الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T J.1015.1

(2020/04)

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

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 (ECI) من أجل الحلول CA/DRM القابلة للمبادلة: نظام الأمن المعزز – مجموعة سلالم المفاتيح: استيقان المعلومات والبيانات المرتبطة 1 ذات الصلة بقواعد استعمال كلمات التحكم

التوصية ITU-T J.1015.1

الاتحاد الدولي للاتصالات

التوصية ITU-T J.1015.1

السطح البيني المشترك المدمج (ECI) من أجل الحلول CA/DRM القابلة للمبادلة: نظام الأمن المعزز – مجموعة سلالم المفاتيح: استيقان المعلومات والبيانات المرتبطة 1 ذات الصلة بقواعد استعمال كلمات التحكم

ملخص

تعد التوصية ITU-T J.1015.1 جزءاً من سلسلة تغطي مجموعة سلّم المفاتيح في نظام الأمن المعزّز فيما يخص السطح البيني المشترك المدمج من أجل توصيف ا حلول النفاذ المشروط/إدارة الحقوق الرقمية (CA/DRM) القابلة للمبادلة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T J.1015.1	2020-04-23	9	11.1002/1000/13837

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

جدول المحتويات

الصفحة

1 مجال التطبيق 1

2 المراجع 1

3 التعاريف 1

1.3 المصطلحات المعرفة في وثائق أخرى 1

2.3 مصطلحات معرفة في هذه التوصية 1

4 الاختصارات والأسماء المختصرة..... 2

5 اصطلاحات 3

6 استيقان المعلومات والبيانات المرتبطة 1 ذات الصلة بقواعد استعمال كلمات التحكم 3

1.6 استيقان المعلومات ذات الصلة بقواعد استعمال كلمات التحكم..... 4

2.6 استيقان البيانات المرتبطة 1 5

التذييل I – مجالات تحتاج لمزيد من التطوير 6

بيبليوغرافيا 8

مقدمة

يتمثل الهدف من هذه التوصية[1] في تيسير قابلية التشغيل البيني والمنافسة في خدمات الاتصالات الإلكترونية، وبشكل خاص، في سوق أجهزة الإذاعة والصوتيات والمرئيات. بيد أن هناك تكنولوجيات أخرى قد تكون مناسبة ومفيدة أيضاً حسب الظروف السائدة في 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 إلى خطوات البروتوكول التي تنفذ داخل الرقاقة بأنها سلم المفاتيح.

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 علني 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 من التوصية [ITU-T J.1015]، تسمح معرفة المفتاح العلني في شهادة الرقاقة **لنظام حماية المحتوى** بتوليد رسائل دخل مناسبة لسلم مفاتيح الرقاقة وآلية الاستيقان.

---

1 حُددت عدة مجالات لمزيد من التطوير في التذييل I.

2 يشير استخدام الخط الداكن في نص هذه التوصية إلى مصطلحات ذات تعاريف خاصة بسياق السطح البيني المشترك المدمج التي يمكن أن تختلف عن تلك المتداولة في الاستعمال الشائع.

السطح البيني المشترك المدمج (ECI) من أجل الحلول CA/DRM القابلة للمبادلة: نظام الأمن المعزز – مجموعة سلالم المفاتيح: استيقان المعلومات والبيانات المرتبطة 1 ذات الصلة بقواعد استعمال كلمات التحكم

1 مجال التطبيق

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

وقد أُعدت هذه التوصية لكي يستعملها مصنعو 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 التوصية، بحد ذاتها، صفة توصية.

[ITU-T J.1015] Recommendation ITU-T J.1015 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The advanced security system – Key ladder block.*

3 التعاريف

1.3 المصطلحات المعرفة في وثائق أخرى

لا يوجد.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 سلطة إصدار شهادات (certification authority): الطرف المسؤول عن إدارة شهادات المفاتيح العلنية في **النظام البيئي للسطح البيني المشترك المدمج (ECI)**. وهو سلطة إصدار الشهادات الموثوق به لدى جميع الأطراف الأخرى في النظام لإجراء العمليات المرتبطة بالشهادات.

2.2.3 هوية الرقاقة (chipset-ID): رقم غير سري يستعمل لتحديد هوية الرقاقة في **النظام البيئي للسطح البيني المشترك المدمج (ECI)**.

3.2.3 نظام حماية المحتوى (content protection system): نظام في **النظام البيئي للسطح البيني المشترك المدمج (ECI)** يستخدم تقنيات التجفير لإدارة النفاذ إلى المحتوى والخدمات. ويمكن في كثير من الأحيان 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): الطرف الذي يوزع المحتوى الرقمي إلى **مستقبِل المحتوى** في **النظام البيئي للسطح البيني المشترك المدمج (ECI)**.

5.2.3 مستقبِل المحتوى (content receiver): جهاز يُستخدم للنفاذ إلى المحتوى الرقمي ضمن **النظام البيئي للسطح البيني المشترك المدمج (ECI)**. ويحتوي مستقبِل المحتوى على رقاقة مزودة **بمزيل تخليط المحتوى**.

6.2.3 مزيل تخليط المحتوى (content descrambler): مكون في رقاقة **النظام البيئي للسطح البيني المشترك المدمج (ECI)** قادر على إزالة تخليط المحتوى. ويمكن أن يكون مزيل تخليط المحتوى قادراً أيضاً على تجفير المحتوى (لغرض إعادة تجفير المحتوى). ويستخدم تجفير/فك تجفير المحتوى في هذه التوصية **مخطط تجفير متناظر**. وبالنسبة لمحتوى MPEG-2، يُشار أيضاً إلى تجفير المحتوى وفك تجفيره باسم التخليط وإزالة التخليط، على التوالي.

7.2.3 كلمة التحكم (control word): المفتاح السري المستخدم لتجفير وفك تجفير المحتوى ضمن **النظام البيئي للسطح البيني المشترك المدمج (ECI)**. وفي أنظمة إدارة الحقوق الرقمية، يُشار عادةً إلى كلمة التحكم على أنها مفتاح المحتوى.

8.2.3 دالة الاختزال التجفيرية (cryptographic hash function): دالة تجفيرية بدون مفتاح في **النظام البيئي للسطح البيني المشترك المدمج (ECI)** تأخذ كمدخلات بيانات ذات مقاس عشوائي، يشار إليها بالرسالة، وتُخرج كتلة بيانات ذات مقاس ثابت، يشار إليها باسم ملخص الرسالة. والخصائص المفترضة **لدالة الاختزال التجفيرية** في هذه التوصية هي أن **دالة الاختزال التجفيرية** تتصرف كدالة عشوائية مقاومة لدخل ثان ينتج الخرج نفسه.

9.2.3 مخطط التوقيع الرقمي (digital signature scheme): مخطط تجفيري غير متناظر ذو مفاتيح يستخدم لحماية أصالة البيانات في **النظام البيئي للسطح البيني المشترك المدمج (ECI)**. ويتكون **مخطط التوقيع الرقمي** من خوارزمية إنشاء المفتاح وعملية إنشاء التوقيع وعملية التحقق من التوقيع. وتتولد المفاتيح كأزواج (مفتاح سري/خصوصي، ومفتاح علني). وتوقَّع البيانات باستخدام مفتاح سري/خصوصي وتُستخدم المفاتيح العلنية المقابلة للتحقق من التوقيع. ويستخدم **مخطط التوقيع الرقمي** الموصَّف في هذه التوصية لحماية أصالة الرسائل على النحو المحدد في المرجع [b-ROEL]؛ وعلى وجه الخصوص، لا يُستخدم المخطط لضمان عدم التنصل أو استيقان المصدر في هذه التوصية.

10.2.3 النظام البيئي للسطح البيني المشترك المدمج (ECI): عملية تجارية تتكون من سلطة استوثاق وعدة منصات ومعدات مباني العملاء المتوافقة مع **السطح البيني المشترك المدمج** في هذا المجال.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

AD1	البيانات المرتبطة 1 *(Associated Data 1)*
AK	مفتاح الاستيقان *(Authentication Key)*
CA	النفاذ المشروط *(Conditional Access)*
CW	كلمة التحكم *(Control Word)*
DRM	إدارة الحقوق الرقمية *(Digital Rights Management)*
ECI	السطح البيني المشترك المدمج *(Embedded Common Interface)*
ID	معرّف الهويّة *(IDentity)*
LK	مفتاح الوصلة *(Link Key)*
SHA	خوارزمية فرم آمنة *(Secure Hash Algorithm)*
SPK	المفتاح العلني للمرسِل *(Sender Public Key)*
SSK	المفتاح السري/الخصوصي للمرسِل *(Sender Secret/private Key)*
T	وسم *(Tag)*
URI	معلومات قواعد الاستعمال *(Usage Rules Information)*

5 اصطلاحات

يشير استخدام الخط الداكن في نص هذه التوصية إلى مصطلحات ذات تعاريف خاصة بسياق السطح البيني المشترك المدمج التي يمكن أن تختلف عن تلك المتداولة في الاستعمال الشائع.

6 استيقان المعلومات والبيانات المرتبطة 1 ذات الصلة بقواعد استعمال كلمات التحكم

فيما يتعلق بتفاصيل التوصيف الواردة في الفقرة 7 من التوصية [ITU-T J.1015]، ورد توصيف عدة مدخلات لمجموعة سلم المفاتيح، وهي تغطي من بين أمور أخرى: CW-URI وAD1 وτ_b وSPK-URI وSPK_i، وLK المجفرة بالإضافة إلى هوية الرقاقة الموقَّعة. وتسلّم بعض هذه المدخلات، مثل LK وهوية الرقاقة، من المرسل إلى مجموعة سلم المفاتيح مجفَّرة ومشفوعة بتطبيق مخطط توقيع رقمي. ومن ناحية ثانية، تسلّم مدخلات مثل CW-URI وAD1 وτ_b وSPK-URI وSPK_i دون تطبيق أي مخططات تجفيرية. ويعتمد استيقان هذه المدخلات على الاستيقان الضمني؛ وفي حال تقديم قيمة غير أصلية لأي من مدخلات سلم المفاتيح، تُحسب قيمة غير صالحة لكلمة التحكم، CW، وتتعذر إزالة تخليط المحتوى بنجاح.

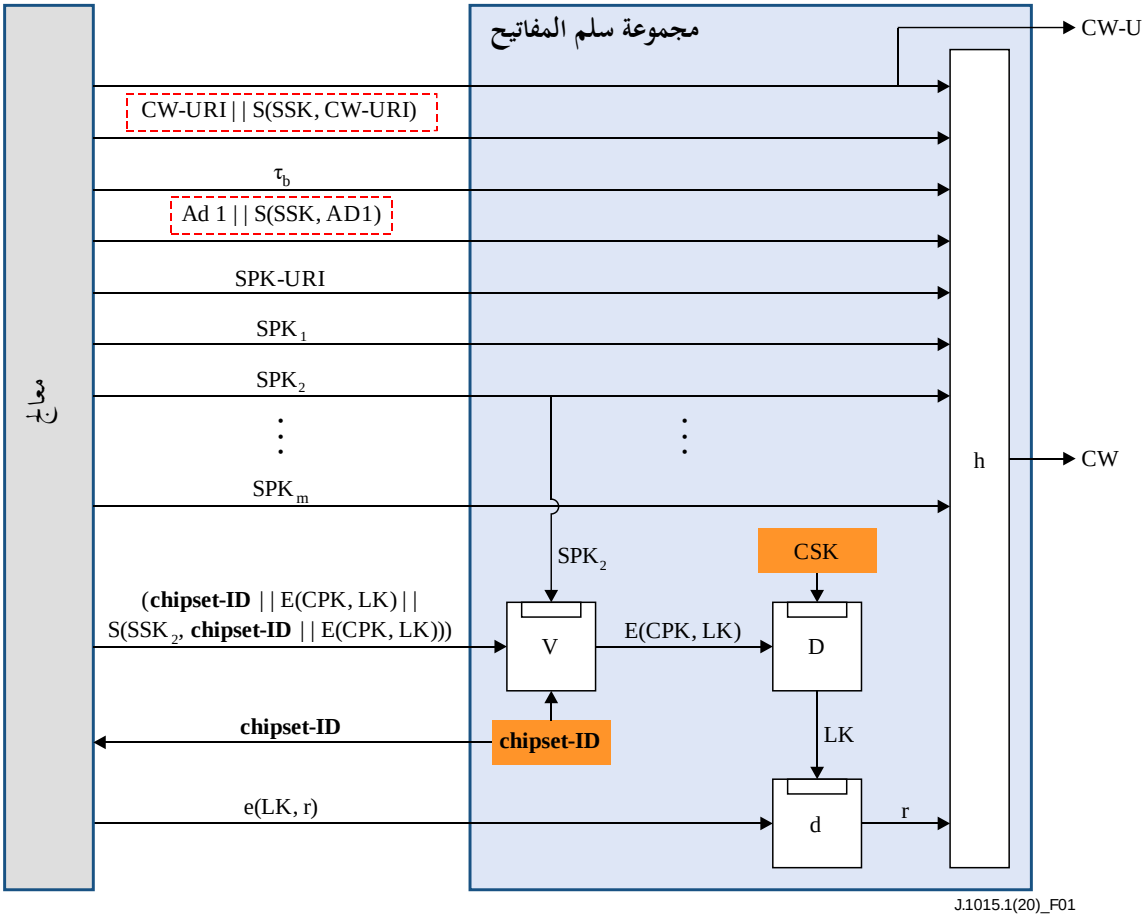
ويمكن للمرسل أن يرسل SPK_i وSPK-URI وτ_b دون تطبيق أي مخطط تجفيري عند النظر في طبيعة خصائص الدخل. وعلى الأخص يمكن التحقق من τ_b باستخدام عمليات التحقق الروتينية من البيانات المرتبطة، وبالتالي لا يُتطلب تطبيق مخطط الاستيقان الصريح عليها.

وفي حال تطلَّب مقدمو الخدمة ذلك، يمكنهم إدخال أسلوب إضافي للاستيقان الصريح بشأن مدخلات CW-URI وAD1 في مجموعة سلم المفاتيح. ويمكن أن تسمح هذه الخواص الوظيفية بزيادة المزايا المحقَّقة للمستخدمين بالإضافة إلى المزايا التشغيلية لمقدمي الخدمة.

وتوصِّف هذه التوصية طريقة لتطبيق مخطط استيقان على CW-URI وAD1 حين يشكلان مدخلات مجموعة سلم المفاتيح. ويمكن تحقيق ذلك بتطبيق مخطط التوقيع الرقمي الذي سبق أن استعمل من أجل Chipset-ID || E(SPK, LK) مع SSK. ويمكن لمشغلي الخدمات أن يستيقنوا بشكل انتقائي من CW-URI أو AD1، أو أن يستيقنوا من الاثنين في الوقت نفسه.

وإذا رغب مشغلو الخدمات في حماية CW-URI و/أو AD1، يُتطلب عندئذ استعمال المخطط المحدد في هذا الملحق.

انظر الشكل 1.



الشكل 1 – استيقان المعلومات والبيانات المرتبطة 1 ذات الصلة بقواعد استعمال كلمات التحكم

1.6 استيقان المعلومات ذات الصلة بقواعد استعمال كلمات التحكم

حساب (CW-URI || التوقيع) (المرسِل)

1) توقَّع سلسلة بتات CW-URI باستعمال المفتاح SSK_i؛ ويرمز إلى التوقيع بالرمز $S(SSK_i, CW\text{-}URI)$.

2) تذيَّل سلسلة بتات CW-URI بهذا التوقيع.

استخراج CW-URI (مجموعة سلم المفاتيح)

1) يُتحقق من طول بيانات الدخل. إذا كان طول CW-URI يساوي 64 بتة، تجري عندئذ مجموعة سلم المفاتيح العملية العادية المحددة في الفقرة 1.3.7 من التوصية [ITU-T J.1015] وتوقف عملية الاستيقان من معلومات CW-URI. وما عدا ذلك، أي إذا كان الطول أكبر من 64 بتة، تتابع عملية الاستيقان من معلومات CW-URI ويُنتقل إلى الخطوة التالية.

2) يُتحقق مما إذا كانت معلومات SPK-URI وقواعد الاستعمال المحددة في الفقرة 2.3.7 من التوصية [ITU-T J.1015] تجيز لعملية التحقق V استخدام SPK_i للتحقق من التوقيع. وفي حال عدم الإجازة، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

3) تُستخدم معلومات (CW-URI || التوقيع) وSPK_i للتحقق من التوقيع. وإذا كان التوقيع غير صالح، فيجب على مجموعة سلم المفاتيح إيقاف الحسابات.

4) تُستخرج معلومات CW-URI.

2.6 استيقان البيانات المرتبطة 1

حساب بيانات AD1 || التوقيع (المرسِل)

1) توقَّع سلسلة بتات AD1 باستعمال المفتاح SSK_i؛ ويرمز إلى التوقيع بالرمز $S(SSK_i, AD1)$.

2) تذيَّل سلسلة بتات AD1 بهذا التوقيع.

استخراج البيانات المرتبطة 1 (مجموعة سلم المفاتيح)

1) يُتحقق من طول بيانات الدخل. إذا كان طول AD1 يساوي 256 بتة، تجري عندئذ مجموعة سلم المفاتيح العملية العادية المحددة في الفقرة 1.3.7 من التوصية [ITU-T J.1015] وتوقف عملية الاستيقان من بيانات AD1. وما عدا ذلك، أي إذا كان الطول أكبر من 256 بتة، تتابع عملية الاستيقان من بيانات AD1 ويُنتقل إلى الخطوة التالية.

2) يُتحقق مما إذا كانت معلومات SPK-URI وقواعد الاستعمال المحددة في الفقرة 2.3.7 من التوصية [ITU-T J.1015] تجيز لعملية التحقق V استخدام SPK_i للتحقق من التوقيع. وفي حال عدم الإجازة، توقف عندئذ مجموعة سلم المفاتيح إجراء الحسابات.

3) تُستخدم معلومات (AD1 || التوقيع) وSPK_i للتحقق من التوقيع. وإذا كان التوقيع غير صالح، فيجب على مجموعة سلم المفاتيح إيقاف الحسابات.

4) تُستخرج بيانات AD1.

التذييل I

مجالات تحتاج لمزيد من التطوير

(لا يشكل هذا التذييل جزءاً من هذه التوصية.)

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

وأعرب 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 المستقلة عن المشغِّل (OTT) وخدمات التلفزيون الخطي وموردو حلول أنظمة النفاذ المشروط (CAS) وإدارة الحقوق الرقمية (DRM) – المنتشرة في شتى أرجاء العالم، عن مخاوفهم من أن السطح البيني ECI لا يفي تماماً بمتطلبات الحماية ECP ولا بمتطلبات حماية المحتوى لدوائر الصناعة على نطاق أوسع.

وبعبارة أدق، أبدى هؤلاء مخاوفهم في مساهمات قُدمت 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، ولكن تعذر التوصل إلى اتفاق بشأنها. وترد قائمة جرد لهذه البنود في المرجع [b-SG9 Report 17 Ann.1].

وهي تتضمن مقترحات من أجل:

1) تبسيط النظام ECI بتضييق نطاقه؛
2) إلغاء إدارة الحقوق الرقمية (DRM)؛
3) إلغاء إعادة تجفير المحتوى؛
4) إلغاء إدارة البرمجيات؛
5) إضافة سطوح بينية لبرمجة التطبيق (API) توخياً لتأمين عمليات التخزين والتجفير؛
6) السماح بسلالم المفاتيح الخاصة بالبائعين؛
7) استخدام متطلبات TEE للتوصية ITU-T J.1027؛
8) إضافة تنفيذ TEE إلى VM؛
9) تعزيز قوة خوارزميات التجفير، باستعمال SHA-384 مثلاً؛
10) استعمال شهادات معيارية، مثل التوصية ITU-T X.509؛
11) إعادة النظر في الاتصالات بين الوسطاء؛
12) إجراء مزيد من الاتصالات مع معهد ETSI؛
13) إجراء المزيد من استعراضات النظراء؛
14) استقصاء بدائل لنموذج سلطة الاستوثاق؛
15) تحديد المزيد من الجوانب التقنية لقواعد التزام السطح البيني ECI ومتانته؛
16) إضافة متطلبات من أجل التنوع، مثل التحديد العشوائي لحيز العنوان؛
17) إضافة متطلبات بشأن التحقق من سلامة وقت التشغيل.

وتبين هذه المقترحات أن حماية المحتوى والتهديدات الخاصة بإصابتها بالخلل تتطور باستمرار. وقد صمم السطح البيني ECI في الأصل قبل الموافقة على توصية قطاع تقييس الاتصالات هذه بعقد من الزمن تقريباً. والأنظمة من شاكلة السطح البيني ECI تحتاج إلى التقييم بصورة منتظمة على محك أحدث تقنيات الهجمات ومتطلبات حماية الصناعة، على السواء.

وهناك آليات أخرى لتمكين قابلية التشغيل البيني. وبالنسبة لحالة استعمال إدارة الحقوق الرقمية، بوجه خاص، نشرت معظم خدمات الفيديو عبر الإنترنت حلولاً أخرى لتحقيق قابلية التشغيل البيني ولتلبية هذه الاحتياجات.

وزيادة الوضوح مهمة في هذا الصدد لأن الكثير من الدول الأعضاء تعتبر معايير الاتحاد مصادر توجيه مؤثرة في 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 أخذ هذه القضايا بعين الاعتبار عندما تتطلب التشريعات أو اللوائح أو الاحتياجات السوقية من معدات التلفزيون الرقمي الاستهلاكية بأن تكون قابلة للتشغيل البيني. ويضمن ذلك أيضاً في حالة مصنعي المعدات التكنولوجية، الذين قد يفضلون استخدام مجموعة فريدة من المتطلبات أو معايير أخرى لتصميم المنتجات، إمكانية أن يأخذوا هذه القضايا بعين الاعتبار 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-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-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 Available at: 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 العلني 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 العلنية للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2020