الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

J.1015
(2020/04)

السلسلة J: الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط

النفاذ المشروط والحماية – الحلول المدمجة القابلة للمبادلة للنفاذ المشروط وإدارة الحقوق الرقمية

السطح البيني المشترك المدمج من أجل الحلول القابلة للمبادلة للنفاذ المشروط/إدارة الحقوق الرقمية: نظام الأمن المعزز – مجموعة سلالم المفاتيح

التوصية ITU-T J.1015

الاتحاد الدولي للاتصالات ITU

التوصية ITU-T J.1015

السطح البيني المشترك المدمج من أجل الحلول القابلة للمبادلة للنفاذ المشروط/ إدارة الحقوق الرقمية: نظام الأمن المعزز – مجموعة سلالم المفاتيح

ملخص

التوصية ITU-T J.1015 جزء من سلسلة تتناول مجموعة سلالم المفاتيح لنظام الأمن المعزز فيما يخص السطح البيني المشترك المدمج من أجل توصيف حلول النفاذ المشروط/إدارة الحقوق الرقمية (CA/DRM) القابلة للمبادلة.

وهذه التوصية الصادرة عن قطاع تقييس الاتصالات هي نقل للمعيار [b-ETSI GS ECI 001-5-2] الصادر عن المعهد الأوروبي لمعايير الاتصالات (ETSI) ونتاج للتعاون بين لجنة الدراسات 9 لقطاع تقييس الاتصالات والفريق ETSI ISG ECI.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T J.1015	2020-04-23	9	11.1002/1000/13576

مصطلحات أساسية

النفاذ المشروط (CA)، إدارة الحقوق الرقمية (DRM)، المبادلة

* 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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

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

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

جدول المحتويات

الصفحة

مقدمة

هذه التوصية الصادرة عن قطاع تقييس الاتصالات[1] هي نقل للمعيار [b-ETSI GS ECI 001-5-2] الصادر عن المعهد الأوروبي لمعايير الاتصالات (ETSI) ونتاج للتعاون بين لجنة الدراسات 9 لقطاع تقييس الاتصالات والفريق ETSI ISG ECI.

والهدف من هذه التوصية هو تيسير إمكانية التشغيل البيني والمنافسة في خدمات الاتصالات الإلكترونية، ولا سيما في سوق أجهزة البث والأجهزة السمعية والبصرية. ومع ذلك، هناك تكنولوجيات أخرى قد تكون مناسبة ومفيدة أيضاً حسب ظروف الدول الأعضاء.

يقوم مقدّم المحتوى بتجفير المحتوى الرقمي الخاص به ويستخدم **نظام حماية المحتوى**[2] لحماية المحتوى من النفاذ غير المرخص. ويستعمل المستهلك **مستقبِل المحتوى** للنفاذ إلى المحتوى المحمي. ولهذه الغاية، يتضمن **مستقبِل المحتوى** رقاقة تنفّذ واحدة أو أكثر من عمليات فكّ تجفير المحتوى. ويستخدم بروتوكول إنشاء المفاتيح المجفرة لتأمين نقل مفاتيح تجفير المحتوى من **نظام حماية المحتوى** إلى الرقاقة. ويشار في هذه التوصية إلى خطوات البروتوكول التي تنفذ داخل الرقاقة بأنها سلم المفاتيح، حيث تحدد سلّم مفاتيح لبروتوكول إنشاء المفاتيح الوارد في [b-ROEL].

ويمكن أيضاً استعمال سلم المفاتيح والبروتوكول لتأمين نقل مفاتيح تجفير المحتوى إلى الرقاقة. وهذه المفاتيح ضرورية لحالات الاستعمال التي تعيد فيها الرقاقة تجفير المحتوى. ولهذا الغرض يمكن للرقاقة أن تنفذ واحدة أو أكثر من عمليات تجفير المحتوى. ويعتبر تسجيل الفيديو الشخصي وإرسال محتوى محمي إلى **نظام مختلف لحماية المحتوى** من الأمثلة النموذجية على حالات استعمال إعادة تجفير المحتوى. ويشار إلى كلّ من مفاتيح فك تجفير المحتوى ومفاتيح تجفير المحتوى **بكلمات التحكم** (CW) في هذه التوصية بأكملها.

كما تحدد هذه التوصية آلية للاستيقان. وترتبط هذه الآلية ارتباطاً وثيقاً بسلم المفاتيح ويمكن استعمالها للاستيقان من الكيان؛ وبعبارة أخرى يمكن استعمال هذه الآلية للاستيقان من الرقاقة.

ويتميز سلم المفاتيح وآلية الاستيقان المحددان في هذه التوصية بأنهما مستقلان عن كل من **نظام حماية المحتوى** و**مقدم المحتوى**. يمكّن ذلك **مقدّم المحتوى** من استعمال أي **نظام مطابق لحماية المحتوى**، ويمكّن المستهلك من استعمال **مستقبِل المحتوى** للنفاذ إلى محتوى أي **مقدّم للمحتوى** يستعمل **نظاماً مطابقاً لحماية المحتوى**.

وتتولى **سلطة إصدار الشهادات** إدارة شهادة مفتاح عمومي لكل رقاقة بواسطة الآليات المحددة في هذه التوصية. وبوجه خاص، توزع **سلطة إصدار الشهادات** هذه الشهادات والمعلومات بشأن إبطال الشهادات إلى **مقدمي المحتوى** الذين يرغبون في الاستفادة من سلم المفاتيح و/أو آلية الاستيقان. بعد ذلك، يستعمل **مقدمو المحتوى** الشهادات والمعلومات بشأن إبطال الشهادات كمدخلات في **نظام حماية المحتوى** المطابق الخاص بهم؛ وكما هو مفصل في الفقرة 7؛ تسمح معرفة المفتاح العمومي في شهادة الرقاقة **لنظام حماية المحتوى** بتوليد رسائل دخل مناسبة لسلم مفاتيح الرقاقة وآلية الاستيقان الخاصتين بالرقاقة.

---

1 تم تحديد العديد من المجالات لمزيد من التطوير في التذييل I.

2 يشير استخدام الخط البارز في نص هذه التوصية إلى المصطلحات ذات التعاريف الخاصة بسياق السطح البيني المشترك المدمج والتي قد تختلف عن الاستخدام الشائع.

السطح البيني المشترك المدمج من أجل الحلول القابلة للمبادلة للنفاذ المشروط/ إدارة الحقوق الرقمية: نظام الأمن المعزز – مجموعة سلالم المفاتيح

1 مجال التطبيق

تحدد هذه التوصية مجموعة سلّم المفاتيح للتنفيذ في رقاقة **مستقبِل المحتوى**. وتتألف مجموعة سلّم المفاتيح من سلم مفاتيح يؤمن نقل **كلمات التحكم** (CW) إلى الرقاقة وآلية استيقان. كما تحدد هذه التوصية الجوانب المتعلقة بإضفاء الصبغة الشخصية على الرقاقة المطابقة.

وقد أُعدّت هذه التوصية لكي يستعملها مصنّعو الرقاقات.

2 المراجع

يشتمل ما يلي من توصيات قطاع تقييس الاتصالات والمراجع الأخرى على أحكام تشكّل، من خلال الإشارة إليها في هذا النص، أحكاماً في هذه التوصية. وكانت الطبعات المشار إليها صالحة وقت نشر هذه التوصية. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة يرجى من جميع المستخدمين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى أي وثيقة في هذه التوصية لا يضفي على الوثيقة، بحد ذاتها، صفة توصية.

[ISO/IEC 9797-1] ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.

[IETF RFC 8017] IETF RFC 8017 (2016), *PKCS #1: RSA cryptography specifications version 2.2*.

[NIST FIPS 180-4] NIST FIPS PUB 180-4 (2015), *Secure Hash Standard (SHS)*.

[NIST FIPS 197] NIST FIPS PUB 197 (2001), *Specification for the Advanced Encryption Standard (AES)*.

[NIST SP 800-107] NIST SP 800-107 Revision 1 (2012), *Recommendation for applications using approved hash algorithms.*

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

لا يوجد.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرَّف في هذه التوصية المصطلحات التالية:

1.2.3 سلطة إصدار الشهادات (certification authority): الطرف المسؤول عن إدارة شهادات المفاتيح العمومية في **نظام إيكولوجي للسطح البيني المشترك المدمج (ECI)**. تثق جميع الأطراف الأخرى في النظام في سلطة إصدار الشهادات لتنفيذ العمليات المرتبطة بالشهادات.

2.2.3 معرف هوية الرقاقة (chipset-ID): رقم غير سري يستعمل لتحديد هوية الرقاقة داخل **نظام إيكولوجي للسطح البيني المشترك المدمج (ECI)**.

3.2.3 نظام حماية المحتوى (content protection system): نظام في **النظام الإيكولوجي للسطح البيني المشترك المدمج (ECI)** يستخدم تقنيات التجفير لإدارة النفاذ إلى المحتوى والخدمات. ويمكن دائماً استخدام المصطلح كمرادف لمصطلح "نظام حماية الخدمة". والأنظمة النموذجية من هذا النوع هي إما "أنظمة النفاذ المشروط" (CA) أو أنظمة إدارة الحقوق الرقمية" (DRM).

4.2.3 مقدم المحتوى (content provider): طرف يقوم بتوزيع المحتوى الرقمي **لمستقبِل المحتوى** في **نظام إيكولوجي للسطح البيني المشترك المدمج**

5.2.3 مستقبِل المحتوى (content receiver): جهاز يستخدم للنفاذ إلى محتوى رقمي داخل **نظام إيكولوجي للسطح البيني المشترك المدمج**. ويتضمن **مستقبِل المحتوى** رقاقة بها **مزيل تخليط المحتوى**.

6.2.3 مزيل تخليط المحتوى (content descrambler): مكون في رقاقة نظام إيكولوجي للسطح البيني المشترك المدمج قادر على فك تجفير المحتوى. وقد يكون **مزيل تخليط المحتوى** قادرًا أيضًا على تجفير المحتوى (لغرض إعادة تجفير المحتوى). وفي هذه التوصية، يستخدم تجفير/فك تجفير المحتوى مخطط تجفير متناظر. وبالنسبة لمحتوى MPEG-2، يُشار أيضًا إلى تجفير المحتوى وفك تجفيره باسم التخليط وإزالة التخليط، على التوالي.

7.2.3 كلمة التحكم (control word): مفتاح سري يستخدم لتجفير وفك تجفير المحتوى داخل **نظام إيكولوجي للسطح البيني المشترك المدمج**. وفي أنظمة إدارة الحقوق الرقمية، يشار إلى كلمة التحكم عادة باسم مفتاح المحتوى.

8.2.3 وظيفة التمويه التجفيري (cryptographic hash function): وظيفة تجفير بدون مفاتيح في **نظام إيكولوجي للسطح البيني المشترك المدمج** تأخذ بيانات ذات حجم عشوائي، يشار إليها بالرسالة، كمدخلات وتنتج مجموعة بيانات مخرجات ذات حجم ثابت، يشار إليها باسم ملخص الرسالة. والخصائص المفترضة **لوظيفة التمويه التجفيري** في هذه التوصية هي أن **وظيفة التمويه التجفيري** تتصرف كوظيفة عشوائية ومقاومة للتكون المسبق للصورة الثانية.

9.2.3 مخطط التوقيع الرقمي (digital signature scheme): مخطط تجفير لا تناظري بمفاتيح يستخدم لحماية استيقان البيانات في **نظام إيكولوجي للسطح البيني المشترك المدمج**. ويتكون **مخطط التوقيع الرقمي** من خوارزمية إنشاء المفتاح وعملية إنشاء التوقيع وعملية التحقق من التوقيع. ويتم إنشاء المفاتيح في صورة أزواج (مفتاح سري/خاص، مفتاح عمومي). ويتم توقيع البيانات باستخدام مفتاح سري/خاص ويتم استخدام المفتاح العمومي المقابل للتحقق من التوقيع. ويستخدم **مخطط التوقيع الرقمي** الموصف في هذه التوصية لحماية استيقان الرسائل على النحو المحدد في [b-ROEL]؛ خاصة أن هذا المخطط لا يستخدم في هذه التوصية لأغراض عدم الرفض أو الاستيقان من المصدر.

10.2.3 النظام الإيكولوجي للسطح البيني المشترك المدمج (ECI ecosystem): عملية تجارية تضم سلطة استوثاق والعديد من المنصات و**سطح بيني مشترك مدمج** – معدات منشآت العملاء المطابقة في الميدان.

11.2.3 خوارزمية شفرة استيقان الرسالة (message authentication code algorithm): خوارزمية تجفير تناظرية بمفاتيح تستخدم لحماية استيقان البيانات في **نظام إيكولوجي للسطح البيني المشترك المدمج**. و**خوارزمية شفرة استيقان الرسالة** تأخذ الرسالة والمفتاح السري كمدخلات وتنتج مجموعة بيانات مخرجات يشار إليها باسم شفرة استيقان الرسالة (MAC). وتستخدم **خوارزمية شفرة استيقان الرسالة** على النحو الموصف في هذه التوصية لربط رسالة نصية مشفرة تجفيرياً بالبيانات الخاصة بها؛ خاصة وأن الخوارزمية لا تستخدم في هذه التوصية لأغراض الاستيقان من المصدر.

12.2.3 مخطط تجفير المفاتيح العمومية (public-key encryption scheme): مخطط تجفير لا تناظري بمفاتيح يستخدم لحماية سرية البيانات في **نظام إيكولوجي للسطح البيني المشترك المدمج**. ويتألف **مخطط تجفير المفاتيح العمومية** من خوارزمية إنشاء مفاتيح وعمليتي تجفير وفك تجفير. ويتم إنشاء المفاتيح في صورة أزواج (مفتاح سري/خاص، مفتاح عمومي). وتُجفر البيانات باستخدام المفتاح العمومي وتستعاد البيانات من النص المشفر باستخدام المفتاح السري/الخاص المقابل.

13.2.3 مخطط التجفير التناظري (symmetric encryption scheme): مخطط تجفير تناظري بمفاتيح يستخدم لحماية سرية البيانات في **نظام إيكولوجي للسطح البيني المشترك المدمج**. ويتألف **مخطط التجفير التناظري** من خوارزمية إنشاء مفاتيح وعمليتي تجفير وفك تجفير. ويستخدم في عمليتي التجفير وفك التجفير الخاصتين **بمخطط التجفير التناظري** نفس المفتاح السري كمدخل.

4 المختصرات والأسماء المختصرة

تُستعمل في هذه التوصية المختصرات والتسميات المختصرة التالية:

AES معيار التجفير المتقدم *(Advanced Encryption Standard)*

AD1 البيانات المرتبطة 1 *(Associated Data 1)*

AD2 البيانات المرتبطة 2 *(Associated Data 2)*

AK مفتاح الاستيقان *(Authentication Key)*

CA النفاذ المشروط *(Conditional Access)*

CID معرّف هوية الشركة *(Company IDentifier)*

CISSA خوارزمية التخليط الشائعة الموجهة للبرمجيات الخاصة بتلفزيون بروتوكول الإنترنت *(Common IPTV Software-oriented Scrambling Algorithm)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

CSA خوارزمية التخليط الشائعة *(Common Scrambling Algorithm)*

CPK المفتاح العمومي للرقاقة *(Chipset Public Key)*

CSK المفتاح السري/الخصوصي للرقاقة *(Chipset Secret/private Key)*

CW كلمة التحكم *(Control Word)*

DRM إدارة الحقوق الرقمية *(Digital Rights Management)*

DVB الإذاعة الفيديوية الرقمية *(Digital Video Broadcasting)*

ECB كتاب الشفرة الإلكتروني *(Electronic Code Book)*

ECI السطح البيني المشترك المدمج *(Embedded Common Interface)*

ECP حماية المحتوى المعززة *(Enhanced Content Protection)*

ID معرّف الهويّة *(IDentity)*

LK مفتاح الوصلة *(Link Key)*

MAC شفرة الاستيقان من الرسالة *(Message Authentication Code)*

MK مفتاح شفرة الاستيقان من الرسالة *(MAC Key)*

OUI المعرّف الفريد على مستوى المنظمة *(Organizationally Unique Identifier)*

RSA ريفيست وشامير وأدلمان *(Rivest Shamir Adleman)*

SHA خوارزمية فرم آمنة *(Secure Hash Algorithm)*

SIM رسالة دخل موقّعة *(Signed Input Message)*

SPK المفتاح العمومي للمرسِل *(Sender Public Key)*

SSK المفتاح السري/الخصوصي للمرسِل *(Sender Secret/private Key)*

T وسم *(Tag)*

URI معلومات قواعد الاستعمال *(Usage Rules Information)*

5 الاصطلاحات

تشير الحروف البارزة في هذه التوصية إلى المصطلحات ذات التعاريف الخاصة بسياق السطح البيني المشترك المدمج والتي قد تختلف عن الاستخدام الشائع.

6 معرف هوية الرقاقة وزوج المفاتيح الرئيسي للرقاقة

تحدد هذه الفقرة الجوانب المتعلقة بإضفاء الصبغة الشخصية على رقاقة متوافقة. وترتبط كل رقاقة متوافقة بمعرف هوية (ID) للرقاقة من سلسلة بتّات، يشار إليه باسم **معرف هوية الرقاقة**، وبزوج مفاتيح رئيسي للرقاقة.

وتعيّن لكل رقاقة متوافقة **هوية رقاقة** فريدة عالمياً تتألف من 64 بتة. وإذا أعطيت بتات **هوية الرقاقة** الأرقام من 0 إلى 63 من اليسار إلى اليمين وأعطيت البتة رقم i ($0 \le i \le 63$) الرمز b_i، عندئذ تحتوي البتات (b_0, b_1, b_2, b_3) على معرّف هوية سلطة التسجيل. وترتبط كل قيمة من قيم معرّف هوية سلطة التسجيل بسلطة تسجيل واحدة على الأكثر. وتحتوي **هوية الرقاقة** أيضاً على معرّف هوية مصنّع الرقاقة. وتتحدد هوية المصنّع الذي أنتج الرقاقة على نحو فريد بقيمة معرّف هوية سلطة التسجيل ومعرّف هوية مصنّع إحدى الرقاقات المتوافقة مع **هوية الرقاقة**. بالإضافة إلى ذلك، تتولى سلطة التسجيل المعرّفة بقيمة السلسلة (b_0, b_1, b_2, b_3) إدارة تخصيص معرفات هوية مصنّعي الرقاقات التي يمكن استعمالها بالاقتران مع هذه القيمة.

وإذا كان (b_0, b_1, b_2, b_3) = (0, 0, 0, 0)، عندئذ تصبح سلطة التسجيل التابعة لمعهد مهندسي الكهرباء والإلكترونيات (IEEE) (https://standards.ieee.org/faqs/regauth.html) هي سلطة التسجيل ويستخدم المعرف الفريد على مستوى المنظمة (OUI) المؤلف من 24 بتة أو معرّف هوية الشركة (CID) المؤلف من 24 بتة لتحديد هوية مصنعي الرقاقة. وبالإضافة إلى ذلك، إذا كان (b_0, b_1, b_2, b_3) = (0, 0, 0, 0)، عندئذ تحتوي السلسلة (b_4, b_5, …, b_{27}) على المعرّف OUI أو CID، حيث تمثل b_4 البتة الأكثر دلالة في الأثمون رقم 0 للمعرّف OUI/CID (انظر أيضاً [b-IEEE-OUI]) وتمثل b_{27} البتة الأقل دلالة في الأثمون رقم 2 للمعرّف OUI/CID.

ويحتفظ بجميع القيم الأخرى لمعرّف هوية سلطة التسجيل لاستخدامها في المستقبل.

يكون زوج المفاتيح الرئيسية للرقاقة مقترناً بمخطط تجفير للمفتاح العمومي، ويتألف من مفتاح سري/خصوصي للرقاقة (CSK) ومفتاح عمومي للرقاقة (CPK). وكما سيرد بشكل مفصل في الفقرتين 0 و0، يعتبر الثنائي (CSK, CPK) زوج المفاتيح الرئيسي لكل من سلم المفاتيح وآلية الاستيقان. وتحدد الفقرة 0 مواصفات **مخطط تجفير المفتاح العمومي** وتمثيل المفتاحين CSK وCPK.

وينبغي للرقاقة المتوافقة أن تولّد زوج المفاتيح الخاص بها (CSK, CPK) لمنع كشف أي جزء من أجزاء النظام لقيمة المفتاح CSK. وفي هذه الحالة يتعين توزيع **معرف هوية الرقاقة** على الرقاقة أثناء إضفاء الصبغة الشخصية عليها، علماً بأنه يجب حماية الاستيقان من **معرف هوية الرقاقة** أثناء هذا التوزيع. وإذا لم تولّد الرقاقة زوج المفاتيح الخاص بها، عندئذ يجب حماية الاستيقان من الثلاثية (**معرف هوية الرقاقة**، CSK، CPK) وسرية المفتاح CSK أثناء توزيع الثلاثية على الرقاقة.

ويجب أن يتصف العدد العشوائي الذي يستخدم كدخل لخوارزمية توليد زوج المفاتيح (CSK, CPK) بأنتروبيا لا تقل عن 128 بتة.

تخزن الرقاقة المتوافقة بصورة دائمة الثلاثية (**معرف هوية الرقاقة**، CSK, CPK) الخاصة بها، وتنفذ تدابير لحماية سرية المفتاح CSK المختزن وسلامة **معرف هوية الرقاقة** المختزن والمفتاح CSK والمفتاح CPK المختزنين.

وتتمتع وحدة المعالجة المركزية (CPU) في **مستقبِل المحتوى** بالنفاذ إلى قراءة **معرف هوية الرقاقة** المختزن والمفتاح العمومي للرقاقة المختزن. يمكّن ذلك **سلطة إصدار الشهادات** من استخدام المعلومات الصادرة بمثابة دخل لإصدار شهادة المفتاح العمومي للرقاقة. بالإضافة إلى ذلك، يسمح **معرف هوية الرقاقة** الصادر **لمقدّم المحتوى** بالتعرّف على الرقاقة والشهادة الخاصة بها.

وتحافظ **سلطة إصدار الشهادات** على الزوج (**معرف هوية الرقاقة**، CPK) لكل رقاقة تقوم بإدارتها. ولا تستبعد هذه التوصية وجود أكثر من **سلطة واحدة لإصدار الشهادات** في النظام. ويجب حماية الاستيقان من الزوج (**معرف هوية الرقاقة**، CPK) خلال توزيعه على **سلطة** (أو سلطات) **إصدار الشهادات** المقترنة به.

7 سلّم المفاتيح

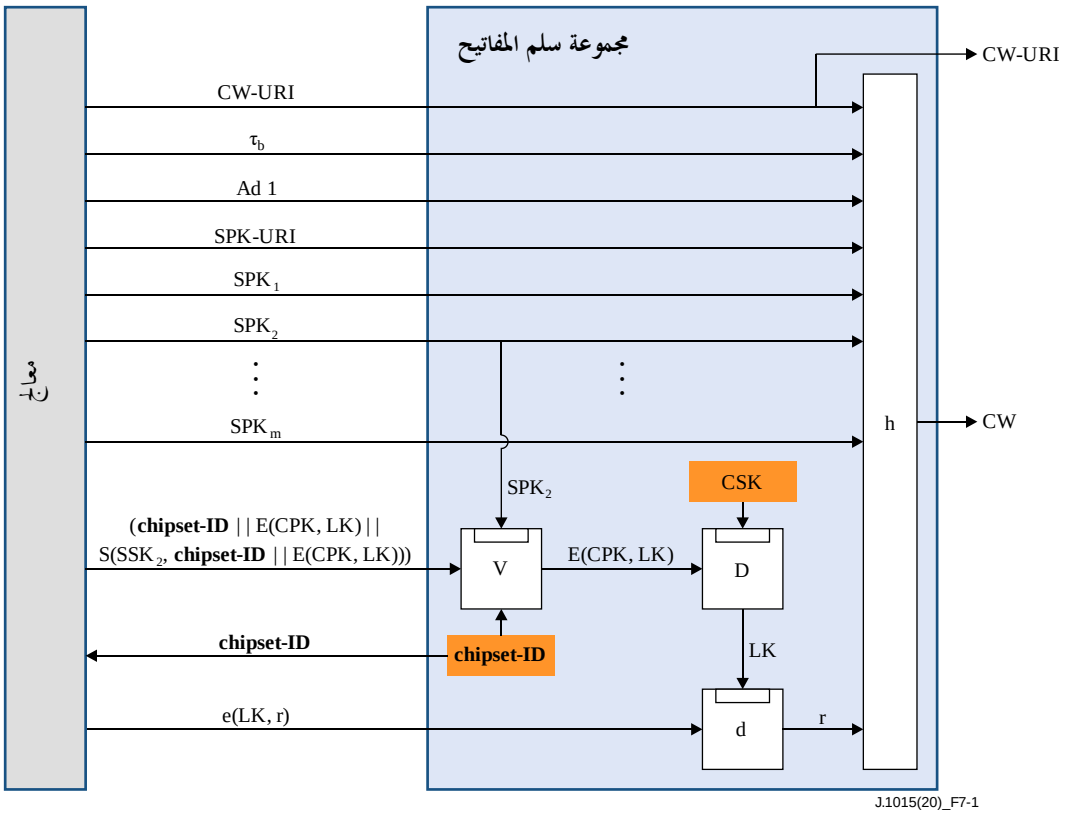
1.7 لمحة عامة

تعرض هذه الفقرة التصميم الوظيفي لسلم المفاتيح. ويشار في هذه التوصية بأكملها إلى المجموعة التي تنفذ سلم المفاتيح في الرقاقة باسم مجموعة سلّم المفاتيح. ويبيّن الشكل 7-1 سلم المفاتيح. وكما ورد في الفقرة 6 وعلى النحو المبين في الشكل، يتم إضفاء الصبغة الشخصية على الرقاقة بواسطة **معرف هوية الرقاقة** وبواسطة المفتاح السري/الخصوصي للرقاقة.

ويتمثل أحد مخرجات مجموعة سلالم المفاتيح **بكلمة التحكم** التي يشار إليها بالرمز CW، والتي تستعمل إما في فك تجفير المحتوى أو تجفيره. وهناك خرج ثانٍ من مجموعة سلالم المفاتيح يتمثل بسلسلة بتات تتألف من معلومات قواعد استخدام كلمة التحكم (CW-URI)، التي تحدد معلومات قواعد استعمال كلمات التحكم (أنظر الفقرة 1.1.6 للحصول على مواصفات السلسلة CW-URI وقواعد الاستعمال المرتبطة بها). وتشكل السلسلتان CW وCW-URI مدخلات **لمزيل تخليط المحتوى** (لا يظهر مزيل تخليط المحتوى في الشكل 7-1).

- تنفَّذ مجموعة سلم المفاتيح و**مزيل تخليط المحتوى** في شريحة سيليكونية واحدة.
- إذا توفر سطح بيني بين **مزيل تخليط المحتوى** والمعالج في **مستقبِل المحتوى** يسمح للمعالج بنقل **كلمات تحكم** مقروءة إلى **مزيل تخليط المحتوى** (أي بتخطي مجموعة سلّم المفاتيح)، يمكن عندئذ إبطال هذه الوظيفة بصورة دائمة.
- إذا أجرى سلم المفاتيح حساب كلمة التحكم CW، عندئذ لن يتمكن من النفاذ إلى هذه الكلمة إلا مجموعة سلّم المفاتيح **ومزيل تخليط المحتوى**.
- يجب حماية الاستيقان من الزوج (CW, CW-URI) وسرية الكلمة CW خلال انتقالهما من مجموعة سلم المفاتيح إلى **مزيل تخليط المحتوى**.

تتفاعل مجموعة سلالم المفاتيح عبر سطح بيني مع معالج **مستقبل المحتوى**. وعلى سبيل المثال، قد يكون المعالج معالج أمن وحدة المعالجة المركزية في **مستقبِل المحتوى**. وكما ورد في الفقرة 6 وعلى النحو المبين في الشكل 7-1، يتمتع هذا المعالج بالنفاذ إلى قراءة **هوية الرقاقة**. ويمكّن ذلك **مقدم المحتوى** من التعرّف على هوية الرقاقة والحصول من **سلطة إصدار الشهادات** على شهادة المفتاح العمومي المقابلة التي تحتوي على المفتاح CPK. ويجب أن تكون قيمة المفتاح CPK معروفة من أجل حساب إحدى رسائل الدخل إلى سلم المفاتيح، كما هو مبين في الفقرة 0.



الشكل 7-1 – سلم المفاتيح

وكما ورد في الفقرة 6، يرتبط الزوج (CSK, CPK) **بمخطط تجفير المفتاح العمومي**. ويشار إلى عمليتي التشفير وفك التشفير المقابلتين بالحرفين E وD على التوالي. وE وD هما عمليتا تجفير المفاتيح لكل منهما دخلان: دخل للمفتاح ودخل للرسالة. وتفترض هذه التوصية أن المفتاح يشكل أول دخل لعملية أو خوارزمية تجفير المفاتيح.

مثال: يكتب تجفير الرسالة M باستخدام E والمفتاح العمومي للرقاقة على الشكل E(CPK, M).

وتستخدم أيضاً الآليات المعروضة في هذه التوصية **مخطط توقيع رقمي**؛ ويشير الحرفان S وV إلى عملية توليد التوقيع وعملية التحقق من التوقيع على التوالي. ويقترن زوج مفاتيح **مخطط التوقيع الرقمي** بالمرسِل ويتألف من مفتاح سري/خصوصي للمرسل (SSK) ومفتاح عمومي للمرسِل (SPK). وتفترض هذه التوصية أن المرسِل هو **نظام حماية المحتوى**. وكما يبين الشكل 7-1، يشكل عدد من المفاتيح SPK المختلفة، التي يشار إليها بالمفاتيح $(m \geq 1)$ $SPK_1, SPK_2, ..., SPK_m$، مدخلات إلى مجموعة سلم المفاتيح. وتدعم المجموعة سلالم المفاتيح لجميع قيم m حيث $1 \leq m \leq 16$. وفي الممارسة العملية، يرتبط كل زوج مفاتيح (SSK_i, SPK_i) حيث $1 \leq i \leq m$ **بنظام واحد لحماية المحتوى**؛ ومع ذلك يمكن أن تشترك نظم متعددة في زوج مفاتيح واحد.

وترتبط السلسلة SPK-URI بالمفاتيح $SPK_1, SPK_2, ..., SPK_m$. ويحدد دخل مجموعة سلالم المفاتيح معلومات قواعد الاستعمال المتعلقة بالمفاتيح $SPK_1, SPK_2, ..., SPK_m$. وتحدد الفقرة 0 مواصفات السلسلة SPK-URI وقواعد الاستعمال المقترنة بها. وكما هو مبين في الشكل 7-1، يستعمل أحد المفاتيح SPK وعملية التحقق V للتأكد من التوقيع على رسالة الدخل (SIM) (**chipset-ID** || E(CPK, LK) || S(SSK_i, **chipset-ID** || E(CPK, LK))). يشار إلى رسالة الدخل الموقعة هذه في النص التالي باسم SIM_{KL}. ويفترض الشكل 7-1 أن $i = 2$ وأن SPK-URI وقواعد الاستعمال تسمح باستعمال SPK_2 للتحقق من التوقيع.

وينفذ سلم المفاتيح أيضاً **مخطط تجفير تناظري**. ويرمز إلى عمليات التجفير وفك التجفير في هذا المخطط بالحرفين e وd، على التوالي. ويستخدم سلم المفاتيح مفتاح الوصلة (LK) كمفتاح لهذا النظام وعدداً عشوائياً r (أو مفتاح وصلة آخر كما هو مبين في الفقرة 1.6) كرسالة. ويُمثل العدد العشوائي r بسلسلة بتات ويبلغ طوله 128 بتة.

أخيراً، تنفذ مجموعة سلم المفاتيح الدالة h. وتستند هذه الدالة إلى **وظيفة التمويه التجفيري** (انظر الفقرة 0 لمعرفة مواصفات الوظيفة h).

وكما هو مبين في الشكل 7-1، يُمثل الدخلان الأخيران لمجموعة سلالم المفاتيح بالكمية τ_b والبيانات المرتبطة 1 التي يشار إليها بالرمز AD1؛ ويُمثل هذان الدخلان على شكل سلاسل بتات:

- يكون طول τ_b بقيمة 8 بتات. وتحدد الفقرة 0 استعمال τ_b.
- يكون طول AD1 بقيمة 256 بتة. ولا تندرج مواصفات AD1 ضمن نطاق هذه التوصية التي تفترض أن مجموعة سلالم المفاتيح لا تقوم بمعالجة AD1 بل تقدمها كدخل للوظيفة h. ويمكن أن تنقل مجموعة سلالم المفاتيح AD1، أو جزءاً من AD1، إلى جانب CW-URI وCW إلى **مزيل تخليط المحتوى**.

وتفترض هذه التوصية أن المفاتيح المتناظرة ورسائل النص التجفيري والتواقيع تتمثل على شكل سلاسل بتات. ويتحدد طول هذه السلاسل في الفقرة 0. كما تتحدد مواصفات هذه المفاتيح المتناظرة في تلك الفقرة.

2.7 حسابات سلم المفاتيح

يستطيع المرسِل الذي يقترن بزوج المفاتيح (SSK_i, SPK_i)، حيث $1 \leq i \leq m$، إنشاء رسالة الدخل الموقعة SIM_{KL}، أي:

(**chipset-ID** || E(CPK, LK) || S(SSK_i, **chipset-ID** || E(CPK, LK)))

باتباع الخطوات التالية.

حساب SIM_{KL} (المرسِل):

1) توليد مفتاح الوصلة LK.

2) حساب النص التجفيري E(CPK, LK).

3) سَلسلة (**chipset-ID** and E(CPK, LK)؛ يُرمز إلى سلسلة البتات الناتجة بالرمز (**chipset-ID** || E(CPK, LK)).

4) توقيع سلسلة البتات (**chipset-ID** || E(CPK, LK)) باستعمال المفتاح SSK_i؛ يرمز إلى التوقيع بالرمز S(SSK_i, **chipset-ID** || E(CPK, LK))).

5) تذييل سلسلة البتات (**chipset-ID** || E(CPK, LK)) بهذا التوقيع.

وبعد استقبال SIM_{KL} والمفتاح العمومي للمرسِل SPK_i، تؤدي مجموعة سلم المفاتيح الخطوات التالية لاسترجاع المفتاح LK (يُفترض في الشكل 1.7-1 أن الخطوات الثلاث الأولى تنفذها عملية التحقق V).

حساب LK (مجموعة سلالم المفاتيح):

1) يتم التحقق مما إذا كانت **هوية الرقاقة** الواردة تساوي **هوية الرقاقة** المختزنة. وإذا كانت القيمتان غير متساويتين، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

2) يتم التحقق ما إذا كان SPK-URI وقواعد الاستعمال المحددة في الفقرة 2.3.7 تجيز لعملية التحقق V استخدام SPK_i للتحقق من التوقيع. وإذا لم يكن التوقيع صالحاً، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

3) يستخدم المفتاحان SIM_{KL} وSPK_i الواردان للتحقق من التوقيع. وإذا لم يكن التوقيع صالحاً، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

4) يحسب المفتاح LK = D(CSK, E(CPK, LK)).

بعد ذلك، تستخدم مجموعة سلم المفاتيح المفتاح LK لمعالجة الرسالة e(LK, *r*) (انظر أيضاً الشكل 7-1). ويمكن أن ينشئ المرسِل هذه الرسالة باتباع الخطوات التالية.

حساب E(LK, *r*) (المرسِل):

1) توليد سلسلة بتات عشوائية *r*.

2) حساب e(LK, *r*).

وبعد استقبال الرسالة e(LK, *r*) وحساب المفتاح LK، تجري مجموعة سلم المفاتيح حساب *r* باتباع الخطوة التالية (انظر أيضاً الشكل 7-1).

حساب R (مجموعة سلم المفاتيح):

1) $r = d(LK, e(LK, r))$.

بعد ذلك، تستخدم مجموعة سلم المفاتيح الدالة h لحساب كلمة التحكم. وكما هو مبين في الشكل 7-1، تمثل الكميات CW-URI، τ_b، AD1، SPK-URI، SPK_1، SPK_2 ... SPK_m و*r* مدخلات الوظيفة h. ويضمن تنفيذ مجموعة سلالم المفاتيح أن المفتاح العمومي الذي استعمل للتحقق من استيقان SIM_{KL} (أو بصورة أدق، المفتاح SIM_{KL} الذي يحتوي على مفتاح الوصلة المرتبط بالعدد العشوائي *r*) متوفر بوصفه أحد المدخلات SPK للدالة h حين تشتق كلمة التحكم CW من *r*. بعد ذلك تنقل مجموعة سلم المفاتيح الكميتين CW-URI وCW إلى **مزيل تخليط المحتوى**.

3.7 معلومات قواعد الاستعمال

1.3.7 معلومات قواعد استعمال كلمة التحكم

يبلغ طول معلومات قواعد استعمال كلمة التحكم (CW-URI) 64 بتة مرقمة من اليسار إلى اليمين من 0 إلى 63. وتحدد قيمة CW-URI الاستعمال المسموح لكلمة التحكم CW (انظر أيضاً الجدول 7-1) وفقاً لقاعدة الاستعمال التالية: إذا كانت قيمة إحدى البتات 1، يكون الاستعمال المحدد مسموحاً، وإلا لا يكون هذا الاستعمال مسموحاً. ويعزز **مزيل تخليط المحتوى** قاعدة الاستعمال هذه. ويتجاهل **مزيل تخليط المحتوى** ما يلي:

'1' قيمة البتات التي تحجز للاستعمال في المستقبل؛

'2' وقيمة البتات التي تقابل التنفيذ الذي لا يدعمه **مزيل تخليط المحتوى**.

الجدول 7-1 – قائمة معلومات قواعد استعمال كلمة التحكم

رقم البتة	الوصف
0	تشفير
1	فك التشفير
7 … 2	محجوزة للاستعمال في المستقبل
8	خوارزمية تخليط مشتركة 2 (CSA2) للإذاعة الفيديوية الرقمية (DVB) [b-ETSI TS 100 289]
9	DVB CSA3 [b-ETSI TS 100 289]
15 … 10	محجوزة للاستعمال في المستقبل
16	الإصدار 1 من خوارزمية التخليط المشتركة القائمة على البرمجيات لتلفزيون بروتوكول الإنترنت (CISSA) للإذاعة الفيديوية الرقمية [b-ETSI TS 103 127]
23 … 17	محجوزة للاستعمال في المستقبل
24	خوارزمية تخليط/فك تخليط مشتركة صادرة عن لجنة أنظمة التلفزيون المتطورة (ATSC) [b-ATSC A/70-1]
31 … 25	محجوزة للاستعمال في المستقبل
32	مخطط تجفير مشترك – مخطط حماية cenc [b-ISO/IEC 23001-7]
33	مخطط تجفير مشترك – مخطط حماية cbc1 [b-ISO/IEC 23001-7]
34	مخطط تجفير مشترك – مخطط حماية cens [b-ISO/IEC 23001-7]

الجدول 7-1 – قائمة معلومات قواعد استعمال كلمة التحكم

رقم البتة	الوصف
35	مخطط تجفير مشترك – مخطط حماية cbcs [b-ISO/IEC 23001-7]
36 … 39	محجوزة للاستعمال في المستقبل
40	ChinaDrm – أسلوب تسلسل كتل التجفير [b-GY/T 277-2014]
41	ChinaDrm – أسلوب العداد [b-GY/T 277-2014]
42 … 63	محجوزة للاستعمال في المستقبل

2.3.7 معلومات قواعد استعمال المفتاح العمومي للمرسل

يبلغ طول معلومات قواعد استعمال المفتاح العمومي للمرسِل (SPK-URI) 64 بتة مرقمة أيضاً من اليسار إلى اليمين من 0 إلى 63. ويحدد الجدول 7-2 قيمة SPK-URI. وبوجه خاص، إذا كانت المفاتيح SPK_1، SPK_2، … وSPK_m متوفرة كمدخلات لسلم المفاتيح إلى جانب SPK-URI (كما يبين الجدول 7-2)، تستعمل عندئذ البتات $0, 1, \ldots, m-1$ والبتات $16, 17, .., 16 + m - 1$، في SPK-URI لتحديد مجموعتين فرعيتين من المجموعة $\{SPK_1, SPK_2, ..., SPK_m\}$: حيث SPK_i ($i = 1, 2, \ldots, m$) هو عنصر من المجموعة الفرعية الأولى وذلك فقط إذا كانت قيمة البتة i-1 تساوي واحد، وSPK_i هو عنصر من المجموعة الفرعية الثانية وذلك فقط إذا كانت قيمة البتة $15 + i$ تساوي واحد. ويرمز إلى هاتين المجموعتين الفرعيتين في النص التالي بالحرفين S_1 وS_2 على التوالي. وباستعمال هذا الترميز، يطبق سلم المفاتيح قاعدة الاستعمال التالية:

قاعدة الاستعمال الأولى للمفتاح SPK: في سلم المفاتيح، يسمح لعملية التحقق V باستعمال المفتاح SPK_i للتحقق من توقيع SIM_{KL} وذلك فقط في حالة $SPK_i \in S_1$.

وعلى مجموعة سلم المفاتيح أن تقوم بإنفاذ قاعدة الاستعمال الأولى للمفتاح SPK.

وتستعمل المجموعة S_2 في حالة إعادة تجفير المحتوى. وإذا أعيد تجفير المحتوى، عندئذ تظهر مجموعتي الدخل في الشكل 7-1: واحدة مرتبطة بكلمة التحكم (CW) المستعملة لفك تجفير المحتوى وواحدة مرتبطة بكلمة التحكم المستعملة لتجفير المحتوى. وفي هذه الحالة، تسهم قاعدة الاستعمال التالية بربط هاتين المجموعتين من المدخلات:

قاعدة الاستعمال الثانية للمفتاح SPK: في سلم المفاتيح، يسمح لعملية التحقق V باستعمال المفتاح SPK_i للتحقق من توقيع SIM_{KL} لكلمة التحكم CW المستعملة لتجفير المحتوى وذلك فقط في حالة $SPK_i \in S_2$ المقترنة بالكلمة CW المستعملة لفك تجفير المحتوى.

وإذا كان **مزيل تخليط المحتوى** يدعم إعادة تجفير المحتوى، ينبغي عندئذ لمجموعة سلم المفاتيح أن تنفذ قاعدة الاستعمال الثانية للمفتاح SPK. وإذا لم تسهم مجموعة سلم المفاتيح بإنفاذ قاعدة الاستعمال هذه، يقوم عندئذ مكوّن آخر في الرقاقة بإنفاذ قاعدة الاستعمال الثانية للمفتاح SPK ويضمن التنفيذ أن قيمة SPK-URI التي تمثل دخل الدالة h تساوي قيمة SPK-URI التي استعملت لإنفاذ قاعدة الاستعمال الثانية للمفتاح SPK.

الجدول 7-2 – معلومات قواعد استعمال المفتاح العمومي للمرسل

رقم البتة	الوصف
0	spk1_in_set1
1	spk2_in_set1
2	spk3_in_set1
…	…
15	spk16_in_set1
16	spk1_in_set2
17	spk2_in_set2
18	spk3_in_set2
…	…
31	spk16_in_set2
32 … 63	محجوزة للاستعمال في المستقبل

4.7 طبقات المفاتيح الإضافية

1.4.7 لمحة عامة

تفترض المواصفات المحددة في الفقرتين 1.7 و2.7 وجود طبقة مفاتيح واحدة في سلم المفاتيح تكون مرتبطة بمفاتيح الوصلة. كما أن سلم المفاتيح يدعم طبقات مفاتيح إضافية من أجل مفاتيح الوصلة، كما هو مبين في الشكل 7-2 (لا يظهر في الشكل سوى المكونات الأساسية لسلم المفاتيح التي تتصل بالمعالجة الواردة في هذه الفقرة).

وكما هو الحال في الشكل 7-2، لنفترض أن t ترمز إلى عدد مفاتيح الوصلة في سلم المفاتيح. تدعم مجموعة سلم المفاتيح سلالم المفاتيح لجميع قيم t حيث $1 \le t \le 24$. ويلاحظ أن $t = 1$ في النظام المحدد في الفقرتين 1.7 و2.7.

2.4.7 حسابات سلم المفاتيح

يمكن للمرسِل أن يولّد رسائل الدخل البالغ عددها t ويرسلها إلى مجموعة سلم المفاتيح باتباع الخطوات التالية:

حساب $e(LK_1, LK_2), e(LK_2, LK_3), \ldots, e(LK_{t-1}, LK_t)$ و$e(LK_t, r)$ (المرسِل):

1) توليد مفاتيح الوصلات LK_i من أجل $i = 1, 2, \ldots, t$ وسلسلة البتات العشوائية r.

2) حساب $e(LK_{i-1}, LK_i)$ من أجل $i = 2, 3, \ldots, t$.

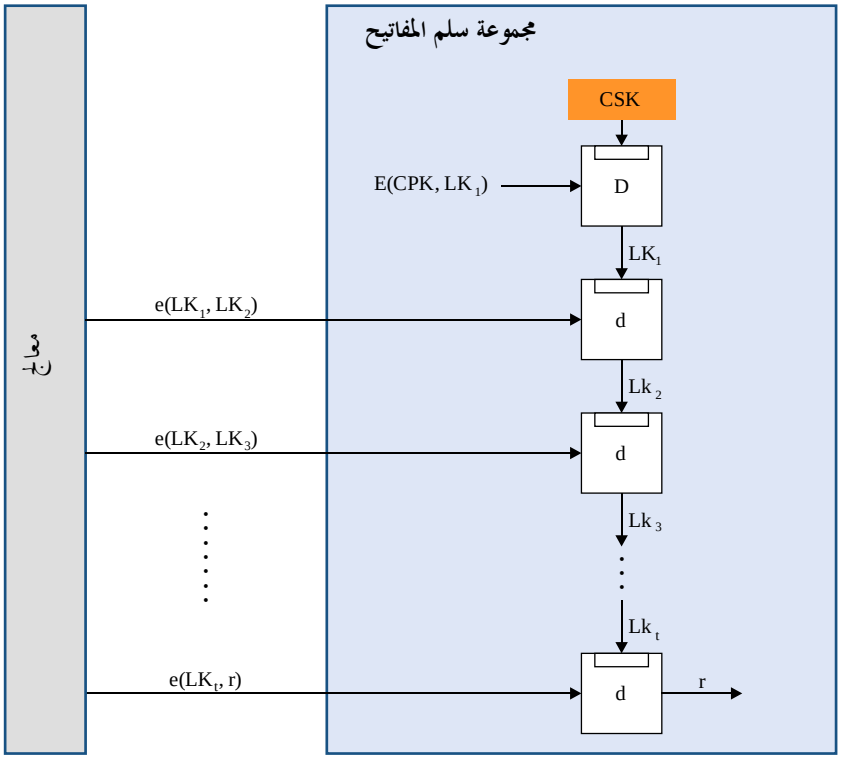
3) حساب $e(LK_t, r)$.

وبعد استقبال $e(LK_1, LK_2), e(LK_2, LK_3), \ldots, e(LK_{t-1}, LK_t)$ and $e(LK_t, r)$، تجري مجموعة سلم المفاتيح حساب r باتباع الخطوات التالية (انظر أيضاً الشكل 7-2).

حساب r (مجموعة سلالم المفاتيح):

1) حساب $LK_i = d(LK_{i-1}, e(LK_{i-1}, LK_i))$ من أجل $i = 2, 3, \ldots, t$.

2) حساب $r = d(LK_t, e(LK_t, r))$.



الشكل 7-2 – طبقات المفاتيح الإضافية

5.7 البيانات المرتبطة 2 (AD2)

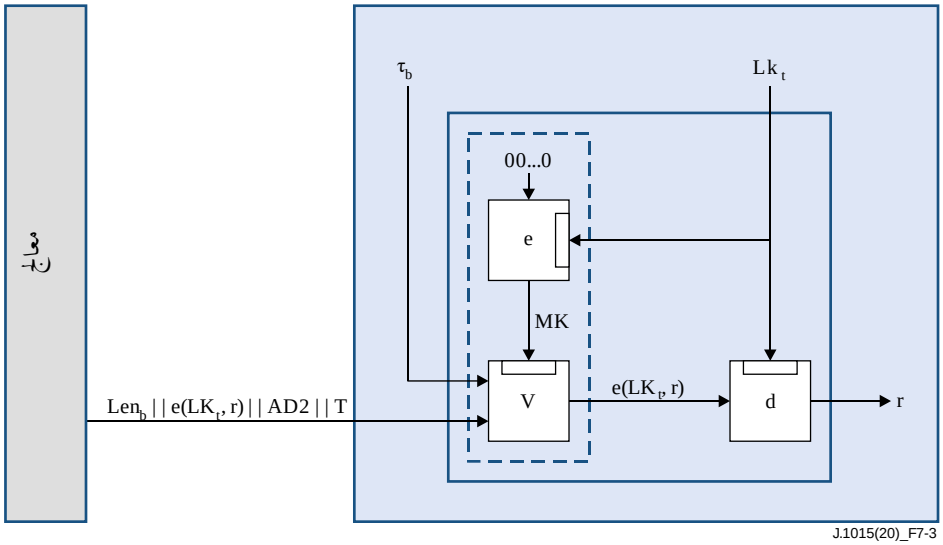
يستطيع المرسِل أن يرسل إلى سلم المفاتيح البيانات المرتبطة 2 (AD2)، إلى جانب $e(LK_t, r)$. وتشير قيم سلسلة البتات τ_b (على النحو الذي عرضت فيه في الفقرة 1.7) إلى وجود البيانات AD2. وكما هو محدد في الفقرة 1.7، فإن طول τ_b يبلغ 8 بتات. وتشير τ في النص التالي إلى تمثيل τ_b بعدد صحيح تقابل فيه البتة الأقل دلالة في τ أقصى بتة إلى اليمين في τ_b. ويدعم سلّم المفاتيح جميع قيم $\tau \in \{0, 64, 96, 128\}$. وإذا كان $\tau = 0$، تكون البيانات AD2 غير موجودة، وعندئذ يستعمل النظام بالشكل الذي عرض فيه في الفقرات من 1.7 إلى 4.7. ويفترض الوصف التالي أن $\tau \neq 0$. وفي هذه الحالة تكون البيانات AD2 موجودة. تتحقق مجموعة سلالم المفاتيح مما إذا كان τ الذي ورد يحقق $\tau \in \{64, 96, 128\}$؛ وإذا لم ينطبق ذلك، توقف مجموعة سلم المفاتيح إجراء الحسابات.

تفترض هذه التوصية أن AD2 ممثلة بسلسلة بتات. لنفترض أن Len ترمز إلى طول البتات في AD2. تدعم مجموعة سلم المفاتيح جميع قيم Len حيث $1 \leq \text{Len} \leq 256$.

ولنفترض أن Len_b ترمز إلى تمثيل العدد الصحيح $\text{Len} - 1$ في النظام الثنائي حيث تقابل أقصى بتة إلى اليمين من Len_b البتة الأقل دلالة في Len - 1. فيكون طول Len_b مساوياً 8 بتات.

تكون سلسلة بتات البيانات AD2 ملزمة من الناحية التجفيرية بالنص التجفيري المقابل $e(LK_t, r)$ خلال نقلها إلى سلم المفاتيح. ولهذه الغاية يستعمل المرسِل ومجموعة سلم المفاتيح **خوارزمية شفرة الاستيقان من الرسالة** ويرمز إليها بالرمز mac. وتتشكل مدخلات هذه الخوارزمية من مفتاح خوارزمية شفرة الاستيقان MAC من الرسالة MK والرسالة AD2 || $e(LK_t, r)$ || Len_b والسلسلة τ. ويمثل خرج الخوارزمية MAC بالوسم (T) الذي يبلغ طوله τ بتات. ويرد وصف الخوارزمية MAC في الفقرة 5.10.

لنفترض أن 0…00 ترمز إلى سلسلة بتات كلها أصفار مؤلفة من 128 بتة. يمكن للمرسل اتباع الخطوات التالية لتوليد رسالة الدخل T || AD2 || $e(LK_t, r)$ || Len_b ونقلها إلى سلم المفاتيح (كما هو مبين في الشكل 7-3).



الشكل 7-3 – البيانات المرتبطة 2

حساب T || AD2 || $e(LK_t, r)$ || Len_b (المرسِل):

1) حساب $MK = e(LK_t, 00…0)$.

2) إلحاق Len_b في بداية سلسلة البتات $e(LK_t, r)$ || AD2.

3) حساب $T = mac(MK, Len_b || e(LK_t, r) || AD2, \tau)$.

4) إلحاق T بسلسة البتات $Len_b || e(LK_t, r) ||$ AD2.

تحل الرسالة T || AD2 || $e(LK_t, r)$ || Len_b محل الرسالة $e(LK_t, r)$ التي تستعمل إذا كان $\tau = 0$. وبعد استقبال الرسالة T || AD2 || $e(LK_t, r)$ || Len_b، تحسب مجموعة سلم المفاتيح $e(LK_t, r)$ باتباع الخطوات التالية (يرمز إلى الخطوات من 2 إلى 4 بالحرف V في الشكل 7-3):

حساب $E(LK_t, r)$ (مجموعة سلالم المفاتيح):

1) حساب $MK = e(LK_t, 00…0)$.

2) حساب $T = mac(MK, Len_b || e(LK_t, r) || AD2, \tau)$.

3) التحقق مما إذا كان الوسم الوارد T يساوي الوسم المحسوب T. وإذا كانت هاتان القيمتان غير متساويتين، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

4) استرجاع $e(LK_t, r)$ من الرسالة الواردة.

لا تندرج مواصفات محتوى البيانات AD2 ضمن نطاق هذه التوصية وتفترض هذه الوثيقة أن مجموعة سلم المفاتيح لا تقوم بمعالجة AD2 غير استعمالها كدخل للخوارزمية MAC. ويمكن لمجموعة سلم المفاتيح أن تنقل AD2، أو جزءاً من AD2، بالإضافة إلى CW-URI وCW، إلى **مزيل تخليط المحتوى**.

وإذا كان $\tau \neq 0$، يضمن عندئذ تنفيذ سلم البيانات أن قيمة τ_b التي قدمت إلى جانب $Len_b || e(LK_t, r) ||$ AD2 كدخل للخوارزمية MAC تقدم أيضاً كدخل للدالة h عند اشتقاق CW من r.

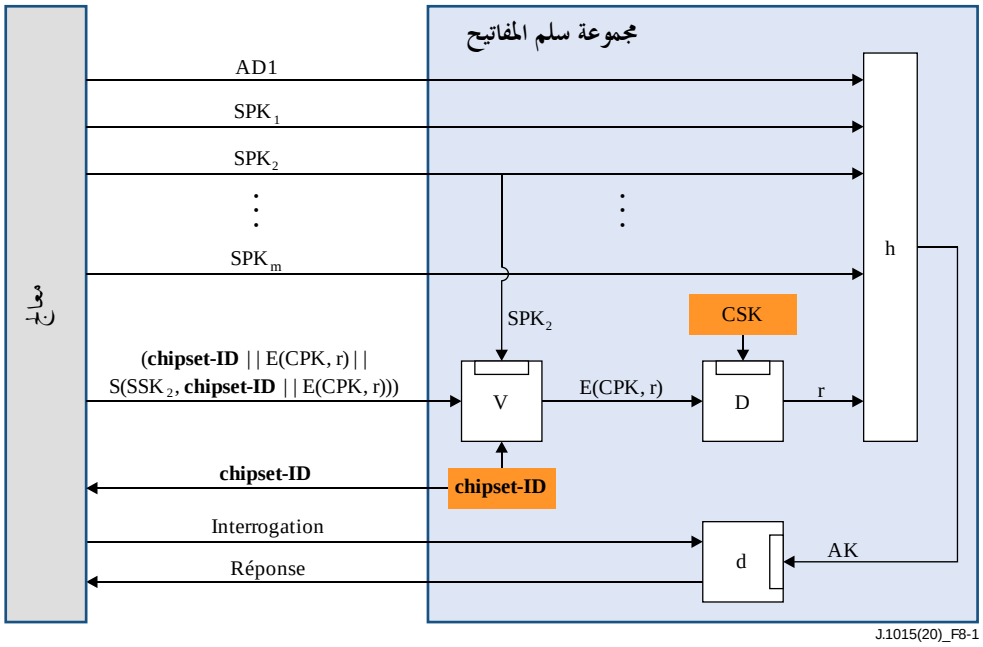
ولا يمكن إلا لمجموعة سلم المفاتيح أن تتمتع بالنفاذ إلى النص العادي CSK, LK_i $(1 \leq i \leq t)$, MK, and r.

8 آلية الاستيقان

1.8 لمحة عامة

تعرض هذه الفقرة التصميم الوظيفي لآلية الاستيقان في مجموعة سلالم المفاتيح. ويبين الشكل 8-1 آلية الاستيقان. وهي ترتبط ارتباطاً وثيقاً بسلم المفاتيح الوارد في الفقرة 7؛ وتستعمل بوجه خاص نفس العمليات V وD والدالة h، ونفس **هوية الرقاقة** والمفتاح CSK. ومع ذلك لا تستعمل آلية الاستيقان مفاتيح الوصلات علماً بأن CW-URI وSPK-URI وτ_b ليست مدخلات لآلية الاستيقان والدالة h. وعلاوةً على ذلك، لا يمثل خرج h **كلمة تحكم** (CW) تستعمل في فك تجفير المحتوى أو تشفيره (وبوجه خاص لا تتفاعل آلية الاستيقان مباشرةً مع **مزيل تخليط المحتوى**)، ولكن كمفتاح استيقان AK. والمفتاح AK هو **نظام التجفير المتناظر** نفسه المستعمل في سلم المفاتيح. وكما يبين الشكل 8-1، لا تستخدم في تنفيذ آلية الاستيقان إلا عملية فك التجفير الخاصة به d.

وفي النص التالي يرمز أيضاً لرسالة الدخل (**chipset-ID** || E(CPK, *r*) || S(SSK$_i$, **chipset-ID** || E(CPK, *r*))) بالرمز SIM$_{\text{AUTH}}$.



الشكل 8-1 – آلية الاستيقان

2.8 حسابات آلية الاستيقان

يمكن للمرسِل المرتبط بزوج المفاتيح (SSK$_i$,SPK$_i$) لأي $1 \le i \le m$ أن ينشئ رسالة الدخل الموقعة SIM$_{\text{AUTH}}$، أي

(**chipset-ID** || E(CPK, *r*) || S(SSK$_i$, **chipset-ID** || E(CPK, *r*))),

باتباع الخطوات التالية.

حساب SIM$_{\text{AUTH}}$ (المرسِل):

1) توليد سلسلة بتات عشوائية *r*.
2) حساب النص التجفيري E(CPK, *r*).
3) سَلسلة **هوية الرقاقة** وE(CPK, *r*)؛ يرمز إلى سلسلة البتات الناتجة بالرمز (**chipset-ID** || E(CPK, *r*)).
4) توقيع الرسالة (**chipset-ID** || E(CPK, *r*)) باستخدام المفتاح SSK$_i$؛ يرمز إلى التوقيع بالرمز S(SSK$_i$, **chipset-ID** || E(CPK, *r*)).
5) إلحاق التوقيع بسلسلة البتات (**chipset-ID** || E(CPK, *r*)).

وبعد استقبال SIM_{AUTH} والمفتاح العمومي للمرسِل SPK_i، تؤدي مجموعة سلم المفاتيح الخطوات التالية لاسترجاع r (يرمز إلى الخطوتين الأوليتين في الشكل 8-1 بالحرف V).

حساب r (مجموعة سلم المفاتيح):

1) التحقق مما إذا كانت **هوية الرقاقة** المسترجعة تساوي **هوية الرقاقة** المختزنة. وإذا كانت هاتان القيمتان غير متساويتين، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

2) استعمال SIM_{AUTH} الذي تم استرجاعه والمفتاح SPK_i للتحقق من التوقيع. وإذا كان التوقيع غير صالح، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

3) حساب $r = D(CSK, E(CPK, r))$.

وفي حالة آلية الاستيقان، يسمح للعملية V باستعمال أي مفتاح SPK_i حيث $1 \leq i \leq m$ للتحقق من توقيع SIM_{AUTH} (يفترض في الشكل 8-1 أن $i = 2$).

بعد ذلك تقدم $AD1, SPK_1, SPK_2, ..., SPK_m$ وr كمدخلات للدالة h. ويتمثل خرج الدالة h بمفتاح الاستيقان AK. ويضمن تنفيذ آلية الاستيقان أن المفتاح العمومي الذي استعمل للتحقق من استيقان SIM_{AUTH} (أو بشكل أدق SIM_{AUTH} الذي يتضمن العدد العشوائي r) يقدم كأحد المدخلات SPK إلى الدالة h حين يكون AK مشتقاً من r.

بعد ذلك يمكن للمرسِل أن ينشئ رسالة دخل يشار إليها بكلمة Challenge. وبعد استلام Challenge من المعالج، تجري آلية الاستيقان حساب Reponse باتباع الخطوة التالية.

حساب Response (مجموعة سلم المفاتيح):

1) حساب Response = d(AK, Challenge).

وكما يبين الشكل 8-1، تُرجع آلية الاستيقان الإجابة إلى المعالج.

ولا يمكن إلا لمجموعة سلم المفاتيح أن تتمتع بالنفاذ إلى النص العادي AK.

9 الخطوات الأولية لتحويل البيانات

1.9 BS2OSP

تستعمل الخطوة الأولية لتحويل سلسلة بتات إلى سلسلة أثمونات BS2OSP لتحديد **نظام تجفير المفاتيح العمومية** الوارد في الفقرة 2.10 و**نظام التوقيع الرقمي** الوارد في الفقرة 3.10.

Function:	BS2OSP(x)	
Input:	x	a bit string of length 8j ($j \geq 1$).
Output:	X	an octet string of length j.

الخطوات:

1) لنفترض أن x_i ترمز إلى بتة من أجل $0 \leq i \leq 8j\text{-}1$، وأن $x = x_0\, x_1 \ldots x_{8j\text{-}1}$.

2) لنفترض أن X_i هو الأثمون المحدد بالقيمة $X_i = x_{8i+1} \ldots x_{8i+7}$ من أجل $0 \leq i \leq j\text{-}1$.

3) يكون الخرج سلسلة الأثمونات $X = X_0\, X_1 \ldots X_{j\text{-}1}$.

2.9 OS2BSP

تستعمل الخطوة الأولية لتحويل سلسلة أثمونات إلى سلسلة بتات OS2BSP لتحديد الخطوة الأولية I2BSP الواردة في الفقرة 3.9 و**نظام تجفير المفاتيح العمومية** الوارد في الفقرة 2.10.

Function: OS2BSP(X)

Input: X an octet string of length j ($j \geq 1$).

Output: x a bit string of length $8j$.

الخطوات:

1) لنفترض أن X_i ترمز إلى أثمون من أجل $0 \leq i \leq j\text{-}1$ وأن $X = X_0 X_1 \ldots X_{j-1}$.

2) لنفترض أن x_i ترمز إلى بتة من أجل $0 \leq i \leq 8j\text{-}1$، وأن هذه البتات محددة بالقيم $X_i = x_{8i+1} \ldots x_{8i+7}$ من أجل $0 \leq i \leq j\text{-}1$.

3) يكون الخرج سلسلة البتات $x = x_0 x_1 \ldots x_{8j-1}$.

3.9 I2BSP

تستعمل الخطوة الأولية لتحويل عدد صحيح إلى سلسلة بتات I2BSP لتحديد الدالة h الواردة في الفقرة 4.10.

Function: I2BSP(x)

Input: x a 2 048-bit integer.

Output: a bit string of length 2 048.

الخطوة: إذا كانت الخطوة الأولية لتحويل عدد صحيح إلى بيانات سلسلة أثمونات I2OSP(x, xLen) محددة في المعيار [IETF RFC 8017]، عندئذ I2BSP(x) = OS2BSP(I2OSP(x, 256)).

10 العمليات التجفيرية

1.10 نظام التجفير المتناظر

يكون **نظام التجفير المتناظر** المستخدم في مجموعة سلالم المفاتيح هو معيار التجفير المتقدم – [NIST FIPS 197] 128 (AES-128) في أسلوب عمل كتاب الشفرة الإلكتروني (ECB).

2.10 نظام تجفير المفتاح العمومي

يرمز إلى **نظام تجفير المفتاح العمومي** بالرمز [IETF RFC 8017] RSAES-PKCS1-v1_5. يتألف هذا النظام من عملية التجفير وعملية فك التجفير. ونذكر من الفقرتين 7 و8 أن عملية فك التجفير وحدها هي التي تنفّذ في مجموعة سلم المفاتيح، وأن نظام المرسل هو الذي ينفذ عملية التجفير.

يكون المفتاح العمومي للرقاقة CPK مساوياً للمفتاح العمومي للمتلقي RSA (n, e) في التوصية [IETF RFC 8017]. وفي هذه التوصية يكون طول البتات في n بقيمة 2 048، أي إن طول الأثمونات في n، الذي يرمز إليه بالحرف k في التوصية [IETF RFC 8017] يساوي 256. ويساوي المفتاح السري/الخصوصي CSK المفتاح الخصوصي RSK للمتلقي في التوصية [IETF RFC 8017]. ويكون تمثيل المفتاح CSK مساوياً لأحد تمثيلات K المحددة في التوصية [IETF RFC 8017].

يرمز إلى الرسالة التي يتعين تجفيرها بالحرف M في التوصية [IETF RFC 8017] ويتم تمثيلها بشكل سلسلة أثمونات. وتعرّف M في هذه التوصية بالقيمة M = BS2OSP(LK) في حالة سلم المفاتيح، وبالقيمة M = BS2OSP(r) في حالة آلية الاستيقان. ونتيجة لذلك يبلغ طول الأثمون في M في هذه التوصية 16.

ويمثل كل من CPK و*M* دخلاً لعملية التجفير:

RSAES-PKCS1-v1_5-Encrypt(CPK, *M*).

يكون خرج هذه العملية نصاً عادياً يرمز إليه بالرمز *C*، ويتمثل بسلسلة أثمونات في التوصية [IETF RFC 8017]. ويساوي طول الأثمون في *C* في هذه التوصية 256. و*C* تساوي (BS2OSP(E(CPK, LK)) في حالة سلم المفاتيح و(BS2OSP(E(CPK, *r*)) في حالة آلية التنسيق.

ويمثل كل من CSK وC دخلاً لعملية فك التجفير:

RSAES-PKCS-v1_5-Decrypt(CSK, *C*).

تنفّذ هذه العملية في مجموعة سلم المفاتيح. ويكون خرج هذه العملية الرسالة *M*، ويرمز إليها بسلسلة أثمونات. بعد ذلك، تقوم مجموعة سلم المفاتيح بحساب LK = OS2BSP(*M*) في حالة سلم المفاتيح و*r* = OS2BSP(*M*) في حالة آلية التنسيق.

3.10 مخطط التوقيع الرقمي

يرمز إلى **مخطط التوقيع الرقمي** بالرمز RSASSA-PKCS1-v1_5 [IETF RFC 8017]. ويتألف هذا النظام من عملية توليد التوقيع وعملية التحقق من التوقيع. ونذكر من الفقرتين 7 و8 أن عملية التحقق من التوقيع وحدها هي التي تنفذ في مجموعة سلم المفاتيح، وأن نظام المرسِل هو الذي ينفذ عملية توليد التوقيع.

يرمز إلى المفتاح العمومي للموقّع RSA بالرمز (*n*, *e*) ويتمثل بزوج من الأعداد الصحيحة في التوصية [IETF RFC 8017]. وفي هذه التوصية، يكون طول المفتاح العمومي للموقّع RSA بالمقياس *n* بقيمة 2 048 بتة، أي إن طول الأثمون في *n* ويرمز إليه بالحرف *k* في التوصية [IETF RFC 8017] يكون بقيمة 256. بالإضافة إلى ذلك، يكون الأس العمومي *e* بقيمة $2^{16} + 1$ في هذه التوصية. وتقوم الرقاقة المطابقة بتخزين هذه القيمة عادة وتنفذ الرقاقة تدابير لحماية سلامة هذه القيمة. ويساوي المفتاح العمومي للمرسِل SPK معامل *n*، مما يعني أن طول SPK يساوي 2 048 بتة وأن SPK ممثل بعدد صحيح. ويساوي المفتاح السري/الخصوصي SSK للمرسل المفتاح الخصوصي RSA للموقّع *K* في التوصية [IETF RFC 8017].

ويرمز إلى الرسالة التي يتعين توقيعها بالرمز *M* ويتم تمثيلها على شكل سلسلة أثمونات في التوصية [IETF RFC 8017]. وفي هذه التوصية، تعرّف *M* كما يلي:

M = BS2OSP(**chipset-ID** || E(CPK, LK))

في حالة سلم البيانات؛

و*M* = BS2OSP(**chipset-ID** || E(CPK, *r*))

في حالة آلية الاستيقان. ونتيجة لذلك، يكون الأثمون في *M* بطول 264 = 256 + 8 في الحالتين.

ويشكل SSK و*M* مدخلان لعملية توليد التوقيع:

RSASSA-PKCS1-v1_5-Sign(SSK, *M*).

ويمثل التوقيع خرج عملية توليد التوقيع، ويرمز إليه بالحرف *S* ويتم تمثيله بسلسلة أثمونات في التوصية [IETF RFC 8017]. ويكون *S* بطول 256 في هذه التوصية. وتكون *S* بقيمة (BS2OSP(S(SSK$_i$, **chipset-ID** || E(CPK, LK)))) في حالة مجموعة سلم المفاتيح وبقيمة (BS2OSP(S(SSK$_i$, **chipset-ID** || E(CPK, *r*)))) في حالة آلية الاستيقان.

وتشكل (SPK, $2^{16} + 1$) و*M* و*S* مدخلات لعملية توليد التوقيع:

RSAES-PKCS-v1_5-Verify((SPK, $2^{16} + 1$), *M*, *S*).

وتنفذ هذه العملية في مجموعة سلم المفاتيح. ويكون خرجها إما "توقيعاً صالحاً" وإما "توقيعاً غير صالح".

4.10 دالّة الفرم h

تحدد هذه الفقرة مواصفات الدالة h. ونذكر من الفقرتين 7 و8 أن دخلي h هما:

- CW-URI, τ_b, AD1, SPK-URI, SPK_1, SPK_2, ..., SPK_m وr في حالة سلم المفاتيح.
- AD1, SPK_1, SPK_2, ..., SPK_m وr في حالة آلية الاستيقان.

وإذا لم تتلق مجموعة سلم المفاتيح أحد هاتين المجموعتين من الدخل، أو إذا لم يكن طول دخل معين كما هو محدد في هذه التوصية، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات. وإلا فإن h تطبق أولاً الخطوة الأولية لتحويل البيانات I2BSP على كل من مدخلات المفتاح SPK. بعد ذلك، تسلسل h سلاسل البتات التي تمثل مدخلاتها على النحو التالي للحصول على الرسالة M. وفي حالة سلم المفاتيح:

$$M = r \,||\, \text{CW-URI} \,||\, \tau_b \,||\, \text{AD1} \,||\, \text{SPK-URI} \,||\, \text{I2BSP}(SPK_1) \,||\, \text{I2BSP}(SPK_2) \,||\, ... \,||\, \text{I2BSP}(SPK_m),$$

وفي حالة آلية الاستيقان:

$$M = r \,||\, \text{AD1} \,||\, \text{I2BSP}(SPK_1) \,||\, \text{I2BSP}(SPK_2) \,||\, ... \,||\, \text{I2BSP}(SPK_m).$$

ونذكر أن طول r وCW-URI وτ_b وAD1 وSPK-URI وI2BSP(SPK_i) يساوي 128 بتة و64 بتة و8 بتات و256 بتة و048 2 بتة على التوالي. ونتيجة لذلك فإن طول البتات في M، الذي يرمز إليه بالرمز l في المعيار [NIST FIPS 180-4]، يبلغ m048 2 + 520، حيث m عدد عناصر I2BSP(SPK_m) في مجموعة الرسالة M في حالة سلم المفاتيح وm048 2 + 384 في حالة آلية الاستيقان.

بعد ذلك تقوم h بحساب خوارزمية التمويه المأمونة SHA-256(M) كما هي موصفة في [NIST FIPS 180-4].

وفي آلية الاستيقان، تقوم h ببتر مختصر الرسالة المؤلف من 256 بتة إلى 128 بتة وتشكل من هذا المختصر المبتور خرجاً لها. وفي حالة سلم المفاتيح، تنقل مجموعة سلم المفاتيح خرج الكمية SHA-256 المؤلف من 256 بتة إلى **مزيل تخليط المحتوى**، وإذا كان طول CW يعادل N بتة، يقوم عندئذ **مزيل تخليط المحتوى** ببتر هذا الخرج إلى N بتة. وفي الحالتين، تستخدم طريقة البتر الموصفة في [NIST SP 800-107].

5.10 خوارزمية شفرة الاستيقان من الرسالة

تحدد هذه الفقرة الخوارزمية mac كما وردت في الفقرة 5.7. وتعرّف **خوارزمية شفرة الاستيقان من الرسالة** هذه على النحو الوارد في [ISO/IEC 9797-1] مع عمليات الاختيار التالية:

- تكون شفرة المجموعة AES-128.
- يتم ملء الرسالة بطريقة الملء 3. تتطلب هذه الطريقة أن يكون طول بتات الرسالة غير الممتلئة A || e(LK_t, r). ويساوي طول البتات هذا Len + 129.
- تستعمل خوارزمية MAC الأولى لحساب MAC من الرسالة والمفتاح السري.
- تكون الخوارمية MAC بطول τ بتة.

التذييل I

مجالات لمزيد من التطوير

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

لقد تحدد أن هذه التوصية في حاجة إلى المزيد من التطوير وإلى التحقق من أنها تفي بالمتطلبات المحددة في التوصية [ITU-T J.1010]، وأن التوصية [ITU-T J.1010] في حاجة إلى التحديث كي تعكس متطلبات مواصفة الحماية المعززة للمحتوى (ECP) الصادرة عن منظمة MoviLabs [b-ECP]. وينبغي تحديث التوصيات [ITU-T J.1011] و[ITU-T J.1012] و[ITU-T J.1013] و[ITU-T J.1014] و[ITU-T J.1015] و[b-ITU-T J.1015.1] لكي تعكس التحديثات المدخلة على التوصية [ITU-T J.1010].

وعبر عدد من الدول الأعضاء وأصحاب المصلحة من مجموعة متنوعة من الصناعات – بما في ذلك مصنعو الأجهزة والمكونات الإلكترونية ومالكو وحائزو تراخيص المحتوى المحمي بحقوق الطبع والنشر وموردو الخدمات المتاحة بحرية على الإنترنت (OTT) وخدمات التلفزيون الخطي وموردو حلول أنظمة النفاذ المشروط (CAS) وإدارة الحقوق الرقمية (DRM) – المنتشرة في شتى أرجاء العالم، عن شواغلهم من أن السطح البيني ECI لا يفي تماماً بمتطلبات الحماية ECP ولا بمتطلبات حماية المحتوى للصناعة بشكل عام.

وبتحديد أكبر، عبر هؤلاء عن شواغلهم في مساهمات إلى اجتماع لجنة الدراسات 9 لقطاع تقييس الاتصالات (SG9) (16-23 أبريل 2020). واقترحت مساهمات مقدمة من إسرائيل وأستراليا وشركة Samsung، أحد أعضاء قطاع تقييس الاتصالات، و Sky Group وMoviLabs، من المنتسبين إلى لجنة الدراسات 9، أن هناك عدداً من التغييرات يجب إدخالها على توصيات السطح البيني ECI، بيد أنه لم يتم التوصل إلى اتفاق بشأنها. وترد قائمة سردية بهذه البنود في [b-SG9 Report 17 Ann.1].

وهي تتضمن مقترحات من أجل:

1) تبسيط النظام ECI بتقليص نطاقه؛
2) إلغاء الإدارة DRM؛
3) إلغاء إعادة تجفير المحتوى؛
4) إلغاء إدارة البرمجيات؛
5) إضافة سطوح بينية API لتأمين عمليات التخزين والتجفير؛
6) السماح بسلالم المفاتيح الخاصة بالبائعين؛
7) استخدام متطلبات TEE للتوصية J.1027P
8) إضافة تنفيذ TEE إلى VM؛
9) تعزيز قوة خوارزميات التجفير، مثل استعمال SHA-384؛
10) استعمال شهادات قياسية، مثل التوصية ITU-T X.509؛
11) إعادة النظر في الاتصالات بين الوسطاء؛
12) إجراء مزيد من الاتصالات مع ETSI؛
13) إجراء المزيد من استعراضات النظراء؛
14) استكشاف بدائل لنموذج سلطة الاستوثاق؛
15) تحديد المزيد من الجوانب التقنية لقواعد امتثال السطح البيني ECI ومتانته؛
16) إضافة متطلبات من أجل التنوع، مثل التحديد العشوائي لحيز العنوان؛

17) إضافة متطلبات بشأن التحقق الروتيني من السلامة.

وتؤكد هذه المقترحات أن حماية المحتوى والتهديدات الخاصة بإصابتها بالخلل تتطور باستمرار. وقد صمم السطح البيني ECI بداية قبل الموافقة على توصية قطاع تقييس الاتصالات هذه بعقد من الزمن تقريباً. والأنظمة التي على شاكلة السطح البيني ECI تحتاج إلى التقييم بصورة منتظمة إزاء أحدث ما تم التوصل إليه في تقنيات الهجمات ومتطلبات حماية الصناعة، على السواء.

وهناك آليات أخرى لتمكين التشغيل البيني. وبالنسبة لحالة استعمال الإدارة DRM، بشكل خاص، نشرت معظم خدمات الفيديو عبر الإنترنت حلولاً أخرى لتوفير إمكانية التشغيل البيني ولتلبية هذه الاحتياجات.

ومن المهم توفير مزيد من الوضوح لأن الكثير من الدول الأعضاء تعتبر معايير الاتحاد مصادر توجيه مؤثرة من أجل تطوير أسواقها وصناعاتها. وتؤكد قائمة الشواغل أن تنفيذ السطوح ECI في الأسواق المحلية لهذه الدول يمكن أن ينطوي على تقدير كامل لآثار توصية قطاع تقييس الاتصالات هذه ويضمن النظر في القضايا عندما تلزم الاحتياجات التشريعية أو التنظيمية أو السوقية معدات التلفزيون الرقمي الاستهلاكية بأن تكون قابلة للتشغيل البيني. ويضمن ذلك أيضاً أن مصنعي المعدات التكنولوجية، الذين قد يفضلون استخدام مجموعة فريدة من المتطلبات أو معايير أخرى لتصميم المنتجات، يمكنهم النظر في هذه القضايا عند تطوير منتجات لأسواق مختلفة.

بيبليوغرافيا

[b-ITU-T J.1010] Recommendation ITU-T J.1010 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements*.

[b-ITU-T J.1011] Recommendation ITU-T J.1011 (2016), *Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview*.

[b-ITU-T J.1012] Recommendation ITU-T J.1012 (2020), *Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation*.

[b-ITU-T J.1013] Recommendation ITU-T J.1013 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The virtual machine*.

[b-ITU-T J.1014] Recommendation ITU-T J.1014 (2020), *Embedded common interface for exchangeable CA/DRM solutions; Advanced security – ECI-specific functionalities*.

[b-ITU-T J.1015.1] Recommendation ITU-T J.1015.1 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The advanced security system - Key ladder block: Authentication of control word-usage rules information and associated data 1*.

[b-SG9 Report 17 Ann.1] ITU-T SG9 meeting report, SG9-R17-Annex 1 (2020), Annex 1 to Report 17 of the SG9 fully virtual meeting held 16-23 April 2020. https://www.itu.int/md/T17-SG09-R-0017/en

[b-ISO/IEC 23001-7] ISO/IEC 23001-7:2016: *Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files*.

[b-ATSC A/70-1] ATSC Standard A/70 Part 1:2010, *Conditional access system for terrestrial broadcast*. https://www.atsc.org/standard/a70-part-12010-conditional-access-system-for-terrestrial-broadcast/

[b-ETSI GS ECI 001-5-2] ETSI GS ECI 001-5-2 V1.1.1 (2017-07), *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 2: Key Ladder Block*. https://www.etsi.org/deliver/etsi_gs/ECI/001_099/0010502/01.01.01_60/gs_ECI0010502v010101p.pdf

[b-ETSI TS 100 289] ETSI TS 100 289 V1.1.1 (2011), *Digital video broadcasting (DVB); Support for use of the DVB scrambling algorithm version 3 within digital broadcasting systems*: https://www.etsi.org/deliver/etsi_ts/100200_100299/100289/01.01.01_60/ts_100289v010101p.pdf

[b-ETSI TS 103 127] ETSI TS 103 127 V1.1.1 (2013), *Digital video broadcasting (DVB); Content scrambling algorithms for DVB-IPTV services using MPEG2 transport streams*: https://www.etsi.org/deliver/etsi_ts/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf

[b-GY/T 277-2014] ChinaDRM Lab, GY/T 277-2014: 互联网电视数字版权管理技术规范 [Technical specification for digital rights management for internet television].

[b-IEEE-OUI] IEEE Standards Association (2017), *Guidelines for use of extended unique identifier (EUI), organizationally unique identifier (OUI) and company ID (CID)*.
https://standards.ieee.org/develop/regauth/tut/eui.pdf

[b-ROEL] Roelse, P. (2014). *A new key establishment protocol and its application in pay-TV systems*.
https://arxiv.org/pdf/1308.4371.pdf

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2
https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2020