                   -- key encryption
    keyDerivationOID        OBJECT IDENTIFIER OPTIONAL, -- key derivation
                                                   -- method
    ...,
    genericKeyMaterial      OCTET STRING OPTIONAL -- ASN.1-encoded key material
                        -- form is dependent on associated media encryption tag

}


END  -- End of H235-SECURITY-MESSAGES DEFINITIONS
```

الملحق باء

مواضيع خاصة بالتوصية ITU-T H.324

(يشكل هذا الملحق جزءاً أساسياً من هذه التوصية)

للدراسة.

التذييل I

تفاصيل تطبيق التوصية H.323

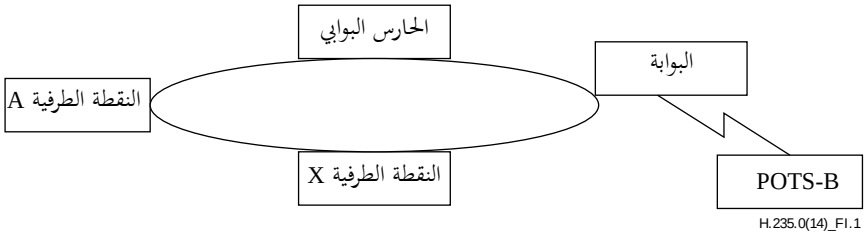
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I أمثلة التطبيق

تصف الفقرات التالية أمثلة التطبيق التي يمكن تطويرها في إطار ITU-T H.235. وليس المقصود منها تقييد الإمكانيات العديدة الأخرى المقترحة في هذه التوصية، بل هي تهدف بالأحرى إلى إعطاء المزيد من الأمثلة الملموسة بشأن الاستعمال في إطار التوصية [ITU-T H.323].

1.1.I العلامات

تصف هذه الفقرة مثالاً على استعمال علامة الأمن لحجب معلومات عنونة المقصد أو إخفائها. وسيناريو المثال نقطة طرفية تود أن تجري نداءً إلى نقطة طرفية أخرى باستعمال اسمها المستعار المعروف. وبشكل أدق تتألف الشبكة ITU-T H.323 من نقطة طرفية وحارس بوابي وبوابة وجهاز هاتف POTS كما هو مبين في الشكل أدناه.



الشكل 1.I – العلامات

يمكن لشبكة ITU-T H.323 أن تعمل حالياً بطريقة مماثلة لشبكة هاتفية مع خدمة تعرف هوية الطالب. ويوضح هذا السيناريو حالة *مطلوب* لا يرغب أن يصرح بعنوانه المادي في الوقت الذي يقبل بإنشاء النداء. وقد يكون ذلك هاماً في البوابات POTS-H.323 عند ضرورة إبقاء رقم هاتف المقصد خاص.

لنفترض أن النقطة A تحاول الاتصال بالنقطة POTS-B وأن هذه النقطة الأخيرة لا تريد أن تصرح برقم هاتفها للنقطة A حسب المخطط ITU-T E.164 (الطريقة التي وضعت فيها هذه السياسة لا تدخل في مجال تطبيق هذا المثال.)

- ترسل النقطة EPA طلب **ARQ** إلى حارسها البوابي لتفكك عنوان الجهاز POTS كما هو مبين في اسمه المستعار/البوابة. يتعرف الحارس البوابي على هوية هذا العنوان كاسم "خاص" مع العلم بضرورة إعادة إرسال عنوان البوابة مع الجهاز POTS من أجل إتمام التوصيل. (هذه الحالة مماثلة لحالة إعادة عنوان بوابة ITU-T H.320 إذا كانت النقطة الطرفية ITU-T H.320 مطلوبة من نقطة ITU-T H.323).
- يرسل الحارس البوابي في الرسالة **ACF** المعاد إرسالها عنوان البوابة مع الجهاز POTS كالمعتاد. وترسل معلومات العنونة اللازمة لنداء الجهاز البعيد (أي رقم الهاتف) في علامة مجفرة ضمن الرسالة **ACF**. وتحتوي هذه العلامة المجفرة على الرقم ITU-T E.164 الحقيقي (للهاتف) للجهاز الذي يتعذر فك تجفيره حتى من قبل الطالب (أي النقطة EPA).
- وترسل النقطة الطرفية إلى بوابة رأس الخط (التي تم إرسال عنوان تشوير ندائها في الرسالة **ACF**) رسالة SETUP تضم العلامة أو العلامات غير الشفافة التي استلمتها في الرسالة **ACF**.
- ترسل البوابة طلبها **ARQ** فور استلامها الرسالة SETUP إلى حارسها البوابي، ومعه جميع العلامات التي استلمتها في الرسالة SETUP.

- يستطيع الحارس البوابي أن يفك تجفير العلامة أو العلامات وأن يرسل رقم الهاتف في الرسالة **ACF**.

ويرد أدناه على سبيل المثال جزء من الترميز ASN.1 لبنية علامة مع وصف محتوى المجالات. ويفترض استعمال المعلمة **cryptoEncodedGeneralToken** لإدراج رقم الهاتف المجفر فيها.

وباستطاعة التطبيق أن يختار معرف هوية غرض العلامة، **tokenOID**، للدلالة على أن هذه العلامة تضم رقم الهاتف ITU-T E.164. وتدرج الطريقة الخاصة التي ستستعمل في تجفير رقم الهاتف هذا (مثال: معيار DES يضم 56 بتة) في التعريف "ENCRYPT" الموجود في معرف هوية الخوارزمية **algorithmOID**.

```
CryptoToken::= CHOICE
{
     cryptoEncodedGeneralToken SEQUENCE    -- General purpose/application
                                           --  specific token
     {
          tokenOID  OBJECT IDENTIFIER,
          ENCRYPTED { EncodedGeneralToken }
     },
.
.
. [abbreviated text]
.

}
```

وترسل الرسالة **CryptoToken** ضمن الرسالة SETUP (من النقطة EPA إلى البوابة) والرسائل **ARQ** (من البوابة إلى الحارس البوابي) كما هو مبين أعلاه. وبعد فك تجفير العلامة (رقم الهاتف) يرسل الحارس البوابي جزء النص الواضح منها (غير المجفر) في المعلمة **clearToken**.

2.1.I استعمال العلامات في الأنظمة ITU-T H.323

لقد سبب استعمال العلامات **CryptoH323Tokens** بالطريقة التي تم تسييرها في الرسائل RAS بعض الالتباس. فهناك فئتان رئيسيتان من العلامات **CryptoH323Tokens**: فئة العلامات المستعملة للإجراءات ITU-T H.235 وفئة العلامات المستعملة بطريقة خاصة مرتبطة بالتطبيق. ويستحسن استعمال هذه العلامات طبقاً للقواعد التالية:

- ينبغي استعمال جميع الحقول المحددة في ITU-T H.235 (مثال: **cryptoEPPwdHash** و**cryptoGKPwdHash** و**cryptoEPPwdEncr** و**cryptoGKPwdEncr** و**cryptoGKCert** و**cryptoFastStart**) طبقاً للإجراءات وباستعمال الخوارزميات المحددة في هذه التوصية).
- ينبغي للفيش الخاصة بالتطبيقات والعلامات المستقلة أن تستعمل في تبادلاتها العلامة **nestedcryptoToken**.
- ينبغي للعلامة **nestedcryptoToken** أن تستعمل العلامة **tokenOID** (معرف هوية الغرض) التي تعرف هويتها دون أي لبس.

3.1.I استعمال القيمة العشوائية في الأنظمة ITU-T H.235 ITU-T H.323

يمكن للحارس البوابي تحديث القيمة العشوائية المرسلة في تتابع **xCF/xRQ** بين النقاط الطرفية والحارسات البوابية. كما ورد في الفقرة 1.3.8 يمكن تحديث هذه القيمة العشوائية في كل رسالة **xCF** بغية استعمالها في رسالة **xRQ** اللاحقة الذاهبة من النقطة الطرفية. ونظراً إلى وجود احتمال فقدان الرسائل RAS (بما فيها الرسائل **xRJ/xCF**) فإن القيمة العشوائية المحدثة قد تضيع أيضاً. وتكون الاستعادة في مثل هذه الحالة إعادة تدميث سياق الأمن، غير أن هذا الأمر متروك للتطبيق.

وستكون التطبيقات التي تتطلب استعمال عدة طلبات RAS بالانتظار محدودة بتحديث القيم العشوائية المستعملة في كل استيقان. وإذا حصل تحديث هذه القيمة عند كل استجابة لطلب ما، تكون الطلبات الموازية غير ممكنة. وهناك حل ممكن يكمن في توفير "نافذة" منطقية تبقى خلالها القيمة العشوائية ثابتة. وهذه مسألة على التطبيق أن يتكفل بحلها.

4.1.I كلمة السر

يفترض في هذا المثال أن المستعمل مشترك في خدمة الحارس البوابي (أي أنه موجود في نفس المنطقة) وأنه يمتلك معرف هوية المشترك مع كلمة السر ويسجل هذا المستعمل نفسه لدى الحارس البوابي باستخدام معرف هوية اشتراكه (كما كان قد أرسل في معرف هوية الاسم H.323) وبتجفير سلسلة الاختبار التي يقدمها له الحارس البوابي. وتفترض هذه العملية أن الحارس البوابي يعرف أيضاً كلمة السر التي تصاحب معرف هوية الاشتراك. ويستيقن الحارس البوابي هوية المستعمل بالتحقق من أن سلسلة الاختبار قد تم تجفيرها بشكل صحيح.

وإجراء التسجيل مع الاستيقان الذي يجريه الحارس البوابي في هذا المثال هو كالتالي:

1) إذا استعملت النقطة الطرفية الطلب **GRQ** من أجل استكشاف حارس بوابي يكون أحد الأسماء التي تتضمنها الرسالة موجود في معرف هوية الاشتراك (في شكل معرف هوية **H.323ID**). وتضم الرسالة **authenticationcapability** آلية استيقان **AuthenticationMechanism** تستند إلى تشفير كلمة السر **pwdSymEnc** وتكون معلمات معرفات هوية الخوارزميات **algorithmOID** على نحو تدل فيه على المجموعة الكاملة لخوارزميات التجفير التي توفرها هذه النقطة الطرفية. (كأن تكون إحدى هذه الخوارزميات المعيار DES الذي يضم 56 بتة في الأسلوب ECB مثلاً).

2) يجيب الحارس البوابي على هذه الرسالة برسالة تأكيد **GCF** (مع افتراض أنه يعرف الاسم) تسيّر عنصر **tokens** يضم علامة واحدة بنص واضح **ClearToken**. وتتألف هذه العلامة من جزأين: سلسلة الامتحان **challenge** والمؤشر الزمني **timeStamp**. تجفر السلسلة **challenge** في 16 أثموناً (بهدف الوقاية من اعتداءات التكرار وتضم علامة النص الواضح **ClearToken** العنصر **timeStamp**). يوضع أسلوب الاستيقان **authenticationmode** على القيمة **pwdSymEnc** ويدل معرف هوية الخوارزمية **algorithmOID** على خوارزمية التجفير التي يتطلبها الحارس البوابي (مثال: المعيار DES بـ 56 بتة بالأسلوب ECB).

وإذا لم يوفر الحارس البوابي أياً من معرفات هوية الخوارزميات **algorithmOID** المشار إليها في الطلب **GRQ**، يجيب برسالة رفض **GRJ** تضم رسالة السبب **GatekeeperRejectReason** التي تساوي **resourceUnavailable**.

3) يحاول تطبيق النقطة الطرفية عندئذ التسجيل في الحارس البوابي (أو في أحد الحارسات البوابية) الذي قد سبق وأجاب بإرسال رسالة تأكيد **GCF**، وذلك بإرسال طلب **RRQ** يضم عنصر **cryptoEPPwdEncr** في المعلمة **cryptoTokens**. ويضم هذا العنصر **cryptoEPPwdEncr** معرف هوية خوارزمية التجفير **algorithmOID** المناسبة خلال تبادل الرسائل **CRQ/GCF** وامتحان التجفير.

ويُبنى مفتاح التجفير على أساس كلمة السر الذي يضعها المستعمل بواسطة الإجراء الوارد في الفقرة 1.2.8. وستستعمل "سلسلة" الأثمونات الناتجة عندئذ كمفتاح DES لأغراض تجفير الامتحان **challenge**.

4) عندما يستقبل الحارس البوابي رسالة الامتحان المجفرة في الطلب **RRQ** يقارنها مع رسالة امتحان مجفرة بطريقة مماثلة بغية استيقان المستعمل الطالب. في حال عدم تطابق السلسلتين المجفرتين يجيب الحارس البوابي بإرسال رسالة رفض **RRJ** مع السبب **RegistrationRejectReason** موضوعاً على القيمة **securityDenial** أو شفرة خطأ أمني أخرى (طبقاً للفقرة 1.11). أما إذا تطابقت السلسلتان أرسل الحارس البوابي رسالة تأكيد **RCF** إلى النقطة الطرفية.

5) إذا استقبل الحارس البوابي طلب **RRQ** لا يحتوي على عنصر **cryptoTokens** مقبول، عليه أن يرسل رسالة رفض **RRJ** مع السبب **GatekeeperRejectReason** موضوعاً على القيمة **discoveryRequired**. وعند استلام النقطة الطرفية لهذه الرسالة **RRJ** تستطيع أن تقوم بالبحث الذي يسمح للثنائي الحارس البوابي/النقطة الطرفية بتبادل رسالة امتحان جديدة.

ملاحظة – يمكن إرسال الرسالة **GRQ** إلى الحارس البوابي بأسلوب من نقطة إلى نقطة.

IPsec 5.1.I

تستعمل الطريقة IPsec ([IETF RFC 2401] و[b-IETF RFC 2406] ESP و[b-IETF RFC 2409] IKE) عادة لتأمين الاستيقان وخياراً لتأمين السرية (أي التجفير) في طبقة بروتوكول الإنترنت بطريقة شفافة لكل بروتوكول (تطبيقي) عامل في الطبقات العليا. ولا يحتاج البروتوكول التطبيقي إلى التحديث من أجل القيام بهذه العملية؛ ولا يشترط سوى تطابق سياسة الأمن في كل نقطة طرفية.

وعلى سبيل المثال يمكن اتباع السيناريو الوارد أدناه من أجل الإفادة بقدر كبير من الأمن IPsec في حال اتصال بسيط من نقطة إلى نقطة:

1) تحدد النقطة الطرفية الطالبة وحارسها البوابي السياسة التي تتطلب استعمال طريقة الأمن IPsec (الاستيقان وخياراً السرية) وذلك باستعمال البروتوكول RAS. وقبل إرسال أول رسالة RAS من النقطة الطرفية إلى الحارس البوابي، يجري برنامج المراقبة ISAKMP [IETF RFC 2407]/Oakley [b-IETF RFC 2412] الموجود في النقطة الطرفية تفاوضاً بشأن خدمات الأمن الواجب استعمالها للرزم الذاهبة إلى والواردة من النفاذ المعروف للقناة RAS. وبعد انتهاء التفاوض تعمل القناة RAS تماماً كما لو كانت غير أمينة. ويبلغ الحارس البوابي النقطة الطرفية عنوان ورقم نفاذ قناة تشوير النداء الموجود في النقطة الطرفية المطلوبة وذلك بواسطة القناة الأمينة.

2) بعد حصول النقطة الطرفية الطالبة على عنوان ورقم النفاذ إلى قناة تشوير النداء، تقوم بتحديث سياسة أمنها دينامياً بهدف طلب الأمن IPsec المرغوب به لهذا العنوان لأغراض الثنائي بروتوكول/نفاذ. ثم عندما تحاول النقطة الطرفية الطالبة الاتصال مع هذا العنوان/النفاذ توضع الرزم في صف الانتظار أثناء القيام بالتفاوض بالطريقة ISAKMP [IETF RFC 2407]/Oakley [b-IETF RFC 2412] بين النقاط الطرفية. وعند الانتهاء من هذا التفاوض سينشأ تجمع أمن IPsec لهذا الثنائي عنوان/نفاذ ويستطيع التشوير ITU-T Q.931 عندئذ أن يبدأ.

3) يجوز للنقاط الطرفية أن تفاوض بشأن استعمال الأمن IPsec لأغراض القناة ITU-T H.245 أثناء تبادل الرسائل ITU-T Q.931، SETUP وCONNECT. مما يتيح للنقاط الطرفية تحديث قواعد معطياتها دينامياً لأغراض سياسة الأمن IPsec وفرض هذه السياسة على هذا التوصيل.

4) كما هو الحال في قناة تشوير النداء سيجري تفاوض ISAKMP [IETF RFC 2407]/Oakley [b-IETF RFC 2412] شفاف قبل إرسال أي رزمة ITU-T H.245 كانت. ويكون الاستيقان الذي يجريه هذا التبادل المحاولة الأولية للاستيقان من مستعمل إلى مستعمل. فهو ينشئ قناة أمينة (على الأغلب) بين المستعملين الاثنين تتيح التفاوض بشأن خصائص القناة السمعية. وإذا لم يرض أحد المستعملين عن نتيجة الاستيقان بعد الحوار مع مراسله، يمكن اختيار شهادات مختلفة كما يمكن تكرار التبادل ISAKMP [IETF RFC 2407]/Oakley [b-IETF RFC 2412].

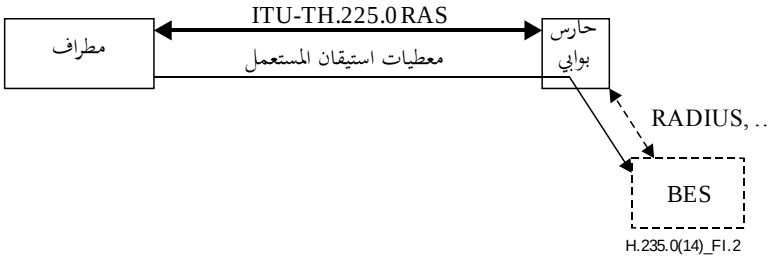
5) يتم تبادل معطيات مفتاحية جديدة متصلة بالقناة السمعية بالبروتوكول RTP بعد كل استيقان ITU-T H.245 ISAKMP [IETF RFC 2407]/Oakley [b-IETF RFC 2412]. ويوزع الكيان الرئيسي هذه المعطيات على القناة ITU-T H.245 الأمينة. وبما أن البروتوكول ITU-T H.245 محدد على نحو يوزع فيه الرئيس المعطيات المفتاحية متعددة الوسائط على القناة ITU-T H.245 (بهدف إتاحة الاتصالات متعددة النقاط) فلا يوصى باستعمال الطريقة IPsec لأغراض القناة RTP.

وقد تطرح قناة ITU-T H.245 مجفرة مشكلة للمخدمات الوسيطة أو لجدران النار NAT لأن أرقام النفاذ الموزعة دينامياً مسيرة في البروتوكول ITU-T H.245. ومن أجل أن تعمل جدران النار هذه بشكل صحيح عليها أن تجفر البروتوكول وتعدله وتعيد تجفيره. ولهذا السبب تم إدراج القناة المنطقية "للأمن" في التوصية [ITU-T H.245]. وفي حال استعمال هذه القناة تستطيع القناة ITU-T H.245 أن تبقى غير أمينة؛ ويسمح التشوير عبر القناة المنطقية بحماية هذه القناة باستعمال الطريقة IPsec، ويفيد مفتاح السر المستخدم وفي القناة المنطقية "للأمن" في حماية التزامن **EncryptionSync** الذي يخصصه الكيان الرئيسي للقناة ITU-T H.245.

6.1.I توفير خدمات مخصصة (BES)

تنطوي المخدمات المخصصة على وظيفة إضافية هامة في مجمل البيئة متعددة الوسائط من النمط ITU-T H.323. ويقدم المخدم BES على سبيل المثال خدمات لاستيقان المستعمل والترخيص بالخدمة والمحاسبة والترسيم والفوترة وغيرها من الخدمات. والحارس البوابي قادر في نموذج بسيط على تقديم مثل هذه الخدمات لكنه غير قادر على عمل ذلك دائماً في معمارية مفككة إما لعدم تيسر نفاذه إلى قواعد المعطيات BES بالضرورة وإما لانتمائه إلى مجال إداري مختلف. ومن ناحية أخرى لا يعرف المطراف والمستعمل عادة BES التابع لهما.

ويقدم الشكل 2.I سيناريوهاً يتضمن مطرافاً متعدد الوسائط (مثل جهاز SASET) وحارساً بوابياً ومخدم BES. والطريقة الصحيحة التي يتصل فيها المخدم BES مع الحارس البوابي لا تدخل ضمن مجال تطبيق التوصية [ITU-T H.323]. ويمكن استخدام عدة طرائق وبروتوكولات ومنها التكنولوجيا RADIUS انظر [IETF RFC 2865] التي تعتبر إحدى أهم الطرائق والتي غالباً ما يستعملها كثيرون من مزودي الخدمات.



الشكل 2.I – سيناريو مع المخدم المختص

وينبغي للحارس البوابي الذي يوفر الخدمات BES أن يقترح الأسلوبين التاليين:

1) الأسلوب **default mode**: ولا يعرف المطراف في هذا الأسلوب المخدم BES حيث يتوجب وجود علاقة ثقة مع الحارس البوابي. ويرسل معطيات استيقان المستعمل بعد تجفيرها (**cryptoEncryptedToken**) إلى الحارس البوابي؛ ويفك هذا الأخير التجفير ويستخرج المعلومات المتعلقة باستيقان المستعمل ويرسلها إلى المخدم BES. ويتم تجفير كلمة السر في العلامة **ClearToken** بتطبيق سر منفصل يعرفه الكيانان المطراف والحارس البوابي على العلامة **ClearToken**. ويمكن الحصول على مفتاح التجفير استناداً إلى كلمة السر التي يتسجل بواسطتها المطراف عند الحارس البوابي بطريقة أمينة.

وتسيّر العلامة **CryptoToken** المجال **cryptoEncryptedToken** حيث يوضع المعرف **tokenOID** على "M" للدلالة على اتباع الأسلوب BES بالتغيب: وتحتوي المعلمة **token** على:

- المعرف **algorithmOID** الذي يشير إلى خوارزمية التجفير؛ "Y" (DES56-CBC) و"Z" (3DES-OCBC)؛ راجع الفقرة 11 [ITU-T H.235.6]؛
- المجال **paramS** غير مستعمل؛
- المعلمة **encryptedData** موضوعة على تمثيل العلامة **ClearToken** المجفرة بالأثمونين.

وتحتوي العلامة **ClearToken** بكونها **password** على معطيات استيقان المستعمل. وقد تكون المعلومات **ClearToken** المحمية أو رقم الشفرة PIN وتعرف هوية المستعمل ورقم بطاقة مسبقة الدفع أو رقم بطاقة الائتمان. ويوضع **timestamp** على ساعة المطراف ويحتوي **random** على رقم تتابع يتزايد بوتيرة واحدة ويوضع **sendersID** على معرف هوية المطراف و**generalID** على معرف هوية الحارس البوابي. وينبغي المحافظة على القيمة الأولية لخوارزمية التجفير ثابتة؛ ولا يمكنها أن تشكل جزءاً من السر الذي يخصص حين الاشتراك.

ملاحظة – لا ترسل العلامة **ClearToken**.

2) الأسلوب **RADIUS mode**: في هذا الأسلوب يكون عند المخدم BES ومستعمل المطراف سر مشترك، ولا يعتبر الحارس البوابي "موثوقاً" فيما يخص استيقان الأسلوب موضوع الدراسة. ويسير الحارس البوابي حتى المطراف وببساطة امتحان RADIUS

يستقبله من المخدم BES في امتحان *Access-Challenge* ويرسل استجابة المستعمل في شكل استجابة RADIUS في الطلب *Access-Request* في الاتجاه المعاكس. ويجري المطراف والحارس البوابي تفاوضاً بشأن هذه المقدرة للامتحان/الإجابة بالأسلوب **radius** في **AuthenticationBES** للمجال **AuthenticationMechanism** أثناء اكتشاف الحارس البوابي.

وعندما يستلم الحارس البوابي رسالة RADIUS *Access-Challenge* محتوية على الامتحان، يدخل الامتحان الموجود في 16 أثموناً ضمن المجال **challenge** للعلامة **ClearToken** عند استجوابه للمطراف بواسطة الرسالة **GCF** أو أي رسالة RAS أخرى. ويشير المعرف 'K' **tokenOID** للعلامة **ClearToken** إلى الامتحان RADIUS.

ويستطيع المطراف بعد ذلك أن يقدم الامتحان للمستعمل وينتظر إجابة الدخول. وعلى المطراف أن يجيب باستعمال رسالة RAS تظهر فيها الإجابة في المجال **challenge** للعلامة **ClearToken**. ويشير المعرف "L" **tokenOID** للعلامة **ClearToken** إلى الإجابة RADIUS.

يتضمن الجدول 1.I جميع معرّفات هوية الأغراض (OID) المذكورة.

الجدول 1.I – معرّفات هوية الأغراض المستعملة في الفقرة 6.1.I

مرجع هوية المعرف OID	قيمة هوية المعرف	الوصف
"K"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 31}	يدل على امتحان RADIUS في العلامة ClearToken
"L"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 32}	يدل على إجابة RADIUS (مسيرة في المجال challenge) في العلامة ClearToken
"M"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 33}	يدل على الأسلوب BES بالتغيب مع كلمة سر محمية في العلامة ClearToken

التذييل II

تفاصيل التطبيق ITU-T H.324

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

للدراسة.

التذييل III

تفاصيل أخرى عن تطبيق السلسلة ITU-T H

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

للدراسة.

التذييل IV

تقابل أقسام ITU-T H.235v3Amd1Cor1
مع توصيات السلسلة الفرعية ITU-T H.235v4

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يبين هذا التذييل الإعلامي مواقع كل فقرات ITU-T H.235v3Amd1Cor1 مع توصيات السلسة الفرعية ITU-T H.235v4.

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
الجزء الرئيسي	–	–	–
1	مجال التطبيق	ITU-T H.235.0	1
2	المراجع المعيارية	ITU-T H.235.0 ITU-T H.235.1 ITU-T H.235.2 ITU-T H.235.3	2 2 2 2
3	المصطلحات والتعاريف	ITU-T H.235.0 ITU-T H.235.2 ITU-T H.235.6	3 3 3
4	الرموز والمختصرات	ITU-T H.235.0 ITU-T H.235.3 ITU-T H.235.6	4 4 4
5	المصطلحات	ITU-T H.235.0 ITU-T H.235.2 ITU-T H.235.6	5 5 5
6	مدخل إلى النظام	ITU-T H.235.0	6
1.6	الملخص	ITU-T H.235.0	1.6
2.6	الاستيقان	ITU-T H.235.0	2.6
1.2.6	الشهادات	ITU-T H.235.0	1.2.6
3.6	أمن إقامة النداء	ITU-T H.235.0	3.6
6.4	أمن التحكم بالنداء (H.245)	ITU-T H.235.0	4.6
6.5	خصوصية الاتصالات في تدفقات الوسائط	ITU-T H.235.0	5.6
6.6	عناصر موثوقة	ITU-T H.235.0	6.6
1.6.6	إيداع المفتاح	ITU-T H.235.0	1.6.6
7.6	عدم النكران	ITU-T H.235.0	7.6
8.6	الأمن في بيئة متنقلة	ITU-T H.235.0	8.6
9.6	مواصفات الأمن	ITU-T H.235.0	9.6
7	عمليات إجراء التوصيل	ITU-T H.235.0	7
1.7	المدخل	ITU-T H.235.0	–
8	تشوير وإجراءات ITU-T H.245	ITU-T H.235.6	7
1.8	تشغيل آمن للقناة ITU-T H.245	ITU-T H.235.6	1.7

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
2.8	تشغيل قناة التوصية ITU-T H.245 غير الآمن	ITU-T H.235.6	2.7
3.8	تبادل المقدرات	ITU-T H.235.6	3.7
4.8	الدور الرئيسي	ITU-T H.235.6	4.7
5.8	تشوير القناة المنطقية	ITU-T H.235.6	5.7
6.8	الأمن بالتوصيل السريع	ITU-T H.235.6	6.7
1.6.8	أمن أحادي الاتجاه بالانطلاق السريع	ITU-T H.235.6	1.6.7
1.1.6.8	استعمال خوارزميات التجفير المتعددة في الإجراء fast connect	ITU-T H.235.6	1.1.6.7
2.6.8	أمن التوصيل السريع ثنائي الاتجاه	ITU-T H.235.6	2.6.7
7.8	إشارات DTMF ITU-T H.245 مشفرة	ITU-T H.235.6	7.7
1.7.8	سلسلة مجفرة أساسية	ITU-T H.235.6	1.7.7
2.7.8	السلسلة المجفرة iA5	ITU-T H.235.6	2.7.7
3.7.8	السلسلة المجفرة العامة	ITU-T H.235.6	3.7.7
4.7.8	قائمة بمعرّفات هويات الأغراض	ITU-T H.235.6	4.7.7
8.8	العمل بأسلوب ديفي–هيلمان	ITU-T H.235.6	7.8
9	الإجراءات متعددة النقاط	ITU-T H.235.6	8.8
1.9	الاستيقان	ITU-T H.235.6	1.8.8
2.9	الخصوصية	ITU-T H.235.6	2.8.8
10	تشوير الاستيقان وإجراءاته	ITU-T H.235.0	8
1.10	المدخل	ITU-T H.235.0	---
2.10	طريقة ديفي–هيلمان مع الاستيقان الخياري	ITU-T H.235.0	1.8
3.10	استيقان قائم على الاشتراك	ITU-T H.235.0	2.8
1.3.10	المدخل	ITU-T H.235.0	–
2.3.10	كلمة سر مع تشفير تناظري	ITU-T H.235.0	1.2.8
3.3.10	كلمة السر مع التظليل	ITU-T H.235.0	2.2.8
4.3.10	استيقان بالشهادة مع تواقيع	ITU-T H.235.0	3.2.8
5.3.10	استعمال السر المتقاسم وكلمات السر	ITU-T H.235.0	4.2.8
11	إجراءات تجفير تدفقات الوسائط	ITU-T H.235.6	9
1.11	مفاتيح دورة الوسائط	ITU-T H.235.6	1.9
2.11	حماية الوسيط من الغرق	ITU-T H.235.6	2.9
1.2.11	قائمة بمعرّفات هوية الأغراض	ITU-T H.235.6	1.2.9
12	استرداد الخطأ الأمني	ITU-T H.235.0	11
13	الاستيقان اللاتناظري وتبادل المفاتيح بواسطة أنظمة التجفير بالمنحنى الإهليلجي	ITU-T H.235.0	9
1.13	إدارة المفاتيح	ITU-T H.235.0	1.9
2.13	التوقيع الرقمي	ITU-T H.235.0	2.9
التذييل I	تفاصيل تطبيق التوصية ITU-T H.323	ITU-T H.235.0	التذييل I
1.I	طرائق حشو النص التجفيري	ITU-T H.235.6	1.I
2.I	مفاتيح جديدة	ITU-T H.235.6	2.7.8
3.I	عناصر التوصية ITU-T H.323 الموثوقة	ITU-T H.235.6	3.7.8

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
4.I	أمثلة التطبيق	ITU-T H.235.0	1.I
1.4.I	العلامات	ITU-T H.235.0	1.1.I
2.4.I	استعمال العلامات في الأنظمة ITU-T H.323	ITU-T H.235.0	2.1.I
3.4.I	استعمال القيمة العشوائية ITU-T H.235 في الأنظمة ITU-T H.323	ITU-T H.235.0	3.1.I
4.4.1	كلمة السر	ITU-T H.235.0	4.1.I
5.4.I	IPsec	ITU-T H.235.0	5.1.I
I.4.6	دعم المخدمات المختصة	ITU-T H.235.0	6.1.I
التذييل II	تفاصيل تطبيق ITU-T H.324	ITU-T H.235.0	التذييل II
التذييل III	تفاصيل أخرى عن تطبيق السلسلة H	ITU-T H.235.0	التذييل III
التذييل IV	بيبليوغرافيا	ITU-T H.235.0	2.2
الملحق ألف	**ITU-T H.235 ASN.1**	**ITU-T H.235.0**	**الملحق ألف**
الملحق باء	**مواضيع خاصة بالتوصية ITU-T H.323**	**ITU-T H.235.6**	–
1.B	الخلفية	ITU-T H.235.0	6
2.B	التشوير والإجراءات	ITU-T H.235.6	8
1.2.B	مواءمة المراجعة 1	ITU-T H.235.6	1.8
2.2.B	تشوير الأخطاء	ITU-T H.235.0	1.11
3.2.B	الدلالات الوظيفية في الطبعة 3	ITU-T H.235.6	2.8
4.2.B	تسيير المفتاح	ITU-T H.235.6	3.8
1.4.2.B	تسيير محسّن للمفتاح حسب الطبعة 3 من التوصية ITU-T H.235	ITU-T H.235.6	1.3.8
5.2.B	الأسلوب OFB المحسّن	ITU-T H.235.6	4.8
6.2.B	تحديث المفاتيح والتزامن	ITU-T H.235.6	6.8
1.6.2.B	تحديث المفاتيح دون إشعار بالاستلام	ITU-T H.235.6	1.6.8
2.6.2.B	تحديث المفاتيح المحسّن	ITU-T H.235.6	2.6.8
3.6.2.B	تحديث المفتاح وتزامنه استناداً إلى نمط الحمولة النافعة	ITU-T H.235.6	3.6.8
3.B	مصادر RTCP/RTP	ITU-T H.235.6	3.9
1.3.B	متجهات التدميث	ITU-T H.235.6	1.3.9
1.1.3.B	متجهات التدميث CBC	ITU-T H.235.6	1.1.3.9
2.1.3.B	متجهات التدميث في الأسلوب EOFB	ITU-T H.235.6	2.1.3.9
2.3.B	الحشو	ITU-T H.235.6	2.3.9
3.3.B	حماية البروتوكول RTCP	ITU-T H.235.6	3.3.9
4.3.B	تدفق الحمولة النافعة الأمنية	ITU-T H.235.6	4.3.9
5.3.B	التشغيل البيني مع التوصية ITU-T J.170	ITU-T H.235.6	5.3.9
4.B	تشوير/إجراءات RAS للاستيقان	ITU-T H.235.0	3.8
1.4.B	مقدمة	ITU-T H.235.0	–
2.4.B	الاستيقان بين النقطة الطرفية والحارس البوابي (غير قائم على الاشتراك)	ITU-T H.235.0	1.3.8
3.4.B	الاستيقان بين النقطة الطرفية والحارس البوابي (القائم على الاشتراك)	ITU-T H.235.0	2.3.8
1.3.4.B	كلمة السر بالتجفير التناظري	ITU-T H.235.0	1.2.3.8

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
2.3.4.B	كلمة السر مع التظليل	ITU-T H.235.0	2.2.3.8
3.3.4.B	الاستيقان باستعمال الشهادة مع التواقيع	ITU-T H.235.0	3.3.3.8
5.B	التفاعلات غير المطرافية	ITU-T H.235.6	7.8
1.5.B	البوابة	ITU-T H.235.6	1.7.8
6.B	إدارة المفتاح في القناة RAS	ITU-T H.235.0	4.8
7.B	الوظيفة شبه العشوائية (PRF)	ITU-T H.235.0	10
الملحق جيم	**مواضيع خاصة بالتوصية ITU-T H.323**	**ITU-T H.235.0**	**الملحق باء**
الملحق دال	**مواصفة الأمن الأساسي**	**ITU-T H.235.1**	
1.D	مقدمة	ITU-T H.235.1	
2.D	اصطلاحات المواصفة	ITU-T H.235.1	5
3.D	مجال التطبيق	ITU-T H.235.1	1
4.D	المختصرات	ITU-T H.235.1	4
5.D	المراجع المعيارية	ITU-T H.235.1	1.2
6.D	مواصفة الأمن الأساسي	ITU-T H.235.1	
1.6.D	لمحة عامة	ITU-T H.235.1	1.6
1.1.6.D	مواصفة الأمن الأساسي	ITU-T H.235.1	2.6
2.1.6.D	مواصفة الأمن بالتجفير الصوتي	ITU-T H.235.6	1.6
2.6.D	الاستيقان والتكامل	ITU-T H.235.1	1.3
3.6.D	المتطلبات ITU-T H.323	ITU-T H.235.1	3.6
1.3.6.D	لمحة عامة	ITU-T H.235.1	4.6
2.3.6.D	تفاصيل استيقان رسائل التشوير بمفتاح تناظري (الإجراء I)	ITU-T H.235.1	7
3.3.6.D	حساب التظليل القائم على كلمة السر	ITU-T H.235.1	1.7
1.3.3.6.D	الشفرة HMAC-SHA1-96	ITU-T H.235.1	2.7
2.3.3.6.D	الاستيقان والتكامل	ITU-T H.235.1	3.7
3.3.3.6.D	الاستيقان بمفرده (الإجراء IA)	ITU-T H.235.1	8
4.3.6.D	عرض استخدام الإجراء I	ITU-T H.235.1	9
1.4.3.6.D	استيقان الرسالة RAS وتكاملها	ITU-T H.235.1	1.9
2.4.3.6.D	استيقان الرسالة ITU-T H.225.0 وتكاملها	ITU-T H.235.1	2.9
3.4.3.6.D	استيقان الرسالة ITU-T H.245 وتكاملها	ITU-T H.235.1	3.9
4.6.D	سيناريو التسيير المباشر	ITU-T H.235.1	4.9
5.6.D	توفير خدمة طرفية متخصصة	ITU-T H.235.1	10
6.6.D	المواءمة مع السياق H.235 الطبعة 1	ITU-T H.235.1	11
7.6.D	سلوك التوزيع المتعدد	ITU-T H.235.1	12
7.D	مواصفة الأمن بالتجفير الصوتي	ITU-T H.235.6	1.6
1.7.D	إدارة المفتاح	ITU-T H.235.6	5.8
2.7.D	تحديث المفتاح وتزامنه	ITU-T H.235.6	6.8
3.7.D	المعايير 3-DES بالأسلوب CBC الخارجي	ITU-T H.235.6	4.9
4.7.D	خوارزمية المعيار DES العاملة بالأسلوب EOFB	ITU-T H.235.6	5.9

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
5.7.D	تجفير المعيار 3-DES العامل بالأسلوب EOFB الخارجي	ITU-T H.235.6	6.9
8.D	الالتقاط القانوني	ITU-T H.235.6	10
9.D	قائمة برسائل التشوير الأمينة	ITU-T H.235.1	13
1.9.D	الرسالة H.225.0 RAS	ITU-T H.235.1	1.13
2.9.D	تشوير النداء H.225.0	ITU-T H.235.1	2.13
3.9.D	التحكم بالنداء H.245	ITU-T H.235.1	3.13
10.D	استعمال المعرّفين sendersID وgeneralID	ITU-T H.235.1	14
11.D	قائمة معرّفات هوية الغرض	ITU-T H.235.1 ITU-T H.235.6	15 11
12.D	بيبليوغرافيا	ITU-T H.235.1 ITU-T H.235.6	2.2 2.2
الملحق E	**مواصفة الأمن بالتوقيع**	**ITU-T H.235.2**	
1.E	لمحة عامة	ITU-T H.235.2	6
2.E	اصطلاحات المواصفة	ITU-T H.235.2	5
3.E	المتطلبات H.323	ITU-T H.235.2	1.6
4.E	خدمات الأمن	ITU-T H.235.2	5
5.E	التواقيع الرقمية مع تفاصيل أزواج المفاتيح العمومية/الخاصة (الإجراء II)	ITU-T H.235.2	7
6.E	إجراءات المؤتمر متعدد النقاط	ITU-T H.235.2	8
7.E	الاستيقان من طرف إلى طرف (الإجراء III)	ITU-T H.235.2	9
8.E	الاستيقان بمفرده	ITU-T H.235.2	10
9.E	الاستيقان والتكامل	ITU-T H.235.2	11
10.E	حساب التوقيع الرقمي	ITU-T H.235.2	12
11.E	التحقق من التوقيع الرقمي	ITU-T H.235.2	13
12.E	معالجة الشهادات	ITU-T H.235.2	14
13.E	مثال على استعمال الإجراء II	ITU-T H.235.2	15
1.13.E	استيقان الرسائل RAS وتكاملها وعدم نكرانها	ITU-T H.235.2	1.15
2.13.E	استيقان الرسائل RAS فقط	ITU-T H.235.2	2.15
3.13.E	استيقان الرسالة H.225.0 وتكاملها وعدم نكرانها	ITU-T H.235.2	3.15
4.13.E	استيقان الرسالة H.245 وتكاملها	ITU-T H.235.2	4.15
14.E	المواءمة مع البيئة H.235 في الطبعة 1	ITU-T H.235.2	16
15.E	سلوك التوزيع المتعدد	ITU-T H.235.2	17
16.E	قائمة برسائل التشوير الأمينة	ITU-T H.235.2	18
1.16.E	الرسالة H.225.0 RAS	ITU-T H.235.2	1.18
2.16.E	تشوير النداء H.225.0	ITU-T H.235.2	2.18
17.E	استعمال المعرّفين sendersID وgeneralID	ITU-T H.235.2	19
18.E	قائمة معرّفات هوية الغرض	ITU-T H.235.2	20
التذييل IV (الملحق E)	بيبليوغرافيا	ITU-T H.235.2	2.2

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
الملحق F	**مواصفة الأمن الهجينة**	**ITU-T H.235.3**	
1.F	لمحة عامة	ITU-T H.235.3	6
2.F	المراجع المعيارية	ITU-T H.235.3	1.2
3.F	المختصرات	ITU-T H.235.3	4
4.F	اصطلاحات المواصفة	ITU-T H.235.3	5
5.F	المتطلبات ITU-T H.323	ITU-T H.235.3	1.6
6.F	الاستيقان مع التكامل	ITU-T H.235.3	2.6
7.F	الإجراء IV	ITU-T H.235.3	7
8.F	تجميع الأمن لأغراض النداءات المتآونة	ITU-T H.235.3	8
9.F	تحديث المفتاح	ITU-T H.235.3	9
10.F	أمثلة مع مخططات إيضاحية	ITU-T H.235.3	11
11.F	سلوك التوزيع المتعدد	ITU-T H.235.3	12
12.F	قائمة رسائل تشوير الأمن	ITU-T H.235.3	13
1.12.F	الرسالة RAS ITU-T H.225.0	ITU-T H.235.3	1.13
2.12.F	تشوير النداء ITU-T H.225.0 (مجال إداري وحيد)	ITU-T H.235.3	2.13
3.12.F	تشوير النداء ITU-T H.225.0 (عدة مجالات إدارية)	ITU-T H.235.3	3.13
13.F	قائمة بمعرّفات هويات الأغراض	ITU-T H.235.3	14
التذييل IV	ببيليوغرافيا	ITU-T H.235.3	2.2
الملحق G	**استعمال بروتوكول النقل الأمين في الوقت الفعلي (SRTP) مع بروتوكول إدارة مفتاح MIKEY في إطار التوصية ITU-T H.235**	**ITU-T H.235.7**	
1.G	مجال التطبيق	ITU-T H.235.7	1
2.G	المراجع	ITU-T H.235.7	2
1.2.G	المراجع المعيارية	ITU-T H.235.7	1.2
2.2.G	المراجع الإعلامية	ITU-T H.235.7	2.2
3.G	المصطلحات والتعاريف	ITU-T H.235.7	3
4.G	الرموز والمختصرات	ITU-T H.235.7	4
5.G	اصطلاحات المواصفة	ITU-T H.235.7	5
6.G	مقدمة	ITU-T H.235.7	6
7.G	لمحة عامة وسيناريوهات	ITU-T H.235.7	7
1.7.G	تنفيذ بروتوكولات MIKEY عند "سوية الدورة"	ITU-T H.235.7	1.7
2.7.G	تنفيذ بروتوكولات MIKEY عند "سوية الوسائط"	ITU-T H.235.7	2.7
3.7.G	التفاوض بشأن مقدرات MIKEY	ITU-T H.235.7	3.7
8.G	مواصفة أمن تستخدم تقنيات الأمن التناظري	ITU-T H.235.7	8
1.8.G	إنهاء نداء H.323	ITU-T H.235.7	1.8
2.8.G	إعادة حساب مفتاح TGK وتحديث CSB	ITU-T H.235.7	2.8
3.8.G	دعم الأنفاق H.245	ITU-T H.235.7	3.8
4.8.G	خوارزميات SRTP	ITU-T H.235.7	4.8
5.8.G	قائمة بمعرّفات هويات الأغراض	ITU-T H.235.7	5.8
9.G	مواصفة أمن تستخدم تقنيات الأمن التناظري	ITU-T H.235.7	9

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
1.9.G	إنهاء نداء H.323	ITU-T H.235.7	1.9
2.9.G	إعادة حساب مفتاح TGK وتحديث CSB	ITU-T H.235.7	2.9
3.9.G	دعم الأنفاق H.245	ITU-T H.235.7	3.9
4.9.G	خوارزميات SRTP	ITU-T H.235.7	4.9
5.9.G	قائمة بمعرّفات هويات الأغراض	ITU-T H.235.7	5.9
I.G	خيار MIKEY-DHHMAC	ITU-T H.235.7	التذييل I
1.I.G	إنهاء نداء ITU-T H.323	ITU-T H.235.7	1.I
2.I.G	إعادة حساب مفتاح TGK وتحديث CSB	ITU-T H.235.7	2.I
II.G	استعمال الملحق I من التوصية H.235 لإقامة سر متقاسم مسبقاً	ITU-T H.235.7	التذييل II
1.II.G	إنهاء نداء H.323	ITU-T H.235.7	1.II
2.II.G	إعادة حساب مفتاح TGK وتحديث CSB	ITU-T H.235.7	2.II
الملحق H	**إدارة المفتاح RAS**	**ITU-T H.235.5**	
1.H	مقدمة	ITU-T H.235.5	–
2.H	مجال التطبيق	ITU-T H.235.5	1
3.H	المراجع	ITU-T H.235.5	2
1.3.H	المراجع المعيارية	ITU-T H.235.5	1.2
2.3.H	المراجع الإعلامية	ITU-T H.235.5	2.2
4.H	التعاريف	ITU-T H.235.5	3
5.H	المختصرات	ITU-T H.235.5	4
6.H	إطار أساسي	ITU-T H.235.5	6
1.6.H	مقدرات تفاوض محسنة في ITU-T H.235v3	ITU-T H.235.5	1.6
2.6.H	الاستعمال بين النقطة الطرفية وحارس البوابة	ITU-T H.235.5	2.6
3.6.H	استعمال المواصفة بين حراس البوابات	ITU-T H.235.5	3.6
4.6.H	تجفير واستيقان قناة التشوير	ITU-T H.235.5	4.6
7.H	مواصفة أمن خاصة (SP1)	ITU-T H.235.5	7
8.H	تمديدات الإطار (للإعلام)	ITU-T H.235.5	9
1.8.H	استعمال المفتاح الرئيسي لحماية قناة تشوير النداء عبر بروتوكول TLS	ITU-T H.235.5	1.9
1.1.8.H	تسجيل النقطة الطرفية	ITU-T H.235.5	1.1.9
2.8.H	استعمال الشهادات من حارس البوابة	ITU-T H.235.5	2.9
3.8.H	استعمال آليات بديلة خاصة بأمن التشوير	ITU-T H.235.5	3.9
9.H	تهديدات (للإعلام)	ITU-T H.235.5	10
1.9.H	هجمات منفعلة	ITU-T H.235.5	1.10
2.9.H	هجمات تستهدف وظيفة رفض الخدمة	ITU-T H.235.5	2.10
3.9.H	هجمات المعترض	ITU-T H.235.5	3.10
4.9.H	توقع الهجمات	ITU-T H.235.5	4.10
5.9.H	نصف مفتاح غير مجفر لحارس البوابة	ITU-T H.235.5	5.10
الملحق I	**دعم النداءات ذات التسيير المباشر**	**ITU-T H.235.4**	
1.I	مجال التطبيق	ITU-T H.235.4	1

الجدول 1.IV – تقابل الفقرات

الفقرة ITU-T H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الفقرة
2.I	مقدمة	ITU-T H.235.4	6
3.I	اصطلاحات المواصفة	ITU-T H.235.4	5
4.I	المصطلحات والتعاريف	ITU-T H.235.4	3
5.I	الرموز والمختصرات	ITU-T H.235.4	4
6.I	المراجع المعيارية	ITU-T H.235.4	2
7.I	لمحة عامة	ITU-T H.235.4	7
8.I	القيود	ITU-T H.235.4	8
9.I	الإجراء DRC	ITU-T H.235.4	9
10.I	إجراء الحصول على المفتاح بواسطة وظيفة PRF	ITU-T H.235.4	12
11.I	إجراء حساب المفتاح باستعمال المعيار FIPS-140	ITU-T H.235.4	13
12.I	قائمة بمعرّفات هويات الأغراض	ITU-T H.235.4	14
التذييل I (الملحق I)	بيبليوغرافيا	ITU-T H.235.4	2.2

التذييل V

تقابل أشكال ITU-T H.235v3Amd1Cor1
وتوصيات السلسلة الفرعية ITU-T H.235v4

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يبين هذا التذييل الإعلامي مواقع جميع أشكال ITU-T H.235v3Amd1Cor1 في توصيات السلسلة الفرعية ITU-T H.235v4.

الجدول H.235.0/1.V – تقابل الأشكال

الشكل ITU-T H.235v3Amd1Cor1 C	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الشكل
الشكل 1	تبادل بأسلوب ديفي–هيلمان مع الاستيقان الخياري	ITU-T H.235.0	4
الشكل 2a	استيقان باستعمال كلمة السر مع التظليل؛ ممران	ITU-T H.235.0	5
الشكل 2b	استيقان باستعمال كلمة السر مع التظليل؛ ثلاثة ممرات	ITU-T H.235.0	6
الشكل 3a	كلمة السر مع التظليل، ممران	ITU-T H.235.0	7
الشكل 3b	كلمة السر مع التظليل، ثلاثة ممرات	ITU-T H.230.0	8
الشكل 4a	الاستيقان باستعمال شهادة بتوقيع؛ ممران	ITU-T H.235.0	9
الشكل 4b	الاستيقان باستعمال شهادة بتوقيع؛ ثلاثة ممرات	ITU-T H.235.0	10
الشكل 5	تجفير الوسائط	ITU-T H.235.6	7
الشكل 6	إزالة تجفير الوسائط	ITU-T H.235.6	8
الشكل 7	نسق رزم RTP لحماية الوسائط من الإغراق	ITU-T H.235.6	9
الشكل 1.I	استعارة نص تجفير في أسلوب ECB	ITU-T H.235.6	1.I
الشكل 2.I	استعارة نص تجفير في أسلوب CBC	ITU-T H.235.6	2.I
الشكل 2a.I	حشو الأصفار في أسلوب CBC	ITU-T H.235.6	3.I
الشكل 3.I	حشو الأصفار في أسلوب CFB	ITU-T H.235.6	4.I
الشكل 4.I	حشو الأصفار في أسلوب OFB	ITU-T H.235.6	5.I
الشكل 1.4.I	أسلوب EOFB مع حشو الأصفار	ITU-T H.235.6	6.I
الشكل 5.I	الحشو الذي يقضي البروتوكول RTP باستعماله	ITU-T H.235.6	7.I
الشكل 6.I	العلامات	ITU-T H.235.0	1.I
الشكل 7.I	سيناريو مع مخدم مختص	ITU-T H.235.0	2.I
الشكل 1.B	لمحة عامة	ITU-T H.235.0	2
الشكل 1.1.B	توزيع/تحديث مفاتيح الدورة الرئيسية للقائد نحو المنقاد أو المنقادين	ITU-T H.235.6	4
الشكل 2.1.B	تحديث مفتاح الدورة على القناة المنطقية للمنقاد	ITU-T H.235.6	5
الشكل 3.1.B	تحديث مفتاح الدورة على القناة المنطقية للقائد	ITU-T H.235.6	6
الشكل 2.B	كلمة السر مع تجفير تناظري	ITU-T H.235.0	11
الشكل 3.B	كلمة السر مع التظليل	ITU-T H.235.0	12
الشكل 4.B	الاستيقان بواسطة شهادة مع تواقيع	ITU-T H.235.0	13
1.D	توضيح استخدام الإجراء I في سيناريو حارس البوابة إلى حارس البوابة، مع وجود النقطتين الطرفيتين في مناطق تسيير حراس البوابات	ITU-T H.235.1	1

الجدول H.235.0/1.V – تقابل الأشكال

الشكل ITU-T H.235v3Amd1Cor1 C	العنوان	توصية السلسلة الفرعية ITU-T H.235v4.x	الشكل
الشكل 2.D	توضيح استخدام الإجراء I في سيناريو مختلط مع وجود النقطة الطرفية 1 في منطقة تسيير حارس البوابة والنقطة الطرفية 2 في منطقة بتسيير مباشر	ITU-T H.235.1	2
الشكل 3.D	توضيح استخدام الإجراء I بالنسبة إلى سيناريو توجد فيه النقطتان الطرفيتان في مناطق تستعمل حارسا بوابياً بتسيير مباشر	ITU-T H.235.1	3
الشكل 4.D	تجفير 3-DES في أسلوب CBC خارجي	ITU-T H.235.6	10
الشكل 5.D	تجفير 3-DES في أسلوب EOFB خارجي	ITU-T H.235.6	11
الشكل 1.E	الاستعمال الآني من قفزة إلى قفزة والاستيقان من طرف إلى طرف	ITU-T H.235.2	1
الشكل 2.E	مثال على استعمال المفاتيح العمومية في نموج مسير من حارس البوابة إلى حارس البوابة	ITU-T H.235.2	2
الشكل 1.F	جمع الأمن فيما يتعلق بالنداءات المتلازمة	ITU-T H.235.3	1
الشكل 2.F	مخطط تدفق الرسائل في مجال إداري وحيد	ITU-T H.235.3	2
الشكل 3.F	مخطط تدفق الرسائل في عدة مجالات إدارية	ITU-T H.235.3	3
الشكل 1.G	سيناريو	ITU-T H.235.7	1
الشكل 2.G	سيناريو الأمن مع MIKEY وSRTP	ITU-T H.235.7	2
الشكل 3.G	سيناريو من قفزة إلى قفزة مع الأسرار المتقاسمة فحسب	ITU-T H.235.7	3
الشكل 4.G	مثال على نداء النقطة الطرفية B للنقطة الطرفية A (تسيير بواسطة حارس البوابة) مع MIKEY-PS	ITU-T H.235.7	4
الشكل 5.G	معالجة MIKEY-PS بواسطة النقطة الطرفية B	ITU-T H.235.7	5
الشكل 6.G	معالجة MIKEY-PS بواسطة النقطة الطرفية B	ITU-T H.235.7	6
الشكل 7.G	مثال على إنهاء النقطة الطرفية B للنداء	ITU-T H.235.7	7
الشكل 8.G	مثال على تحديث النقطة الطرفية B للنداء	ITU-T H.237.7	8
الشكل 9.G	سيناريو من طرف إلى طرف مع بنية تحتية PKI (عدة حراس للبوابات)	ITU-T H.235.7	9
الشكل 10.G	مثال على نداء النقطة الطرفية B للنقطة الطرفية A (تسيير بواسطة عدة حراس للبوابات) مع MIKEY-PK-SIGN	ITU-T H.235.7	10
الشكل 11.G	معالجة MIKEY-PK-SIGN بواسطة النقطة الطرفية B	ITU-T H.235.7	11
الشكل 12.G	معالجة MIKEY-PK-SIGN بواسطة النقطة الطرفية A	ITU-T H.235.7	12
الشكل 13.G	مثال على إنهاء النقطة الطرفية B للنداء	ITU-T H.235.7	13
الشكل 14.G	مثال على شروع النقطة الطرفية B (مدمث) في إعادة حساب مفتاح TGK وتحديث CBS	ITU-T H.235.7	14
الشكل 1-I.G	مثال على نداء النقطة الطرفية B للنقطة الطرفية A (تسيير بواسطة حراس البوابات) مع MIKEY-DHHMAC	ITU-T H.235.7	1.I
الشكل 2-I.G	مثال على إنهاء النقطة الطرفية B للنداء	ITU-T H.235.7	2.I
الشكل 3-I.G	مثال على تحديث النقطة الطرفية B للمفتاح	ITU-T H.235.7	3.I
الشكل 1-II.G	مثال على نداء النقطة الطرفية B للنقطة الطرفية A (تسيير دون حارس البوابة) مع MIKEY-PS والإجراء DRC1 للتوصية H.235.4	ITU-T H.235.7	1.II
الشكل 1.H	تدفق المعلومات بالنسبة إلى مواصفة الأمن والبروتوكول TLS	ITU-T H.235.5	1
الشكل 1.I	سيناريو نداء بتسيير مباشر	ITU-T H.235.4	1
الشكل 2.I	تدفق الاتصالات الأساسية	ITU-T H.235.4	2

التذييل VI

تقابل بين جداول ITU-T H235v3Amd1Cor1
وجداول توصيات السلسلة الفرعية ITU-T H.235v4

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يبين هذا التذييل الإعلامي مواقع كل جداول ITU-T H.235v3Amd1Cor1 في توصيات السلسة الفرعية ITU-T H.235v4.

الجدول VI.1 – تقابل الجداول

الجدول H.235v3Amd1Cor1	العنوان	توصية السلسلة الفرعية H.235v4.x	الجدول
الجدول 1	معرف هوية الغرض بالنسبة إلى التجفير NULL	ITU-T H.235.6	2
الجدول 2	معرفات هويات الأغراض بالنسبة إلى تجفير الإشارات DTMF ITU-T H.245	ITU-T H.235.6	3
الجدول 3	معرفات هويات الأغراض المستعملة للحماية من الإغراق	ITU-T H.235.6	5
الجدول 1.I	معرفات هويات الأغراض المستعملة في الجزء 6.4.I	ITU-T H.235.0	1.I
الجدول 1.D	ملخص مواصفات الأمن للملحق D	–	–
الجدول 2.D	مواصفة الأمن الأساسي	ITU-T H.235.1	1
الجدول 3.D	مواصفة التجفير الصوتي	ITU-T H.235.6	1
الجدول 4.D	مجموعات ديفي–هيلمان	ITU-T H.235.6	4
الجدول 5.D	استعمال معرفي الهوية sendersID وgeneralID	ITU-T H.235.1	2
الجدول 6.D	معرفات هويات الأغراض المستعملة في الملحق D	ITU-T H.235.1 ITU-T H.235.6	3 6
الجدول 1.E	مواصفة التوقيع الأمني	ITU-T H.235.2	1
الجدول 2.E	استعمال معرفي الهوية sendersID وgeneralID	ITU-T H.235.2	2
الجدول 3.E	معرفات هويات الأغراض المستعملة في الملحق E	ITU-T H.235.2	3
الجدول 1.F	لمحة عامة عن مواصفة الأمن الهجين	ITU-T H.235.3	1
الجدول 2.F	معرفات هويات الأغراض المستعملة في الملحق F	ITU-T H.235.3	2
الجدول 1.G	بروتوكولات إدارة مفتاح MIKEY	ITU-T H.235.7	1
الجدول 1.H	عناصر المواصفة	ITU-T H.235.5	1
الجدول 0.I	حساب مفاتيح التجفير والتمليح انطلاقاً من سر متقاسم	ITU-T H.235.4	1
الجدول 1.I	معرفات هويات الأغراض المستعملة في الملحق ITU-T H.235/4	ITU-T H.235.4	2

بيبليوغرافيا

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

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

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

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

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

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

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

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	**الأنظمة السمعية المرئية والأنظمة متعددة الوسائط**
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	البنية التحتية العالمية للمعلومات، وجوانب بروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2017