الاتحـــــاد الدولـــــي للاتصـــــالات

ITU-T J.197

(2005/11)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة J: الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية وإشارات أخرى متعددة الوسائط

المودمات الكبلية

متطلبات رفيعة المستوى لجسر إدارة الحقوق الرقمية (DRM) من شبكة نفاذ كبلية إلى شبكة منـــزلية

التوصيـــة ITU-T J.197

ITU-T

متطلبات رفيعة المستوى لجسر إدارة الحقوق الرقمية (DRM) من شبكة نفاذ كبلية إلى شبكة منـــزلية

ملخص

تُحدد هذه التوصية متطلبات جسر إدارة الحقوق الرقمية انطلاقاً من شبكة نفاذ كبلية إلى شبكة منـــزلية يمكن لمشغل الشبكة أن ينقل إليها عدة أنماط من المحتويات (مثل الفيديو والصوت، الخ) مع ضمان عدم استعمال هذا المحتوى لأغراض تمثل انتهاكاً لأي من اتفاقات الخدمة أو المتطلبات القانونية.

المصدر

وافقت لجنة الدراسات 9 (2005-2008) لقطاع تقييس الاتصالات في الاتحاد بتاريخ 29 نوفمبر 2005 على التوصية ITU-T J.197 بموجب الإجراء الوارد في التوصية ITU-T A.8.

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) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

متطلبات رفيعة المستوى لجسر إدارة الحقوق الرقمية (DRM) من شبكة نفاذ كبلية إلى شبكة منـــزلية

1 مجال التطبيق

تُحدد هذه التوصية متطلبات جسر إدارة الحقوق الرقمية انطلاقاً من شبكة نفاذ كبلية إلى شبكة منـــزلية يمكن لمشغل الشبكة أن ينقل إليها عدة أنماط من المحتويات (مثل الفيديو والصوت، الخ) مع ضمان عدم استعمال هذا المحتوى لأغراض تمثل انتهاكاً لأي من اتفاقات الخدمة أو المتطلبات القانونية.

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 بتوصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

- NIST FIPS 140-2 (2002)، *متطلبات أمنية للوحدات التجفيرية*.

2.2 المراجع الإعلامية

- التوصية ITU-T J.192 (2005)، *بوابة منـــزلية لدعم توزيع خدمات المعطيات الكبلية*.
- DTCP (2005)، *مواصفة حماية محتوى الإرسال الرقمي، المجلد 1 (طبعة إعلامية)*.
- Intel (2005)، *نظام حماية المحتوى الرقمي عريض النطاق، المراجعة 1.1*.

3 المصطلحات والتعاريف

تعرف هذه التوصية المصطلحات التالية:

1.3 بتات نظام الحماية التماثلي أو (بتات APS): البتتان 3 و2 من معلومات التحكم في النسخ (CCI)، وتدلان على حالة الحماية التماثلية لوحدة فك التشفير.

2.3 قواعد التقييد: هي القواعد التي تنطبق على وحدات فك التشفير للحيلولة دون النسخ غير المسموح به للمحتوى المتحكم فيه.

3.3 علامة "مائية" متفق عليها: هي علامة مائية قياسية استحدثت بغرض استعمالها في نظام إدارة الحقوق الرقمية (DRM).

4.3 الصورة المقيدة: المعادل المرئي لما لا يتجاوز 000 520 بكسل في الرتل الواحد (مثال ذلك صورة ذات استبانة تحتوي على 540 خط رأسي و960 خط أفقي بالنسبة إلى النسبة الباعية 16:9). ويمكن إخراج الصورة المقيدة أو عرضها باستعمال تقنيات معالجة الإشارات الفيديوية مثل مضاعفة الخطوط أو شحذها لتحسين النوعية المدركة للصورة.

5.3 إطلاق الصورة المقيدة (CIT): المجال أو البتات المستعملة لإطلاق خرج "صورة مقيدة" في الخرج التماثلي عالي الوضوح لوحدة فك التشفير.

6.3 حماية المحتوى: تطبيق الحماية التقنية التي تحول دون عمليات النسخ و/أو إعادة التوزيع غير المسموح بها للمحتوى الموزع بواسطة الشبكة.

7.3 المحتوى المتحكم فيه: هو المحتوى الذي يرسل من شبكة مزود الخدمة الفيديوية مع استعمال بتات مؤشر أسلوب التجفير (EMI) المحددة عند قيمة تختلف عن الصفر، صفر (0,0) ("نسخ غير مقيد").

8.3 معلومات التحكم في النسخ (CCI): مجال يتكون من بايتة واحدة يحتوي على المعلومات التي تستعملها وحدة فك التشفير للتحكم في نسخ المحتوى. انظر الملحق A لمزيد التفاصيل.

9.3 إدارة الحقوق الرقمية (DRM): تعريف مجموعة من قواعد استعمال المحتوى وإدارتها وتطبيقها. وتوضح قواعد الاستعمال هذه بعض الأمور من قبيل حق النسخ أو المشاهدة أو توزيع جزء محدد من المحتوى.

10.3 الحماية الرقمية لمحتوى الإرسال (DTCP): طريقة خاصة بتجفير وإزالة تجفير وتبادل المفاتيح والقابلية للتجدد التي يرد وصفها في المواصفة بعنوان "حماية محتوى الإرسال الرقمي 5C – الإصدار 1.0".

11.3 جسر إدارة الحقوق الرقمية: البنية التحتية والتكنولوجيات المتعلقة بالتوزيع والشبكة المنـــزلية المستعملة بغرض تمكين حماية المحتوى وإدارة الحقوق الرقمية للمحتوى الموزع بواسطة الشبكة، وتخزينه وتوزيعه في شبكة منـــزلية.

12.3 بتات مؤشر أسلوب التجفير (بتات EMI): بتتان ترتبطان بالمحتوى المحمي، وتحددان عمليات النسخ التي يُسمح بها بالنسبة إلى المحتوى ذي الصلة.

13.3 صيغة أو خرج تماثلي عالي الوضوح: نسق أو خرج غير رقمي، له استبانة أعلى من الوضوح المعياري للصيغة أو للخرج التماثلي.

14.3 حماية المحتوى الرقمي عريض النطاق (HDCP): طريقة الاستيقان والتجفير وإزالة التجفير وقابلية التجدد التي يرد وصفها في المواصفة بعنوان "نظام حماية المحتوى الرقمي عريض النطاق، المراجعة 1.1".

15.3 المنتج: أداة و/أو تكنولوجيا تستقبل، ومن الممكن أن توزع، محتوى يجرى التحكم في إعادة توزيعه و/أو نسخه.

16.3 قواعد المتانة: هي القواعد الموصوفة في الفقرة 6، وتنطبق على وحدات فك التشفير، وقد وضعت بغرض التصدي لمحاولات تغيير وحدات فك التشفير بغرض إلغاء وظائف قواعد التقيد.

17.3 الخدمة: الإشارات الفيديوية أو الصوتية أو إشارات البيانات، سواء كانت في نسق تماثلي أم في نسق رقمي، ترسل على شبكة مقدم الخدمة الفيديوية إلى (أو من) وحدة فك التشفير، بغرض استقبال أو إرسال محتوى إعلامي أو مسلي أو ترابطي.

18.3 وحدة فك التشفير (STB): جميع التجهيزات التي تستقبل المحتوى مباشرة من مقدم الخدمة الفيديوية، وتشمل التجهيزات المنفصلة عن جهاز العرض وتجهيزات العرض التي تمتلك الوظائف المترسخة المناسبة. وتعمل الوحدة STB كبوابة خدمة للشبكة المنـــزلية، وتشمل نظام النفاذ المشروط (CA) ونظام إدارة الحقوق الرقمية (DRM).

19.3 الصيغة أو الخرج التماثلي معياري الوضوح: نسق أو خرج غير رقمي (مثل PAL RF أو NTSC RF أو Composite أو S-Video أو YUV أو Y أو R-Y أو B-Y أو RGB)، ليس له أكثر من 483 خط من خطوط المسح النشيط التشذيري أو التدريجي.

20.3 نظام حماية المحتوى الفيديوي (VCPS): خاص بتسجيل محتوى مجفر على وسائط ضوئية رقمية (قرص رقمي متعدد الأغراض – قابل لإعادة التسجيل (DVD+RW) وقرص رقمي متعدد الأغراض – قابل للتسجيل (DVD+R)) محمي بواسطة تكنولوجيا النظام VCPS.

21.3 مقدم الخدمة الفيديوية (VSP): مقدم الخدمة يقدم "خدمات" على النحو المحدد في هذه التوصية.

4 المختصرات والتسميات المختصرة والاصطلاحات

تستعمل هذه التوصية المختصرات التالية:

AES: معيار تجفير متطور (*Advanced Encryption Standard*)

APS: نظام الحماية التماثلي (*Analogue Protection System*)

CCI: معلومات التحكم في النسخ (*Copy Control Information*)

CGMS-A: نظام إدارة توليد النسخ – تماثلي (*Copy Generation Management System Analogue*)

CIT: إطلاق الصورة المقيدة (*Constrained Image Trigger*)

DRM: إدارة الحقوق الرقمية (*Digital Rights Management*)

DTCP: حماية محتوى الإرسال الرقمي (*Digital Transmission Content Protection*)

DVD-RW: قرص رقمي متعدد الأغراض – قابل لإعادة التسجيل (*Digital Versatile Disk – Re-Writable*)

DVD+R: قرص رقمي متعدد الأغراض – قابل للتسجيل (*Digital Versatile Disk + Recordable*)

DOCSIS: مواصفة السطح البيني لخدمة نقل المعطيات بواسطة الكبل (*Data Over Cable Service Interface Specification*)

DVI: السطح البيني المرئي الرقمي (*Digital Visual Interface*)

EEPROM: ذاكرة للقراءة فقط قابلة للبرمجة والمحو كهربائياً (*Electrically Erasable Programmable Read-Only Memory*)

EMI: مؤشر أسلوب التجفير (*Encryption Mode Indicator*)

HDCP: حماية المحتوى الرقمي عريض النطاق (*High-Bandwidth Digital Content Protection*)

HDMI: سطح بيني للوسائط المتعددة عالي الوضوح (*High-Definition Multimedia Interface*)

IP: بروتوكول الإنترنت (*Internet Protocol*)

LSB: البتة الأقل دلالة (*Least Significant Bit*)

MPEG: فريق خبراء الصور المتحركة (*Moving Picture Experts Group*)

NTSC RF: اللجنة الوطنية لأنظمة التلفزيون – التردد الراديوي (*National Television System Committee Radio Frequency*)

OOB: خارج النطاق (*Out of Band*)

PAL: خط تناوبي الطور (*Phase Alternate Line*)

PCI: السطح البيني للمكونات المطرافية (*Peripheral Component Interface*)

PCMCIA: الرابطة الدولية لبطاقات ذاكرة الحاسوب الشخصي (*Personal Computer Memory Card International Association*)

QoS: نوعية الخدمة (*Quality of Service*)

RF: التردد الراديوي (*Radio Frequency*)

RGB: أحمر، أخضر، أزرق (*Red, Green, Blue*)

SRM: رسالة قابلية تجدد النظام (*System Renewability Message*)

STB: وحدة فك التشفير (*Set Top Box*)

S-Video: فيديو فائق (*Super-Video*)

VCPS: نظام حماية المحتوى الفيديوي (*Video Content Protection System*)

VSP: مقدم الخدمة الفيديوية (*Video Service Provider*)

WTSA: الجمعية العالمية لتقييس الاتصالات (*World Telecommunication Standardization Assembly*)

5 نظرة إجمالية

شهد استعمال تكنولوجيا الشبكات المنـــزلية وقبولها بها حداً من التطور جعل الشبكة المنـــزلية تتحول إلى شبكة تسلية لا يمكن الاستغناء عنها، إذ تسمح للمستعمل بتخزين المحتويات وتوزيعها على مختلف التجهيزات الموصلة بالشبكة المنـــزلية. ولعل من مصلحة الصناعة أن تدعم هذه البيئة وذلك بتوسيع تقديم الخدمات الترفيهية إلى الشبكة المنـــزلية. ولأن الخدمات الكبلية غالباً ما تنطوي على محتوى رفيع المستوى يخضع لحقوق الملكية الفكرية، ظهرت الحاجة إلى تحديد آليات بغرض حماية هذا المحتوى وتطبيق قواعد الاستعمال ذات الصلة، وذلك لعدة أسباب قانونية وتجارية. وتحدد هذه التوصية متطلبات جسر إدارة الحقوق الرقمية انطلاقاً من شبكة النفاذ بواسطة الكبل إلى شبكة منـــزلية يمكن أن ينقل إليها مشغل الشبكة عدة أنماط من المحتويات مع ضمان عدم استعمال المحتوى استعمالاً يؤدي إلى انتهاك اتفاقات الخدمة أو المتطلبات القانونية.

1.5 الأهداف الرئيسية

تشتمل الأهداف الرئيسية لتنفيذ جسر إدارة الحقوق الرقمية على ما يلي:

- ما يكفي من المتانة من منظور مقدم المحتوى.
- عدم التدخل من منظور المشترك.
- الانسجام مع البيئة التنظيمية والتشريعية.

2.5 السمات الرئيسية

فيما يلي السمات الرئيسية لجسر إدارة الحقوق الرقمية:

- استيقان جميع التجهيزات المشاركة في إرسال و/أو استهلاك المحتوى الفيديوي.
- توسيع مجموعة غنية بالقواعد التجارية لحماية المحتوى بواسطة إدارة الحقوق الرقمية (تقييد عدد النسخ، عدد المشاهدات، الحدود الزمنية، الخ) التي وضعت كجزء من الوحدة STB.
- تجفير/إزالة تجفير المحتوى الفيديوي المعد بغرض الإرسال والاستهلاك.

3.5 النقاط التقنية الرئيسية

فيما يلي بعض النقاط التقنية الرئيسية لجسر إدارة الحقوق الرقمية:

- يمدد جسر إدارة DRM العناصر الأساسية لإدارة DRM إلى خارج الوحدة STB؛
- يدعم جسر إدارة DRM إرسال وتخزين المحتويات التي يوزعها المشغل الكبلي والمشغل غير الكبلي على حد سواء؛
- لا يمكن للمحتوى ذي التحكم في إعادة التوزيع أو النسخ أن يخرج من الوحدة STB أو من عناصر تدفق الاتجاه الهابط إلا عن طريق خرج معتمد.
- يمكن استهلاك وتخزين المحتوى الذي يفتقد إلى التحكم في إعادة التوزيع أو النسخ في الوحدة STB أو في عناصر تدفق الاتجاه الهابط؛

- يمكن للمحتوى الذي يفتقد إلى التحكم في إعادة التوزيع أو النسخ أن يخرج بكل حرية من الوحدة STB أو من عناصر تدفق الاتجاه الهابط.

4.5 متطلبات عامة تتعلق بجسر إدارة الحقوق الرقمية

G-1	**سهولة الاستعمال بالنسبة إلى المشترك**: يجب أن يكون جسر إدارة DRM شفافاً بالنسبة إلى المشترك، وأن يسمح باستهلاك ملائم للمحتوى وألا يمثل أي عائق أمام الاستعمال.
G-2	**نموذج استعمال بسيط**: سيستخدم جسر إدارة DRM نموذج استعمال بسيط، يسمح باستعمال المحتوى المشترى من مشغل الشبكة والموزع بواسطته في الشبكة المنـــزلية وفقاً للحقوق المعطاة لهذا المحتوى.
G-3	**حماية المحتوى**: يمنع جسر إدارة DRM إرسال ونسخ المحتويات المحمية خارج الشبكة المنـــزلية.
G-4	**الحيلولة دون سرقة الخدمة**: يمنع جسر إدارة DRM سرقة الخدمة ويحمي قواعد استعمال المحتوى (مثل سرقة المحتوى على إحدى الشبكات اللاسلكية في وحدات منـــزلية متعددة).
G-5	**التوافق مع تكنولوجيات DRM الأخرى**. لا يحول جسر إدارة DRM دون استعمال تكنولوجيات أخرى لحماية المحتوى بالنسبة إلى المحتوى المقدم بواسطة مشغل غير كبلي.
G-6	**استقلالية تكنولوجيا النقل**: تكون تكنولوجيا النقل المستعملة في تنفيذ جسر إدارة DRM مستقلة عن تكنولوجيات الشبكات المنـــزلية.
G-7	**الملاءمة الرجعية**: لا تؤثر تكنولوجيا جسر إدارة DRM في عقود التوزيع الفيديوي الحالية.
G-8	**استقلالية التوزيع**: يدعم جسر إدارة DRM مختلف تكنولوجيات التوزيع، بما في ذلك إذاعة MPEG وتدفق IP وبروتوكول نقل الملفات (FTP).
G-9	**الحماية في الوقت الفعلي**: تكون التكنولوجيا المستعملة في تنفيذ جسر إدارة DRM قابلة للتطبيق على الوسائط المتعددة في الوقت الفعلي (مثلما هو الحال بالنسبة إلى إذاعة MPEG ومصادر التدفق IP).
G-10	**التكامل**: ينبغي لتكنولوجيات وعمليات جسر إدارة DRM أن تتوافق مع المبادرات الصناعية الأخرى ذات الصلة مثل DOCSIS (توصيات السلسلة ITU-T J.112/J122) وIPCablecom (توصيات السلسلة ITU-T J.16x وJ.17x) وIPCable2Home (توصيات السلسلة J.19x).
G-11	**مواصفة مفتوحة**: تسمح مواصفة جسر إدارة DRM بالتشغيل البيني بين تجهيزات مختلف البائعين.
G-12	**الجدوى الاقتصادية**: ينبغي لتكلفة التطبيق والصيانة وإثبات الصحة وتنفيذ تكنولوجيا وعمليات جسر إدارة DRM أن تسمح بتحقيق نماذج اقتصادية ذات جدوى.
G-13	**إدارة دينامية**: تكون المعلومات المستعملة في حماية المحتوى قابلة للتشكيل والإدارة بصفة دينامية.
G-14	**قابلية التجدد**: تكون برمجية أمن جسر إدارة DRM قابلة للتجدد.
G-15	**دعم التشغيل أثناء التوقف**: يدعم توزيع المحتوى المتحكم فيه وغير المتحكم فيه إلى الشبكة المنـــزلية في حالة حدوث عطب في النفاذ إلى نظام النفاذ المشروط.
G-16	**المحتوى غير المحمي**: لا يؤثر جسر إدارة DRM بأي شكل من الأشكال **في** استعمال المحتوى غير المحمي.
G-17	**مدى حماية المحتوى**: تكون حماية المحتوى متيسرة، على النحو المنصوص عليه في مجموعة قواعد نظام إدارة DRM، بالنسبة إلى كل الإرسالات الفيديوية في الشبكة المنـــزلية.
G-18	**تمديد مجموعة قواعد إدارة DRM**: مجموعة غنية بقواعد إدارة DRM (النسخ، إعادة المشاهدة، وقت المشاهدة، إلخ) متيسرة في نظام DRM ويجب أن تدار بواسطة وحدة STB وأن تمتد إلى عناصر تدفق الاتجاه الهابط.
G-19	**استيقان الزبون**: يدعم استيقان جميع العناصر الملحقة بالشبكة المنـــزلية التي تشارك في إرسال و/أو استهلاك المحتويات الفيديوية.
G-20	**التجفير**: يوفر تجفير المحتوى بالنسبة إلى الإرسالات الفيديوية في الشبكة المنـــزلية.
G-21	**إلغاء التجهيزات**: يجب إتاحة القدرة على رفض نفاذ المحتوى إلى جهاز محدد، حتى وإن كان ذلك الجهاز في وقت ما عنصراً شبكياً صحيحاً لجسر إدارة DRM.

5.5 معلومات أساسية

من الضروري عند التعامل مع توزيع المحتويات المحمية عبر شبكة توزيع آمنة، وضع تكنولوجيا لحماية المحتويات من عمليات النسخ أو إعادة التوزيع غير المسموح بها. وعلاوة على ذلك، يجب أن يكون الجهاز في حد ذاته متيناً وقادراً على مقاومة الخطر الأمني. وتشرح هذه التوصية بالتفصيل متطلبات تكنولوجيا حماية المحتوى وكذلك متطلبات المتانة والتقيد بالنسبة إلى التجهيزات التي تتعامل مع المحتويات المحمية. وقد كُتبت هذه المتطلبات المتعلقة بتكنولوجيا المحتوى ومتانته من منظور جهاز استقبال الزبون (أي وحدة فك التشفير) الذي يستقبل المحتوى من مقدم الخدمة الفيديوية كجزء من شبكة توزيع كبلية التي يجب أن تحمي محتوى عالي القيمة. ويحفر المحتوى عند المصدر وتجري حمايته في كافة أرجاء شبكة مقدم الخدمة. وترمي هذه التوصية إلى التأكد من إتاحة مستوى أمني مماثل في الشبكات المنـــزلية. ويمثل إدراج تدفق المحتوى هذا في بيئات تدفق الاتجاه الهابط على نحو متين وآمن الموضوع الرئيسي لهذه التوصية.

وينبغي لتكنولوجيات حماية المحتوى والخرج الرقمي التي تسمح لمحتوى مقدم الخدمة بالخروج من وحدة فك التشفير أن تضمن استمرار احتفاظ مقدم الخدمة بالتحكم في نسخ ذلك المحتوى وإعادة توزيعه، حتى بعد خروج المحتوى من وحدة فك التشفير إلى تجهيزات أخرى. وينبغي لتجهيزات الاتجاه الهابط وحدة فك التشفير التي تحتوي على خرج رقمي معين، إدارة DRM، أو تكنولوجيا حماية المحتوى، أن تتوافق أيضاً مع قواعد المتانة والتقيد التي نصت عليها هذه التوصية بشأن وحدة فك التشفير. وتتحكم قواعد المتانة والتقيد الموضوعة بالنسبة إلى وحدة فك التشفير في إجمالي النظام البيئي لتدفق الاتجاه الهابط.

6 متطلبات المتانة

يجب أن تتقيد التجهيزات التي تستقبل والتي من الممكن أن توزع محتوى محمياً أن تتمثل بعدد متطلبات المتانة لضمان حماية كافية للمحتوى. ومن المسلم به أن المتانة يمكن أن تتغير تبعاً للمحتوى المتاح للجهاز وأنها قد تحتاج إلى التغير عبر الزمن مع تطور تكنولوجيا الأمن وتطور أساليب قرصنة هذه التكنولوجيا. وتبرز هذه الفقرة مجموعة تنوعية من متطلبات متانة التجهيزات الموصى بها.

1.6 البناء

1.1.6 اعتبارات عامة

تستوفي المنتجات قواعد التقيد وتُصمم وتُصنع على نحو يُبطل فعلياً محاولات تعديل مثل هذه المنتجات بغرض التغلب على قواعد التقيد.

2.1.6 وظائف الإخفاق

لا تشتمل المنتجات على ما يلي:

i) مفاتيح أو أزرار أو وصلات عبور أو أسلاك معينة يمكن قطعها، أو أي مكافئ برمجي للعناصر السابقة؛ أو

ii) قوائم خدمة أو وظائف (بما في ذلك وظائف التحكم عن بعد)،

التي يمكن بواسطتها في كل حالة التغلب على تكنولوجيات حماية المحتوى أو أنظمة الحماية التماثلية أو إعادة الحماية أو قيود الخرج أو حدود التسجيل، أو الأحكام الإلزامية الأخرى لقواعد التقيد أو التي يمكن أن يتعرض بواسطتها المحتوى المتحكم فيه إلى نسخ غير مسموح به. وفي مفهوم هذه التوصية، يعني تعبير "إعادة الحماية" تطبيق تكنولوجيا حماية معتمدة، عند الاقتضاء، على محتوى متحكم فيه يُستقبل من شبكة التوزيع الفيديوي، ويجب أن يكون هذا المحتوى مستخرجاً من وحدة فك التشفير، كما يقصد به تكامل النظام والطرائق التي يُضمن بموجبها هذا التطبيق.

3.1.6 المحافظة على الأسرار

لإبطال محاولات بعض الأطراف غير المسموح لها الرامية إلى تهديد أمن المنتجات، تصمم المنتجات وتُصنع على نحو يحول بطريقة فعالة دون المحاولات الرامية إلى الاكتشاف أو الكشف عن:

i) الرقم الوحيد لطول بتات محدد، يخصص لكل وحدة فك تشفير، أو الأرقام المستعملة في عملية التحفير أو إزالة تحفير المحتوى المتحكم فيه (أرقام يشار إليها جماعياً بتعبير"مفاتيح")؛

ii) الطرائق وخوارزميات التحفير المستعملة لتوليد هذه المفاتيح.

2.6 مسيرات المحتوى المتحكم فيه

لا يكون المحتوى متاحاً عند مخرج آخر خلاف المخرج المحدد في قواعد التقيد، وفي مثل هذه المنتجات، يجب ألا يتواجد المحتوى المتحكم فيه على أيٍّ من أدوات التوصيل التي ينفذ إليها المستعمل (على النحو المحدد أدناه) في صيغة غير مجفرة ومضغوطة. وبالمثل، يجب ألا تتواجد المفاتيح غير المجفرة المستعملة لدعم تجفير و/أو إزالة تجفير المحتوى في معطيات المنتج على موصلات ينفذ إليها المستعمل. و"أداة التوصيل التي ينفذ إليها المستعمل" هي أداة توصيل للبيانات معطيات صُممت بغرض عمليات التحيين التي يضطلع بها المستعمل النهائي أو بالنسبة إلى النفاذ مثل أداة توصيل PCI التي تملك مقبساً (أو التي ينفذ إليها المستعمل من ناحية أخرى)، أو SmartCard أو PCMCIA أو Cardbus.

3.6 طرائق تعزيز متانة الوظائف

تستعمل المنتجات التقنيات التالية على الأقل لتعزيز متانة الوظائف والحماية المحددة في هذه التوصية:

1.3.6 الوظائف الموزعة

تُصمم وتُصنع أجزاء المنتج التي تقوم بالاستيقان وإزالة التحفير، وكذلك الشأن بالنسبة إلى مزيل الشفرة MPEG (أو أي جهاز مماثل) بالترابط إن لم يكن بالتكامل مع بعضها بعضاً بحيث يمكن تأمين المحتوى المتحكم فيه بأي شكل تدفق يمكن استعماله إلى مستوى الحماية الموصوفة في الفقرة 5.3.6 من التعرض إلى الاستيلاء أو النسخ.

2.3.6 البرمجية

يشتمل كل جزء من المنتج الذي يطبق جزءاً من تكنولوجيا حماية المحتوى في البرمجية على كل الخصائص الواردة في الفقرتين 1.6 و2.6. وفي مفهوم هذه التوصية، يعني تعبير "البرمجية" تنفيذ الوظائف حسب المتطلبات التي تنص عليها هذه التوصية بواسطة شفرة برمجية الحاسوب التي تتألف من تعليمات أو بيانات، بخلاف التعليمات أو البيانات التي يحتوي عليها العتاد. وتكون عمليات التنفيذ هذه:

أ) متقيدة بالفقرة 3.1.6 بأية طريقة معقولة تشمل، ولكن لا تقتصر على التحفير وتنفيذ جزء من التطبيق بأسلوب حلقة مستوى الصفر أو المشرف، و/أو التضمين في تطبيق مادي آمن؛ وفي كل حالة من حالات التنفيذ في شكل برمجية، باستعمال التقنيات الفعالة للتعتيم أو للحد أو التقييد من المحاولات الرامية إلى اكتشاف النهج المستعملة؛

ب) مصممة بهدف الاضطلاع بدور التحقق الذاتي من تكامل العناصر المكونة لها بحيث يمكن للتعديلات غير المسموح بها أن تؤدي إلى إخفاق في التنفيذ لتوفير الوظيفة المسموح بها للاستيقان و/أو إزالة التحفير. ولأغراض هذا الحكم، يشمل التعديل أي تغيير أو تشويش أو انتهاك للسمات أو الخصائص أو توقف المعالجة، ذات الصلة بالفقرتين 1.6 و2.6. ويتطلب هذا الحكم كحد أدنى استعمال شفرة التحقق من الإطناب الدوري الذي يجفر بعد ذلك بواسطة مفتاح خصوصي أو خوارزمية تظليل آمنة؛

ج) مستوفية لمستوى الحماية الموصوفة في الفقرة 5.3.6.

د) مصممة بغرض توفير آليات حماية ضد هجمات البرمجيات غير المسموح بها.

3.3.6 العتاد

يشمل كل جزء من المنتج الذي ينفذ متطلبات هذه التوصية في العتاد كل الخصائص المنصوص عليها في الفقرتين 1.6 و2.6. ولغايات قواعد المتانة، يُقصد بتعبير "العتاد" تجهيز مادي، بما في ذلك المكون الذي ينفذ أي متطلب من متطلبات حماية المحتوى التي تقضي بها هذه التوصية ويتقيد المنتج بها وأن:

i) لا يشمل تعليمات أو بيانات أخرى خلاف هذه التعليمات أو البيانات التي تدرج بشكل دائم في هذه التجهيزات أو المكونات؛ أو

ii) يشمل التعليمات أو البيانات التي لا تدرج بشكل دائم في هذه المنتجات أو المكونات حيث تتكيف هذه التعليمات أو البيانات لهذا المنتج أو لهذا المكون وأن هذه التعليمات أو البيانات لا يسهل نفاذ المستعمل النهائي إليها من خلال هذا المنتج أو المكون.

وينبغي لهذه التطبيقات أن:

أ) تتقيد بالفقرة 3.1.6 بأية طريقة معقولة دون أن تقتصر على: المفاتيح المدمجة وطرائق توليد المفاتيح وخوارزميات التجفير المدمجة في الدارات المتكاملة أو في البرمجيات الثابتة التي لا يمكن قراءتها بطريقة معقولة، أو التقنيات الموصوفة أدناه بخصوص البرمجيات؛

ب) تصمم على نحو من شأنه أن تؤدي محاولات إعادة البرمجة أو إزالة أو استبدال عناصر البرمجية بشكل يُعرِّض أمن أو خواص محتوى التكنولوجيا قيد التقييم أو وحدة فك التشفير لخطر جسيم بالمنتج بحيث لا يكون قادراً على استقبال أو تجفير أو فك تشفير المحتوى المتحكم به (مكون ملحوم لا "منشوب في مقبس")؛

ج) تستوفي مستوى الحماية الموصوفة في الفقرة 5.3.6.

4.3.6 عتاد هجين

تصمم السطوح البينية بين أجزاء العتاد والبرمجيات للمنتج على نحو يسمح لها بإتاحة سوية حماية مماثلة للسوية التي يتيحها التنفيذ المادي البحت أو البرمجي البحت، الموصوف أعلاه.

5.3.6 مستوى الحماية

يجب تطبيق الوظائف الأساسية للتجفير (الإبقاء على سرية المفاتيح، وطرائق توليد المفاتيح والخوارزميات التجفيرية، ومطابقة قواعد التقيد وتفادي النسخ أو المشاهدة غير المسموح بها للمحتوى المتحكم فيه الذي أزيل تجفيره) وفقاً لمتطلبات "المستوى 2" من المواصفة FIPS PUB 140-2: "متطلبات أمن النماذج التجفيرية" وعلى أدنى تقدير، على نحو:

أ) لا يمكن بشكل معقول التنبؤ بتفاديها أو الحيلولة دونها بمجرد استعمال أدوات أو تجهيزات مخصصة للاستعمال العام المتاحة على نطاق واسع بثمن معقول مثل المِفكات والموصلات والمشابك وكاويات اللحام ("أدوات متيسرة على نطاق واسع")، أو باستعمال أدوات إلكترونية متخصصة أو أدوات برمجية متخصصة تتاح على نطاق واسع بأسعار معقولة مثل أجهزة قراءة وتسجيل الذاكرة القابلة للبرمجة للقراءة فقط وقابلة للمحو إلكترونياً وبرمجيات إزالة المشاكل وفض التجميع EEPROM أو ما شابهها من أدوات تطوير البرمجيات ("أدوات متخصصة") بخلاف التجهيزات أو التكنولوجيات سواء كانت تتعلق بالعتاد أو البرمجيات التي صُممت وأتيح استعمالها لغرض محدد يتمثل في تفادي تكنولوجيات الحماية المطلوبة أو تجنبها ("تجهيزات التجنب")؛

ب) لا يمكن التغلب عليها أو تجنبها إلا بصعوبة باستعمال أدوات أو تجهيزات مهنية (باستثناء تجهيزات التجنب والأدوات أو المعدات المهنية التي لا تتاح إلا بمقتضى اتفاق عدم الإفصاح) مثل أجهزة التحليل المنطقية، وأنظمة فك تجميع الدارات المتكاملة، أو أجهزة التحويل في الدارات أو الأدوات الأخرى والتجهيزات والطرائق غير المدرجة في تعريف الأدوات التي تتاح على نطاق واسع والأدوات المتخصصة المذكورة في الفقرة أ) أعلاه.

7 قواعد التقيد

1.7 مقدمة

يجب أن يستوفي الجهاز عدداً معيناً من الشروط حتى يُقبل إلحاقه بشبكة مقدم الخدمة الفيديوية لاستقبال المحتوى المحمي.

2.7 عمليات الخرج

1.2.7 اعتبارات عامة

لا يُخرِّج المنتج المحتوى أو يرسل المحتوى الذي يُستقبل بواسطة الخدمة إلى أي خرج، ما لم تسمح بذلك هذه التوصية. وفي مفهوم هذه التوصية، ينبغي أن يشتمل الخرج، دون أن يقتصر، على جميع الإرسالات إلى أي جهاز داخلي للنسخ أو للتسجيل أو التخزين، ولكن يجب ألا يشتمل على الإرسالات الداخلية غير المستمرة أو الانتقالية التي تستجيب علاوة على ذلك إلى هذه القواعد المتعلقة بالتقيد والمتانة.

2.2.7 الخرج التماثلي معياري الوضوح

لا تخرج المنتجات ذات المخرج التماثلي معياري الوضوح إلا محتوى مستقبل بواسطة الخدمة ولا ترسل محتوى مستقبل بواسطة الخدمة، ما لم يكن هذا المحتوى محمياً حماية ملائمة وفقاً للمعايير الوطنية أو الإقليمية المناسبة التي تتعلق بالحماية من نسخ المحتوى التماثلي.

3.2.7 الخرج التماثلي عالي الوضوح

تكون المنتجات قادرة على أن تنحصر في صورة مقيدة، عندما تستوجب بتة إطلاق الصورة المقيدة (CIT) لمعلومات التحكم في النسخ (CCI)، استبانة محتوى عالي الوضوح يجب أن يخرج بواسطة توصيلة قادرة على إرسال محتوى في صيغة تماثلية عالية الوضوح. وتشتمل المنتجات على خرج أو عدة مخارج رقمية معتمدة. وتولد المنتجات وتبث إشارات CGMS-A فيما يتعلق بالخرج التماثلي عالي الوضوح؛ ولكن ليس من الضروري مراعاة مسبب CGMS-A ما لم يقض بذلك تشريع أو تنظيم ملائم.

4.2.7 عمليات الخرج الرقمية

لا تخرج المنتجات ذات الخرج الرقمي سوى المحتوى المستقبل بواسطة الخدمة، ولا ترسل سوى المحتوى المستقبل بواسطة الخدمة وفقاً لما تسمح به هذه التوصية. ويحتوي التذييل I على قائمة بالتكنولوجيات التي اختبرت مطابقتها مع هذه التوصية.

5.2.7 عدم التداخل مع العلامة المائية

لا تنتزع المنتجات والمكونات أو تعتم أو تسبب التداخل في العلامة المائية المتفق بشأنها في محتوى متحكم فيه أُزيل تجفيره.

3.7 نسخ وتسجيل وتخزين المحتوى المتحكم فيه

1.3.7 اعتبارات عامة

ينبغي للمنتجات، بما في ذلك، دون أي تقييد، المنتجات التي لها قدرة ملازمة أو متكاملة للنسخ أو التسجيل أو التخزين ألا تقوم بنسخ أو تسجيل أو تخزين المحتوى المتحكم فيه، ما لم تسمح بذلك هذه الفقرة.

2.3.7 مجرد دارئ للعرض

بإمكان المنتجات أن تُخزِّن المحتوى المتحكم فيه بصفة مؤقتة بغرض تمكين العرض المباشر فقط للمحتوى المتحكم فيه، شريطة:

أ) عدم استمرار هذا التخزين بعد عرض المحتوى؛

ب) عدم تخزين البيانات بطريقة تدعم نسخ هذه البيانات وتسجيلها وتخزينها لغايات أخرى.

3.3.7 التوقف عن النسخ

لا تنسخ المنتجات أو تسجل أو تخزن المحتوى المتحكم فيه المشار إليه في البتات EMI باعتباره قد نُسخ ولكن ينبغي عدم نسخه بعد الآن ("التوقف عن النسخ") باستثناء ما يسمح به في الفقرتين 2.3.7 و2.5.3.7.

4.3.7 عدم النسخ قط

ينبغي للمنتجات، بما في ذلك، دون أي تقييد، تجهيز يتمتع بقدرة تسجيل متكاملة، مثلما يعرف باسم "مسجل الفيديو الشخصي" عدم نسخ المحتوى المتحكم فيه المشار إليه في البتات EMI باعتباره لا ينسخ قط، باستثناء ما تسمح به الفقرة 2.3.7.

وبإمكان هذا الجهاز أن يخزن داخلياً هذا المحتوى، بما في ذلك بغرض التوقف المؤقت للبرنامج، إذا كان المحتوى المُخزَّن موصولاً بطريقة آمنة بالمنتج الذي يقوم بالتسجيل بحيث يصبح غير قابل للمحو وألا يتعرض بذاته لاحقاً إلى تسجيل مؤقت أو آخر في المنتج قبل أن يصبح غير قابل للاستعمال؛ شريطة أن يكون الجهاز مطابقاً لمتطلبات المتانة المحددة لتجنب التحايل على هذه القيود. وخلال التخزين الداخلي لهذا المحتوى، بما في ذلك لغايات تطبيق التوقف المؤقت كما تسمح به هذه الفقرة، ينبغي تجفير المحتوى وتخزينه على نحو يتيح أمناً لا يقل عن معيار التجفير المتطور (AES) القائم على 128 بتة.

وتُصمم المنتجات وتُصنع بحيث تكون قادرة على محو المحتوى المُخزن أو جعله غير قابل للاستعمال بعد فترة زمنية محددة، رتلاً تلو رتل، دقيقة تلو دقيقة، وميغابايت تلو ميغابايت.

5.3.7 نسخة من الجيل الأول

1.5.3.7 وظيفة النسخ

يجوز للمنتجات أن تعد نسخة من المحتوى المتحكم فيه المشار إليه في البتات EMI باعتباره يمكن نسخه على جيل واحد ("نسخة من الجيل الأول")، على غرار ما ورد في الفقرتين 2.3.7 أو 4.3.7 وشريطة أن تكون النسخة:

أ) مختلطة أو مشفرة أو موصلة بصفة أحادية بهذا الجهاز، في كل حالة باستعمال شكل حماية ضد النسخ الذي يُحدد بتعديل هذه الفقرة 5.3.7، عند الاقتضاء؛

ب) موسومة بشكل يفيد بالتوقف عن النسخ ("عدم النسخ قط") بطريقة تحدد بإدخال تعديل على الفقرة 5.3.7، عند الاقتضاء، على نحو يحول فعلاً دون إجراء نسخ جديدة بواسطة أجهزة قادرة على استقبال إرسال مثل هذه البيانات الموسومة من خلال نقاط الخروج المحددة في الفقرة 4.2.7. وفي غيبة إدخال أي تعديل على الفقرة 5.3.7، لا يمكن إجراء نسخة من هذا المحتوى المتحكم فيه ما لم تسمح به الفقرة 2.3.7 أو الفقرة 4.3.7، أو ما تنص عليه الفقرة 2.5.3.7.

2.5.3.7 وظيفة النقل

لا يجوز لمنتج يقوم بنسخ المحتوى المشار إليه في المعلومات CCI باعتباره "نسخة من الجيل الأول" وفقاً للفقرة 5.3.7 أن ينقل هذا المحتوى إلى وسيط تسجيل وحيد يمكن محوه أو إلى تجهيز تسجيل خارجي وحيد، ما لم:

أ) يشير تجهيز التسجيل الخارجي إلى أنه من المسموح به تأدية وظيفة النقل هذه وفقاً لمتطلبات هذه الفقرة، ونسخ هذا المحتوى المتحكم فيه وفقاً لمتطلبات الفقرة 5.3.7؛

ب) يوسم هذا المحتوى المتحكم فيه للإرسال بواسطة المنتج الأصلي باعتباره "نسخة من الجيل الأول"؛

ج) يخرج المحتوى المتحكم فيه صوب خرج محمي وفقاً للفقرات 2.2.7 أو 3.2.7 أو 4.2.7؛

هـ) قبل إتمام النقل، يكون تسجيل المنتج الأصلي غير قابل للاستعمال ويوسم المحتوى المتحكم فيه بواسطة "عدم النسخ قط"؛

و) التجهيز الذي يحول إليه وسيط التسجيل القابل للمحو غير قادر أو أصبح غير قادر على تخريج المحتوى المتحكم فيه، إلا من خلال مخارج تسمح بها قواعد التقيد هذه؛

ح) تخزن النسخة:

i) باستعمال بروتوكول تجفير معتمد بواسطة تعديل قواعد التقيد هذه، التي تربط بشكل استثنائي هذه النسخة بجهاز وحيد بحيث لا يمكن قراءته على جهاز آخر أو، إذا كانت مخزنة على وسيط قابل للمحو، بحيث لا يمكن إجراء نسخة قابلة للاستعمال؛

ii) خلاف ذلك باستعمال الطرائق الأخرى المذكورة كمراجع في الفقرة 1.5.3.7.

ويحد التنفيذ الحالي عمليات النقل في عملية نقل وحيدة. وتجري حالياً دراسة وسائل إضافية للتحكم في المحتوى ومن الممكن تطبيقها عندما يتم تحديد الجيل المقبل من أنظمة إدارة الحقوق الرقمية (DRM).

8 التحكم في التغير

ينبغي إعادة تقييم كل تعديل مادي أو جوهري في التكنولوجيا باستعمال المعايير والعمليات المحددة هنا. وتشمل التعديلات المادية أو الجوهرية، دون أن تقتصر على:

1) التقابل مع نقل وسائط متعددة جديدة؛

2) تغييرات في التشفير أو في معالجة المحتوى؛

3) تغييرات قد يكون لها أثر مادي وسلبي على تكامل التكنولوجيا أو أمنها؛

4) تغييرات في طريقة التجفير المستعملة (باستثناء حالة عدم تغير الخوارزمية وتوسيع طول المفتاح)؛

5) تغييرات في مجال تطبيق إعادة التوزيع؛

6) أي تغير أساسي في طبيعة التكنولوجيا.

الملحق A

معلومات التحكم في النسخ

تمرر معلومات التحكم في النسخ (CCI) انطلاقاً من مقدم الخدمة الفيديوية على قناة البيانات لإبلاغ وحدة فك التشفير بالمستوى المطلوب للحماية من النسخ. وتُرسل معلومات التحكم في النسخ (CCI) دون تشفير إلى وحدة فك التشفير. ولكن يحتفظ بكامل المعلومات عن طريق استيقان معلومات التحكم في النسخ باستعمال بروتوكول بسيط. وتتكرر هذه العملية بالنسبة إلى كل عنصر من عناصر تدفق الاتجاه الهابط انطلاقاً من وحدة فك التشفير.

وتحتوي البايتة الوحيدة لمجال معلومات التحكم في النسخ (CCI) على المعلومات التي تستعملها وحدة فك التشفير وعناصر تدفق الاتجاه الهابط للتحكم في نسخ المحتوى. وتتحكم البتتان EMI في النسخ على نقاط الخرج الرقمية لوحدة فك التشفير، وتتحكم بتتا نظام الحماية التماثلي (APS) في النسخ على نقاط الخرج التماثلية، وتعمل بتة تحكم واحدة في إطلاق الصورة المقيدة وتُحجز ثلاث بتات.

1.A تغيير القناة

عندما يحدث تغيرٌ في القناة، ينبغي لوحدة فك التشفير أن تعالج جميع المحتويات المحمية بواسطة التخليط كما لو كانت البتات EMI مضبوطة على "عدم النسخ قط"، ولكن لا ينبغي تطبيق الصورة المقيدة إلى حين استقبال الرسالة الجديدة لمعلومات التحكم في النسخ (CCI). وتبدأ وحدة فك التشفير على الفور في استعمال قيم معلومات التحكم في النسخ (CCI) عندما تُستقبل من مقدم الخدمة الفيديوية. وإذا لم تُستقبل رسالة جديدة خاصة بمعلومات التحكم في النسخ (CCI) في ظرف 10 ثوان، تطبق وحدة فك التشفير القيود على الصورة كما لو كانت بتة إطلاق الصورة المقيدة (CIT) مضبوطة على 1. ولا يتسبب تغيير القناة في تجديد المفتاح.

2.A تعريف معلومات التحكم في النسخ (CCI)

معلومات التحكم في النسخ (CCI) هي بايتة وحيدة، 8 بتات، تُنقل من وحدة فك التشفير إلى عناصر شبكة تدفق الاتجاه الهابط. وقد حُددت خمس بتات من بين 8 بتات. وحجزت البتات الثلاث الأخرى. وتضبط تحديد البتات المحجوزة على الصفر على النحو المبين في الجدول 1.A. ولا يستعمل عنصر تدفق الاتجاه الهابط قيم البتة المحجوزة التي يستقبلها من وحدة فك التشفير الفيديوية إلا لتنفيذ بروتوكول النفق المستيقن الموصوف أدناه. وينبغي لوحدة فك التشفير أن تتجاهل القيم التالية للبتة المحجوزة.

الجدول J.197/1.A – تخصيص بتات معلومات التحكم في النسخ

رقم بتات CCI	7	6	5	4	3	2	1	0
VSP يحدد عند	0	0	0	CIT	APS1	APS0	EMI1	EMI0
يفسر STB بكونه	rsvd	rsvd	rsvd	CIT	APS1	APS0	EMI1	EMI0

3.A EMI – بتات التحكم في النسخة الرقمية

البتتان الأقل دلالة في بايتة معلومات التحكم في النسخ هما البتتان EMI. وينبغي لهما التحكم في السماح بالنسخ فيما يتعلق بالنسخ الرقمية. وتتاح البتات EMI في كل المنافذ الرقمية لخرج وحدة فك التشفير للتحكم في عدد النسخ التي أُعدت انطلاقاً من هذا الخرج. وتُعرف البتات EMI في الجدول 2.A.

الجدول J.197/2.A – قيمة ومحتوى EMI

قيمة EMI	السماح بنسخة رقمية	نمط المحتوى
00	نسخ غير مقيد	ليست "قيمة عالية"
01	لا يسمح بأي نسخ قط	قيمة عالية
10	نسخ من الجيل الأول مسموح بها	قيمة عالية
11	نسخ محظور	قيمة عالية

4.A نظام الحماية التماثلي (APS)

البتتان 3 و2 لمعلومات التحكم في النسخ (CCI) هما على التوالي، كما هو مبين في الجدول 1.A، البتتان APS 1 و0. وينبغي لوحدة فك التشفير أن تستعمل البتات APS للتحكم في تشفير الحماية من النسخ عند الخرج التماثلي المركب على النحو الموصوف في الجدول 3.A.

الجدول J.197/3.A – تعريف قيم نظام الحماية التماثلي APS

APS	الوصف
00	تشفير الحماية ضد النسخ المخمد
01	معالجة AGC نشيطة، رشقة إشارات لونية مشكلة مخمد
10	معالجة AGC نشيطة، رشقة إشارات لونية مشكلة نشيطة على خطين
11	معالجة AGC نشيطة، رشقة إشارات لونية مشكلة نشيطة على 4 خطوط

5.A إطلاق الصورة المقيدة (CIT)

البتة 4 لمعلومات التحكم في النسخ (CCI) هي، كما يرد توضيحها في الجدول 4.A، إطلاق الصورة المقيدة (CIT). وينبغي للوحدة المطرافية للمشترك أن تستعمل بتة إطلاق الصورة المقيدة (CIT) للتحكم في الصورة المقيدة في الخرج التماثلي المركب عالي الوضوح.

الجدول J.197/4.A – قيم وتطبيق بتة إطلاق الصورة المقيدة (CIT)

قيمة البتة CIT	تطبيق الصورة المقيدة
0	لم تثبت صحة تقييد الصورة
1	التقييد المطلوب للصورة

6.A بروتوكول النفق المستيقن

تحسب وحدة فك التشفير القيمة CCI_auth باستعمال قيمة معلومات التحكم في النسخ (CCI) المستقبلة وتقارنها مع القيمة CCI_auth المستقبلة من مقدم الخدمة الفيديوية. ويولد الإخفاق في التعادل حالة خطأ وتضبط وحدة فك التشفير البتات EMI على 11 ثم تطبق قيد الصورة كما لو كانت القيمة مساوية للقيمة 1.

الملحق B

قائمة التحقق من المتانة

يجب على القائم بتنفيذ التكنولوجيا، قبل تسويق المنتج، إجراء اختبارات وتحاليل لضمان متانة التنفيذ. ويمكن استعمال قائمة التحقق من المتانة الواردة أدناه لمساعدة المنفذ على إجراء اختبارات تغطي بعض الجوانب الهامة للمتانة. ونظراً إلى أن قائمة التحقق من المتانة لا تشمل كل العناصر المطلوبة لتصنيع منتج متقيد، يُرجى بشدة من القائم بالتنفيذ أن يجري تقييماً شاملاً لإجراءات الاختبارات ومدى تقيد منتجاته على حد سواء.

أسئلة عامة تتعلق بالتنفيذ

1) هل صُمم المنتج وصُنع بحيث لا يحتوي على أية مفاتيح أو أزرار أو موصلات، أو أي مكافئ برمجي للعناصر سالفة الذكر، أو أسلاك محددة يمكن قطعها، يمكن بواسطتها إبطال تكنولوجيات حماية المحتوى أو أنظمة الحماية التماثلية أو قيود الخرج، أو حدود التسجيل أو التدابير الإلزامية الأخرى لقواعد التقيد، أو يمكن بواسطتها تعريض المحتوى المتحكم فيه إلى نسخ غير مسموح به؟

2) هل صُمم المنتج وصُنع بحيث لا يحتوي على أية قائمة خدمة أو أية وظيفة خدمة (مثل وظائف التحكم عن بعد، المفاتيح، الخانات التي يتعين تعليمها أو وسائل أخرى) بإمكانها اعتراض تدفق المحتوى المتحكم فيه أو تعريضه لنسخ غير مسموح به؟

3) هل صُمم المنتج وصنع بحيث لا يحتوي على أية قائمة خدمة أو أية وظيفة خدمة (مثل وظائف التحكم عن بعد، المفاتيح، الخانات التي يتعين تعليمها أو وسائل أخرى) بإمكانها تعطيل جميع أنظمة الحماية التماثلية أو قيود الخرج أو حدود التسجيل أو التدابير الإلزامية الأخرى لقواعد التقيد؟

4) هل يحتوي المنتج على قوائم خدمة أو وظائف خدمة أو مرافق خدمة بإمكانها تغيير المحتوى المتحكم فيه داخل الجهاز أو الكشف عنه؟
إذا كان الرد بالإيجاب، يُرجى وصف قوائم الخدمة أو وظائف الخدمة أو مرافق الخدمة هذه والإجراءات الجاري اتخاذها لضمان عدم استعمال أدوات الخدمة هذه في الكشف عن المحتوى المتحكم فيه أو إساءة توجيهه.

5) هل يحتوي المنتج على قوائم خدمة أو وظيفة خدمة أو مرافق خدمة بإمكانها تعطيل أي أنظمة للحماية التماثلية أو قيود الخرج أو حدود التسجيل أو الأحكام الأخرى لقواعد التقيد؟
إذا كان الرد بالإيجاب، يُرجى وصف قوائم الخدمة أو وظائف الخدمة أو مرافق الخدمة هذه والإجراءات الجاري اتخاذها لضمان عدم استعمال أدوات الخدمة هذه في إبطال خصائص تجفير المنتج (بما في ذلك الامتثال لقواعد التقيد).

6) هل يحتوي المنتج على موصلات يمكن للمستعمل النفاذ إليها (كما ورد تحديدها في الفقرة 2.6 من قواعد المتانة)؟
إذا كان الأمر كذلك، هل ينقل المحتوى المتحكم فيه على هذه الأداة الموصلة؟
إذا كان الأمر كذلك، عندئذ:
يرجى تحديد الأداة الموصلة ووصفها، وبيان ما إذا كان المحتوى المتحكم فيه مضغوطًا أم غير مضغوط. فإذا كانت هذه البيانات مضغوطة، ينبغي عندئذ إجراء شرح بالتفصيل عن الكيفية والوسائل التي سيُعاد بها تجفير البيانات على النحو المطلوب في الفقرة 2.6 من قواعد المتانة.

7) اشرح بالتفصيل كيف يحمي المنتج سرية جميع المفاتيح.

8) اشرح بالتفصيل كيف يحمي المنتج سرية خوارزميات التجفير السرية المستعملة في المنتج.

9) إذا كان المنتج ينقل محتوى متحكماً فيه من جزء إلى آخر من هذا المنتج، سواء بين النماذج البرمجية، أو بين الدارات المدمجة، أو خلاف ذلك، أو بين التركيبات التابعة لها، اشرح الكيفية التي صُممت بها أجزاء المنتج التي تؤدي الاستيقان وإزالة التجفير ومزيل الشفرة MPEG (أو أي جهاز مماثل)، والكيفية التي ترتبط بها وتتكامل معاً بحيث يكون المحتوى المتحكم فيه محمياً ضد عمليات الاستيلاء والنسخ وفقاً للفقرة 1.3.6 من قواعد المتانة.

10) هل طبقت وظائف الحماية في العتاد؟
إذا كان الرد بالإيجاب، يُرجى الرد على الأسئلة المتعلقة بالتنفيذ في العتاد.

11) هل طبقت وظائف حماية المحتوى في البرمجية؟
إذا كان الرد بالإيجاب، يُرجى الرد على الأسئلة المتعلقة بالتنفيذ البرمجي.

مسائل تتعلق بالتنفيذ البرمجي

12) في المنتج، يرجى وصف الطريقة التي تخزن بواسطتها كل المفاتيح بطريقة محمية.

13) باستعمال مرفق GREP أو ما يعادله، هل يصعب عليكم اكتشاف أي مفتاح في الصور الاثنينية للتجهيزات ذات الذاكرة المستمرة؟

14) في المنتج، يرجى وصف الطريقة المستعملة لإخفاء خوارزميات التجفير السرية والمفاتيح المطبقة في البرمجية.

15) يرجى وصف الطريقة التي أُنشأت بواسطتها قيم التجفير الوسيطة (أي القيم التي أنشأت خلال عملية الاستيقان بين الوحدات أو التجهيزات في المنتج) واحتُفظ بها بطريقة محمية في المنتج.

16) يرجى وصف الطريقة المستعملة لتفادي استعمال أدوات إزالة المشاكل وفض التجميع المتيسرة على نطاق واسع (مثل Softice) بحيث يمكن التقسيم إلى خطوات، أو إزالة المشاكل أو فض التجميع، أو بحث تطبيق وظائف حماية المحتوى المطبقة في البرمجية.

17) يرجى وصف الطريقة التي يتحقق بها المنتج ذاتياً من تكامل العناصر المكونة بحيث أن التعديلات تؤدي إلى إخفاق الترخيص أو إزالة التجفير على النحو المبين في الفقرة 2.3.6.ب من قواعد المتانة. يرجى وصف ماذا يحدث عند انتهاك التكامل.

18) للتأكد من إجراء التحكم الذاتي من التكامل، يُرجى إجراء الاختبار والتأكد من أن المنفذ لن يتوصل إلى التشغيل متى كان المحرر الاثنيني يستعمل لتغيير بايتة عشوائية للصورة القابلة للتنفيذ التي تحتوي على وظائف حماية المحتوى؛ ويرجى وصف الطريقة ونتائج هذا الاختبار.

مسائل تتعلق بالتنفيذ على العتاد

19) في المنتج، يرجى وصف الطريقة التي تخزن بواسطتها كل المفاتيح بطريقة محمية وكيفية المحافظة على سريتها.

20) باستعمال مرفق GREP أو ما يعادله، هل يصعب عليكم اكتشاف أي مفتاح في الصور الاثنينية للتجهيزات ذات الذاكرة المستمرة؟

21) في المنتج، يرجى وصف الكيفية التي طبقت بها خوارزميات التجفير السرية والمفاتيح السرية التي طبقت في الدارات المتكاملة أو في البرمجيات الثابتة بحيث لا يمكن قراءتها.

22) يرجى وصف الطريقة التي أُنشأت بواسطتها قيم التجفير الوسيطة (أي القيم التي أنشأت خلال عملية الاستيقان بين الوحدات أو التجهيزات في المنتج) واحتُفظ بها بطريقة محمية في المنتج.

23) يرجى وصف الوسائل المستعملة لتفادي محاولات استبدال أو إزالة أو تغيير عناصر أو نماذج العتاد المستعملة لتنفيذ وظائف حماية المحتوى؟

24) في المنتج، هل من شأن إزالة أو استبدال عناصر أو نماذج العتاد تعريض عناصر خدمة حماية المحتوى للمنتج (بما في ذلك قواعد التقيد وقواعد المتانة) المنتج للضرر إلى حد يصبح المنتج عاجزاً عن استقبال أو وإزالة تجفير أو فك شفرة المحتوى المتحكم فيه؟

التذييل I

عمليات الخرج الرقمية

سيكون من الضروري التحقق من تقيد الخرج الرقمي مع المتطلبات المنصوص عليها في هذه التوصية. وقد اختبر توافق قائمة عمليات الخرج الرقمية التالية مع هذه التوصية، وهي ترد هنا للعلم بها. ومن المتوقع أن تتوافق في المستقبل عمليات خرج إضافية مع متطلبات هذه التوصية.

1.I اختبرت شركة مختبرات التلفزيون الكبلي *(Cable Television Laboratories)* الخرج التالي ولاحظت أنه يتوافق مع هذه التوصية:

- **1394 مع DTCP**: يمكن للمنتج أن يستخرج محتوى متحكماً فيه وأن ينقل المحتوى المتحكم فيه إلى خرج، في صيغة رقمية على السطوح البينية IEEE 1394، حيث يكون هذا الخرج محمياً بواسطة DTCP. ويجب أن يدعم المنتج DTCP "استيقاناً كاملا"؛ كما يمكن له أن يدعم كذلك DTCP "استيقان مقيد". وإذا كان ذلك مطلوباً بموجب الترخيص المطبق على DTCP، يجب استخرج المحتوى الذي لا يعد محتوى متحكماً فيه على الخرج IEEE 1394 دون حماية DTCP.

2.I اختبرت شركة مختبرات التلفزيون الكبلي *(Cable Television Laboratories)* ولاحظت أنه يتوافق مع هذه التوصية:

- **خرج DVI/HDMI مع HDCP**: يمكن للمنتج أن يستخرج محتوى مستقبل بواسطة الخدمة وأن ينقل المحتوى المستقبل بواسطة الخدمة إلى خرج معين، في صيغة رقمية على السطوح البينية DVI بما في ذلك السطوح البينية HDMI، وحيث يكون للخرج حماية HDCP نشيطة بصفة دائمة. ويجب أن ينقل المنتج كل الرسائل HDCP SRM المستقبلة بطريقة مشروعة إلى الوظيفة HDCP.

التذييل II

معايير التقييم

ينبغي لمعايير التقييم، تبعاً للخرج المحدد أو للتكنولوجيا المستعملة، أن تحتوي على ما يلي:

1.II نقل الإشارات الفيديوية

هل حددت طرائق تحويل معلومات التحكم في النسخ (CCI) وتوزيعها من وحدة فك التشفير إلى بيئة أو ملامح الجهاز المقترح؟

i) *الخرج الرقمي المضغوط*

- هل يستعمل نظام الانضغاط الرقمي الأصلي على السطح البيني، أو هل أعيد ضغط الإشارة؟
- إذا أعيد ضغط الإشارة، ما هو النظام والملامح والاستبانة ومعدلات البيانات المطلوبة؟
- إذا احتفظ بالانضغاط الأصلي، هل أرسل تعدد إرسال النقل الكامل إلى السطح البيني، أو هل يقتصر السطح البيني على تدفق برنامج وحيد يرسل بعد إزالة تعدد الإرسال؟
- إذا كان الخرج ينقل تدفق النقل الكامل، كيف يمكن نقل معلومات النظام (أي البيانات الخارجة عن النطاق)؟
- ما هي الطرائق المستعملة لضمان عدم انقطاع تدفق البرامج على هذا السطح البيني، بصرف النظر عن الحركة الأخرى التي يمكن أن توجد على هذا السطح البيني (QOS)؟
- ما هو الحد الأدنى لصبيب البيانات الذي يمكن ضمانه على السطح البيني؟
- ما هي الطرائق المستعملة لتمكين التوزيع أو فك الشفرة أو عرض البيانات التماثلية أو الرقمية ذات الحواشي المشفرة، السويات الاستشارية للمحتوى والرسائل في نطاق نظام الإنذار بالطوارئ؟
- كيف يمكن الاحتفاظ بخدمات البرمجة التماثلية بشفافية على هذا السطح البيني؟

ii) *الخرج الرقمي غير المضغوط:*

- ما هو الحد الأدنى لصبيب البيانات الذي يمكن ضمانه على السطح البيني؟
- كيف يمكن الحفاظ على شفافية خدمات البرمجة التماثلية على هذا السطح البيني؟
- ما هي الطرائق المستعملة لتمكين التوزيع أو فك الشفرة أو عرض المعطيات التماثلية أو الرقمية ذات الحواشي المشفرة، السويات الاستشارية للمحتوى والرسائل في نطاق نظام الإنذار بالطوارئ؟

2.II السطوح البينية للأمن

- كيف يستعمل الأمن خلال نقل الإشارات الفيديوية وكيف يرتبط هذا النقل بمواصفات حماية المحتوى وطرائق الاستيقان وحماية مواصفات حماية المحتوى؟
- ما هي الطرائق المستعملة في توليد المفاتيح وحمايتها وتبادلها؟
- هل هناك مناطق واضحة يكون فيها المحتوى غير مشفر؟

3.II نقاط الهجمات ومواطن ضعف النظام

- هل يمكن تجنب التكنولوجيا في مكان ما؟

- أين توجد الحواجز الأكثر ضعفاً التي يمكن مهاجمتها؟
- أين يهاجم القراصنة وما هي الموارد المطلوبة؟
- ما هي مواطن الضعف أو التهديد المحتملة وما هو التعويض الأمني في مقابل التكاليف المطبقة؟

4.II فعالية التكنولوجيا المقترحة

- هل تحمي التكنولوجيا المقترحة بطريقة ملائمة المحتوى عند مروره من الخرج الرقمي أو عند تسجيله أو تخزينه الآمن لمشاهدته لاحقاً؟
- ما هو مجال تطبيق إعادة توزيع المحتوى؟ وهل تحمي تكنولوجيا الخرج الرقمي أو إدارة الحقوق الرقمية بفعالية المحتوى من إعادة التوزيع غير المسموح بها، من خلال التحكم في تحديد الموقع أو القيود الأخرى ذات الطابع الجغرافي أو القيود الخاصة بالمستعمل؟

5.II معالجة الأمن

- هل تعتبر المفاتيح والأسرار محمية من القراءة والكتابة خلال حسابات التجفير؟
- هل تعتبر معلومات التحكم في النسخ، والقيود على الصورة وأوامر التحكم الأخرى محمية طوال عملية تصميم النظام؟

6.II إلغاء وتجديد المفاتيح

- هل يوفر المنتج حلاً لإلغاء مفاتيح النظام؟
- هل يوفر المنتج حلاً لإعادة تجديد مفاتيح النظام؟
- ما هي المعايير والعمليات المستعملة للإلغاء وإعادة التجديد؟ من هم المشاركون في هذه العملية؟
- ما هو الحجم الأدنى والحجم الأقصى لرسالة إعادة تجديد النظام (SRM)، وما هو النسق الذي توزع به هذه الرسالة؟
- كيف توزع عادة رسالة إعادة تجديد النظام (SRM)؟ وما هي الآثار التشغيلية وآثار البنية التحتية لحل الإلغاء وإعادة التجديد في شبكة مقدم الخدمة الفيديوية (بما في ذلك الأجهزة الرأسمالية أو عمليات تحسين الشبكة التي قد تكون مطلوبة)؟ وماذا يتعين على مقدم الخدمة الفيديوية عمله لاعتماد الحلول المقترحة بشأن الإلغاء وإعادة التجديد؟

7.II خوارزميات جديدة

- ما هي القوة النسبية للخوارزمية؟
- ما هي القوة النسبية للاستيقان مقارنةً مع التكنولوجيات الأخرى؟

8.II الحفاظ على تكامل الخدمة

- هل يتداخل الخرج/التكنولوجيا المقترحة مع جهاز وحدة فك التشفير الذي يستوفي التزاماته الأخرى بشأن الترخيص أو الاختبار؟ هل يعتبر تبديل المصدر التماثلي أو النقل عالي الوضوح ضرورياً للخرج الرقمي المقترح؟
- هل يوفر الخرج وسيلة لحفظ تطبيقات الملاحة وخدمات مقدم الخدمة؟
- هل يتداخل الخرج/التكنولوجيا المقترحة مع التجهيزات والسطوح البينية الأخرى المتاحة في الأسواق؟

- هل يثير الخرج/التكنولوجيا المقترحة مشاكل تتعلق بالتشغيل البيني مع التجهيزات والسطوح البينية الأخرى في العمليات التجارية؟
- هل يعتبر السطح البيني المقترح قابلاً للتشغيل البيني مع منتجات المصنّعين الآخرين، أم هل يمثل حلاً يخضع لحقوق الملكية الفكرية أو حقوق أخرى حصرية؟
- هل يُحدد التشغيل البيني من خلال معايير صناعية (ما هي هذه المعايير؟) أو بواسطة ترخيص، أو بكليهما؟
- هل تتطلب التكنولوجيا إجراء اختبارات توافق لضمان التشغيل البيني؟

9.II شروط منح الترخيص

- ينبغي لشروط منح الترخيص أن تتقيد بممارسات الاتحاد الدولي للاتصالات ومع المتطلبات الوطنية.

10.II التأثير الإجمالي في شبكة توزيع الفيديوي

- ما هي الآثار التشغيلية والآثار المتعلقة بالبنية التحتية للتكنولوجيا المقترحة على شبكة التوزيع الفيديوي (بما في ذلك الأجهزة الرأسمالية أو عمليات تحسين الشبكة التي قد تكون مطلوبة)؟
- ماذا يجب على مقدم الخدمة الفيديوية عمله لاعتماد حل التكنولوجيا المقترحة؟

التذييل III

استعراض عناصر التكنولوجيا المقدمة

تشتمل التكنولوجيات التي تتناولها عملية التقييم هذه الموصى بها على السطوح البينية الرقمية المحمية وتسجيل المحتوى وتخزينه بشكل آمن، ومشاهدة المحتوى وإدارة الحقوق الرقمية. وقد تختلف إجراءات الأمن المحددة التي تستعملها هذه التكنولوجيات. وعلاوة على ذلك، قد تستعمل تكنولوجيات الخرج المختلفة آليات وبروتوكولات نقل تفرض بعض الحدود أو القيود على صعيد التنفيذ. ويحدد هذا التذييل العديد من العناصر الأساسية التي ينبغي أن تكون قاسماً مشتركاً بين كل التكنولوجيات المتوقع استعمالها والتي تعتبر قيد الدراسة، غير أن هذا التذييل لا يعتبر قائمة شاملة تستبعد أنماطاً أخرى من المعلومات التي يمكن أن تكون ضرورية لإجراء تقييم شامل لإحدى التكنولوجيات المحددة. ويجب للعطاءات أن تتفادى أي إغفال أو تقديم بيانات خاطئة تتعلق بمواصفات المواد أو الوقائع أو غيرها من التفاصيل اللازمة لإجراء تحليل متعمق ودقيق للتكنولوجيا.

ويمكن للتكنولوجيات قيد الاستعراض أن تحتوي على عناصر مختلطة ترتبط بالسطوح البينية الرقمية المحمية وبتسجيل المحتوى وتخزينه بشكل آمن، وبتكنولوجيات إدارة الحقوق الرقمية. وتوضح الفقرات التالية العناصر الموصى بها التي ينبغي تقديمها لإجراء تحليل متعمق للتكنولوجيات التي يتوقع استعمالها.

1.III شروط منح الترخيص

ينبغي أن تتقيد شروط منح الترخيص بممارسات الاتحاد الدولي للاتصالات وبالمتطلبات الوطنية.

ملاحظة بخصوص قواعد المتانة والتقيد – ينبغي لتجهيزات تدفق الاتجاه الهابط لوحدة فك التشفير التي تحتوي على أية تكنولوجيا خرج رقمي أو إدارة الحقوق الرقمية أو حماية المحتوى أن تمتثل أيضاً مع قواعد المتانة والتقيد المنصوص عليها في هذه التوصية بشأن وحدة فك التشفير. وتتحكم قواعد المتانة والتقيد المنصوص عليها بشأن وحدة فك التشفير في إجمالي النظام البيئي لتدفق الاتجاه الهابط. وكنتيجة لذلك، يجب ألا تتناقض قواعد المتانة والتقيد التي تشترط في أي ترخيص لتكنولوجيا المُصنّع مع قواعد المتانة والتقيد المنصوص عليها في هذه التوصية.

2.III نظرة إجمالية للأمن

ينبغي أن تشتمل مواصفة وتوثيق الأمن على مقدمة ونظرة إجمالية للأمن تحتوي على:

1) نظرة إجمالية لمعمارية الأمن ولمكوناتها (مثل مخدم الترزيم، مخدم الترخيص، الزبون، الخ)، ولوظائفها والسطوح البينية الرئيسية، ومتطلبات التوصيل للخرج والأمن.

2) مخطط تفصيلي لمعمارية الأمن يحدد المكونات والسطوح البينية الرئيسية اللازمة لتطبيق الحل من طرف إلى طرف، بما في ذلك المستقبل وعناصر الوسائط المتعددة الأخرى (حواسيب شخصية، التخزين، العرض، الخ)

3) ينبغي لهذه النظرة الإجمالية أن تحدد أيضاً بوضوح خيارات نقل الإشارات الفيديوية في حالة وجود بدائل تتعلق بالتطبيق، مثل خوارزميات تجفير نقل الإشارات الفيديوية (AES، 3-DES، إلخ) وخوارزميات تبادل المفاتيح (ديفي–هيلمان، RSA، الخ).

4) وصف تفصيلي لتقابل قواعد أو تراخيص حماية محتوى وحدة فك التشفير مع التكنولوجيا المقترحة لحماية المحتوى التي ينبغي إدخالها في تجهيزات "تدفق الاتجاه الهابط"، وذلك بتناول مسألة المحافظة الإجمالية على الأمن وحماية المحتوى في كل النظام البيئي للتوزيع.

3.III نقل الإشارات الفيديوية

ينبغي لمواصفة الأمن أن تشمل التفاصيل المتعلقة بطريقة نقل الإشارات الفيديوية وخصوصيات الطريقة التي يتم بها تحويل معلومات التحكم في النسخ (CCI) التي تقدمها وحدة فك التشفير في البيئة أو المواصفة المقترحة. وينبغي للمواصفة أن تُفصل

أيضاً الطريقة التي ترتبط بها الإشارات الفيديوية مع أي من مواصفات حماية المحتوى وطرائق الاستيقان وحماية مواصفات حماية المحتوى.

وعلاوة على ذلك، يجب توفير المواصفات أو الأوصاف التقنية الأخرى لكي يشرح بالتفصيل كيف يمكن للخرج الرقمي المقترح أن يدعم بروتوكولاً أو عدة بروتوكولات لتوزيع كل الخدمات الصوتية والفيديوية التي ترتبط بوحدة فك التشفير دون إيقاف أو معاوقة أو إضعاف تقديم هذه الخدمات حتى جهاز العرض النهائي. وتشمل هذه الخدمات أيضاً، دون أن تقتصر على التوزيع وإزالة التشفير وعرض البيانات التماثلية أو الرقمية ذات الحواشي المشفرة، والمستويات الاستشارية للمحتوى ورسائل نظام الإنذار بالطوارئ.

وينبغي إجراء تحليل تكنولوجي لكل آلية ولكل بروتوكول للنقل الذي تتضمنه تكنولوجيا حماية المحتوى. وينبغي إجراء هذه الاستعراضات على أساس نقل تلو نقلٍ، أو وسيط متعدد تلو وسيط متعدد. وإذا استوفت إحدى التكنولوجيات بنجاح المعايير المحددة هنا، فلا ينبغي اعتبار تلكً التكنولوجيا بوصفها تتمتع "بموافقة عامة" بالنسبة إلى أي نقل أو إلى بروتوكول.

4.III ملامح حماية المحتوى

ينبغي لمواصفة الأمن أن تشمل التفاصيل المتعلقة بالنسق واستعمال جميع ملامح حماية المحتوى الموقعة رقمياً المستعملة في النظام. وينبغي لمواصفة الأمن أن تحدد أيضاً البنية والخيارات المستعملة في هذا النظام وكل وظائف المراسلة والتشوير التي يتطلبها التطبيق.

5.III خوارزميات تبادل المفاتيح

ينبغي لمواصفة الأمن أن تشمل التفاصيل المتعلقة باستيقان تجهيزات الاستقبال، وتجهيزات التخزين وكل التجهيزات الموصلة بها. كما ينبغي لمواصفة الأمن أن تشمل طرائق استيقان مخدم الترخيص، ومخدم الترزيم والزبون. وينبغي لجميع مفاتيح دورة الاستعمال المتبادلة وبروتوكولات التجفير المستعملة أن تحدد تحديداً جيداً لإجراء استعراض كامل. ويمكن كذلك استخدام بدائل عدم التجفير، ولكن ينبغي شرحها بالكامل.

6.III السطوح البينية للأمن

ينبغي أن تحتوي المواصفة على التفاصيل التي تحدد بالكامل السطوح البينية لأمن إجمالي النظام وعلى إنشاء وحماية المفاتيح التناظرية واللاتناظرية. وثمة حاجة لوضع تعاريف مفصلة لمكونات الأمن المطبقة في العتاد والبرمجية بحيث يمكن تحليل السطوح البينية للأمن.

7.III معالجة الأمن

ينبغي أن تشمل المواصفة التفاصيل التي تبين كيفية حماية المفاتيح والأسرار من القراءة والكتابة في أثناء الحسابات التجفيرية وكيف يمكن حماية معلومات CCI والقيود على الصورة والمعلومات الأخرى في النظام.

8.III إدارة الشهادات

ينبغي أن تشمل المواصفة تفاصيل تحدد بالكامل استعمال الشهادات، وطرائق حماية المفاتيح الخاصة، وطرائق الإلغاء والطريقة التي ترتبط بها الشهادات بالمحتوى وبمخدمات الترزيم/الترخيص. وينبغي أيضاً إدراج تفاصيل تتعلق بالتركيب والتوقيع والتسلسل حتى الجذر، بالإضافة إلى البنية الإجمالية وإثبات صحة الأمن والحماية من استنساخ الشهادات.

9.III الإلغاء/إعادة تجديد المفاتيح

ينبغي أن تشمل المواصفة الطريقة التي يتحقق بها إلغاء مفاتيح النظام وإعادة تجديدها.

10.III نقاط الهجمات ومواطن الضعف المحتملة

ينبغي أن تحتوي المواصفة على استعراضات أو تحليلات خاصة بالتهديد التي قد تكون متاحة لاستعراض مواطن الضعف والتهديدات المحتملة والتبادل مقابل التكاليف المطبقة. وينبغي كذلك إعداد استعراضات أمنية مستقلة. عند الاقتضاء، يمكن تنفيذ قيود عدم الإفصاح لتغطية هذا الاستعراض.

11.III الاستعمال التجاري

ينبغي أن تتضمن العروض جميع الاستعمالات التجارية المعروفة للخرج أو التكنولوجيا المقترحة وعلى أي تأثير من مصروف في أداء التجهيزات وفي مسائل التشغيل البيني. وينبغي لمقدم العرض أن يقدم قائمة بالمعتمدين (المنفذين) والمؤدين (الملاك القائمون على تطوير المحتوى، الخ) وتحديد كل العلاقات التجارية بين القائم بعرض التكنولوجيا وملاك المحتوى.

12.III معلومات الاتصال

ينبغي أن يحتوي العرض على الأسماء وعلى معلومات الاتصال بأخصائي الأمن وبالأشخاص الآخرين الذين يمكن الاتصال بهم فيما يتعلق بمسائل العرض.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	**الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية 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 والأمن
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2006