الاتحـــــاد الـــدولـــــي للاتصـــــــالات

ITU-T H.235.2

(2005/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة H: الأنظمة السمعية المرئية وتعدد الوسائط

البنية التحتية للخدمات السمعية المرئية – جوانب الأنظمة

أمن H.323: مواصفة الأمن بالتواقيع

التوصيـــة ITU-T H.235.2

الاتحاد الدولي للاتصالات

توصيات السلسلة H الصادرة عن قطاع تقييس الاتصالات

الأنظمة السمعية المرئية وتعدد الوسائط

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

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

أمن H.323: مواصفة الأمن بالتواقيع

ملخص

تتضمن هذه التوصية مواصفة أمن اختيارية من أجل استعمال التواقيع الرقمية لتأمين تشوير H.225.0

وفي طبعات سابقة للسلسلة الفرعية H.235، كانت هذه المواصفة متضمنة في الملحق E، H.235. وتبين التذييلات IV وV وVI للتوصية H.235.0 التقابل الكامل في الفقرات والأرقام والجداول بين الطبعتين 3 و4 من التوصية H.235.

المصدر

وافقت لجنة الدراسات 16 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 13 سبتمبر 2005 على التوصية ITU-T H.235.2 بموجب الإجراء المحدد في التوصية A.8.

كلمات أساسية

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

تمهيـــد

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

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

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

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

أمن H.323: مواصفة الأمن بالتواقيع

1 مجال التطبيق

تصف هذه التوصية مواصفة أمن اختيارية من أجل استعمال التواقيع الرقمية لتأمين تشوير H.225.0

2 المراجع

1.2 المراجع المعيارية

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

- التوصية ITU-T H.225.0 (2003)، *بروتوكولات تشوير النداء ووضع قطار متعدد الوسائط في الرزم لأغراض أنظمة الوسائط المتعددة العاملة بأسلوب الرزم.*
- التوصية ITU-T H.235 (1998)، *أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من النمط H.245).*
- التوصية ITU-T H.235.0 (2005)، *الأمن بمقتضى التوصية H.323: هيكلية الأمن في أنظمة تعدد الوسائط في السلسلة H (H.323 وأخرى على أساس H.245).*
- التوصية ITU-T H.235.1 (2005)، *الأمن بمقتضى التوصية H.323: مواصفة أمن خط الأساس.*
- التوصية ITU-T H.235.6 (2005)، *أمن H.323: مواصفة التجفير الصوتي مع إدارة مفاتيح H.235/H.245 الأصلية.*
- التوصية ITU-T H.245 (2005)، *بروتوكول التحكم لأغراض الاتصالات متعددة الوسائط.*
- التوصية ITU-T H.323 (2003)، *أنظمة الاتصالات متعددة الوسائط بأسلوب الرزم.*
- التوصية ITU-T Q.931 (1998)، *مواصفات الطبقة 3 من السطح البيني بين المستعمل وشبكة ISDN للتحكم بالنداء الأساسي.*
- التوصية ITU-T X.509 (2005) | المعيار ISO/IEC 9594-8:2005، *تكنولوجيا المعلومات– التوصيل البيني للأنظمة المفتوحة– الدليل: أطر التصديق العمومية الرئيسية وتصديق النعوت.*
- التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.*
- التوصية ITU-T X.803 (1994) | المعيار ISO/IEC 10745:1995، *تكنولوجيا المعلومات– التوصيل البيني للأنظمة المفتوحة– نموذج الأمن في الطبقات العليا.*
- التوصية ITU-T X.810 (1995) | المعيار ISO/IEC 10181-1:1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – هيكليات الأمن للأنظمة المفتوحة – نظرة عامة.*

– التوصية ITU-T X.811 (1995) | المعيار ISO/IEC 10181-2:1996، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – هيكليات الأمن للأنظمة المفتوحة – هيكلية الاستيقان.*

– المعيار ISO/IEC 9798-3:1998، *تكنولوجيا المعلومات – تقنيات الأمن – استيقان الكيانات – الجزء 3: آليات تستخدم تقنيات التوقيع الرقمي.*

– IETF RFC 3280 (2002)، *شهادة هيكلية المفاتيح العمومية X.509 للإنترنت ومواصفة قائمة إبطال الشهادات (CRL).*

2.2 المراجع البحثية

[ISO/IEC 14888-3] ISO/IEC 14888-3:1998، *تكنولوجيا المعلومات – تقنيات الأمن – التواقيع الرقمية مع التذييل الجزء 3: آليات قائمة على الشهادات.*

[PKCS] PKCS #1 v2.0: *معيار تجفير RSA؛* مختبرات *RSA؛* 1 اكتوبر 1998؛ http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *معيار تجفير تركيب الرسائل،* مذكرة تقنية صادرة عن مختبرات RSA، الإصدار 1.5، منقح في 1 نوفمبر 1993؛ http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[RFC1321] IETF RFC 1321 (1992)، *خوارزمية تمثل الرسائل MD5.*

[RFC3447] IETF RFC 3447 (2003)، *معايير تجفير المفاتيح العمومية (PKCS) رقم 1: الإصدار 2.1 من مواصفة تجفير RSA.*

3 المصطلحات والتعاريف

لأغراض هذه التوصية، تنطبق التعاريف الواردة في الفقرات 3/H.323 و3/H.225.0 و3/H.245 جنباً إلى جنب التعاريف الواردة في هذه الفقرة. وبعض المصطلحات المستخدمة في هذه التوصية معرَّفة أيضاً في توصيات قطاع تقييس الاتصالات X.800 | ISO 7498-2 وX.803 | ISO/IEC 10745 وX.810 | ISO/IEC 10181-1 وISO/IEC 10181-2 | X.811.

1.3 سلطات إصدار الشهادات: سلطات إصدار الشهادات (CAs) تضطلع، عندما تُستخدم في سياق التوقيع الإلكتروني باعتماد، مفاتيح التحقق العمومية من خلال إصدار "شهادات".

2.3 إدارات محفوظات الشهادات: تضم إدارات محفوظات الشهادات (مثلاً الدليل X.500) شهادات المستعمِلين وقوائم الشهادات الملغاة (CRLs). وهي موثوقة من حيث توفير سبل النفاذ إلى تلك المعلومات ولكنها ليست مسؤولة عن محتوى المعلومات التي تتلقاها من سلطات إصدار الشهادات (CAs) أو من سلطات التسجيل، ولا عن دقة هذه المعلومات.

3.3 التوقيع الرقمي: هو تحويل تجفيري (يستخدم تقنية تجفيرية تناظرية) للتمثيل الرقمي لرسالة معطيات بحيث يمكن لأي شخص يحوز الرسالة الموقَّعة والمفتاح العمومي ذي الصلة أن يحدد:

i) أن التحويل أُنشئ باستعمال مفتاح خاص مماثل للمفتاح العمومي ذي الصلة؛ و

ii) أن الرسالة الموقَّعة لم تغيَّر منذ التحويل المجفَّر.

4.3 مقدمو الوضع القانوني للشهادة على الخط: يمكِّن بروتوكول الوضع القانوني للشهادة على الخط (OCSP) التطبيقات من تحديد حالة إلغاء شهادة معرَّفة. ويمكن استخدام البروتوكول OCSP لتلبية بعض المتطلبات التشغيلية المتمثلة في توفير معلومات خاصة بالإلغاء على نحو زمني أنسب مما يمكن تحقيقه مع قوائم الشهادات الملغاة. ويمكن اعتبار مقدمو الوضع القانوني للشهادة على الخط بمثابة بديل عن استعمال قوائم الشهادات الملغاة خارج الخط.

5.3 المخدِّم الوكيل: المخدِّم الوكيل هو كيان H.323 وسيط مماثل للحارس البوابي. ويمكن للمخدِّم الوكيل أن يكون عقدة شبكة منفصلة أو أن يكون واقعاً في نفس الموقع الوظيفي لكيان H.323 من مثل الحارس البوابي. ويمكن للمخدم الوكيل أن يؤدي مهام أمنية من مثل التوقيع والتحقق من صلاحية الشهادة والتحكم في النفاذ.

6.3 سلطات التسجيل: تعمل سلطات التسجيل باعتبارها سلطات وسيطة بين المستعملين وسلطات إصدار الشهادات. وهي تتلقى الطلبات من المستعملين وتحيلها إلى سلطات إصدار الشهادات في نسق ملائم.

7.3 سلطات تسجيل الوقت: سلطات تسجيل الوقت إلزامية بالنسبة لعدم الإنكار في حالة فقدان المفتاح أو إتلافه. وهي توفر في الممارسة توقيعاً مصدَّقاً عليه لأي كان بما في ذلك وقت موثوق على قيمة تظليل ومعرِّف تظليل.

8.3 مقدِّم خدمة موثوقة: هو كيان يمكن أن تستخدمه كيانات أخرى كوسيط موثوق في عملية اتصال أو تحقق، أو كمقدم خدمة معلومات موثوقة.

وتستخدم هذه التوصية المصطلحات التالية من أجل توفير خدمات الأمن.

9.3 الاستيقان بمفرده: تدعِّم خدمة الأمن هذه لمواصفة الأمن بالتواقيع استيقان المستعمِل حيث يستيقن المستعمِل بالتوقيع الرقمي السليم بعض أجزاء المعطيات بواسطة المفتاح الخاص. ويلاحظ أن هذه الخدمة الأمنية لا توفر توقيعات مصدَّق عليها في حالات استخدام القص واللصق التعسفيين، أو التلاعب بالرسائل أو الهجمات بالتلاعب. ويمكن أن يكون الاستيقان بمفرده مفيداً لمخدِّمات الأمن الوكيلة التي تتحقق من استيقان الرسالة (استيقان أصل المعطيات) عند إرسال الرسالة إلى مقصد آخر (مثلاً، الحارس البوابي).

ملاحظة – يغيِّر الإرسال في العادة بعض أجزاء الرسالة؛ ومن ثم لا يمكن تحقيق التكامل من طرف إلى طرف.

وعلى الرغم من ذلك، يمكن تطبيق الاستيقان بمفرده على أساس قفزة قفزة أيضاً. ويحدد الإجراء III خدمة الأمن هذه بالنسبة لسيناريو من طرف إلى طرف في حين يحدد الإجراء II خدمة الأمن هذه بالنسبة لحالة القفزة قفزة.

10.3 الاستيقان والتكامل: هذه خدمة أمنية مزدوجة توفّر تكامل الرسالة بالاقتران مع استيقان المستعمل. ويُستيقن المستعمل عندما يوقع رقمياً على نحو صحيح بعض المعطيات بالمفتاح الخاص. وبالإضافة إلى ذلك تُحمى الرسالة من التلاعب. وتوفر آلية الأمن ذاتها خدمتي الأمن على السواء. ولا يمكن تحقيق الاستيقان أو التكامل معاً إلا على أساس قفزة قفزة. ويحدد الإجراء II هذه الخدمة الأمنية.

ملاحظة – عندما تطبَّق التواقيع الرقمية، يمكن توفير خدمة أمن عدم إنكار؛ وتتوقف هذه الخدمة أيضاً على قيمة بتات استعمال مفتاح التوقيع في الشهادة (انظر أيضاً RFC 3280).

4 الرموز والمختصرات

تستعمل هذه التوصية المختصرات التالية:

ARQ طلب القبول *(Admission Request)*

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

CA سلطة إصدار الشهادة *(Certification Authority)*

CRL قائمة بالشهادات الملغاة *(Certificate Revocation List)*

DH "ديفي هيلمان" *(Diffie-Hellman)*

DNS أسماء الميادين *(Domain Name Service)*

EP نقطة طرفية *(Endpoint)*

EPID معرِّف هوية نقطة طرفية *(Endpoint Identifier)*

GK حارس بوابي *(Gatekeeper)*

GKID معرِّف هوية حارس بوابي *(Gatekeeper Identifier)*

GRQ طلب حارس بوابي *(Gatekeeper Request)*

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

IP بروتوكول الإنترنت *(Internet Protocol)*

ITU الاتحاد الدولي للاتصالات *(International Telecommunication Union)*

LDAP البروتوكول السريع للنفاذ إلى الدليل *(Light-weight Directory Access Protocol)*

LRQ طلب تحديد الموقع *(Location Request)*

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

MD5 ملخص الرسالة رقم 5 *(Message Digest 5)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

OID معرف هوية غرض *(Object Identifier)*

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

PKCS نظام تجفير بمفتاح عمومي *(Public-Key Crypto System)*

RA سلطة التسجيل *(Registration Authority)*

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

RSA خوارزمية ريفست وشامير وأدلمان بالمفتاح العمومي *(Rivest, Shamir, Adleman)*

RTP بروتوكول النقل بالوقت الفعلي *(Real-Time Protocol)*

SHA خوارزمية تظليل أمين *(Secure Hash Algorithm)*

URL موقع الموارد الموحد *(Uniform Resource Locator)*

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

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

ويمكن لمواصفة الأمن بالتواقيع أن تستخدم **مواصفة الأمن بالتجفير الصوتي** H.235.1 لتحقيق السرية الصوتية إذا لزم ذلك.

ويحدد الإجراءان II وIII كيفية تطبيق خدمات الأمن لسيناريوهات مختلفة من مثل سيناريوهات قفزة قفزة وطرف إلى طرف مع آليات أمن مختلفة من مثل تقنيات التجفير اللاتناظري (التوقيع الرقمي).

ولئن كانت خدمة تكامل الرسائل توفر دائماً استيقان الرسائل فإن العكس ليس صحيحاً دائماً. وبالنسبة لأسلوب الاستيقان بمفرده، فإن التكامل المؤمَّن يمتد فقط على مجموعة فرعية معينة من مجالات الرسالة. وينطبق هذا على خدمات التكامل التي يتم تحقيقها بوسائل لا تناظرية (مثلاً التواقيع الرقمية). وهكذا وفي التطبيق تَستعمل خدمة الاستيقان والتكامل المزدوجة معطيات المفتاح ذاتها دون أن تُحدث ضعفاً أمنياً.

وبالإضافة إلى ذلك فإن جميع معلومات الأمن قفزة قفزة توضع في المجال **CryptoSignedToken**. ويعاد حساب هذه المعلومات عند كل قفزة وفقاً للإجراء II.

ومن ناحية أخرى، وبصفة أساسية، تُحسب معلومات الأمن من طرف إلى طرف (ممكنة فقط عند استعمال المخدّم الوكيل H.323 والإجراء III) معلومات مماثلة للمعلومات الموضوعة في المجال **CryptoSignedToken** لكنها تخزن تلك المعلومات في

فيشة **CryptoToken** منفصلة للرسالة. ولا تتغير هذه المعلومات أثناء العبور. ويتيح معرِّف غرض منفصل التمييز بين الفيشة **CryptoTokens** قفزة قفزة، والفيشة ذاتها من طرف إلى طرف.

ويمكن تطبيق التقنيات اللاتناظرية التي تستعمل التواقيع الرقمية على أساس قفزة قفزة و/أو على أساس طرف إلى طرف.

6 لمحة عامة

تصف هذه التوصية مواصفة أمن بتواقيع رقمية مقترحة كخيار من أجل استخدام التواقيع الرقمية لتأمين تشوير H.225.0. وتستطيع كيانات الأمن H.323 (المطاريف، الحارسات البوابية، البوابات، الوحدات MCU وغيرها) تطبيق مواصفة الأمن بالتواقيع هذه بهدف تحسين الأمن أو توفيره عند الحاجة.

وتفرض مواصفة الأمن بالتواقيع استعمال نموذج التسيير عبر الحارس البوابي على نحو إلزامي وهو نموذج يستند إلى تقنيات التسيير النفقي H.245؛ ويتطلب توفير نماذج مختلفة عن تلك المسيّرة عبر الحارسات البوابية مزيداً من الدراسة.

وتطبق مواصفة الأمن بالتواقيع على المهاتفة IP "العالمية" القابلة للقياس؛ وتتغلب مواصفة الأمن هذه على التقييدات التي تتسم بها مواصفة الأمن البسيطة الأساسية H.235.1. على سبيل المثال لا ترتبط مواصفة أمن التواقيع بإدارة الأسرار المتقاسمة المتبادلة للقفزات في مختلف الميادين. وتؤمن التسيير النفقي للرسائل H.245 لأغراض تكاملها وتوفر أيضاً أحكاماً تتعلق بعدم نكران الرسائل. وبذلك تقدم مواصفة الأمن بالتواقيع الأمن قفزة قفزة والاستيقان الحقيقي من طرف إلى طرف مع الاستعمال المتآون للمخدمات الوكيلة H.235 أو للحارسات البوابية الوسيطة.

والخصائص التي تقدمها هذه المواصفات بالنسبة إلى الرسائل RAS وH.225.0 وH.245، هي التالية:

- استيقان المستعمل لدى كيان مرغوب بغض النظر عن عدد قفزات الرسالة في التطبيق.

  الملاحظة 1 – تُفهم نقطة "Hop" "قفزة" هنا بمعنى عنصر شبكة H.235 موثوق (مثلاً حارس بوابي، بوابة، وحدة التحكم متعددة النقاط، مخدّم وكيل، حائط الحماية) ومن ثم، فإن الأمن من خلال القفزة قفزة في التطبيق، لا يوفر، عندما يُستعمل مع تقنيات تناظرية، أمناً حقيقياً بين المطاريف من طرف إلى طرف.
- تكامل جميع الأجزاء الهامة (المجالات) من الرسائل الواصلة إلى كيان ما، بمعزل عن عدد قفزات الرسالة في التطبيق. ويقترح أن يكون تكامل الرسالة ذاتها التي يتم الحصول عليها بواسطة عدد عشوائي قوي خياراً ممكناً.
- يوفر استيقان الرسالة قفزة قفزة في التطبيق؛ والتكامل وعدم النكران خدمات الأمن هذه لمحمل الرسالة؛
- يمكن أيضاً توفير عدم نكران الرسائل التي يتم تبادلها بين كيانين بصرف النظر عن عدد قفزات الرسالة في مستوى التطبيق التي تعبرها الرسالة. وبشكل أدق يتوفر عدم النكران للأجزاء الهامة (المجالات) من الرسالة. كما هو الحال على سبيل المثال عندما ترسل نقطة طرفية ما رسالة SETUP إلى حارسها البوابي وبينما يفصل بينهما (النقطة EP والحارس البوابي GK) عدة مخدمات وكيلة.

ويتوفر التصدي الصحيح لاعتداءات مختلفة بواسطة خدمات الأمن الواردة فيما يلي، وهي:

- الاعتداءات التي تستهدف وظيفة رفض الخدمة: باستطاعة التحقق السريع من التواقيع الرقمية توفير الوقاية من مثل هذه الاعتداءات؛
- اعتداءات داخل على الخط: يحمي إجراءا الاستيقان وتكامل الرسالة قفزة قفزة في التطبيق من مثل هذه الاعتداءات التي تحصل عند دخول شخص على الخط بين قفزة تطبيقية ومسيّر معاد، مثلاً. وعندما يكون الداخل كياناً تطبيقياً، يمنع وجود استيقان المستعمل والتكامل من طرف إلى طرف بالنسبة إلى الأجزاء المنتقاة من الرسالة، مثل هذه الاعتداءات؛
- الاعتداءات التكرارية: يحمي استخدام طابعات الوقت وأرقام التتابع من مثل هذه الاعتداءات؛
- الخداع: يحمي استيقان المستعمل من مثل هذه الاعتداءات؛
- اختطاف التوصيل: يمنع استعمال الاستيقان/التكامل لكل رسالة تشوير مثل هذه الاعتداءات.

ومواصفة الأمن هذه قابلة للتطبيق في سياقات ذات المطاريف الكثيرة المحتملة التي لا يكون تخصيص كلمة سر/مفتاح تناظري فيها عملياً، مثلاً في السيناريوهات الواسعة النطاق أو العالمية النطاق. وتوفر مواصفة الأمن بالتواقيع خدمات أمن إضافية بالنسبة لعدم الإنكار تستعمل تواقيع رقمية وشهادات. ويمكن للتواقيع الرقمية أن تستعمل خوارزمية تظليل أمين 1 أو تلخّص الرسالة رقم 5 مع التظليل كما توفّر الاستيقان و/أو التكامل (انظر الإجراءين II وIII).

وينبغي لكيانات H.323 التي تستعمل الاستيقان والتكامل أو الاستيقان بمفرده على أساس قفزة قفزة أن تستعمل الإجراء II. ومن شأن الكيانات H.323 التي تستخدم مجرد الاستيقان بمفرده ألا تنفِّذ التكامل. وينبغي لكيانات H.323 التي تستعمل الاستيقان بمفرده أن تستخدم الإجراء III من أجل إجراء استيقان حقيقي من طرف إلى طرف.

ويجوز تطبيق هذه التوصية على حماية تكامل الرسائل التي تشمل الرسالة بأكملها. وبالنسبة للرسائل H.225.0 RAS تغطي حماية التكامل الرسالة RAS بأكملها؛ وبالنسبة لتشوير النداء فإنها تغطي رسالة تشوير النداء H.225.0 بأكملها بما في ذلك رأسيات Q.931.

وتتيح مواصفة الأمن بالتواقيع إرسال وحدات المعطيات البروتوكولية PDU للتحكم ضمن رسائل وظيفية H.225.0 في قنوات نفقية بأمان تام. وتتطلب آليتي تحديث المفاتيح H.245 وتزامنها التسيير في القنوات النفقية المفيد في حالات الاتصالات الطويلة المدى للغاية، على سبيل المثال.

الملاحظة 2 – يجب على نحو خياري تحديث المفاتيح لأغراض تشفير الكلام G.711 المؤمَّن بعد إرسال 2^{30} فدرة تتألف كل منها من 64 بتة، أي ما يعادل أكثر من 12 يوماً من المحادثة المتواصلة.

تمثل المنطقة المظللة عمودياً (بالأزرق في النسخة الإلكترونية) في الجدول 1 مجال مواصفة الأمن بالتوقيع. وعند إلغاء التكامل المشار إليه في المنطقة المظللة أفقياً (بالأخضر في النسخة الإلكترونية) تنتج مواصفة الأمن بالاستيقان فقط. وينطوي خيار مواصفة الأمن بالتوقيع على الاختيار بين التوقيعين الرقميين RSA-SHA1 وRSA-MD5. ويجوز خيارياً استعمال مواصفة الأمن بالتجفير الصوتي الواردة في H.235.6 (انظر الفقرة H.235.6/6.1) بالترافق مع مواصفة الأمن بالتوقيع.

الجدول H.235.2/1 – مواصفة التجفير الصوتي

خدمات الأمن	وظائف النداء			
	RAS	H.225.0	H.245 (ملاحظة)	RTP
الاستيقان	MD5 / SHA1	MD5 / SHA1	MD5 / SHA1	
	توقيع رقمي	توقيع رقمي	توقيع رقمي	
عدم النكران	MD5 / SHA1	MD5 / SHA1	MD5 / SHA1	
	توقيع رقمي	توقيع رقمي	توقيع رقمي	
التكامل	MD5 / SHA1	MD5 / SHA1	MD5 / SHA1	
	توقيع رقمي	توقيع رقمي	توقيع رقمي	
السرية				
التحكم بالنفاذ				
إدارة المفاتيح	توزيع الشهادة	توزيع الشهادة		
ملاحظة – رسالة H.245 موضوعة في قناة نفقية أو رسالة H.245 مدمجة في توصيل سريع H.225.0.				

الملاحظة 3 – ينبغي أن توفر كيانات H.235 أخرى أيضاً (مثل حارسات بوابية وبوابات ومخدمات وكيلة H.235) مواصفة الأمن بالتوقيع.

الملاحظة 4 – تستطيع بتات استعمال المفتاح المتوفرة في الشهادة أيضاً تحديد خدمة الأمن التي يقدمها مطراف ما (مثال: عدم نكران مؤكد).

يستحسن فيما يخص الاستيقان أن يفيد المستعمل من نظام توقيع بمفتاح عمومي أو خاص. ويقدم هذا النظام عادة تكاملاً وعدم نكران أفضل للنداء.

ولا تحدد هذه التوصية إجراءات:

- للتسجيل والشهادة وتوزيع الشهادة استناداً إلى مركز موثوق أو لتوزيع مفاتيح خاصة/عمومية أو لخدمات الدليل والمعلمات الخاصة بإصدار الشهادة وإلغاء الشهادات وتحديث/استرجاع أزواج المفاتيح وغيرها من الإجراءات التشغيلية الإدارية الأخرى الخاصة بالشهادات مثل تسليم الشهادة أو المفاتيح العمومية/الخاصة والشهادات وكذلك التركيب في المطاريف.

ويمكن تنفيذ مثل هذه الإجراءات بوسائل لا ترد في هذا الملحق.

كيانات الاتصالات المعنية قادرة على تحديد ضمني لاستعمال مواصفة الأمن الأساسي H.235.1 أو مواصفة الأمن بالتواقيع هذه وذلك بواسطة تقييم معرفات هوية أغراض الأمن التي يشار إليها في الرسالتين (**tokenOID** و**algorithmOID**؛ انظر أيضاً الفقرة 20).

تتمثل الإجراءات المخصصة للاستعمال في هذه المواصفة فيما يلي:

الإجراء II يستند إلى التواقيع الرقمية باستعمال أزواج مفاتيح خاصة/عمومية لتوفير استيقان وتكامل وعدم إنكار الرسائل RAS، Q.931 وH.245. ويمكن للمطاريف استعمال هذه الطريقة إذا كان عدم الإنكار والتكامل المتطوِّر مطلوبين.

وتبعاً لسياسة الأمن، يمكن أن يكون الاستيقان وحيد الطرف أو متبادَلاً بتطبيق الاستيقان/التكامل في الاتجاه العكسي أيضاً ومن ثم زيادة توفير الأمن. ويمكن لسياسة الأمن الخاصة بأحد المطاريف أن تتيح "الاستيقان بمفرده" بدون حساب التكامل المجفَّر (انظر الفقرة 9).

وعندما تكتشف حارسات بوابية التثبت من فشل الاستيقان و/أو فشل التكامل في رسالة RAS/أو رسالة تشوير النداء مستقبَلة من مطراف/حارس بوابي ند، فإن الحارسات البوابية ترد برسالة رفض مماثلة تبين إخفاق الأمن من خلال وضع سبب الرفض على **securityDenial** أو على أي شفرة خطأ أمن أخرى مناسبة وفقاً للفقرة H.235.0/11.1. وتبعاً للقدرة على تمييز حدوث هجوم، وعلى أنسب وسيلة لمواجهته، يجب على أي حارس بوابي يستقبل رسالة **xRQ** مؤمَّنة تحتوي على معرِّفات غرض غير محدد (**tokenOID**، **algorithmOID**) أن يستجيب برسالة **xRJ** غير مؤمَّنة أو يمكن أن يتجاهل تلك الرسالة. وينبغي تسجيل حدث الأمن الذي تتم مواجهته. ومن ناحية أخرى، ينبغي للنقطة الطرفية أن تتجاهل الرسالة غير المؤمَّنة المستقبَلة، والإمهال ويمكن أن تكرر المحاولة مرة أخرى من خلال توخي اختيار معرِّفات OIDs مختلفة. كذلك يجب لحارس بوابي يستقبل رسالة H.225.0 SETUP مؤمَّنة مع معرِّفات غرض غير محدد (**tokenOID**، **algorithmOID**) أن يستجيب برسالة RELEASE COMPLETE غير مؤمَّنة، وأن يضع السبب على **securityDenied** أو يمكن أن يتجاهل تلك الرسالة. وبالمثل، يجب تسجيل حدث الأمن الذي جرت مواجهته.

ويتيح تشوير ضمني H.235 إمكانية الدلالة على استعمال الإجراء II كما أن آلية الأمن المطبَّقة تستند إلى قيمة معرِّفات الغرض (انظر أيضاً الفقرة 20) ومحتويات مجالات الرسالة. وتعيَّن معرفات الغرض رمزياً من خلال حروف (مثلاً حرف "A") في هذا النص.

ولا تستخدم هذه المواصفة المجالات H.235 ICV، بل بالأحرى توضع قيم التحقق من التكامل المجفَّر في مجال **signature** إلى الفيشة **token** من المجال **cryptoSignedToken**.

1.6 المتطلبات H.323

يفترض أن توفر الكيانات H.323 التي تطبق هذه المواصفة الخاصيتين H.323 التاليتين:

- التوصيل السريع؛
- نموذج التسيير عبر حارس بوابي.

7 التواقيع الرقمية مع تفاصيل أزواج المفاتيح العمومية/الخاصة (الإجراء II)

من الضروري التقيد بالإجراءات التالية في حال استعمال الإجراء II لأغراض الأمن قفزة قفزة:

- يستحسن استخدام الخوارزمية SHA1 أو MD5 مع الخوارزمية RSA لإنتاج توقيع رقمي. ويعزز التقيد بالنظامين PKCS رقم 1 وPKCS رقم 7 قابلية التشغيل البيني.

وينبغي أن يتضمن المجال **CryptoH323Token** لكل رسالة RAS/H.225.0 المجالات التالية:

– **nestedCryptoToken** متضمناً **CryptoToken** يضم المجال **cryptoSignedToken** مع المجالات التالية:

- **tokenOID** موضوعاً على:

– "A" للدلالة على أن حساب الاستيقان/التكامل يضم جميع مجالات الرسالة RAS H.225.0 أو تشوير النداء (انظر الفقرة 11)؛

– "B" للدلالة على أن حساب الاستيقان/التكامل لا يضم سوى مجموعة فرعية من المجالات (انظر الفقرة 16) من الرسالة RAS/H.225.0 لأغراض الاستيقان بمفرده؛

- **token** يضم المجالات التالية:

– **toBeSigned** يضم المجال **EncodedGeneralToken** وهو فعلياً مجال **ClearToken** يضم المجالات التالية:

- **tokenOID** موضوعاً على "S" للدلالة على أن **ClearToken** قيد الاستعمال لأغراض الاستيقان/التكامل/عدم النكران لرسالة ما؛
- **timeStamp** محتوياً على طابعة الوقت؛
- **random** محتوياً على رقم التتابع المتزايد بوتيرة واحدة؛
- **generalID** محتوياً على معرف هوية المرسل إليه (في حالة الإذاعة الأحادية)؛
- **SendersID** محتوياً على معرف هوية المرسل؛
- **dhkey** مستخدماً في نقل المعلمات ديفي–هيلمان كما هو محدد في هذه التوصية خلال الفترة المنقضية بين **Setup** و**Connect**:

– **halfkey** محتوياً على مفتاح عمومي عشوائي لجزء من الأجزاء؛

– **modsize** محتوياً على DH-prime (انظر الجدول H.235.6/4)؛

– **generator** محتوياً على DH-group (انظر الجدول H.235.6/4).

الملاحظة 1 – عند استعمال مواصفة الأمن بالتوقيع دون مواصفة الأمن بالتحفير الصوتي ينبغي عدم إرسال معلمات ديفي–هيلمان وعدم وجود **dhkey**؛ ويمكن بدلاً من ذلك وضع المجالات **halfkey** و**modsize** و**generator** على {'0'B، '0'B، '0'B}.

- **certificate** محتوياً على الشهادة الرقمية للمرسل حيث يدل نمطها على نمط الشهادة ("V" تدل على الشهادات MD5-RSA و"W" على شهادات SHA1-RSA) ويسير المجال **certificate** الشهادة الحقيقية (انظر الفقرة 14).
- **algorithmOID** موضوعاً على:

– "V" للدلالة على استعمال التوقيع MD5-RSA؛

– "W" للدلالة على استعمال التوقيع SHA1-RSA.

- **params** موضوعاً على NULL.
- **signature** محتوياً على التوقيع المحسوب بواسطة الخوارزمية SHA1 أو MD5 RSA في مجمل المجالات (إذا كان **tokenOID** موضوعاً على "A" انظر الفقرة 11) أو بعض المجالات الهامة (إذا كان **tokenOID** موضوعاً على "B"، انظر الفقرة 10) من الرسالة H.225.0 RAS أو من تشوير النداء.

عندما يوضع **tokenOID** على "A" لحماية الوحدات H323-UU-PDU المسيرة في القناة النفقية بما في ذلك محتوى الرسالة H.245 ينبغي إجراء حساب التواقيع في مجمل الرسالة H.225.0 من تشوير النداء مع مجمل المجالات بموجب إجراء المذكور في الفقرة 11. وإذا كان **tokenOID** موضوعاً على "B" يتم الاستيقان بمفرده في **CryptoToken** بتطبيق الإجراء III (انظر الفقرة 10).

- يتحقق الكيان الذي يرسل إليه التوقيع (وقد يبعد عنه قفزة سوية تطبيق واحدة أو أكثر) من هذا التوقيع.

الملاحظة 2 – بإمكان المرسل إليه أن يكشف استعمال الإجراء II بتقييم المعرّف **algorithmOID** في الفيشة **cryptoSignedToken** (بواسطة كشف حضور "V" أو "W").

8 إجراءات المؤتمر متعدد النقاط

ينبغي أن توفر الوحدات MCU توزيع الشهادات الأمين على طلب المطاريف عن طريق الأمرين H.245: **ConferenceRequest** و**ConferenceResponse** المسيرين في القناة النفقية كما هو مبين في الفقرة H.235.6/8.8.1. مما يتيح للمطاريف طلب الشهادات لمطاريف أخرى في سياق مؤتمر متعدد النقاط والحصول بهذه الطريقة وبشكل مؤكد على هوية المشاركين الآخرين في المؤتمر.

ويسيّر الأمر **ConferenceRequest** الطلب **requestTerminalCertificate** وفيه المجالات التالية:

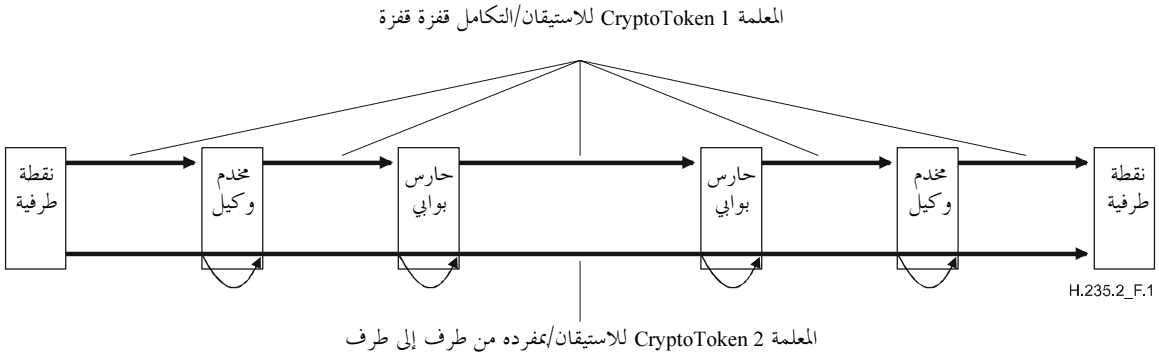
- **terminalLabel**: ويستعمل كوسيلة لعنونة المطراف البعيد عبر الوحدة MCU؛
- **certSelectionCriteria**: ولا يمكن للمرسل أن يطلب بواسطته إلا شهادات من نمط معين؛
- **sRandom**: امتحان عشوائي يقوم به المرسل الطالب.

وتسيّر الرسالة **ConferenceResponse** الرسالة **terminalCertificateResponse** وفيها المجالات التالية:

- **terminalLabel**: وتتيح ضم الشهادة المرسلة إلى المطراف
- **CertificateResponse**: يسير استجابة الوحدة MCU مع المجالات موضوعة على:
  - **terminalLabel**: تعرّف هوية المطراف البعيد؛
  - **certificateResponse**: وهو بالواقع عبارة عن سلسلة أثمونات ASN.1 مشفرة استناداً إلى **EncodedReturnSig** باعتباره:
    - **generalID**: تعرّف هوية مطراف المقصد؛
    - **responseRandom**: قيمة امتحان عشوائي تنتجه الوحدة MCU؛
    - **requestRandom**: ويعيد **sRandom** إنتاج ما يلي؛
    - **certificate**: ويسيّر الشهادة المعاد إرسالها التي يدل فيها **type** على نمط الشهادة باعتبارها معرّف هوية OID وتسيّر المعلمة **certificate** الشهادة الرقمية (انظر الفقرة 14).

9 الاستيقان من طرف إلى طرف (الإجراء III)

يعرض الشكل 1 سيناريو تفصل فيه المخدمات الوكيلة بين الحارسات GK والنقاط EP، وتستعمل فيه قيمتا معلمة CryptoToken للاستيقان قفزة قفزة وللاستيقان من طرف إلى طرف و/أو التكامل قفزة قفزة. ولا تطبق قيمة **CryptoToken** للاستيقان قفزة قفزة إلا على المقطع المحصور بين كيانين وينبغي إعادة حسابها في كل مقطع جديد. ومن ناحية أخرى، تنتج قيمة **CryptoToken** للاستيقان من طرف إلى طرف مرة واحدة في النقطة الطرفية المرسلة ولا تتغير أثناء نقل العقد الوسيطة لها. وتستطيع هذه العقد أن تتحقق من صلاحية التواقيع والشهادات المسيرة في **CryptoToken** من طرف إلى طرف وينبغي لها أن تسير القيمة **CryptoToken** أثناء النقل.



الشكل H.235.2/1 – استعمال متآون للأمن قفزة قفزة والاستيقان من طرف إلى طرف

الملاحظة 1 – قد يكون المخدم الوكيل عقدة شبكة منفصلة كما هو مبين في الشكل 1 أو قد يقع في مكان وظيفة كيان H.323 كأن يشكل جزءاً من الحارس البوابي.

الملاحظة 2 – تبعاً للمعرّف **tokenOID** المبين، يكون المخدم الوكيل قادراً على تحديد ما إذا كان مقصد القيمة **CryptoToken** المستقبلة هو المخدم الوكيل ("S") أو مرسلاً إليه آخر ("R").

الملاحظة 3 – نظراً إلى أن الكيانات الوسيطة تغير محتوى رسالة التشوير لكل مقطع تتعذر إمكانية التكامل من طرف إلى طرف.

من أجل الحصول على استيقان حقيقي من طرف إلى طرف من جهتي المخدمات الوكيلة H.323 والعناصر الوسيطة للشبكة، ينبغي أن تحسب النقطة الطرفية/المطراف التوقيع الرقمي بالطريقة التالية:

ينبغي أن يضم المجال **CryptoH323Token** في كل رسالة RAS/H.225.0 المجالات التالية:

- **nestedCryptoToken** محتوياً على **CryptoToken** يحوي بدوره **cryptoSignedToken** مع المجالات التالية:
  - **tokenOID** موضوعاً على:
    - "A" للدلالة على أن حساب الاستيقان/التكامل قفزة قفزة يضم جميع مجالات الرسالة RAS/H.225.0 (انظر الفقرة 11)؛
    - "B" للدلالة على أن حساب الاستيقان لا يضم إلا مجموعة فرعية من المجالات (انظر الفقرة 10) من الرسالة H.225.0 RA أو تشوير النداء بهدف إجراء الاستيقان بمفرده.
- **token** محتوياً على المجالات التالية:
  - **toBeSigned** محتوياً على المجال **ClearToken** المستعمل مع المجالات التالية:
    - **tokenOID** موضوعاً على "R" للدلالة على أن **ClearToken** قيد الاستعمال لأغراض الاستيقان بمفرده/عدم النكران من طرف إلى طرف؛

الملاحظة 4 – تتوقف أي خدمة أمنية يجري تطبيقها فعلياً على بتات استعمال المفتاح في الشهادة.

- **random** محتوياً على رقم التتابع المتزايد بوتيرة واحدة؛
- **timeStamp** يستعمل خيارياً للحصول على أمن محسن في حال تزامن الكيانات حصراً؛
- **generalID** محتوياً على معرّف هوية النقطة الطرفية للمرسل إليه (في حالة الإذاعة الأحادية حصراً). ويكون على صعيد التطبيق قفزة قفزة معرف هوية القفزة التالية؛ أما على الصعيد من طرف إلى طرف فهو معرف هوية النقطة الطرفية البعيدة؛
- **sendersID** ويحتوي على هوية المرسل في النقطة الطرفية؛
- **certificate** محتوياً على الشهادة الرقمية للمرسل حيث يدل **type** على نمط الشهادة ("V" تدل على الشهادة MD5-RSA أو "W" على الشهادة SHA1-RSA) وتسيّر المعلمة **certificate** الشهادة بحد ذاتها (انظر الفقرة 14)؛
- **dhkey**، يستخدم لتسيير المعلمات ديفي–هيلمان المحددة في هذه التوصية من **Setup** إلى **Connect**:
  - **halfkey** محتوياً على مفتاح عمومي عشوائي لجزء من الأجزاء؛
  - **modsize** محتوياً على DH-prime (انظر الجدول H.235.6/4)؛
  - **generator** محتوياً على DH-group (انظر الجدول H.235.6/4).

الملاحظة 5 – عند استخدام مواصفة الأمن بالتوقيع دون مواصفة الأمن بالتجفير الصوتي ينبغي عدم إرسال أي معلمة ديفي–هيلمان وعدم وجود المجال **dhkey**؛ ويمكن وضع **halfkey** و**modsize** و**generator** على {'0B'، '0B'، '0B}.

- **algorithmOID** موضوعاً على:
  - "V" للدلالة على استعمال التوقيع MD5-RSA؛
  - "W" للدلالة على استعمال التوقيع SHA1-RSA.
- **params** موضوعاً على NULL.
- **signature** محتوياً على التوقيع محسوباً بواسطة الخوارزمية SHA1-RSA أو MD5- RSA في مجمل المجالات (إذا كان **tokenOID** موضوعاً على "A") أو بعض المجالات الهامة (إذا كان **tokenOID** موضوعاً على "B") من الرسالة H.225.0 RAS أو من تشوير النداء.

ويستطيع المخدم الوكيل التحقق من التوقيع الرقمي أو من الشهادة المستقبلة ويمكنه تجاهل الرسالة التي يعتبرها غير ملائمة مراعاة للسياسة المحلية، أو أن يواصل إرسال **CryptoToken** المستقبلة. وينبغي أن ينتج المخدم الوكيل عناصر جديدة لمعلومات التشوير H.235 لأغراض الأمن قفزة قفزة وفقاً للإجراء II أو III.

ويستحسن أن يتحقق الكيان الذي ينهي المقطع (كالمطراف مثلاً) من معلومات الأمن المستقبلة في **CryptoToken**، ويمكنه تبعاً لوجود عناصر الأمن من طرف إلى طرف، أن يقيم أيضاً المعلومة **CryptoToken** من طرف إلى طرف. وقد تتغير إجراءات التحقق القيمة التي ينبغي تطبيقها في مطراف أو كيان وسيط H.323 بتغير السياسة المحلية.

10 الاستيقان بمفرده

تستطيع المطاريف أن تقرر تطبيق الاستيقان بمفرده (باستعمال المعرّف "B" OID). ويحسب في هذه الحالة المستيقن في مجموعة فرعية فقط (**ClearToken** من **CryptoToken**) من الرسالة RAS/H.225.0. وقد يكون الاستيقان بمفرده مفيداً للاستيقان الحقيقي من طرف إلى طرف (انظر الفقرة 9). وتستعمل المجالات التالية من البنية **ClearToken** باعتبارها مجموعات فرعية:

- **tokenOID**: معرف هوية غرض فيشة مستقلة ("B" tokenOID) لتطبيق الاستيقان بمفرده.
- **random**: رقم التتابع المتزايد بوتيرة واحدة.
- **timeStamp**: طابعة الوقت.

- **generalID**: معرّف هوية المرسل إليه (بأسلوب الإذاعة الأحادية). ويكون على صعيد القفزة قفزة معرّف هوية القفزة اللاحقة؛ وعلى الصعيد من طرف إلى طرف معرّف النقطة الطرفية البعيدة.
- **sendersID**: معرّف هوية المرسل.
- **dhkey**: معلمات ديفي–هيلمان. ولا تستعمل هذه المجالات والمجالات الفرعية إلا أثناء الرسائل من **Setup** إلى **Connect**.

يتم حساب المستيقن في **ClearToken** الموجود داخل **EncodedGeneralToken** (أي **ClearToken**) من المجال **token** في **cryptoSignedToken**. ويتم حساب التوقيع الرقمي في السلسلة الرقمية المشفرة بالترميز ASN.1 في **ClearToken**. وينبغي قبل حساب التوقيع الرقمي وضع المجال **tokenOID** في **ClearToken** على {0 0}.

11 الاستيقان والتكامل

فيما يلي إجراء الاستيقان والتكامل في مجمل مجالات الرسالة المشفرة ASN.1 (المعرّف "A" OID):

ينبغي أن يحسب مرسل الرسالة التوقيع بالطريقة التالية:

1) وضع قيمة التوقيع لنموذج التغيب الخاص ذي الطول الثابت (مثال: 1024 بتة). ويجب في هذه المرحلة حجز مكان لطول الحد الأقصى لتوقيع رقمي، وهذا ممكن بوجود شهادة معينة. وتشكيلة البتات الصحيحة غير هامة غير أنه من المفضل اختيار تشكيلة لا ترد في بقية الرسالة.

2) تشفير مجمل الرسائل بالترميز ASN.1؛ وينبغي أن يضم ذلك بالنسبة إلى الرسائل RAS كامل الرسالة H.225.0 RAS؛ أما بالنسبة إلى تشوير النداء فذلك يضم كامل رسالة تشوير النداء H.225.0.

3) تحديد موقع تشكيلة التغيب في الرسالة المشفرة وطمسها ببتات الأصفار.

الملاحظة 1 – وقد ينطوي ذلك على بعض المحاولات والأخطاء في الحالة النادرة جداً حيث ترد تشكيلة التغيب في الرسالة عدة مرات.

4) حساب التوقيع الرقمي استناداً إلى الرسالة المشفرة ASN.1 بالطريقة التي يشير إليها المعرّف **algorithmOID** أي "V" أو "W" (انظر الفقرة 12).

5) الاستعاضة عن تشكيلة التغيب في الرسالة المشفرة بالقيمة المقابلة للتوقيع الرقمي المحسوب. وإذا كان التوقيع الرقمي أقصر من الفراغ المحجوز، توضع أصفار قبل البتات الأكثر دلالة لقيمة التوقيع.

ويستقبل المرسل إليه الرسائل ثم يعمل بالطريقة التالية:

1) يفك تشفير الرسالة ASN.1.

2) يستخرج قيمة التوقيع الرقمي المستقبل ويحتفظ بها في المتغير الأولي (SV) المحلي.

3) يبحث عن قيمة التوقيع SV ويحدد موقعها في الرسالة المشفرة المستقبلة.

الملاحظة 2 – في الحالة النادرة حيث ترد سلسلة فرعية من قيمة التوقيع عدة مرات في مجمل الرسالة، يستحسن تكرار القفزات من 3 إلى 6 من مواقع مختلفة لانطلاق البحث.

4) يطمس تشكيلة بتات الرسالة المشفرة بواسطة الأصفار.

5) يحسب التوقيع الرقمي استناداً إلى الرسالة المشفرة بالترميز ASN.1 باتباع الطريقة المشار إليها في **algorithmOID** أي "V" أو "W" (انظر الفقرة 12).

6) يقارن قيمة المتغير SV مع قيمة التوقيع المحسوب. ولا تعتبر الرسالة خالية من الأخطاء وأصلية إلا إذا كانت قيم التوقيع متماثلة؛ وفي هذه الحالة ينجح الاستيقان وينتهي الإجراء.

7) وإلا، تكرر العمليات من 3 إلى 7 بإعادة وضع المتغير SV في الموقع السابق والبحث عن توافقيات. وإذا لم تعط أي توافقية قيم توقيع متشابهة بشكل صحيح يكون الاستيقان فاشلاً والرسالة متأثرة (عرضاً أو عمداً) إبان النقل أو لأي سبب آخر.

12 حساب التوقيع الرقمي

ينطوي البدء في عملية إنتاج التوقيع الرقمي على وجود سلسلة مشفرة ASN.1 وينطوي على نتيجة عملية حساب ملخص الرسالة والمفتاح الخاص للموقّع. وترتبط تفاصيل إنتاج التوقيع الرقمي بخوارزمية التوقيع المستعملة؛ وتحدد الشهادة خوارزمية التوقيع التي يستحسن تطبيقها؛ وعند ظهور تمديد استعمال المفتاح في الشهادة، ينبغي وضع البتة **digitalSignature** بطريقة تقابل المفتاح الممكن استخدامه في التوقيع. وتشفر قيمة التوقيع الذي ينتجه الموقع على شكل سلسلة بتات وتسير في المجال **signature**.

وينبغي استعمال الطريقة الواردة في [PKCS الرقم 1، القسم 1.1.8.E] لحساب التوقيع الرقمي من النمط RSA بواسطة التذييل (RSASSA-PKCS1-v1_5-SIGN) والإجراءات OS2IP، RSASP1، I2OSP وطريقة التشفير EMSA-PKCS1-v1_5-ENCODE.

13 التحقق من التوقيع الرقمي

يأتي البدء في عملية التحقق من التوقيع نتيجة لعملية حساب ملخص الرسالة والمفتاح العمومي للموقّع. ويستطيع المرسل إليه الحصول على المفتاح العمومي الصحيح للموقّع بأي وسيلة ولكن الطريقة المفضلة هي طريقة الشهادة التي يتم الحصول عليها في المجال **certificate** ثم صلاحيتها بواسطة تظليل شهادة الموقّع. وقد تستند صلاحية المفتاح العمومي للموقع إلى معالجة مسير إصدار الشهادة (RFC 3280). وتتعلق تفاصيل التحقق من التوقيع بخوارزمية التوقيع المستخدمة.

وينبغي استعمال الطريقة الواردة في [RKCS رقم 1، القسم 2.1.8.E] من أجل التحقق من توقيع رقمي من النمط RSA بواسطة التذييل (RSASSA-PKCS1-v1_5-VERIFY) والإجراءات OS2IP، RSAVP1، I2OSP والطريقة EMSA-PKCS1-v1_5-ENCODE.

14 معالجة الشهادات

فيما يخص التحقق من التواقيع الرقمية ينبغي أن يتمتع كيان الاستقبال بالنفاذ إلى شهادة المرسل الموقعة من سلطة إصدار شهادات معروفة (CA). وهناك عدة إمكانيات تتيح للمرسل إليه النفاذ إلى شهادة المرسل:

- الشهادة مدرجة في تبادل الرسالة كما يرد في الإجراءين II وIII؛ وفي هذه الحالة تضم المعلمة **certificate** الشهادة الحقيقية والمعلمة **type** المعرف "V" أو "W".
- يعرف المرسل إليه الشهادة فهي مسجلة محلياً أثناء تبادل سابق.
- بدلاً من أن يدرج المرسل الشهادة بحد ذاتها فإنه يعطي عنوان URL يمكن فيه إيجاد الشهادة. ولذا فإن المعلمة **certificate** تضم العنوان URL والمعلمة **type** موضوعة على المعرف "P" OID.
- يحصل المرسل إليه على إصدار الشهادة بطريقة أخرى لا تتماشى مع هذه التوصية (كاستشارة دليل ببروتوكول LDAP مثلاً).

وفي كل مرة ترسل شهادة رقمية في رسالة ينبغي أن يتأكد الكيان المستقبل من أن هوية المرسل (الحارس البوابي، النقطة الطرفية) موجودة في الشهادة من أجل منع أي اعتداء يقوم به الدخيل.

وفيما يخص الرسائل بالتوقيع الرقمي المرسلة من الحارس البوابي إلى النقطة الطرفية، هناك عدة إمكانيات لتحقق النقطة الطرفية من هوية الحارس البوابي:

- إذا كان اسم المضيف موجوداً مثلاً في أحد نعوت الأسماء العامة لمجال الموضوع أو للموضوع subjectAltName للشهادة، يجوز للنقطة الطرفية التحقق من أن اسم المضيف هذا يقابل معرف الحارس البوابي. وعلاوة على ذلك، تستطيع النقطة الطرفية أن تستعمل النظام DNS لاستجواب العنوان IP المصاحب والتحقق مما إذا كان هذا هو بالفعل عنوان IP للحارس البوابي كما هو وارد في رسالة الاستجابة الموقعة من الحارس البوابي.
- على سبيل المثال، قد يتألف معرّف هوية الحارس البوابي من العنوان IP (فمثلاً بقيمة مدرجة في أربعة أثمونات في نفس ترتيب أثمونات الشبكة) تليه معلومة أخرى لتعرف هوية معرف هوية الحارس البوابي مقطوعة من الطول الأقصى للمجال ID للمرسل أو التي تسيّر هوية الحارس البوابي. وإضافة إلى ذلك تستطيع النقطة الطرفية أن تتحقق مما إذا العنوان IP لاسم المضيف يقابل بالضبط العنوان IP الموجود في الرأسية IP لاستجابة الحارس البوابي.

  ملاحظة – لا تعمل هذه الطريقة بوجود أجهزة NAT على النحو المتوقع.
- في حال عدم وجود اسم المضيف في الشهادة ينبغي مباشرة استخراج العنوان IP الذي يشكل جزءاً من الشهادة (*iPAddress subjectAltName*) من أجل إجراء التحققات المذكورة أعلاه.

ينبغي أن يتفحص المستعملون بأناة الشهادة المقدمة من الحارس البوابي من أجل تحديد ما إذا كانت تستجيب لتوقعاتهم. وإذا توفرت في النقطة الطرفية معلومات خارجية عن هوية الحارس البوابي المنتظرة يمكن إلغاء عملية التحقق من اسم المضيف. فعلى سبيل المثال يمكن توصيل نقطة طرفية مع حارس بوابي له عنوان واسم مضيف ديناميان، بينما تعرف النقطة الطرفية الشهادة التي سيقدمها الحارس البوابي. ومن الهام في مثل هذه الحالة تنقيص عدد الشهادات المقبولة ما أمكن بغية تفادي اعتداءات الدخيلين. وقد يكون من المفيد للنقطة الطرفية في بعض الحالات الخاصة، أن تتجاهل ببساطة هوية الحارس البوابي ولكن يجب توضيح أن ذلك يترك التوصيل مفتوحاً للاعتداءات النشيطة.

في حال عدم توافق اسم المضيف مع هوية الشهادة ينبغي أن تبلغ النقاط الطرفية الموجهة للمستعمل المستعمل عن ذلك (تستطيع النقاط الطرفية إعطاء المستعمل إمكانية المتابعة مع التوصيل في أي حال من الأحوال) أو أن توقف التوصيل مع الإشارة إلى خطأ الشهادة الخاطئة. وينبغي أن تدون النقاط الطرفية المؤتمتة الخطأ في سجل المراقبة الملائم (إن وجد) وأن توقف التوصيل (مع دلالة "خطأ شهادة خاطئة").

تستطيع النقاط الطرفية المؤتمتة أن تضع قيد الاستعمال تشكيلة توقف هذا التحقق شريطة أن تكون مزودة بتحكم يتيح تنشيطه من جديد.

وكذلك يوصى بأن يقوم الحارس البوابي بالتحقق من هوية كل رسالة بتوقيع رقمي مرسلة من نقطة طرفية إلى الحارس البوابي. وتعتبر صيغ التطبيق الصحيحة لمثل هذا التحقق عن طريق الحارس البوابي مسألة محلية ومرتبطة بسياسة أمن الحارس البوابي فمثلاً يمكن تصور أن اسم مستعمل مدرج في الشهادة يمكن أيضاً أن يشكل جزءاً من معرّف الهوية H.323. ويستطيع الحارس البوابي بعد ذلك أن يجري تحققاً للتأكد من معلومة الهوية هذه مع معطيات المستعمل التي تتم إدارتها/تشكيلتها محلياً إن توفرت وأن يتخذ قراراً استناداً إلى النتيجة.

وإذا كان الحارس البوابي مزوداً بمعلومات تتعلق بالهوية المتوقعة للنقطة الطرفية يمكن إلغاء التحقق من اسم المضيف. وعلى سبيل المثال قد يكون الحارس البوابي بصدد الاتصال بنقطة طرفية لها عنوان واسم مضيف ديناميان ولكنه يعرف الشهادة التي ستقدمها النقطة الطرفية. وفي مثل هذه الحالة يستحسن التنقيص من عدد الشهادات التي يمكن قبولها قدر الإمكان بغية تفادي الاعتداءات عن طريق الدخيل. ويستطيع الحارس البوابي في بعض الحالات الخاصة أن يتجاهل ببساطة هوية النقطة الطرفية ولكن يجب إدراك أن ذلك يترك التوصيل مفتوحاً لاعتداءات نشيطة.

وفي حال عدم تطابق اسم المضيف مع الهوية الموجودة في الشهادة ينبغي أن يدوّن الحارس البوابي الخطأ في سجل حسابات لهذا الغرض وأن ينهي التوصيل (مع إشارة خطأ شهادة خاطئة).

وفي حال وجود تمديد subjectAltName من النمط dNSName، ينبغي استعمال هذا التمديد كهوية. وفي الحالات الأخرى، ينبغي استعمال المجال Common Name (الأكثر خصوصية) في المجال Subject من الشهادة. ورغم أن استعمال المجال Common Name وارد حالياً، إلا أنه غير مقبول ويتم تشجيع سلطات إصدار الشهادة على استعمال الاسم dNSName.

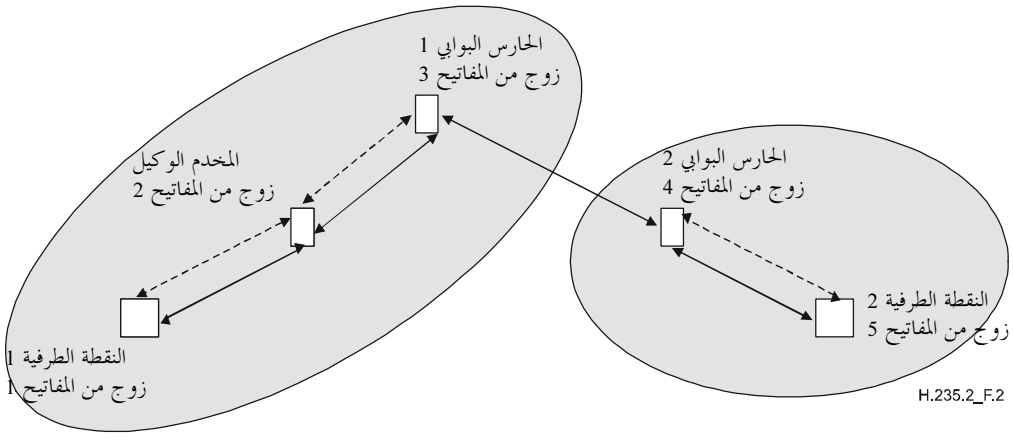
وينبغي إجراء التحقق باستعمال قواعد التوافق الخاصة الواردة في RFC 3280. وفي حال وجود عدة هويات لنمط معين في الشهادة (مثل عدة أسماء) يعتبر توافق إحدى هذه المجموعات مقبولاً. وقد تضم الأسماء صفة البديل * المعتبرة بمثابة مكونة ما من أسماء المجالات أو جزءاً من مكونة. مثال: تضم a.com*. الجزء foo.a.com وليس الجزء bar.foo.a.com وتضم f*.com الجزء foo.com وليس الجزء bar.com.

ويقدم الإجراءان II وIII طرقاً لتسيير الشهادة الرقمية. ولأسباب عملية ينبغي نقل الشهادات الرقمية للكيانات مرة واحدة كحد أقصى ما عدا إذا كانت غير متيسرة في الكيانات (عن طريق وسائل أخرى لا تدخل في إطار هذه التوصية). وبالتالي ينبغي ألا يتم تبادل الشهادات إلا في بداية إنشاء الاتصال: وينتج ذلك بالنسبة إلى الرسائل RAS أثناء اكتشاف الحارس البوابي أو، في حال إلغاء هذه المرحلة، عند تسجيل الحارس البوابي. والأمر كذلك أيضاً في حالة التوصيل السريع حيث يمكن إدراج الشهادة في الرسائل الأولية لتشوير الرسالة ويمكن إلغاؤها بكل أمان في الرسائل اللاحقة لتشوير النداء.

وفيما يخص مواصفة الأمن هذه يجب استعمال الشهادة X.509v3 (1997) وتتطلب الأنساق الأخرى للشهادات مزيداً من الدراسة.

15 مثال لاستعمال الإجراء II

لنأخذ حالة الشكل 2 حيث يمتلك كل كيان زوج مفاتيحه العمومية أو الخاصة أو شهادته الخاصة به وقد يكون الكيان مزوداً أيضاً بعدة أزواج من المفاتيح. وفي الشكل المذكور هناك مخدم وكيل H.323 يفصل بين النقطة EP1 والحارس البوابي GK1.



الشكل H.235.2/2 – مثال لاستعمال المفاتيح العمومية في نموذج التسيير من حارس GK إلى GK آخر

وللمخدم الوكيل H.323 سلوك مزدوج: فهو من جهة ينهي الاستيقان والتكامل لكل مقطع من مقاطعه. ويدرج فعلياً معلومات الاستيقان/التكامل التي فرغ للتوّ من حسابها في الرسائل RAS الخارجة بطريقة مماثلة للطريقة الواردة في الإجراء I من التوصية H.235.1. ومن جهة أخرى، يمرر معلومات الأمن من طرف إلى طرف دون تغيير. كما أنه يستطيع مع ذلك التحقق من الشهادات و/أو التواقيع الرقمية المستقبلة في طريق العبور.

وفيما يلي توضيح لتفاصيل إجراء الاستيقان والتكامل وعدم النكران الرسائل RAS وتشوير النداء H.225.0 وH.245.

1.15 استيقان الرسائل RAS وتكاملها وعدم نكرانها

لنأخذ حالة الاتصال قفزة قفزة حيث ترغب النقطة EP1 بإرسال رسالة RAS – مثلاً رسالة **ARQ** – إلى الحارس البوابي GK1. تولد النقطة EP1 طابع الوقت وكذلك رقم التتابع اللذين تدرجهما في المجالين **timeStamp** و**random** على التوالي مع اسم المخدم الوكيل في المجال **generalID** ومعرف هوية النقطة EP1 في المجال **sendersID**. وهذان المجالان موجودان في المجال **ClearToken** من **EncodedGeneralTokens** الموجود في **token** من **cryptoSignedToken** للمجال **CryptoToken** من **cryptoH323Token** للرسالة **ARQ**. وهذه الفيشة **cryptoH323Token** هي واحدة (كحد أدنى) من الفيش العديدة من التتابع **cryptoTokens**. ويوضع المجال **tokenOID** من **cryptoSignedToken** على "A" للدلالة على أن جميع مجالات الرسائل **ARQ** موقعة. وللمعلمة **token** من **cryptoSignedToken** مجالها **algorithmOID** الموضوع على "V" للدلالة على استعمال المجموعة MD5-RSA أو على "W" للدلالة على استعمال الخوارزمية SHA1-RSA، ويوضع المجال **params** على NULL. ثم تحسب النقطة EP1 بعد ذلك التوقيع استناداً إلى خوارزمية التوقيع المعنية باستعمال مفتاحها الخصوصي الخاص. ويحسب التوقيع في مجمل مجالات الرسالة **ARQ** عندما يكون **tokenOID** موضوعاً على "A". وتضم النقطة EP1 التوقيع المحسوب في **signature** من المجال **token** للمجال **cryptoSignedToken** من **CryptoToken** الموجود في **cryptoH323Token** من الرسالة **ARQ** وتضم شهادتها في المجال **certificate**.

وبنفس الطريقة التي يتم فيها الاتصال من طرف إلى طرف مروراً بالمخدم الوكيل، تنتج النقطة EP1 فيشة **CryptoToken** أخرى تحتوي على توقيع رقمي يغطي بعض المجالات الهامة (انظر الفقرة 9) في **ClearToken** من الرسالة **ARQ**. ويوضع المجال **tokenOID** من **CryptoSignedToken** على "B" للدلالة على وجود الاستيقان بمفرده في المجال **ClearToken** هذا؛ ويوضع المجال **tokenOID** من **ClearToken** على "R" للدلالة على الاستيقان من طرف إلى طرف ويملأ المجالات **timeStamp** و**random** و**sendersID** و**generalID** (وإذا كان أيضاً **SETUP/CONNECT** من **dhkey**) أو من المجالات التالية في **token**: **algorithmOID** بالقيمة "V" أو "W" للدلالة على خوارزمية التوقيع و**params** بالقيمة NULL و**signature** بقيمة التوقيع الرقمي المحسوب بدلالة المجالات **ClearToken**. ويسيّر المجال **certificate** الشهادة الرقمية للنقطة EP1. وترسل الرسالة **ARQ** بعد ذلك إلى المخدم الوكيل.

وعندما يستقبل المخدم الوكيل الرسالة **ARQ** يتحقق من توقيع الفيش المرسلة إليه (وفي هذه الحالة مثلاً هناك الفيش ذات القيمة "A" **tokenOID**) استناداً إلى عدة معايير منها:

- حداثة التاريخ والساعة وفرادة المجال **random**؛
- هوية **generalID** ومعرّفه الخاص؛
- تراخيص النفاذ للمرسل **sendersID**؛
- توافق توقيع الرسالة **ARQ** مع الرسالة التي يقوم الحارس GK1 بحسابها؛
- التحقق من المعلمات ديفي–هيلمان مع التحقق من صحة المعلمتين "prime" و"generator" المؤلفتين من 1024 بتة. والتحقق من المعلمات DH عملية طويلة لا تجري إلا إذا اشترطتها السياسة المحلية؛
- التحقق من الشهادة المستقبلة.

وإذا كان التحقق من التوقيع إيجابياً، يحسب المخدم الوكيل توقيعاً جديداً يدرجه عوضاً عن التوقيع القديم في الرسالة **ARQ** قبل إرسالها إلى الحارس البوابي GK1 بالطريقة التالية: يستعيض المخدم الوكيل عن المجالات **timeStamp** و**random** و**sendersID** و**generalID** في **ClearToken** (**toBeSigned**) بالقيم التي تطبق على مقطع يقع بين المخدم الوكيل والحارس البوابي GK1. ويضم المجال **timestamp** الطابع النافذ للوقت والساعة، ويضم المجال **random** رقم التتابع التالي المتزايد بوتيرة واحدة للمقطع بين المخدم الوكيل والحارس البوابي GK1، ويضم المجال **sendersID** للمخدم الوكيل والمعرّف **generalID** الاسم المستعار للحارس البوابي GK1. ويحسب المخدم الوكيل بعد ذلك توقيعاً جديداً للرسالة **ARQ** هذه باستعمال مفتاحه

الخاص وخوارزمية التوقيع ويدرجه في المجال **signature** من **token** ويضيف شهادته **certificate**. ويدرج المخدم الوكيل أيضاً **CryptoToken** من طرف إلى طرف مع **ClearToken** التابع له والذي استقبله في الرسالة الجديدة الخارجة ويرسل الرسالة **ARQ** إلى الحارس البوابي GK1. ويتم أيضاً إرسال التوقيع الذي تحسبه النقطة EP1 على أساس انتقاء مجالات الرسالة **ARQ** (**tokenOID** بالقيمة "B") والذي لم يكن موجهاً إلى المخدم الوكيل، بدون تغيير في الرسالة **ARQ** إلى الحارس البوابي GK1.

وعندما يستلم الحارس البوابي GK1 الرسالة **ARQ** يتحقق من التواقيع ويحسب التوقيع الجديد بعد تغيير المجالات **ClearToken** بالقيمة **toBeSigned** بالشكل المناسب ويدرجه في المجال **signature** ويضيف شهادته **certificate** ويرسل الرسالة **Setup** إلى النقطة EP2. وهنا أيضاً ينبغي أن يرسل الحارس البوابي GK1 كل معلومة مستقبلة من طرف إلى طرف في المجالات **CryptoTokens** المنفصلة إلى الحارس البوابي الند GK2 واضعاً هذه المعلومات دون تغيير في **CryptoToken** منفصل.

2.15 استيقان الرسائل RAS بمفرده

لنأخذ حالة اتصال قفزة قفزة ترغب فيه النقطة EP1 بإرسال رسالة RAS – رسالة **ARQ** مثلاً – إلى الحارس البوابي GK1. تطبع النقطة EP1 الوقت والساعة ورقم التتابع وتدرجها في المجالين **timeStamp** و**random** على التوالي مع اسم المخدم الوكيل في المجال **generalID** ومعرّف هوية النقطة EP في **sendersID**. وتوجد هذه المجالات في المجال **ClearToken** من **toBeSigned** الموجود في **token** من **cryptoSignedToken** للمجال **CryptoToken** من **cryptoH323Token** من الرسالة **ARQ**. ويوضع المجال **tokenOID** من **cryptoSignedToken** على "B" للدلالة على أن المجموعة الفرعية المحددة من مجالات الرسالة **ClearToken** هي وحدها موقعة. ويوضع المجال **algorithmOID** من **token** من **cryptoSignedToken** على "V" للدلالة على استخدام المجموعة MD5-RSA ، أو على "W" للدلالة على استخدام الخوارزمية SHA1-RSA، ويوضع المجال **params** على NULL. وتحسب EP1 بعد ذلك التوقيع استناداً إلى خوارزمية التوقيع المعني باستعمال مفتاحها الخاص. ويحسب التوقيع في المجالات **ClearToken** المحددة في **ARQ**. وتشمل النقطة EP1 التوقيع المحسوب في **signature** من المجال **token** للمجال **cryptoSignedToken** من **CryptoToken** الموجود في **cryptoH323Token** في الرسالة **ARQ** وتدرج شهادتها **certificate**.

وبنفس الطريقة تنتج النقطة EP1 توقيعاً رقمياً آخر للاستيقان من طرف إلى طرف الذي يغطي عدة مجالات **ClearToken** في **CryptoToken** منفصل للرسالة **ARQ**. ويدرج هذا التوقيع الرقمي (المعرَّف بالمعرِّف **tokenOID** بالقيمة "V" أو "W"). ثم ترسل الرسالة **ARQ** إلى المخدم الوكيل.

وعندما يستقبل المخدم الوكيل الرسالة **ARQ** يتحقق من توقيع الفيش المرسلة إليه (الفيش ذات القيمة "B" **tokenOID** في هذه الحالة مثلاً) استناداً إلى عدة معايير هي:

- حداثة التاريخ والساعة وفرادة **random**؛
- هوية **generalID** ومعرفه الخاص؛
- تراخيص النفاذ للمرسل **sendersID**؛
- توافق توقيع الرسالة **ARQ** مع التوقيع الذي يقوم الحارس البوابي GK1 بحسابه؛
- التحقق من الشهادة المستقبلة.

إذا كان التحقق من التوقيع إيجابياً يحسب المخدم الوكيل توقيعاً جديداً يستعيض به عن التوقيع القديم في الرسالة **ARQ** قبل أن يرسلها إلى الحارس البوابي GK1 بالطريقة التالية: يستعيض المخدم الوكيل عن المجالات **timeStamp** و**random** و**sendersID** و**generalID** في المجال **ClearToken** من **toBeSigned** بالقيم التي تطبق على المقطع الواقع بين المخدم الوكيل والحارس البوابي GK1. ويضم المجال **timestamp** طابع الوقت النافذ ويضم المجال **random** رقم التتابع التالي المتزايد بوتيرة واحدة للمقطع الواقع بين المخدم الوكيل وGK1 ويضم **generalID** اسم الحارس البوابي GK1. ويحسب المخدم

الوكيل بعد ذلك توقيعاً جديداً لهذا المجال **ClearToken** مستخدماً مفتاحه الخصوصي وخوارزمية التوقيع MD5-RSA أو SHA1-RSA (**algorithmOID**) بالقيمة "V" أو "W")، ويدخله في **signature** للمجال **token** من **cryptoSignedToken** ويضيف شهادته **certificate** ويرسل الرسالة **ARQ** إلى الحارس البوابي GK1. ويرسل أيضاً التوقيع الذي تحسبه النقطة EP1 على أساس انتقاء المجالات **ClearToken** للرسالة **ARQ** (**tokenOID**) بالقيمة "B") والذي لم يكن موجهاً إلى المخدم الوكيل دون أن يدخل أي تغيير في الرسالة **ARQ**، إلى الحارس البوابي GK1.

وعندما يستقبل الحارس البوابي GK1 الرسالة **ARQ** يتحقق من التواقيع ويقوم بحساب توقيع جديد تغيير المجالات **ClearToken** إلى **toBeSigned** بالشكل المناسب، ويدرجه في المجال **signature** وينقل الرسالة **Setup** إلى النقطة EP2. وتدرج معلومات التوقيع من طرف إلى طرف للنقطة EP1 في الرسالة **Setup** دون أي تغيير.

3.15 استيقان الرسالة H.225.0 وتكاملها وعدم نكرانها

الإجراء المطبق على الرسائل H.225.0 هو ذاته للرسائل RAS. ويكمن الاختلاف الوحيد في ضرورة تعرف هوية مجمل المجالات التي يستحسن توقيعها عندما يكون المعرّف **tokenOID** موضوعاً على "B" في كل رسالة من رسائل تشوير النداء H.225.0.

4.15 استيقان الرسالة H.245 وتكاملها

لنأخذ الحالة التي ترغب فيها النقطة EP1 بإرسال رسالة H.245، ولتكن رسالة **TerminalCapabilitySet** مثلاً، على النقطة EP2. وتحدد النقطة EP1 ما إذا كانت الرسالة H.225.0 بحاجة لأن ترسل إلى المخدم الوكيل. وفي هذه الحالة تسيّر الرسالة H.245 عبر النفق ضمن هذه الرسالة H.225.0. وتوضع مجالات الرسالة H.225.0 على القيم المذكورة سابقاً لأغراض إرسال الرسائل H.225.0. ونظراً إلى أن الرسالة H.245 مسيرة في النفق فإن المجالات **h323-uu-pdu** من الرسالة **h323-UserInformation** توضع على النحو التالي:

- يوضع المجال **h323-message-body** على نمط الرسالة H.225.0 قيد الإرسال.
- يوضع المجال **h245Tunnelling** على TRUE.
- يضم المجال **h245Control** سلسلة أثمونات وحدة المعطيات البروتوكولية H.245 PDU.

لكن في حال عدم وجود أي رسالة H.225.0 بانتظار الإرسال، فإن الرسالة H.245 تسيّر في النفق ضمن رسالة H.225.0 **facility** خاصة. وتوضع المجالات **h323-uu-pdu** للرسالة **h323-UserInformation** على النحو التالي:

- **h323-message-body** على القيمة **facility** التي تضم:
  - **reason** على القيمة **undefinedReason**؛
  - **tokens** و**cryptoTokens** كما هو الحال في كل رسالة H.225.0.
- **h245Tunnelling** على TRUE.
- يضم **h245Control** سلسلة أثمونات الوحدة H.245 PDU.

ثم ترسل النقطة EP1 الرسالة **facility** إلى المخدم الوكيل.

وفي كلا الحالتين (حالة رسالة H.225.0 بانتظار الإرسال أو استعمال رسالة **facility** H.225.0 خاصة) يتحقق المخدم الوكيل من التوقيع المخصص لهذا الغرض (وفي هذه الحالة مثلاً في "A" **tokenOID**) عند استقبال الرسالة. ثم إذا كانت الرسالة H.225.0 تنتظر الإرسال إلى مقطع المخدم الوكيل – الحارس البوابي GK1، تسيّر الرسالة H.245 في النفق ضمن هذه الرسالة؛ وإلا فإنها تسيّر في النفق ضمن رسالة **facility** H.225.0 خاصة. وكما هو الحال بالنسبة إلى إرسال كل رسائل تشوير النداء H.225.0، يتم حساب توقيع جديد لهذه الرسالة قبل إرسالها من المخدم الوكيل إلى الحارس البوابي GK1. ويتم

إرسال التوقيع الذي كان سبق إرساله من النقطة EP1 إلى المخدم الوكيل والذي لم يكن موجهاً إلى المخدم الوكيل دون أي تغيير من المخدم الوكيل إلى الحارس GK1.

وتقدم هذه الفقرة ملخصاً للكيفية والرسائل التي تتبعها مواصفة الأمن من أجل توفير الأمن لمختلف رسائل التشوير H.323.

16 المواءمة مع السياق H.235 في الطبعة 1

بالرغم من أن مواصفات الأمن المذكورة قد أعدت للسياق H.235 طبعة 2 (التوصية ITU-T H.235v2) إلا أنه يمكن تطبيقها في بيئة H.235 طبعة 1 (التوصية ITU-T H.235v1) مع إدخال بعض التعديلات الطفيفة. وباستطاعة المرسل إليه أن يكشف وجود الطبعة في البروتوكول H.235 الذي يستعمله المرسل عن طريق تقويم معرفات هوية أغراض مواصفة الأمن (انظر الفقرة 20).

التطبيقات H.235 طبعة 1 (التوصية ITU-T H.235v1) هي:

- عدم إعطاء قيمة للمجال **sendersID** من **ClearToken** أو عدم تقييمه.

17 السلوك في الإذاعة المتعددة

ينبغي أن تضم الرسائل H.225.0 متعددة الإذاعة مثل **GRQ** و**LRQ** مجالاً **CryptoToken** طبقاً للإجراءين II وIII عند عدم وضع أي قيمة في المجال **generalID**. وعندما تكون إذاعة مثل هذه الرسائل أحادية ينبغي أن تحتوي الرسالة على المعلمة **CryptoToken**.

18 قائمة برسائل التشوير المؤمَّنة

1.18 الرسالة RAS H.225.0

الرسالة RAS H.225.0	مجالات التشوير H.235	استيقان بمفرده	استيقان مع تكامل	عدم نكران
جميعها	cryptoTokens	الإجراء III/II	الإجراء III/II	الإجراء III/II

ملاحظة – في حال الإذاعة الأحادية للرسائل ينبغي تطبيق الإجراء II أو الإجراء III مع استعمال مجالات الأمن في المعلمة **CryptoToken**.

2.18 تشوير النداء H.225.0

رسالة تشوير النداء H.225.0	مجالات التشوير H.235	استيقان بمفرده	استيقان مع تكامل	عدم نكران
Alerting-UUIE, CallProceeding-UUIE, Connect-UUIE, Setup-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	cryptoTokens	الإجراء III/II	الإجراء III/II	الإجراء III/II

19 استعمال المعرّفين sendersID وgeneralID

تضم المعلمة **ClearToken** مجالات المعرفين **sendersID** و**generalID**. وفي حال توفر معلومة تعرف الهوية تكون قيمة المعرّف **sendersID** هي قيمة معرف هوية الحارس البوابي (GKID) بالنسبة للرسالة القادمة من الحارس البوابي GK، وقيمة معرّف هوية النقطة الطرفية (EPID) بالنسبة للرسائل القادمة من النقطة الطرفية. وفي حال توفر معلومة تعرف الهوية أيضاً تكون قيمة المعرف **generalID** هي قيمة المعرف GKID بالنسبة للرسائل القادمة من النقطة الطرفية، وقيمة المعرف EPID بالنسبة للرسائل القادمة من الحارس البوابي. وفي حال عدم توفر معلومات عن الهوية أو في حال التباس الإذاعة/الإذاعة المتعددة يكون المجال غائباً أو يضم سلسلة من الأصفار. ويلخص الجدول 2 الوارد أدناه هذه الحالة.

الجدول H.235.2/2 – استعمال المعرفين sendersID وGeneralID

الرسالة	sendersID	generalID
Unicast **GRQ**	**EPID** إن توفر وإلا **NULL**	**GKID**
Multicast **GRQ**	**EPID** إن توفر وإلا **NULL**	
GCF, GRJ	**GKID**	**EPID** إن توفر وإلا **NULL**
Initial **RRQ**		**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (EP-to-GK)	**EPID**	**GKID**
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (GK-to-EP)	**GKID**	**EPID**
ARQ, IRQ, RAI	**EPID**	**GKID**
ACF, ARJ, BCF, LCF, LRJ, IRR, IRQ, RAC, LCF, LRJ, IACK, INAK	**GKID**	**EPID**
Unicast **LRQ** (EP-to-GK)	**EPID**	**GKID**
Unicast **LRQ** (GK-to-GK)	**GKID**	**GKID**
Multicast **LRQ**	**EPID**	
ملاحظة – GKID هو معرف هوية الحارس البوابي وEPID معرف هوية النقطة الطرفية. ويدل الفراغ على سلسلة تعرف هوية ناقصة أو معدومة القيمة.		

20 قائمة معرّفات هوية الغرض

يضم الجدول 3 جميع المعرّفات OID التي ورد ذكرها (انظر أيضاً [OIW] و[WEBOIDs]). وهناك معرّفات للطبعة H.235v1 [H.235v1] وللطبعة H.235v2 [H.235v2].

الجدول H.235.2/3 – معرّفات هوية الغرض

اسم المعرف OID	قيمة (قيم) المعرف OID	الوصف
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	يستعمل في الإجراء II لأغراض CryptoToken-tokenOID للدلالة على أن التوقيع يضم **جميع** مجالات الرسالة H.225.0 RAS أو رسالة تشوير النداء (استيقان مع تكامل).
"B"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 2}	يستعمل في الإجراء II لأغراض CryptoToken-tokenOID للدلالة على أن التوقيع يضم مجموعة فرعية **subset** من مجالات الرسالة RAS/H.225.0 (ClearToken) لأغراض المطاريف مع الاستيقان بمفرده دون التكامل. يستعمل في الإجراء IA الوارد في H.235.1 لأغراض CryptoToken-tokenOID للدلالة على أن التظليل يضم مجموعة فرعية من مجالات الرسالة RAS/H.225.0 (ClearToken) لأغراض المطاريف مع الاستيقان بمفرده دون التكامل.
"P"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 4} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 4}	يستعمل في الإجراء I أو الإجراء II للدلالة على أن المجال **certificate** يسيّر عنواناً URL.
"R"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 3} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 3}	يستعمل في الإجراء II لأغراض ClearToken-tokenOID للدلالة على أن المعلمة ClearToken قيد الاستعمال للقيام بالاستيقان/التكامل من طرف إلى طرف
"S"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 7} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 7}	يستعمل في الإجراء II ويدل هذا المعرف tokenOID على الاستيقان والتكامل وعدم نكران الرسالة.
"V"	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}	يستعمل في الإجراء II أو III كمعرف OID خوارزمية ويدل على استعمال التوقيع الرقمي MD5-RSA.
"W"	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}	يستعمل في الإجراء II أو III كمعرف OID خوارزمية ويدل على استعمال التوقيع الرقمي SHA1-RSA.

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

طُبع في سويسرا
جنيف، 2006