

J.1011

(2016/09)

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة J: الشبكات الكبلية وإرسال إشارات تلفزيونية
وبرامج صوتية وإشارات أخرى متعددة الوسائط
النفاز المشروط والحماية - الحلول المدمجة القابلة للمبادلة
للنفاز المشروط وإدارة الحقوق الرقمية

السطح البيني المشترك المدمج من أجل الحلول
القابلة للمبادلة للنفاز المشروط/إدارة الحقوق
الرقمية؛ المعمارية والتعاريف ولمحة عامة

التوصية ITU-T J.1011

السطح البيني المشترك المدمج من أجل الحلول القابلة للمبادلة لتنفيذ المشروط/إدارة الحقوق الرقمية؛ المعمارية والتعاريف ولمحة عامة

ملخص

تحدد التوصية ITU-T J.1011 معمارية متعلقة بالحلول المدمجة القابلة للمبادلة لتنفيذ المشروط/إدارة الحقوق الرقمية (CA/DRM)، لتمكين معدات منشآت العملاء (CPE) القادرة على استقبال المحتوى الإذاعي وعريض النطاق، من تنزيل عملاء CA/DRM في بيئة موثوقة. ومن خلال استعمال خدمة التنفيذ المشروط المتعدد/إدارة الحقوق الرقمية القابلة للتنزيل، يمكن للمستهلكين المخولين استعمال المحتوى الإذاعي وعريض النطاق الذي تتحكم فيه إدارة الحقوق الرقمية (DRM) و/أو أنظمة التنفيذ المشروط (CA)، حتى وإن كانت معدات منشآت العملاء لا يوجد لديها العميل CA/DRM المطلوب المتعلق بالمحتوى والمتاح عن طريق تنزيله من مصدر موثوق في مختلف أنواع معدات منشآت العملاء بما في ذلك أجهزة فك التشفير (STB) و/أو الأجهزة التلفزيونية الذكية و/أو الحواسيب الشخصية و/أو الهواتف الذكية والحواسيب اللوحية الذكية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T J.1011	2016-09-02	9	11.1002/1000/12773

مصطلحات أساسية

التنفيذ المشروط/ إدارة الحقوق الرقمية، السطح البيني المشترك المدمج القابل للمبادلة، البيع بالتجزئة لمعدات منشآت العملاء

* للنفذ إلى التوصية، يرجى 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 والتعريف، 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 الكهروتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها. والتقييد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيئي والتطبيق مثلاً). ويعتبر التقييد بهذه التوصية حاصلاً عندما يتم التقييد 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 التقييد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يستعري 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
1	 المراجع	2
1	 التعاريف	3
1	 1.3 المصطلحات المعرّفة في وثائق أخرى	
1	 2.3 مصطلحات معرّفة في هذه التوصية	
2	 الاختصارات والأسماء المختصرة	4
3	 اصطلاحات	5
4	 معمارية من أجل حلول CA/DRM مدمجة وقابلة للتبادل	6
4	 1.6 ملاحظات عامة	
6	 2.6 المفهوم التقني للنظام ECI	
12	 7 البيئة الموثوقة	
13	 1.7 تدفقات العمل التشغيلية اللازمة	
15	 التذييل I - تنفيذ نظام ثقة مطابق للسطح البيئي ECI	
17	 بييلوغرافيا	

حماية الخدمة والمحتوى المتحققة بالنفاذ المشروط (CA) وإدارة الحقوق الرقمية (DRM) ضرورية في مجال الإذاعة الرقمية والنطاق العريض الذي يتسم بالتطور السريع، بما في ذلك المحتوى والخدمات والشبكات ومعدات منشآت العمل (CPE)، وذلك لحماية نماذج الأعمال للملكية المحتوى ومشغلي الشبكات ومشغلي التلفزيون غير المجاني (PayTV). ففي حين يركز النفاذ المشروط من المنظور المفاهيمي على آليات النفاذ إلى محتوى محمي موزع بواسطة مورد خدمة عبر شبكة ما، فإن إدارة الحقوق الرقمية توضح في الأساس نوع ومدى حقوق الاستعمال، طبقاً لتعاقد المشترك.

وقد أنشأ مشغلو التلفزيون (PayTV) منصات التلفزيون الرقمي التي تطبق معايير من أجل وظائف أساسية، يتم توسيع نطاقها بعناصر قائمة على الملكية. وتستعمل معظم أنظمة النفاذ CA والإدارة DRM من أجل الإذاعة الرقمية التقليدية وتلفزيون بروتوكول الإنترنت (IPTV) والخدمات المتاحة بحرية على الإنترنت (OTT) التي تلتقط معدات منشآت العمل وربطها بعناصر قائمة على الملكية خاصة بالأمن. ونتيجة لذلك، فإن معدات منشآت العمل المشكّلة لكي تستعمل في الشبكة أو المنصة A، لا يمكن استعمالها في الشبكة أو المنصة B، أو العكس. وبالتالي، فإن سوق الإلكترونيات الاستهلاكية بالنسبة للتلفزيون الرقمي لا يزال منقسماً، حيث تختلف المواصفات، ليس فقط من بلدٍ لآخر، ولكن من منصة إلى أخرى أيضاً. والوحدات النمطية CA/DRM الملحقة لا توفر إلاّ جزءاً من الحل: فالوحدات النمطية، ثانياً، مملوكة للنظام CA/DRM، كما أنها ليست رخيصة، وتستعمل في الأساس من أجل التلفزيون الكبلي أو الساتلي ولا يمكن استعمالها في الأنواع الحديثة من المعدات مثل الأجهزة اللوحية نظراً لعدم وجود سطح بيني مادي مناسب.

والحلول المنفذة حالياً، سواء كانت عتاداً مدمجاً أو ملحقة، تؤدي إلى آثار "الاحتكار". ويقيّد هذا الأمر بشكل كبير حرية الكثير من الأطراف الفاعلة في أسواق محتوى الوسائط المتعددة الرقمي. ونتيجةً للتقدم التكنولوجي، فقد أصبحت حلول CA/DRM المبتكرة القائمة على البرمجيات مجدية. وتعظيم هذه الحلول لقابلية التشغيل البيئي مع الحفاظ في الوقت نفسه على مستوى مرتفع من الأمن، يتوقع أن تلبّي الطلب في السوق مستقبلاً، بما يوفر مجالات جديدة للأعمال ويوسع من اختيارات المستهلك.

ومن مصلحة المستهلك أن يكون قادراً على مواصلة استعمال أجهزة منشآت العمل التي اشتراها، بعد الانتقال أو تغيير مورد الخدمة أو حتى عند استعماله أجهزة لخدمات خاصة ببوابات فيديو تجارية مختلفة، على سبيل المثال. ولا يمكن تحقيق ذلك إلا بقابلية التشغيل البيئي لمعدات منشآت العمل فيما يتعلق بالنفاذ CA والإدارة DRM، استناداً إلى معمارية أمنية مناسبة. ولن يتسنى منع زيادة تقسيم السوق بالنسبة لمعدات منشآت العمل وتشجيع المنافسة إلا بضمان قابلية تبادل أنظمة النفاذ CA والإدارة DRM بصورة تتسم بالسهولة بالنسبة للمستهلك والحساسية بالنسبة للسياق.

السطح البيني المشترك المدمج من أجل الحلول القابلة للمبادلة للنفاد المشروط/إدارة الحقوق الرقمية؛ المعمارية والتعاريف ولمحة عامة

1 مجال التطبيق

تهدف هذه التوصية إلى توصيف كيانات وظيفية لمعمارية من أجل سطح مشترك مدمج قابل للتبادل من أجل تحميل أي نظام CA/DRM ضروري لمعدات منشآت العميل. وتجري عملية التحميل في إطار بيئة موثوقة وتمكن من استهلاك محتوى محمي مزود عبر توصيلات إذاعية و/أو عريضة النطاق بأنواع مختلفة من المعدات الانتهازية طبقاً لحقوق المحتوى المكتسبة للمستخدمين النهائيين. وهذه التوصية واحدة من سلسلة توصيات توصف كامل النظام الإيكولوجي للسطح البيني المشترك المدمج (ECI).

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 الطباعات 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 الواردة أدناه. وتنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى أي وثيقة في هذه التوصية لا يضيفي على الوثيقة، بحد ذاتها، صفة توصية.

- [ETSI GS ECI 001-1] ETSI GS ECI 001-1 (2014), *Embedded Common Interface for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview.*
- [ETSI GS ECI 001-2] ETSI GS ECI 001-2 (2014), *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements.*

3 التعاريف

1.3 المصطلحات المعروفة في وثائق أخرى

لا يوجد.

2.3 مصطلحات معروفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الأمن المتقدم (advanced security): وظيفة لمعدّة من معدّات منشآت العميل مطابقةً للسطح البيني ECI، توفر وظائف معززة للأمن (العتاد والبرمجيات) لوسيط السطح البيني ECI. يلاحظ أن التفاصيل ترد في المعيار [b-ETSI GS ECI 001-5].

2.2.3 السطح البيني المشترك المدمج (ECI (embedded CI): المعمارية والنظام الموصفان في المعيار "السطح البيني المشترك المدمج" لفريق المواصفات الصناعية (ISG) التابع للمعهد الأوروبي لمعايير الاتصالات (ETSI)، واللذان يسمحان بتطوير وتنفيذ وسطاء للسطح البيني ECI قابلين للتبادل وقائمين على البرمجيات في معدّات منشآت العميل، وبالتالي توفير قابلية التشغيل البيني لهذه المعدّات بالنسبة للسطح البيني ECI.

3.2.3 وسيط السطح البيئي ECI (ECI Client (embedded CI client)): تنفيذ وسيط CA/DRM يمثل لمواصفات السطح البيئي ECI. ويلاحظ أن الوحدة النمطية البرمجية في معدّة منشآت العميل هي المسؤولة عن توفير جميع وسائل تلقي استحقاقات وحقوق المستهلك، بصورة محمية والتحكم في تنفيذها، فيما يتعلق بمحتوى موزع بواسطة موزع محتوى أو مشغل. كما تتلقى هذه الوحدة الشروط التي يمكن بموجبها استعمال مستهلك لحق أو استحقاق، والمفاتيح اللازمة لتجفير الرسائل والمحتويات المختلفة.

4.2.3 وحدة تحميل وسيط السطح البيئي ECI (ECI client loader): وحدة نمطية برمجية تعد جزءاً من مضيف السطح البيئي ECI، تسمح بتحميل برمجية وسيط السطح البيئي الجديدة والتحقق منها وتثبيتها في حاوية من حاويات السطح البيئي ECI لمضيف السطح البيئي ECI.

5.2.3 حاوية السطح البيئي ECI (ECI container (embedded CI container)): مفهوم مجرد يوفر بيئة منعزلة تضم آلة افتراضية ووسيط وحيد للسطح البيئي ECI.

6.2.3 مضيف السطح البيئي ECI (ECI host): نظام من عتاد وبرمجيات لمعدّة من معدّات منشآت العميل، يغطي الوظائف المتعلقة بالسطح البيئي ECI ولديه سطوح بيئية مع وسيط السطح البيئي ECI. ويلاحظ أن هذا المضيف هو جزء من البرمجيات الثابتة لمعدّات منشآت العميل، وهو المسؤول عن ضمان عزل كل حاوية من حاويات السطح البيئي ECI وتوفير التحميل المستيقن منه لوسطاء السطح البيئي ECI.

7.2.3 وحدة تحميل مضيف السطح البيئي ECI (ECI host loader): وحدة نمطية برمجية تسمح بتحميل برمجية مضيف السطح البيئي ECI (الجديدة) والتحقق منها وتثبيتها في معدّة من معدّات منشآت العميل. ويلاحظ أن هذا المصطلح يستعمل في تشكيلة التحميل متعدد المراحل للإشارة إلى جميع وظائف التحميل الحساسة من حيث الأمن المتضمنة في عملية تحميل مضيف السطح البيئي ECI.

8.2.3 سلطة الاستوثاق (TA) (trust authority): محطة تحكم جميع القواعد واللوائح التي تطبق لتنفيذ السطح البيئي ECI. ويلاحظ أن سلطة الاستوثاق كياناً قانونياً كي تتمكن من تحقيق الشكاوى القانونية. ويتعين أن تكون سلطة الاستوثاق محايدة بالنسبة لجميع الأطراف الفاعلة في النظام CA/DRM الإيكولوجي القابل للتحميل.

9.2.3 الطرف الثالث الموثوق (TTP) (trusted third party): مورد خدمة تقنية يصدر الشهادات والمفاتيح اللازمة لامتثال المصنعين للمكونات ذات الصلة من أي نظام ECI قيد المراقبة من قبل سلطة الاستوثاق (TA).

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

API	السطح البيئي لبرمجة التطبيقات (Application Programming Interface)
CA	النفذ المشروط (Conditional Access)
CENC	تجفير مشترك (Common Encryption)
CI	سطح بيئي مشترك (Common Interface)
CPE	معدّات منشآت العميل (Customer Premises Equipment)
DRM	إدارة الحقوق الرقمية (Digital Rights Management)
DVB	إذاعة فيديو رقمية (Digital Video Broadcasting)
ECI	سطح بيئي مشترك مدمج (Embedded Common Interface)

HD	عالي الاستبانة (High Definition)
HTTP	بروتوكول نقل النصوص المترابطة (Hypertext Transfer Protocol)
iDTV	تلفزيون رقمي مدمج (integrated Digital TV)
IP	بروتوكول الإنترنت (Internet Protocol)
IPTV	خدمات التلفزيون الموصل عبر بروتوكول الإنترنت (Internet Protocol Television)
LA	اتفاق ترخيص (License Agreement)
MPEG	فريق خبراء الصور المتحركة (Motion Picture Experts Group)
OS	نظام تشغيل (Operating System)
OSD	عرض على الشاشة (On Screen Display)
OTT	خدمات متاحة بحرية على الإنترنت (Over The Top)
PIN	رقم تعرف الهوية الشخصي (Personal Identification Number)
PVR	مسجلة فيديو شخصية (Personal Video Recorder)
ROM	ذاكرة للقراءة فقط (Read Only Memory)
SI	معلومات الخدمة (Service Information)
STB	جهاز فك التشفير (Set-Top Box)
TA	سلطة استوثاق (Trust Authority)
TTP	طرف ثالث موثوق (Trusted Third Party)
TV	تلفزيون (Television)
UI	سطح بيني للمستخدم (User Interface)
VM	آلة افتراضية (Virtual Machine)

5 اصطلاحات

في هذه التوصية:

"يجب"، أو "يلزم"، أو "مطلوب" كلمات تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وكلمة "يُوصى" تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا حاجة تدعو لتوفر هذا المتطلب لزعم المطابقة.

وكلمة "يحظر" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وكلمات "يمكن اختيارياً" أو "يجوز" أو "من الجائز" أو "ربما" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا ترمي هذه المصطلحات إلى إلزام التطبيق بتوفير الجهة البائعة لهذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مقدم الخدمة اختيارياً. بل إن الجهة البائعة يمكنها إدراج هذا الخيار وزعم مطابقة المواصفة في نفس الوقت.

وفي متن هذه التوصية وملحقاتها، تظهر في بعض الأحيان كلمات "يتعين"، و"يتعين ألا"، و"ينبغي"، و"يمكن". وفي هذه الحالة يكون تأويلها، على التوالي، على "يجب"، أو "يلزم"، أو "مطلوب"، و"يجب ألا"، أو "يلزم ألا"، أو "يحظر"، و"يوصى"، و"ربما"، أو "يجوز"، أو "من الجائز". ويأول انتفاء القصد المعياري عند ظهور مثل هذه العبارات أو الكلمات الرئيسية في تذييل أو في مادة موسومة صراحةً على أنها إعلامية.

6 معمارية من أجل حلول CA/DRM مدمجة وقابلة للتبادل

1.6 ملاحظات عامة

المعمارية والتعاريف والاستعراض الشامل بالنسبة للسطح البيئي ECI، كما تتناولها هذه التوصية الإطارية، هي جزء من معيار متعدد الأجزاء يوصف معمارية نظام لأنظمة CA/DRM للأغراض العامة قائمة على البرمجيات ومدجة وقابلة للتبادل ستكون الحل المستقبلي الأكثر ملاءمةً للتغلب على انقسام السوق وتمكين قابلية التشغيل البيئي. وفيما يلي الفوائد الرئيسية للنهج المتوخى لأمن المحتوى:

- المرونة وقابلية التوسع نتيجةً للتنفيذ القائم على البرمجيات
 - قابلية التبادل تعزز حل مستقبلي وتتيح الابتكار
 - إمكانية التطبيق على المحتوى الموزع عبر الإذاعة والنطاق العريض، بما في ذلك الخدمات المتاحة بحرية على الإنترنت
 - دعم بيئة الشاشات المتعددة
 - تحفيز السوق بالنسبة لمشغلي المنصات وموردي الشبكات والخدمات والعملاء بتجنب "الاحتكار"
 - مواصفة لنظام إيكولوجي مفتوح يعزز تنمية السوق
- ويرمي نظام السطح البيئي ECI إلى إمكانية تبادل أنظمة النفاذ CA والإدارة DRM في معدّات منشآت العمل على جميع المستويات والجوانب ذات الصلة، بأقل تكلفة ممكنة للمستهلكين وبأدنى قدر من القيود على بائعي خدمات النفاذ CA والإدارة DRM لتطوير منتجاتهم الهادفة من أجل سوق التلفزيون غير المجاني. والعنصر الأساسي للسطح البيئي ECI هو توصيف السطح البيئي بين الوسيط CA/DRM القائم على البرمجيات والنظام المضيف. وبالتالي، يؤدي السطح البيئي ECI، وظائف كثيرة من بينها ما يلي:
- حاوية برمجية من أجل الاستقبال بالنفاذ CA مضمون الإدارة DRM - سيشار إليه فيما بعد باسم وسيط السطح البيئي ECI، بواسطة:
 - سطوح بنية قياسية لجميع الوظائف ذات الصلة لمعدّات منشآت العمل
 - آلة افتراضية (VM) قياسية لكي تشغل عليها
 - دعم الأنظمة التي لا تحتوي على بطاقات ذكية وتلك القائمة عليها
 - إضافة طائفة واسعة من حاويات البرمجيات تلك في معدّة من معدّات منشآت العمل، بحيث تعمل كل حاوية حسب حالة الآلة الافتراضية الخاصة بها
 - تثبيت وسيط السطح البيئي ECI بشكل مستقل عن البرمجيات الأخرى لمعدّات منشآت العمل من خلال مفهوم أداة تحميل مؤقتة وقياسية
 - الأمن المتقدم، ويعرف أيضاً بأمن مجموعة الرقائق، لدعم أحدث وسائل حماية المحتوى
 - وسائل للاستفادة بوظائف الأمن الممكنة بالعتاد
 - أساليب للمستعمل لاكتشاف وسيط السطح البيئي ECI السليم الذي يجب تحميله
 - أساليب من أجل إبطال وظيفة وسيط السطح البيئي ECI ووظيفة معدّات منشآت المستعمل (أو أجزاء منها)

- مناسب من أجل أنظمة الإذاعة الرقمية التقليدية وتلفزيون بروتوكول الإنترنت والأنظمة الحديثة القائمة على الخدمات OTT وعلى الرغم من أن السطح البيني ECI يظهر بعض التشابه مع الحلول المستخدمة بالفعل، فهناك اختلافات جوهرية:
- (1) الوحدة النمطية لوسيط CA/DRM تكمن في البرمجيات ولم تعد موجودة في العتاد. ولذا، لا يتحمل جانب المستهلك أي تكاليف من أجل تبادل نظام نفاذ CA أو إدارة DRM.
- (2) يمكن تنفيذ العديد من وسطاء السطح البيني ECI على التوازي في معدة واحدة من معدّات منشآت العميل بل في نفس المعدّة، دون إضافة التكاليف المترتبة.
- (3) يمكن تشغيل هؤلاء الوسطاء في آنٍ واحد.

ونتيجةً لذلك، فإن مكون النفاذ CA والإدارة DRM يمكن تبادله بصورة أسهل كثيراً، بما يتيح للمستخدمين النهائي تغيير المشغل أو الحصول على الخدمات من مجموعة متنوعة من المشغلين على المعدّة CPE الخاصة به، بدون تبادل وحدات نمطية غالية الثمن. والمعيّار متعدد الأجزاء الكامل يتألف من مجموعة من المواصفات، بما في ذلك مواصفة إطارية، جنباً إلى جنب مع المواصفات الأساسية:

- الجزء 1: المعمارية والتعاريف وعرض مجمل [ETSI GS ECI 001-1]
 - الجزء 2: حالات ومتطلبات الاستعمال [ETSI GS ECI 001-2]
 - الجزء 3: الحاوية، ووحدة التحميل، والسطوح البينية، والإبطال بالنسبة إلى CA/DRM [b-ETSI GS ECI 001-3]
 - الجزء 4: الآلة الافتراضية (VM) [b-ETSI GS ECI 001-4]
 - الجزء 5: نظام الأمن المتقدم [b-ETSI GS ECI 001-5]
 - الجزء 6: البيئة الموثوقة [b-ETSI GS ECI 001-6]
 - الجزء 7: متطلبات موسعة [b-ETSI GS ECI 001-7]
- وهذه المواصفات تصف معاً حلاً يسمح باستبدال وسطاء السطح البيني ECI في أي وقت بمجرد تحميل الوسطاء المطلوبين من عميل نهائي. وثبت الوسطاء ECI في حاوية برمجيات قياسية في المعدّة CPE بواسطة وحدة تحميل منفصلة، وخوارزميات أمن ومفاتيح منفصلة لحماية الوسطاء ECI من الهجمات التي تستهدف سلامتها واستبدالها بكل مستقل عن جميع البرمجيات الأخرى في المعدّة CPE. والسطوح البينية الخاصة بالحاويات مع المعدّة CPE مكونات عامة وهي محددة في المعيار [b-ETSI GS ECI 001-3]، بما يمكن الوسطاء ECI من التفاعل مع الوظائف المختلفة في المعدّة CPE، وما عداها.

ويشغل الوسطاء ECI طبقاً لحالة معينة للآلة الافتراضية محددة في المعيار [b-ETSI GS ECI 001-4].

ويوصف المعيار [b-ETSI GS ECI 001-5] آلية متقدمة للأمن لحماية مفتاح المحتوى أثناء رحلته إلى أداة فك تجفير المحتوى رقاقة معالج المعدّة CPE.

وتتناول التوصية هذه معمارية وعرضاً مجملاً لمواصفات السطوح البينية ذات الصلة من أجل تنفيذ أنظمة CA/DRM قابلة للتشغيل البيني في معدّات ومنشآت العميل.

ولا تطبق مواصفة السطح البيني ECI إلا على الاستقبال والمعالجة التالية للمحتوى وهو ما يتم التحكم فيه عن طريق نظام النفاذ المشروط/أو إدارة الحقوق الرقمية والذي تم تخطيطه بواسطة مورد الخدمة. والمحتوى الذي لا يتم التحكم فيه عن طريق نظام كهذا لا يتم تناوله في هذه التوصية.

ومواصفة المجموعة ECI موضوعة لكي تستعمل بالاشتراك مع إطار تعاقدى (اتفاق ترخيص) وقواعد للائتمان والمثانة وعملية مناسبة لإصدار الشهادات (انظر الملاحظة)، تحت سيطرة سلطة استوثاق، المعيار [b-ETSI GS ECI 001-6]. ويلاحظ أن الإطار التعاقدى (اتفاق الترخيص) وقواعد الائتمان والمثانة والعملية المناسبة لإصدار الشهادات لا تخضع لأعمال التقييس في الفريق ISG ECI.

2.6 المفهوم التقني للنظام ECI

1.2.6 الاعتبارات الأساسية

توصف هذه التوصية، جنباً إلى جنب مع الأجزاء من 2 إلى 5 و 7 من المواصفات ([ETSI GS ECI 001-2] و [b-ETSI GS ECI 001-3] و [b-ETSI GS ECI 001-4] و [b-ETSI GS ECI 001-5] و [b-ETSI GS ECI 001-7])، معمارية تسمح بتحميل وتنشيط وتحديث وإزالة واستبدال وسطاء ECI في أي وقت بشكل مستقل عن الوسطاء ECI الآخرين المشغلين على نفس المضيف، أو برمجيات أنظمة المعدات CPE الخاصة بالمضيف أو التطبيقات المشغلة على هذا المضيف. ويجب أن يكون أي مضيف ECI قادراً على تأمين وتوفير بيئة وقت التشغيل الأكبر عدد من الوسطاء ECI يمكن لموارد المضيف تداوله، اثنان على أقل تقدير. ويجب تشغيل الوسطاء ECI في أي مضيف على التوازي، بما يمكن من التحفير أو فك التحفير المتزامن لتدفقات مختلفة من المحتويات من مشغلين مختلفين.

والمفهوم التقني الموصوف في هذه التوصية والموصف في المعايير [ETSI GS ECI 001-2] و [b-ETSI GS ECI 001-3] و [b-ETSI GS ECI 001-4] و [b-ETSI GS ECI 001-5]، يمكن تطبيقه على كل من أنظمة النفاذ المشروط (CA) المطابقة للتحفير المتعدد وأنظمة إدارة حقوق النفاذ (DRM) المتوافقة مع التحفير المشترك (CENC) في الإذاعة الفيديوية الرقمية (DVB). وتستضيف المعدات CPE أداة تحميل خاصة من أجل الوسطاء ECI فقط مع وظائف الأمن الضرورية لحماية سلامة واستيقان الوسطاء ECI. ويمكن استدعاء وحدة التحميل هذه وتشغيلها في أي وقت لتحميل وسيط ECI آخر والتحقق منه في أي وقت. ويرد توصيف وحدة التحميل إلى جانب الوسائل الأمنية المرتبطة بها في المعيار [b-ETSI GS ECI 001-3].

وفيما يتعلق بهذا المفهوم التقني، يثبت كل وسيط ECI في حاوية برمجيات منفصلة مع حالة الآلة الافتراضية (VM) الخاصة به والتي توصف في المعيار [b-ETSI GS ECI 001-4]. وتوصف الحاوية ECI من أجل الوظيفة CA/DRM فقط، وهو ما ينعكس في المعيار [b-ETSI GS ECI 001-3]. والسطح البيئي مع المعدة CPE الوارد بالتفصيل في المعيار [b-ETSI GS ECI 001-3]، يمكن طلب البيانات وتبادلها وهي أمور مطلوبة للوظائف CA/DRM المختلفة. وهذه الطلبات وعمليات التبادل للبيانات يمكن إجراؤها بين الوسيط ECI والمضيف أو بين وسيطين ECI في نفس المضيف أو بين وسيطين ECI في مضيفين مختلفين.

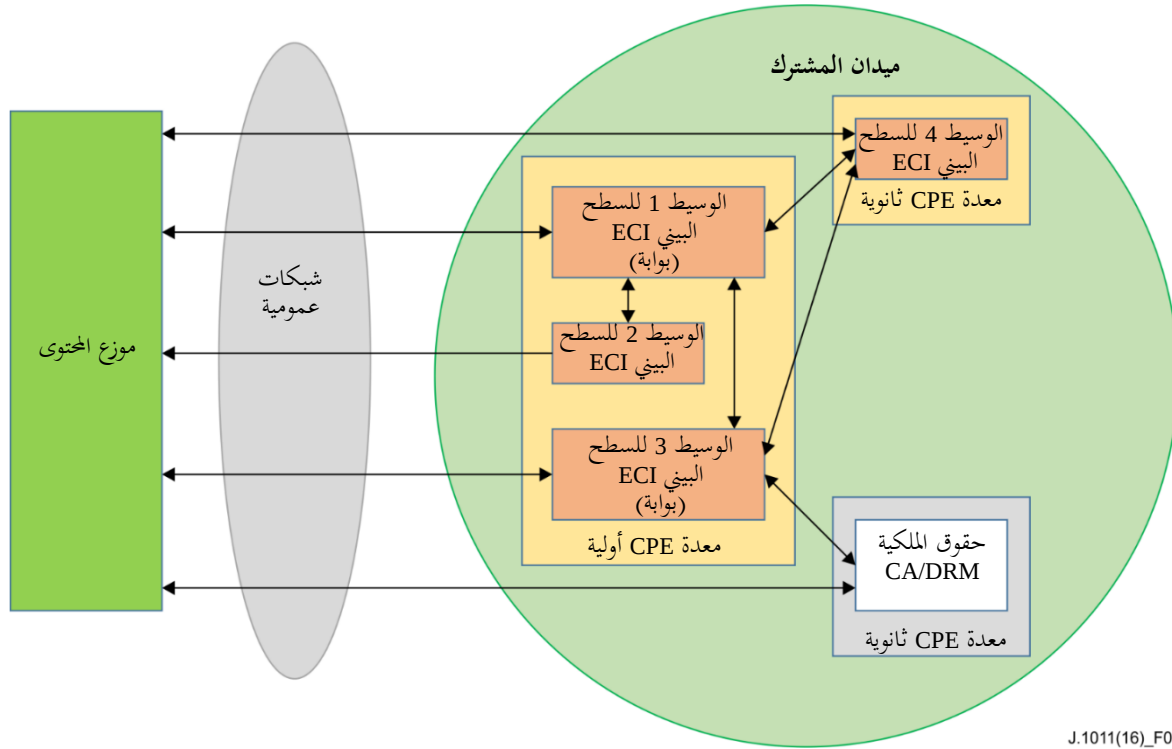
وتعرف الأجهزة المتمحورة حول التلفزيون بأنها أجهزة تتضمن معالجة لقطار نقل MPEG-2 داخل مجموعة الرقاقات. ويلزم السطح البيئي ECI مجموعات الرقاقات هذه بتنفيذ وظائف أمنية متقدمة مطابقة للسطح البيئي ECI. والمعيار [b-ETSI GS ECI 001-5] يوصف أحكاماً من أجل الاستفادة من آليات الأمن المتقدمة في مجموعة الرقاقات، وذلك مثلاً لحماية المفتاح المصاحب للمحتوى أثناء رحلته نحو أداة فك تحفير المحتوى الخاص برقاقة معالج المعدة CPE. ويسمح هذه المفهوم الأمني المتقدم لجميع الوسطاء ECI باستخدام هذه الأداة، إذا استدعى الأمر، للتشغيل في آن واحد أو بشكل مستقل كل عن الآخر.

والأجهزة الخاصة ببيئات أخرى، لا سيما تلفزيون بروتوكول الإنترنت والأجهزة اللوحية والهواتف الذكية وما إلى ذلك، تستخدم عادةً أكثر من وظيفة في البرمجية وتوفر اتصالات IP في الاتجاهين. ويمكن هذا الأمر استخدام الأنواع الجديدة المحددة من آليات تعزيز الأمن. وحيث إن مجموعات الرقاقات المستخدمة في هذه الأجهزة تتضمن عتاداً من أجل وظائف أمن المعالجة المختلفة، فإن السطح البيئي ECI يتطلب تنفيذ وظائف مكرسة ممكنة بالعتاد للأمن والمتانة من أجل تحقيق المطابقة مع السطح البيئي ECI. وبالتالي، تتضمن المواصفة [b-ETSI GS ECI 001-3] طرائق لكي يحصل الوسيط ECI على المعلومات ذات الصلة للقدرات والوظائف التقنية للمضيف، طالما كانت مطلوبة، بما في ذلك إمكانية دعم الأمن المتقدم على النحو الموصف في [b-ETSI GS ECI 001-5].

وتتاح وظائف الأمن المتقدم في آن واحد لأي وسيط ECI نشط في أي معدة CPE. كما يمكن نشر الوسطاء ECI في منصات ذات أنظمة CA مطابقة أو أنظمة DRM مطابقة للتحفير CENC في الإذاعة DVB تشغيل إما في أسلوب التحفير المتزامن أو أسلوب التحفير المتعدد، طالما كان جانباً المخدم لهذه الأنظمة مطابقين لمعايير الطرف الخلفي DVB/CENC ذات الصلة.

2.2.6 نظرة عامة معمارية

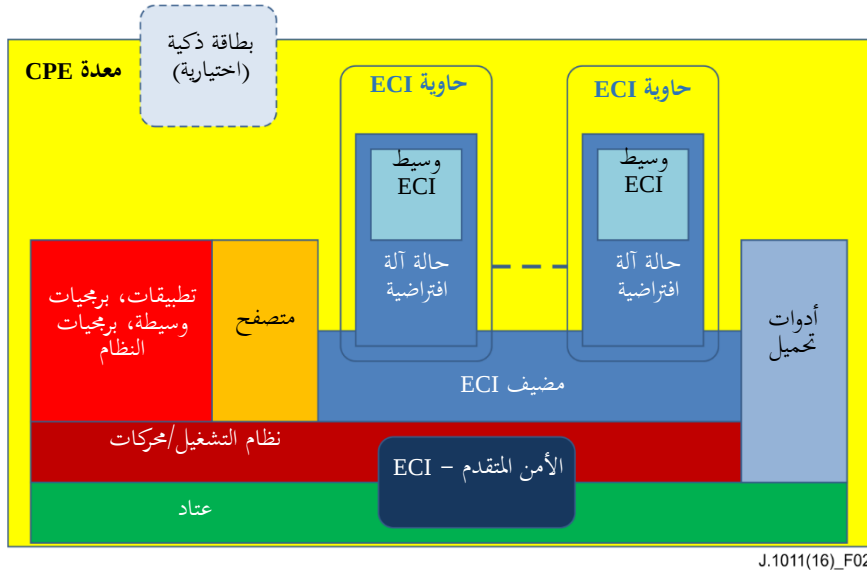
يسمح السطح البيني للموردين CA/DRM بتنفيذ حلول من أجل النفاذ المشروط (CA) وكذلك من أجل إدارة الحقوق الرقمية (DRM) داخل ميدان عميل فردي. ويعرض الشكل 1 تشكيلة مرجعية مدعومة بشكل كامل بتنفيذ سطح بيبي ECI كامل. ولدعم بيئات الشاشات المتعددة داخل ميدان العميل الفردي، يمكن للوسطاء ECI داخل هذا الميدان التواصل مع بعضهم البعض، ويمكنهم الاستفادة من شبكة ثنائية الاتجاه مع المورد، حسب توفر الشبكات المناسبة، ودعم وظائف في الأنظمة CA/DRM والوسطاء ECI التابعين لها. ويوفر المعيار [b-ETSI GS ECI 001-3] المزيد من التفاصيل. ويمكن تنفيذ وسيط ECI بطريقة تجعله قادراً على العمل كبوابة أيضاً لوسطاء غير مطابقين للسطح البيبي ECI. ولذا، توصف الأدوات الضرورية في المعيار [b-ETSI GS ECI 001-5]. والبروتوكولات وعمليات التنفيذ المحددة للوسطاء القائمين على حقوق الملكية خارج نطاق مواصفات السطح البيبي ECI.



J.1011(16)_F01

الشكل 1 - الوسطاء ECI داخل ميدان عميل وحيد

وتحدد مواصفات السطح البيبي ECI، ضمن أمور أخرى، السطح البيبي بين حاوية ECI ومضيف ECI. ويعرض الشكل 2 مخطط وظيفي لمعدّة CPE بحاويات ECI، والوظائف الأخرى في المضيف ECI التي تتصل بها أو يمكن أن تتصل بها الحاويات ECI. وبعض هذه الوظائف اختياري. وأثناء تثبيت وسيط ECI وأثناء طلاقه، يحدد المضيف الوظائف المتاحة للوسيط ECI.



الشكل 2 - مخطط وظيفي لمعدّة CPE وسطاء ECI مدمجين،
كل الحاوية ECI وحالة الآلة الافتراضية الخاصة به

ويقوم المفهوم قبل كل شيء على مفهوم وحدة تحميل معمارية (انظر الشكل 3) تتألف من وحدة تحميل قائمة على الرقاقات ووحدة تحميل البرمجيات النظام ووحدة تحميل الوسيط ECI.

وتحمل وحدة تحميل المضيف ECI برمجيات المضيف ECI. ويشمل ذلك، إضافةً إلى عناصر أخرى، نفاذ الآلة الافتراضية إلى مكونات الأمن ووحدة تحميل الوسيط ECI. ويمكن المضيف ECI واحد تحميل العديد من وسطاء ECI في حالات آلات افتراضية منفصلة، تشغل بشكل مستقل ومعزول عن بعضها البعض.

وعند تحميل وسيط ECI في النظام، تستحدث حالة آلة افتراضية يحمل فيها الوسيط ECI. وتعمل حالة الآلة الافتراضية تلك كوسط افتراضي بين الوسيط والمضيف ECI. والسطح البيئي بين العميل ECI وحالة الآلة الافتراضية هو السطح البيئي الرئيسي الذي توصفه مواصفة المجموعة (GS). ويحدد السطح البيئي إضافةً إلى ذلك تدفق/بروتوكول المعلومات بين حالات متعددة لوسيط ECI كهذا ولوظائف أخرى داخل المعدّة CPE، مثل الأمن المتقدم وشاشة العرض وما إلى ذلك. ويلاحظ أن الوسطاء ECI الآخرين لا يلزم بالضرورة أن يكونوا في نفس المضيف ECI. ويرد توصيف هذا السطح البيئي وبروتوكول الاتصالات في المعيار [b-ETSI GS ECI 001-3].

ويعتمد المضيف ECI نفسه على تنفيذ الجهة المصنعة. وهو موصل بينياً بنظام التشغيل وطبقة المحركات ويوفر جميع الوظائف التي تحددها مواصفة السطح البيئي للوسيط ECI. ولا يوصف المضيف ECI بالسطح البيئي ECI، ولكن يتعين اعتماده من سلطة استوثاق من أجل ضمان المطابقة لمواصفة السطح البيئي للوسيط ECI.

3.2.6 وظائف إلزامية للأجهزة المطابقة للسطح البيئي ECI

يتناول السطح البيئي ECI طائفة من سيناريوهات الاستعمال (انظر الشكل 1). لذا، يتعين أن يتعامل السطح البيئي ECI مع طائفة واسعة من الأجهزة من قبيل التلفزيونات الرقمية المدججة (iDTV) وأجهزة فك التشفير (STB) ومسجلات الفيديو الشخصية (PVR) وتلفزيون بروتوكول الإنترنت (IPTV) والأجهزة اللوحية والهواتف الذكية وغيرها. وتختلف هذه الأجهزة في قدراتها بينما توفر إطاراً أمنياً متناسقاً. ويميز السطح البيئي ECI الأجهزة المتمحورة حول التلفزيون عن الأجهزة الخاصة بالأغراض الأخرى، بما في ذلك، على سبيل الذكر وليس الحصر، تلفزيون بروتوكول الإنترنت والأجهزة اللوحية.

وتعرف الأجهزة المتمحورة حول التلفزيون بأنها أجهزة تتضمن معالجة لقطار نقل MPEG-2 داخل مجموعة الرقاقات. ويلزم السطح البيئي ECI مجموعات الرقاقات هذه بتنفيذ وظائف أمنية متقدمة مطابقة للسطح البيئي ECI. والمعدّات CPE المطابقة للسطح

البيني ECI المتمحورة حول التلفزيون يجب أن تتمثل للوظائف المحددة في المواصفات [b-ETSI GS ECI 001-3] و [b-ETSI GS ECI 001-4] و [b-ETSI GS ECI 001-5].

والأجهزة الخاصة ببيئات أغراض أخرى، خاصةً لتلفزيون بروتوكول الإنترنت وأجهزة الحاسوب والأجهزة اللوحية تنفذ عادةً وظائف أكثر في البرمجيات وتتصل باتصالات IP في الاتجاهين. ويمكن هذا الأمر من تنفيذ الأنواع المختلفة من آليات الأمن وحيث إن مجموعات الرقاقات المستعملة في هذه الأجهزة تتضمن عتاداً من أجل الوظائف المختلفة للمعالجة الأمنية، يستوجب السطح البيني ECI تنفيذ وظائف مكرسة ممكنة بالعتاد من أجل الأمن والمثانة في مجموعات الرقاقات. وتوصف المعايير [b-ETSI GS ECI 001-3] و [b-ETSI GS ECI 001-4] و [b-ETSI GS ECI 001-5] الآليات اللازمة للاستفادة من هذه الوظائف.

4.2.6 السطوح البينية اللازمة بين المضيف ECI والوسيط ECI

الحاوية ECI مفهوم تقني يجمع بين الآلة الافتراضية (VM) والوسيط ECI بهدف عزلها وحجبها عن بقية أجزاء المعدة CPE. والآلة الافتراضية هي إحدى وظائف المضيف ECI. وبتحميل وسيط ECI، ينشئ المضيف ECI حالة آلة افتراضية. وتوفر الآلة الافتراضية السطوح البينية اللازمة بالوسيط ECI وتوصلها بالمضيف ECI. وتعرف المواصفة ECI السطح البيني بين الآلة الافتراضية والوسيط ECI، انظر أيضاً الشكل 2 من أجل معمارية رفيعة المستوى بجهاز مطابق للسطح البيني ECI. ويوفر السطح البيني بعض السطوح البينية لبرمجة التطبيقات (API) وينشئ أيضاً قناة اتصالات مؤمنة.

وتبرز القائمة التالية السطوح البينية البرمجية الهامة:

- سطح بيني لمعلومات المقدرة إلى الوسيط ECI من المضيف ECI والعكس
- سطح بيني لمعالجة إشارات الدخل والخروج للمعدة CPE
- سطح بيني لمجموعة عتاد/محركات الأمن المتقدم
- سطح بيني لوظائف وحدات التحميل
- سطح بيني لدعم تفاعل المستعمل
- سطح بيني لوظائف التجفير وفك التجفير
- سطح بيني لقراءة البطاقات الذكية الاختيارية
- سطح بيني لوظائف أمنية محددة مثل أخذ البصمات والوسم بالعلامات المائية
- سطح بيني للتخزين المحلي

وتوفر جميع السطوح البينية للوسيط ECI بواسطة الآلة الافتراضية.

وإلى جانب ذلك، هناك بروتوكولات اتصالات على قمة السطوح البينية تسمح باتصالات مؤمنة. وهناك بشكل خاص مواصفة البروتوكول لإقامة اتصالات بين الوسطاء ECI، سواء كانوا داخليين أو خارجيين.

ويمكن توصيل المعدة CPE بأي نوع من الشبكات وبالعديد من الشبكات في نفس الوقت، سواء في اتجاه واحد أو في الاتجاهين. ولا يلزم عادةً بتوصيلها بأي شبكة (محتوى محمل/مخزن).

5.2.6 وظيفة دنيا لسطح بيني وشاشة عرض للمستعمل

للاتصالات بالمستعمل، يجب توفر وسيلة دنيا من أجل سطح بيني للمستعمل (UI) وعرض على الشاشة (OSD) للحاويات ECI. ويوصف ذلك في المعيار [b-ETSI GS ECI 001-3]. وهي تستخدم لعرض الرسائل التي أعدت أو أرسلت بواسطة النظام CA/DRM على المستعمل. كما أنها تستخدم لتمكين المستعمل من إدخال مدخلات مثل رقم تعرف الهوية الشخصي (PIN). وتوصف التفاصيل في المعيار [b-ETSI GS ECI 001-3] أيضاً.

ويتفاعل المستعمل محلياً مع النظام CA/DRM عن طريق الوسيط ECI.

6.2.6 الآلة الافتراضية

يُشغل الوسيط ECI على آلة افتراضية قياسية. ويرد توصيف هذا المكون في المعيار [b-ETSI GS ECI 001-4]. ويجب أن يكون لكل وسيط ECI مثبت حالته الخاصة من الآلة الافتراضية. وتوفر حالة الآلة الافتراضية بيئة مؤمنة لتنفيذ مضمون النفاذ المشروط أو تطبيقات الوسائط لإدارة الحقوق الرقمية. وتوفر الآلة الافتراضية السطوح البينية لبرمجة التطبيقات حيث يمكن النفاذ إلى موارد بيئة المضيف ECI بطريقة مقيسة.

7.2.6 وسيلة الأمن المتقدم

يحدد السطح البيني ECI الحد الأدنى من الوظائف الأمنية الضرورية اللازمة لإنشاء نظام مؤمن لحماية المحتوى. ويحتاج السطح البيني ECI إلى تعزيزات استناداً إلى عناصر العتاد. وفي الأجهزة المتمحورة حول التلفزيون، يتم التزويد بذلك عن طريق وظائف مكرسة للأمن المتقدم خاصة بالتلفزيون. ويوصف ذلك ما هو المفضل في أنظمة محتواة ضمن رقاقة (SoC) بوصفه "مجموعة ارتقاء رئيسية". ومن المهام الأساسية لتوصيلة الأمن المتقدم حماية مفاتيح حماية المحتوى أثناء إرساله من الوسيط ECI إلى وحدة تجفير المحتوى في المعدة CPE أو نقل المحتوى المحمي من وسيط ECI إلى وسيط ECI آخر (انظر الشكل 1). ونظام الأمن المتقدم كما هو موصف في [b-ETSI GS ECI 001-5] يدعم قطارات كلمات تحكم مختلفة متزامنة ووسائط ECI مختلفين يطلبون خدماته في آنٍ واحد. وعلاوة على ذلك، لوسيلة الأمن المتقدم دور رئيسي في التحقق من تحميل البرمجيات للمضيف وللوسائط ECI.

والأجهزة الخاصة ببيئات أغراض أخرى، خاصةً تلفزيون بروتوكول الإنترنت وأجهزة الحاسوب والأجهزة اللوحية تنفذ عادةً وظائف أكثر في البرمجيات وتتصل باتصالات IP في الاتجاهين. ويوصف السطح البيني ECI نفس مفاهيم وآليات الأمن المتقدم ولكنه يقابلها بشكل مختلف على معماريات أمن الأجهزة [b-ETSI GS ECI 001-3] و [b-ETSI GS ECI 001-4] و [b-ETSI GS ECI 001-5].

وتيسر الأمن المتقدم في الوحدة CPE يوصل إلى الوسيط ECI أثناء تثبيته وإطلاقه.

8.2.6 عادة التخليط

المحتوى المحمي، الذي تستقبله معدة CPE مطابقة للسطح البيني ECI، قد لا يستهلك في الحال. والوظائف التالية متاحة مع الأجهزة المطابقة للسطح البيني ECI.

- التخزين المحلي
 - تحت سيطرة المعدة CPE
 - تحت سيطرة وسيط CA - أو وسيط DRM
- البوابة
 - توصيل عنصر محتوى محمي لجهاز خارجي تحت سيطرة وسيط DRM
 - توصيل عنصر محتوى محمي لوسيط ECI آخر إما داخل نفس المعدة CPE أو يعمل على معدة CPE أخرى مطابقة للسطح البيني ECI

ولدعم هذه الوظائف، يمكن للجهاز المطابق للسطح البيني ECI إعادة تخليط المحتوى. ولا يوصف النظام ECI آليات النقل ولا وظائف DRM المتاحة لتخزين أو لتوصيل المحتوى المحمي لأجهزة أخرى. وفي المعيار [b-ETSI GS ECI 001-5]، تعرف السطوح البينية اللازمة بين المضيف ECI والوسيط ECI.

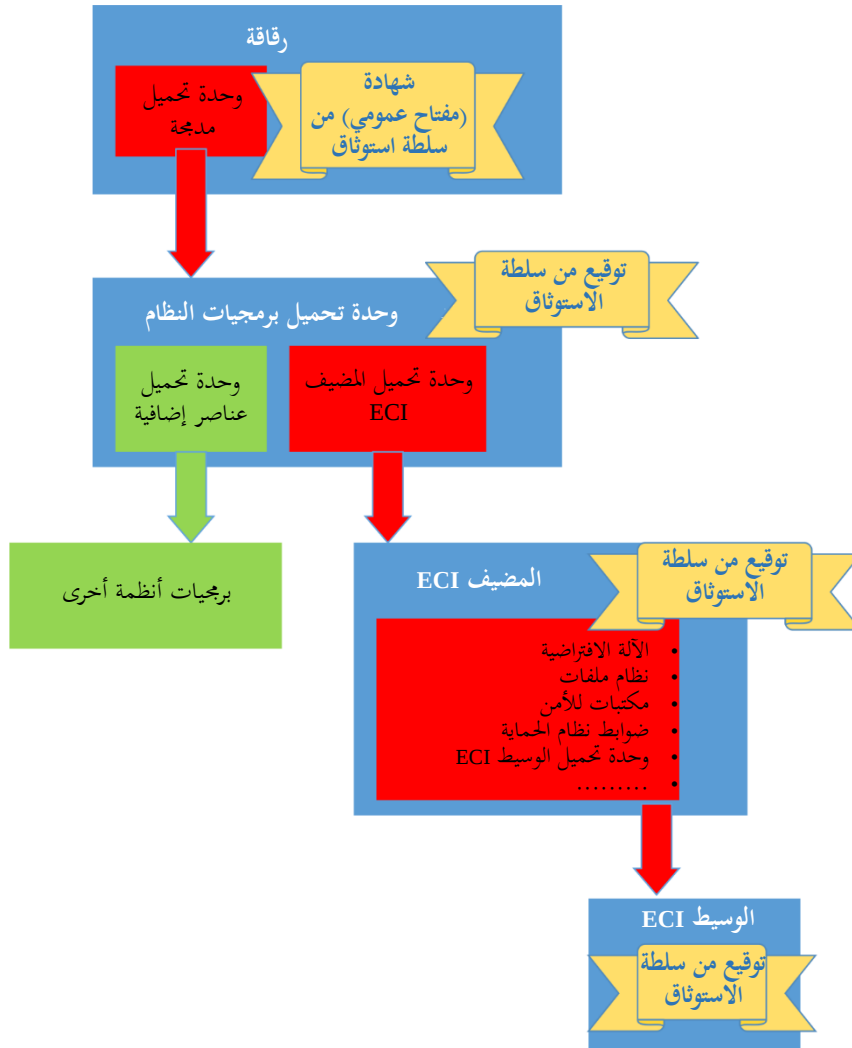
9.2.6 وظائف وحدة التحميل ECI

يجب أن توفر أي معدة CPE مطابقة للسطح البيني ECI وظائف وحدة التحميل، التي تسمح بتحميل وتثبيت الوحدات النمطية للبرمجيات ذات الصلة للنظام ECI إضافةً إلى سلامتها وحمايتها من الاستبدال.

وبدايةً، تحمل وحدة التحميل المدججة في الرقاقة وحدة تحميل برمجيات النظام. والغرض من وحدة التحميل المدججة هذه ضمان عدم تثبيت وإطلاق إلا وحدة تحميل برمجيات نظام معتمدة. وتتضمن وحدة تحميل برمجيات النظام وحدة تحميل المضيف ECI، وبالتالي، يتعين أن تكون وحدة تحميل برمجيات النظام موقعة من سلطة استوثاق. وقد تتضمن وحدة تحميل برمجيات النظام وحدات تحميل لبرمجيات أنظمة أخرى غير ذات صلة بوظائف السطح البيئي ECI وليس لها علاقة بعناصر النظام المتعلقة بالأمن. وتشمل برمجيات المضيف ECI وحدة تحميل الوسيط ECI والتي يمكن فيما بعد تحميل الوسيط ECI، عند الطلب.

وأثناء التثبيت في الحاوية ECI الخاصة به، وكذلك أثناء إطلاقه، يبلغ الوسيط ECI من المضيف ECI بالأدوات الخاصة به، مثل أدوات التسجيل وأدوات القرص الصلب وقارئة البطاقات الذكية وأدوات أخذ البصمات والوسم بالعلامات المائية والشبكات، إضافةً إلى الامتثال للمواصفة الإطارية (التوصية الحالية) والمعايير [b-ETSI GS ECI 001-3] و [b-ETSI GS ECI 001-4] و [b-ETSI GS ECI 001-5]، وربما المعيار [b-ETSI GS ECI 001-6].

ويرد توصيف وحدة التحميل ECI وأدوات الأمن ذات الصلة في المعيار [b-ETSI GS ECI 001-3].



J.1011(16)_F03

الشكل 3 - المفهوم التراتبي لوحدة التحميل

10.2.6 الإبطال

قد تقرر سلطة الاستوثاق وضع معدة CPE أو مجموعة من المعدّات CPE أو نوع من المعدّات CPE أو جميع المعدّات CPE المورد من مصنع محدد في قائمة سوداء. وقد يقوم مورد أو مشغل المحتوى بإبطال هذه المعدّة أو المعدّات CPE المعنية من نقاط توزيع الخدمة الخاصة به. والطرق المستعملة تسمح للمشغلين وموزعي المحتوى الآخرين بمواصلة توفير خدماتهم لهذه المعدّات CPE، إذا رغبوا في ذلك.

ويمكن للإبطال حجب جميع الخدمات المقدمة من المشغل أو مورد المحتوى للمعدّة (المعدّات) CPE المعنية، أو مجموعة من هذه الخدمات. وهذا موضوع يخص وظيفة النظام CA أو النظام DRM ذي الصلة وخارج نطاق هذه التوصية.

ويرد توصيف عملية الإبطال في المعيار [b-ETSI GS ECI 001-3].

7 البيئة الموثوقة

لكي يتسنى تطوير نظام استناداً إلى السطح البيئي ECI، يجب تهيئة بيئة موثوقة. والتفاصيل المتعلقة بهذه البيئة خارج نطاق مواصفات السطح البيئي ECI. ومع ذلك، فإن المبادئ الموصفة في المعيار [b-ETSI GS ECI 001-6]، ضرورية للفهم الوافي للكيفية التي يعمل بها السطح البيئي ECI.

وسلطة الاستوثاق (TA) منظمة تحكم جميع القواعد واللوائح التي تطبق على عمليات التنفيذ الخاصة بالمعمارية ECI. ويجب أن تكون سلطة الاستوثاق كيان لكي يتسنى لها التحقيق في الشكاوي القانونية. ويتعين أن تكون هذه السلطة محايدة بالنسبة لجميع الأطراف الفاعلة في النظام CA/DRM القابل للتحميل، ويشمل ذلك:

- مصنعي المعدّات CPE
- مصنعي الوحدات CA/DRM (الوسطاء ECI)
- مصنعي وحدات الرقاقات، التي تتضمن مكوناتها مفاتيح وشهادات معالج مؤمن غير قابل للتغيير، والتي تعد ضرورية للتفاعل بين المضيف والنظام CA/DRM المطابق
- مشغلي المنصات؛ ومشغل المنصة هو الطرف الذي يتحكم في جميع العناصر الضرورية لأي نظام CA/DRM. ومشغلو المنصات هم، على سبيل المثال، موردو خدمات أو مشغلو شبكات
- موردي التطبيقات، إن وجدوا.

الطرف الثالث الموثوق (TTP) هو مورد خدمة تقنية يصدر الشهادات والمفاتيح لجهات التصنيع المطابقة للمكونات ذات الصلة لأي نظام ECI. وتضمن الثقة في هذه المفاتيح والشهادات سلطة الاستوثاق التي تمسك بيدها بزمام الثقة.

وتشكل سلطة الاستوثاق والطرف الثالث الموثوق الأساس لسلسلة الثقة وبالتالي يتعين مشاركتهما في جميع العمليات التي تتراوح من الإنتاج (الرقاقات والمعدّات CPE) مروراً بالعمليات (التحميل والتفعيل المؤمنان للوسيط ECI) وصولاً إلى تدابير التحكم (الإبطال، مثلاً).

وتضمن سلطة الاستوثاق بوصفها كياناً قانونياً سير وظائف البيئة الموثوقة عبر إطار تعاقد يطلق عليه أيضاً اتفاق ترخيص، تتحمل بموجبه الأطراف الفاعلة المختلفة مسؤولياتها والتزاماتها. وطبقاً لاتفاق الترخيص، تقوم سلطة الاستوثاق/الطرف الثالث الموثوق بتوليد وإصدار أزواج المفاتيح والشهادات ووثائق اعتماد الاختبار ومعرفات هوية المشغلين وما إلى ذلك.

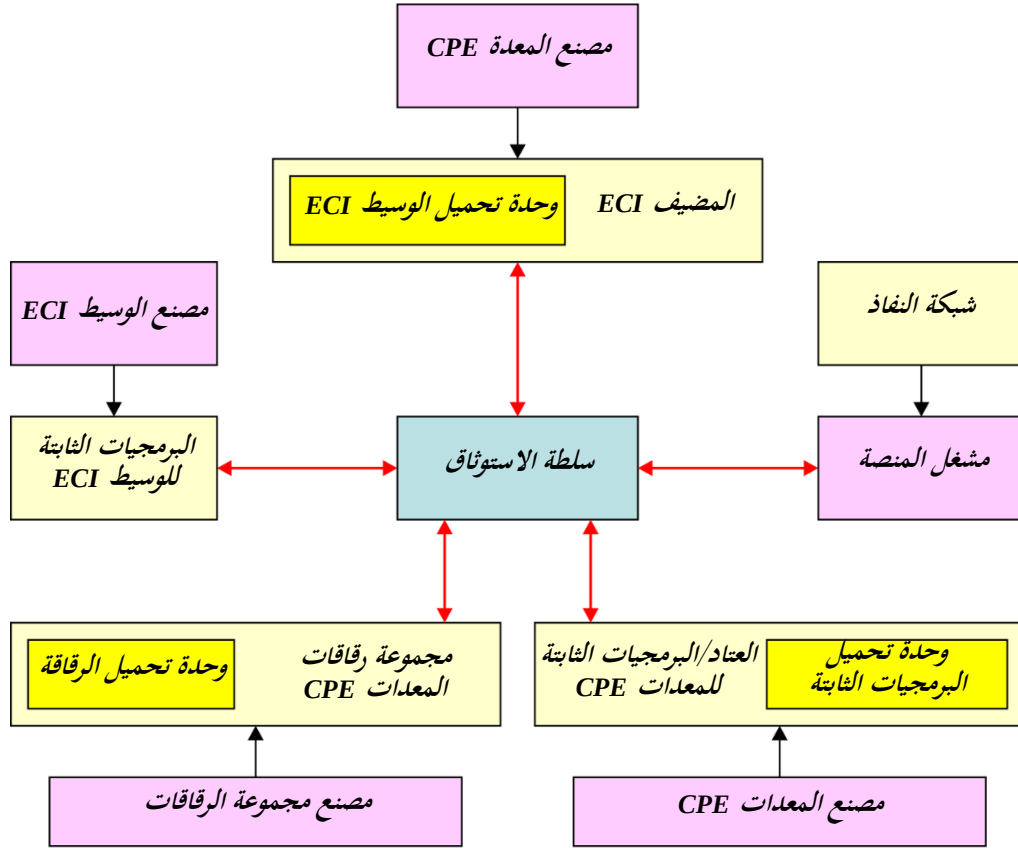
وتوفر إحدى سلطات الاستوثاق الثقة بين جميع المشاركين في السوق. ولا يمكن وجود سلطة استوثاق ثانية لتوفير الثقة "مرة ثانية" لنفس البيئة. ومع ذلك، يمكن وجود سلطات استوثاق متعددة، لكل بلد أو إقليم أو مقاطع أو أنظمة إيكولوجية.

وفي حالة وجود سلطات استوثاق متعددة على التوازي، يشترط وجود ثقة متبادلة بين سلطتي الاستوثاق A و B لكي يتسنى استعمال الأجهزة المسجلة في السلطة A ضمن ميدان السلطة B.

1.7 تدفقات العمل التشغيلية اللازمة

تقدم هذه الفقرة النظرة العامة الأولى لتدفقات العمل التشغيلية اللازمة، التي تخدم احتياجات مختلف المشاركين في السوق لتنفيذ الأعمال القائمة على تكنولوجيا السطح البيئي ECI. وعلاوة على ذلك، تستند تدفقات العمل المبينة إلى العناصر التقنية الضرورية اللازمة لتنفيذ نظام ECI. ويعرض الشكل 4 التفاعلات بين هذه المكونات التقنية والمشاركين المعنيين في السوق.

ملاحظة: الوصف المبين عام وليس مقصوداً به أن يعكس أي حل موجود قائم على الملكية أو أي نشاط تقييس فعلي جارٍ.



J.1011(16)_F04

الشكل 4 - إدارة الثقة اللازمة بين سلطة الاستوثاق (TA) والمشاركين المعنيين بالسوق

المسائل التشغيلية والتعاقدية ذات الصلة (انظر الأسهم الحمراء في الشكل 4) بالنسبة للبيئة الموثوقة هي:

(1) السلامة

السلامة تعني شرط أن يتسنى لأحد المشاركين في السوق التحقق مما إذا كان أحد مكونات العتاد/البرمجيات المورد من مشارك آخر في السوق لم يخضع للتعديل من جانب طرف غير مخول وأنه يلبي المواصفات وقواعد المتانة. ويمكن تحقيق هذا الشرط بوثائق اعتماد وتوقيعات وإجراءات اختبار مناسبة تقوم على وثائق اعتماد الاختبارات المقدمة من سلطة الاستوثاق/الطرف الثالث الموثوق.

(2) الاستيقان

الاستيقان يعني أن أي مكون عتاد/برمجيات منشأة شريك تعاقد للسلطة TA وتجاوز خطوات التحقق والاعتماد اللازمة يمكن ربطه بوضوح بهذا الشريك وبالتالي تمييزه عن أي مكون مقلد. ويثبت أي نظام ECI من استيقان أي مكون ذي صلة من مكونات العتاد/البرمجيات.

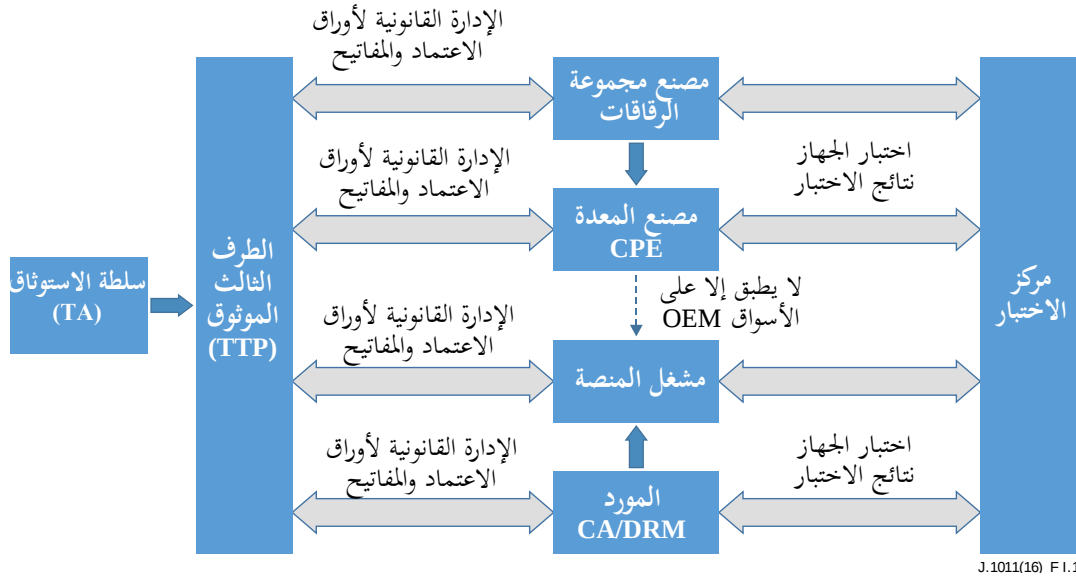
- (3) الإطار التعاقدى
الإطار التعاقدى الذي تضعه السلطة TA بوصفها كياناً قانونياً يجب أن يشمل نظام الامتثال والمتانة وإجراءات منح الشهادات من أجل تهيئة البيئة اللازمة لإنشاء الأنظمة ECI.
- (4) الوسائل العلاجية
في حالة ما إذا أصبحت مكونات العتاد/البرمجيات لأي نظام ECI غير مطابقة، تضع سلطة الاستوثاق إجراءات لمورد هذه المكونات ترمي إلى إعادة توفير السلامة للنظام الإيكولوجي في توقيت زمني معقول.
- والمكونات التقنية الضرورية (الإطارات الصفراء في الشكل 4) هي:
- (1) مجموعة رقاقت المعدّات CPE
مجموعة رقاقت المعدّات CPE هي المكون الرئيسي في عتاد المعدّات CPE حيث تضم عادةً ما يعرف "نظام محتوى ضمن رقاقة" (SoC) نتيجةً للمتطلبات القائمة لمشغلي المنصات وموردي المحتوى. كما توجد وحدة تحميل الرقاقة في الرقاقة CPE.
- (2) عتاد المعدّات CPE
من المسائل الأساسية تنفيذ مجموعة رقاقت CPE مؤمنة ومنع النفاذ غير المخول إلى عناصر التخزين (وحدات الذاكرة Flash و ROM) وحماية السطوح البينية.
- (3) وحدات تحميل مختلفة
تحمّل وحدة تحميل الرقاقة وحدات تحميل إضافية مختلفة، حسب تشكيلة عتاد/برمجيات المعدّة CPE.
- (4) البرمجيات الثابتة للمعدّات CPE
للبرمجيات الثابتة للمعدّات CPE تفاعلات متعددة مع الوسيط ECI وجميع السطوح البينية ذات الصلة لعتاد المعدّات CPE. ويتم ضمان الأمن بمواصفات تفصيلية وقواعد المطابقة والمتانة الملائمة.
- (5) الوسيط ECI
يستخلص الوسيط ECI جميع المعلومات المتعلقة بالنفاذ CA والإدارة DRM الموصلة من الأطراف الأمامية للمعدّات CPE ويستهل عمليات الضبط المقابلة داخل جهاز المعدّة CPE (وحدة إزالة التخليط، السطوح البينية)، والتي تحتاج بداهة إلى تفاعلات مغلقة ومؤمنة مع البرمجيات الثابتة للمعدّات CPE.

التذييل I

تنفيذ نظام ثقة مطابق للسطح البيئي ECI

(لا يشكل هذا التذييل جزءاً من هذه التوصية)

يقدم التذييل I أول إطلالة عامة على تدفقات العمل التشغيلية اللازمة التي تخدم احتياجات المشاركين المختلفين في السوق من أجل تنفيذ أعمال تجارية قائمة على التكنولوجيا ECI. ويقدم الشكل 1.I نظرة مجملية لتدفقات العمل العامة. وعلاوةً على ذلك، تستند تدفقات العمل المبينة إلى عناصر تقنية أساسية ضرورية لتنفيذ أي نظام ECI. ويعرض الشكل 4 في الفقرة 1.5 التفاعلات بين هذه المكونات التقنية والمشاركين المعنيين بالسوق.



ملاحظة - الطرف الثالث الموثوق (TTP) ومركز الاختبار شريكان متعاقدان لسلطة الاستوثاق (TA) من أجل عملية إصدار الشهادات والمفاتيح.

الشكل 1.I - نظرة مجملية لتدفقات العمل العامة

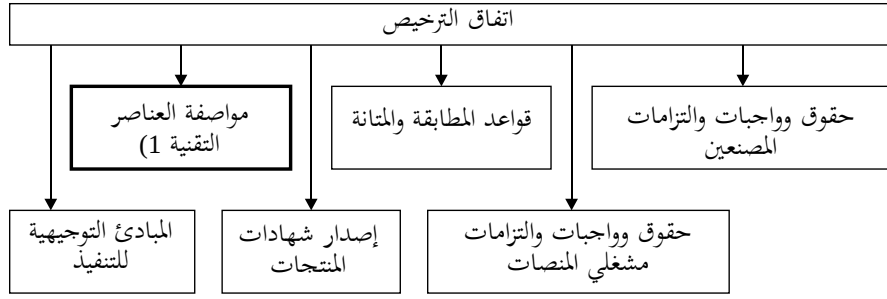
الإطار القانوني/التعاقدي

لا يمكن تحقيق الإدارة المؤمنة للثقة إلا ضمن إطار قانوني وتعاقدي محدد بوضوح يشكل فيه اتفاق الترخيص (LA) العنصر الأساسي. وتمنح سلطة الاستوثاق (TA) اتفاقات الترخيص لأي شخص يسعى إلى تنفيذ المواصفة (المواصفات)، من مصنعي المعدات CPE وبائعي الأنظمة CA/DRM ومصنعي الرقاقات وموردي التكنولوجيات الأخرى ومشغلي المنصات وغيرهم.

ومن ثم، فإن اتفاق الترخيص هو الصك الأساسي الذي يتعين على سلطة الاستوثاق بموجبه إعداد ورعاية وإتاحة طريقة مؤمنة وسهلة للسوق الأفقية لاستقبال وتشغيل جميع المفاتيح والمواد والمعلومات الأخرى ذات الصلة بالأمن عند توصيل معدات CPE بموردين، حسب الاختيار، طالما كانت مطابقة لقواعد الاستعمال المطلوبة. وبالمثل، يمكن إطار اتفاق الترخيص السلطة TA من توفير الرعاية المثلى لعملية إبطال جميع المواد الأمنية عند قيام المورد بفصل مستهلك ما، ما دام الأمر ممكناً من الناحيتين التقنية والاقتصادية.

ويمكن اتفاق الترخيص من التطبيق المنسق والمتسق للعناصر الأخرى للإطار التعاقدي مثل المواصفة التقنية وقواعد المطابقة والمثانة والالتزامات & الواجبات والاختبارات & منح الشهادات والمبادئ التوجيهية الخاصة بالتنفيذ، وما إلى ذلك.

ويبين الشكل 2.I مكونات اتفاق الترخيص.



J.1011(16)_F12

الشكل 2.I - مكونات اتفاق الترخيص

سيتم وضع هذه المواصفات في ETSI ISG ECI كمواصفات مجموعات.

بيليوغرافيا

- [b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006) | ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems*.
- [b-CENELEC EN 50221] CENELEC EN 50221 (1997), *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications*.
- [b-CI Plus Specification] CI Plus Specification (V1.3.1) (2011), *Content Security Extensions to the Common Interface*.
- [b-ETSI EN 300 468] ETSI EN 300 468 V1.13.1 (2012), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*.
- [b-ETSI ISG ECI] ETSI ISG ECI White Paper (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*.
www.etsi.org/deliver/etsi.../ECI/.../gs_ECI00101v010101p.pdf
- [b-ETSI TS 101 699] ETSI TS 101 699 V1.1.1 (1999), *Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification*
<http://webstore.ansi.org/RecordDetail.aspx?sku=ETSI+TS+101+699-v1.1.1-1999-11>
- [b-ETSI TS 103 162] ETSI TS 103 162 V1.1.1 (2010), *Access, Terminals, Transmission and Multiplexing (ATM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification*.
- [b-ETSI TS 103 205] ETSI TS 103 205 V1.1.1 (2014), *Digital Video Broadcasting (DVB); Extensions to the CI PlusTM Specification*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريف 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 المطراية للخدمات البرقية
السلسلة T	المطارييف 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 بروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات