Union internationale des télécommunications

UIT-T J.1010

(09/2016)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Accès conditionnel et protection – Solutions d'accès conditionnel et de gestion des droits numériques intégrées interchangeables

Interface commune intégrée (ECI) pour les solutions CA/DRM interchangeables; Cas d'utilisation et exigences

Recommandation UIT-T J.1010

Recommandation UIT-T J.1010

Interface commune intégrée (ECI) pour les solutions CA/DRM interchangeables; Cas d'utilisation et exigences

Résumé

La Recommandation UIT-T J.1010 spécifie des cas d'utilisation et des exigences pour les solutions CA/DRM intégrées et interchangeables, qui permettent aux équipements CPE pouvant recevoir des contenus de radiodiffusion et large bande de télécharger des clients CA/DRM dans un environnement sécurisé. Grâce au service permettant de télécharger plusieurs systèmes CA/DRM, les consommateurs autorisés peuvent consommer des contenus de radiodiffusion et large bande contrôlés par des systèmes DRM et/ou CAS, même s'ils ne disposent pas dans leur équipement CPE du client CA/DRM requis pour les contenus, car ils peuvent télécharger ce client depuis une source de confiance dans divers types d'équipements CPE, tels que des boîtiers-décodeurs, des téléviseurs intelligents, des ordinateurs personnels, des smartphones et/ou des tablettes intelligentes.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T J.1010	2016-09-02	9	11.1002/1000/12772

Mots clés

CA/DRM, interface commune intégrée interchangeable équipement, CPE de particulier.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
3	Définitions	1
3.1	Termes définis ailleurs	1
3.2	Termes définis dans la présente Recommandation	1
4	Abréviations et acronymes	2
5	Conventions	2
6	Exigences relatives aux solutions CA/DRM intégrées et interchangeables	3
6.1	Généralités	3
6.2	Exigences générales	5
6.3	Exigences relatives à la polyvalence	5
6.4	Exigences relatives aux aspects pratiques	6
6.5	Exigences relatives au changement de client ECI	6
6.6	Exigences relatives à la sécurité des systèmes ECI	6
Annexe A – Cas d'utilisation		8
A.1	Cas d'utilisation 1	8
A.2	Cas d'utilisation 2	9
A.3	Cas d'utilisation 3	9
A.4	Cas d'utilisation 4 (tiers de confiance (TTP))	10

Introduction

La protection des services et des contenus grâce à l'accès conditionnel (CA) et à la gestion des droits numériques (DRM) est essentielle dans le domaine en plein essor de la radiodiffusion et de la diffusion large bande numériques, qui comprend les contenus, les services, les réseaux et les équipements des locaux d'abonné (CPE), si l'on veut protéger le modèle économique des propriétaires des contenus, des opérateurs de réseau et des opérateurs de télévision à péage. Alors que sur le plan de la conception, l'accès conditionnel concerne les mécanismes permettant d'accéder à un contenu protégé distribué par un fournisseur de services sur un réseau, la gestion DRM décrit, au départ, le type et l'étendue des droits d'utilisation, en fonction du contrat souscrit par l'abonné.

Les opérateurs de télévision à péage ont mis en place des plates-formes télévisuelles numériques, qui appliquent des normes pour les fonctions de base, avec des extensions qui sont des éléments propriétaires. La plupart des systèmes CA et DRM utilisés pour la radiodiffusion numérique classique, la TVIP et les nouveaux services OTT captent l'équipement CPE en l'attachant à des éléments de sécurité propriétaires. De ce fait, un équipement CPE configuré pour une utilisation dans un réseau ou une plate-forme A ne peut pas être utilisé dans un réseau ou une plate-forme B et inversement. Par conséquent, le marché de l'électronique grand public (CE) pour la télévision numérique reste fragmenté, les spécifications variant non seulement d'un pays à l'autre, mais aussi d'une plate-forme à l'autre. Les modules CA/DRM séparables n'offrent qu'une solution partielle: les modules sont toujours propres au système CA/DRM, ils ne sont pas bon marché et ils sont utilisés avant tout pour la télévision par câble ou par satellite et ne peuvent pas être utilisés avec des équipements modernes, comme les tablettes, faute d'interfaces physiques adaptées.

Les solutions actuellement mises en oeuvre, qu'il s'agisse de matériels intégrés ou séparables, ont des effets de "verrouillage", ce qui réduit considérablement la liberté de nombreux acteurs des marchés des contenus multimédias numériques. Les avancées technologiques permettent de mettre au point des solutions CA/DRM logicielles innovantes. Parce qu'elles offrent une interopérabilité maximale tout en maintenant un niveau de sécurité élevé, ces solutions devraient répondre aux futures demandes sur le marché, permettre l'arrivée de nouvelles entreprises et offrir un choix plus large aux consommateurs.

Il est dans l'intérêt des consommateurs de pouvoir continuer à utiliser les équipements CPE qu'ils possèdent déjà, par exemple après un déménagement ou un changement de fournisseur de réseau, ou même de pouvoir utiliser des dispositifs permettant d'accéder aux services de différents portails vidéo commerciaux. Cet objectif ne peut être atteint qu'en assurant l'interopérabilité des équipements CPE en matière d'accès conditionnel et de gestion des droits numériques, sur la base d'une architecture de sécurité appropriée. Ce n'est qu'en garantissant la possibilité d'interchanger les systèmes CA et DRM de manière simple pour le consommateur et en fonction du contexte que l'on pourra éviter la poursuite de la fragmentation du marché des équipements CPE et encourager la concurrence.

Recommandation UIT-T J.1010

Interface commune intégrée (ECI) pour les solutions CA/DRM interchangeables; Cas d'utilisation et exigences

1 Domaine d'application

La présente Recommandation porte sur un ensemble d'exigences de base pour une interface commune intégrée et interchangeable permettant de télécharger sur l'équipement CPE tout système CA/DRM nécessaire. Le processus de téléchargement se déroule dans un environnement sécurisé et permet de consommer des contenus protégés fournis via des connexions de radiodiffusion et/ou large bande avec différents types d'équipements terminaux conformément aux droits acquis par l'utilisateur final concernant les contenus. La présente Recommandation fait partie d'une série de Recommandations qui spécifient l'ensemble de l'écosystème ECI.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation. Les documents ci-après cités en référence sont nécessaires pour l'application du présent document.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1:2014, *Embedded Common Interface (ECI) 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 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 interface commune intégrée (ECI): architecture et système à spécifier dans le cadre du groupe ETSI ISG "Embedded CI", qui permettent de créer et de mettre en oeuvre des clients ECI logiciels interchangeables dans l'équipement de locaux d'abonnés (CPE) et assurent ainsi l'interopérabilité des dispositifs CPE en ce qui concerne l'interface ECI.

3.2.2 client d'interface commune intégrée (client ECI): mise en oeuvre d'un client CA/DRM qui est conforme aux spécifications planifiées d'interface commune intégrée. On notera que c'est le module logiciel d'un équipement CPE qui fournit tous les moyens permettant de recevoir, de manière protégée, les crédits et les droits d'un consommateur concernant le contenu distribué par un distributeur de contenu ou un opérateur et de commander l'exécution de ces crédits et droits. Il reçoit en outre les conditions selon lesquelles un droit ou un crédit peut être utilisé par le

consommateur et les clés permettant de déchiffrer les différents messages et contenus. Un client ECI peut avoir une carte à puce associée.

3.2.3 hôte d'interface commune intégrée (ECI): système matériel et logiciel d'un équipement CPE, qui couvre les fonctionnalités liées à l'interface ECI et comporte des interfaces avec un client ECI. On notera que l'hôte ECI est une partie du micrologiciel de l'équipement CPE.

3.2.4 contenus protégés: tous types de médias protégés, en particulier les contenus audio/vidéo et les métadonnées associées, fournis à l'application client par des modes de fourniture linéaires ou non linéaires.

3.2.5 conteneur logiciel: ensemble d'interfaces logicielles avec l'hôte et le client, qui sépare strictement le client CA/DRM de l'hôte. L'allocation des ressources aux interfaces permet d'assurer l'interchangeabilité des clients CA/DRM.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AES norme de cryptage évoluée (*advanced encryption standard*)

CA accès conditionnel (*conditional access*)

CA/DRM accès conditionnel/gestion des droits numériques (*conditional access/digital rights management*)

CE électronique grand public (*consumer electronics*)

CPE équipement des locaux d'abonné (*customer premises equipment*)

CSA algorithme de brouillage commun (*common scrambling algorithm*)

DECE écosystème de contenus de divertissement numériques (*digital entertainment content ecosystem*)

DRM gestion des droits numériques (*digital rights management*)

DVB radiodiffusion vidéonumérique (*digital video broadcasting*)

ECI interface commune intégrée (*embedded common interface*)

IP protocole Internet (*Internet protocol*)

OMA accès mobile ouvert (*open mobile access*)

OTT fourniture de services audio et vidéo par Internet en utilisant les structures existantes installées par un autre acteur (*over the top*)

PVR enregistreur vidéo personnel (*personal video recorder*)

TTP tiers de confiance (*trusted third party*)

TVIP télévision utilisant le protocole Internet

URI informations relatives aux droits d'utilisation (*usage rights information*)

VM machine virtuelle (*virtual machine*)

5 Conventions

Dans la présente Recommandation:

L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "il est interdit" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "peut, à titre d'option" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en oeuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans le corps du présent document et dans ses annexes, on trouve parfois les expressions *doit, ne doit pas, devrait* et *peut*. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions *il est obligatoire, il est interdit,* il *est recommandé* et *peut, à titre d'option*. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données *à titre d'information*, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Exigences relatives aux solutions CA/DRM intégrées et interchangeables

6.1 Généralités

La spécification de groupe (GS) de l'ETSI sur les exigences de base relative à l'**interface ECI**, qui font l'objet de la présente Recommandation, est un élément d'un produit livrable en plusieurs parties spécifiant une architecture pour des systèmes CA/DRM intégrés et interchangeables, fondés sur les logiciels et à vocation générale, qui offriraient la solution la mieux adaptée et la plus pérenne pour résoudre le problème de la fragmentation du marché et permettre l'interopérabilité. L'approche envisagée en matière de sécurité des contenus présente les grands avantages suivants:

- souplesse et modularité grâce à une mise en oeuvre fondée sur des logiciels;
- interchangeabilité qui favorise une solution pérenne et permet l'innovation;
- possibilité d'application aux contenus distribués via la radiodiffusion et la diffusion large bande, y compris les services OTT;
- prise en charge d'un environnement multi-écrans;
- stimulation du marché pour les opérateurs de plates-formes, les fournisseurs de réseaux/services et les consommateurs en évitant le phénomène de "verrouillage";
- spécification d'un écosystème ouvert favorisant le développement du marché.

L'objectif avec le système **ECI** est de disposer de systèmes CA et DRM interchangeables dans les équipements CPE, à tous les niveaux et sur tous les aspects pertinents, au coût le plus bas possible pour les consommateurs, tout en imposant le moins de restrictions possibles aux fabricants de systèmes CA ou DRM en ce qui concerne la conception de leurs produits cibles pour le marché de la télévision à péage. Par conséquent, l'interface ECI a notamment les fonctionnalités suivantes:

- Conteneur logiciel pour le noyau AC où DRM (ci-après appelé **client ECI**) avec:
  - des interfaces normalisées avec toutes les fonctionnalités pertinentes de l'équipement CPE;
  - une **machine virtuelle (VM)** normalisée sur laquelle fonctionner.
- Prise en charge de systèmes sans carte intelligente, mais aussi utilisation dans des systèmes à cartes intelligentes.
- Inclusion d'une multitude de conteneurs logiciels de ce type dans un équipement CPE, chaque conteneur fonctionnant sur sa propre instance de **machine virtuelle**.

- Installation du **client ECI** indépendamment des autres logiciels CPE grâce à un concept de chargeur sécurisé et normalisé.
- **Sécurité évoluée**, également appelée sécurité à jeu de puces, pour prendre en charge la protection des contenus et empêcher l'accès non autorisé à des contenus.
- Méthodes permettant à l'utilisateur de découvrir le bon **client ECI** à télécharger.
- Méthodes permettant de révoquer (en totalité ou en partie) les fonctionnalités du **client ECI** et les fonctionnalités de l'équipement CPE.
- Convient pour la radiodiffusion numérique classique, la TVIP ou les systèmes OTT modernes.

Bien que l'interface ECI présente certaines similitudes avec des solutions déjà déployées, il existe d'importantes différences:

1) Le module se situe dans le logiciel, et non plus dans le matériel. Le fait de changer de système CA ou DRM n'entraîne donc aucun coût pour les consommateurs.
2) Plusieurs **clients ECI** parallèles peuvent être mis en oeuvre dans un seul et même équipement CPE, sans que cela entraîne de coûts supplémentaires.
3) Ces clients peuvent fonctionner simultanément sur le même équipement.

Ces propriétés rendent les composants CA ou DRM beaucoup plus faciles à échanger, de sorte que l'utilisateur final peut changer d'opérateur ou recevoir des services en provenance de différents opérateurs sans avoir à échanger des modules coûteux.

Les différentes parties qui, ensemble, constituent le produit livrable complet, sont un groupe de spécifications, comprenant une Spécification de groupe sur les cas d'utilisation et les exigences et des spécifications sous-jacentes associées:

Partie 1: Architecture, définitions et vue d'ensemble [ETSI GS ECI 001-1]

Partie 2: Cas d'utilisation et exigences [ETSI GS ECI 001-2]

Partie 3: Conteneur CA/DRM: chargeur, interfaces et révocation [b-ETSI GS ECI 001-3]

Partie 4: Machine virtuelle (VM) [b-ETSI GS ECI 001-4]

Partie 5: Système de sécurité évoluée [b-ETSI GS ECI 001-5]

Partie 6: Environnement de confiance [b-ETSI GS ECI 001-6]

Partie 7: Exigences étendues [b-ETSI GS ECI 001-7]

qui, ensemble, décrivent une solution qui permet de remplacer les **clients ECI** à tout moment, simplement en téléchargeant les **clients ECI** demandés par un client final. Les **clients ECI** sont installés dans un conteneur logiciel type dans l'équipement CPE par un chargeur séparé, avec des algorithmes et des clés de sécurité distincts qui protègent les **clients ECI** contre les attaques visant l'intégrité ou les attaques par substitution, indépendamment de tous les autres logiciels installés dans l'équipement CPE. Les interfaces entre le conteneur et l'équipement CPE sont génériques et définies dans la norme GS ECI 001-3 [b-ETSI GS ECI 001-3], et permettent au **client ECI** d'interagir avec les différentes fonctions dans l'équipement CPE et ailleurs.

Les **clients ECI** fonctionnent sur une instance de machine virtuelle qui est définie dans la norme GS ECI 001-4 [b-ETSI GS ECI 001-4].

La norme GS ECI 001-5 [b-ETSI GS ECI 001-5] spécifie un mécanisme de sécurité évoluée qui protège la clé d'accès aux contenus pendant son trajet dans le mécanisme de déchiffrement des contenus de la puce du processeur de l'équipement CPE.

La présente Recommandation décrit les cas d'utilisation et les exigences devant servir de base à la mise en oeuvre de systèmes CA/DRM interopérables dans les équipements CPE.

La spécification **ECI** s'applique uniquement à la réception et au traitement subséquent des contenus qui sont contrôlés par un système d'accès conditionnel et/ou de gestion des droits numériques et a été embrouillé par le fournisseur de services. La présente Recommandation ne couvre pas les contenus qui ne sont pas contrôlés par un système d'accès conditionnel et/ou DRM.

La Spécification de groupe **ECI** est destinée à être utilisée en association avec un cadre contractuel (accord de licence), des règles de conformité et de robustesse et un processus de certification approprié (voir note), sous le contrôle d'une **autorité de confiance** (voir la norme GS ECI 001-6 [b-ETSI GS ECI 001-6]).

La sécurité de bout en bout d'un système CA/DRM conforme aux spécifications ECI ne dépend pas uniquement des spécifications techniques. La technologie ECI constitue seulement un élément d'un écosystème conforme aux spécifications ECI (voir la norme ECI, GS ECI 001-1 [ETSI GS ECI 001-1]), qui doit être établi par une autorité de confiance, en tenant également compte d'un cadre juridique, de la certification des dispositifs et d'autres aspects. Les exigences suivantes sont basées sur les cas d'utilisation présentés dans l'Annexe A.

6.2 Exigences générales

[R 01] L'**interface ECI** doit être applicable à tous les services de radiodiffusion, services large bande et services hybrides (c'est-à-dire, qui associent la radiodiffusion et la diffusion large bande), et prendre en charge la fourniture de contenus protégés via tous types de réseaux d'accès appropriés à destination de tout type de dispositif concerné.

[R 02] L'**interface ECI** doit définir un **conteneur logiciel** pour le logiciel noyau ECI et les fonctionnalités logicielles CA/DRM étroitement liées, clairement séparé des autres éléments d'un équipement CPE.

[R 03] L'**interface ECI** doit offrir des fonctionnalités de sécurité évoluée comparables à celles dont les systèmes CA/DRM de technologie récente permettent de disposer.

[R 04] L'**interface ECI** doit permettre de concevoir des mises en oeuvre sécurisées pour les systèmes CA/DRM, dont l'utilisation et la maintenance puissent durer pendant une longue période, dans tous les cas pendant au moins cinq ans.

6.3 Exigences relatives à la polyvalence

[R 05] L'**interface ECI** doit prendre en charge la mise en oeuvre de plus d'un client CA/DRM dans un équipement CPE qui offre une solution pour le traitement simultané d'au moins deux événements concernant des **contenus protégés**.

[R 06] L'architecture doit permettre de faire en sorte que différents clients ECI dans un équipement CPE puissent se reconnaître, établir entre eux une relation de confiance et se transférer l'un l'autre des contenus et les **informations URI** associées.

[R 07] L'architecture doit permettre de faire en sorte que les **clients ECI** puissent établir une relation de confiance avec l'**hôte ECI** auquel ils sont connectés et transférer des informations **URI** à l'**hôte ECI** d'une manière sécurisée.

[R 08] L'**interface ECI** doit permettre d'assurer la conformité avec la législation et la réglementation nationales, par exemple la protection des données confidentielles et la protection des mineurs.

[R 09] L'**interface ECI** doit prendre en charge l'exportation de **contenus protégés** obtenus de manière conforme à la législation vers d'autres terminaux (y compris des terminaux mobiles) à l'intérieur d'un domaine ou réseau domestique. Cela suppose que l'architecture contienne les interfaces nécessaires pour qu'un client ECI dans un équipement CPE soit capable de communiquer avec un autre client ECI dans le même dispositif. Cette opération ne doit être possible que sous réserve du respect des droits d'utilisation émis par les propriétaires respectifs des contenus.

[R 10] Un client ECI peut être mis en oeuvre de façon à pouvoir exporter des **contenus protégés** vers un dispositif non conforme aux spécifications ECI. Cette opération ne doit être possible que sous réserve du respect des droits d'utilisation émis par les propriétaires respectifs des contenus.

6.4 Exigences relatives aux aspects pratiques

[R 11] L'**interface ECI** doit fournir des interfaces API pour la mise en œuvre d'interfaces utilisateur offrant une grande commodité d'utilisation et permettant d'exécuter facilement les interactions d'utilisateur.

[R 12] L'**interface ECI** ne devrait pas ajouter de délai perceptible par rapport aux solutions CA/DRM comparables, même si les deux voies (services) concernées utilisent des systèmes CA/DRM différents. On notera que l'on ne suppose pas qu'il soit nécessaire de changer de système CA/DRM lors d'un changement de voie (service) régulier.

[R 13] Toutes les activités liées à l'interface ECI (par exemple, fonctionnement normal ou téléchargement d'un **client ECI**) ne devraient pas avoir d'**incidence** perceptible sur l'expérience utilisateur et la qualité de fonctionnement.

6.5 Exigences relatives au changement de client ECI

[R 14] L'**interface ECI** doit permettre d'opter pour un nouveau fournisseur de services sans avoir besoin de l'accord du fabricant de systèmes CA/DRM, du fabricant de dispositifs, de la plate-forme ou de l'opérateur de services.

[R 15] En cas de changement de client ECI, l'interruption de services doit être limitée au minimum.

[R 16] Après un changement de **client ECI**, l'utilisation de **contenus protégés** (par exemple, des contenus PVR embrouillés) obtenus conformément à la législation avant le changement doit être possible sans que des opérations complexes soient nécessaires de la part de l'utilisateur.

[R 17] L'**interface ECI** ne doit pas restreindre d'une manière excessive les possibilités dont disposent les fabricants de systèmes CA/DRM pour créer différents **clients ECI** interopérables/échangeables en fonction des besoins du marché.

6.6 Exigences relatives à la sécurité des systèmes ECI

[R 18] Le **client ECI** d'un équipement CPE doit pouvoir être téléchargé, installé et échangé d'une manière sécurisée et normalisée. Le téléchargement et l'installation du **client ECI** doivent se faire uniquement au moyen de solutions normalisées.

[R 19] L'équipement CPE doit comporter un **conteneur logiciel**, qui doit fournir une couche d'abstraction unifiée à tout client ECI. On notera que la couche d'abstraction unifiée est ce qu'une machine virtuelle fournirait au client ECI.

[R 20] Les **clients ECI** et le système **hôte** doivent pouvoir déclarer et prouver à tout moment qu'ils sont dignes de confiance.

[R 21] L'**interface ECI** doit prendre en charge l'élaboration et l'établissement d'une **autorité de confiance**.

[R 22] L'**interface ECI** ne doit pas dépendre de la présence d'un matériel (composant) ou d'un système d'exploitation en particulier. Cette exigence n'est généralement pas incompatible avec des fonctionnalités de sécurité avancée, à condition que les spécifications de ces fonctionnalités soient librement accessibles et que ces fonctionnalités elles-mêmes soient conformes aux architectures de sécurité actuellement utilisées par les fabricants de puces pour équipement CPE concernés. On notera que les systèmes décrits dans un document en libre accès ne sont pas considérés comme des matériels particuliers.

[R 23] Le **système ECI** doit permettre la migration des systèmes CA/DRM existants compatibles avec les normes DVB/ETSI vers ce nouveau **système ECI**. On notera que cela suppose qu'un

opérateur puisse prendre en charge avec son système CA/DRM existant à la fois les dispositifs existants et les nouveaux dispositifs conformes aux spécifications ECI qui exécutent un client ECI compatible avec le système CA/DRM existant.

[R 24] L'**interface ECI** doit comporter des éléments permettant d'assurer d'une manière rétrocompatible le développement ultérieur des **interfaces ECI** et des mises en oeuvre ECI. Les mises en oeuvre ECI existantes doivent pouvoir appliquer les droits d'utilisation introduits par des extensions ultérieures des fonctionnalités de l'équipement CPE ou du client ECI.

[R 25] L'**interface ECI** doit prendre en charge les mises en oeuvre de système indépendamment du fait que des cartes intelligentes soient utilisées ou non comme dispositifs de sécurité, et doit fournir des ressources pour les deux types de solution.

[R 26] L'**interface ECI** doit assurer les fonctionnalités nécessaires pour tous les niveaux de sécurité des contenus requis pour les différentes applications des systèmes CA/DRM. Elle doit être applicable aux marchés grand public et à toute la gamme des produits commercialisés, du bas de gamme au haut de gamme.

[R 27] L'**interface ECI** ne doit nécessiter le remplacement d'aucun composant matériel en cas de changement de client ECI. Toutefois, en ce qui concerne l'application de cette exigence, le fait de changer une carte intelligente sur un système CA/DRM utilisant ce type de dispositif n'est généralement pas considéré comme le remplacement d'un composant matériel.

[R 28] L'**interface ECI** ne doit pas nécessiter une quantité de ressources du dispositif CPE (puissance de traitement, mémoire, etc.) beaucoup plus grande que les systèmes CA/DRM intégrés comparables actuellement disponibles, et la mise en oeuvre de l'architecture de système ne doit pas entraîner de coûts plus élevés/supplémentaires importants.

[R 29] L'**interface ECI** doit au minimum prendre en charge les systèmes d'embrouillage DVB CSA et AES (norme de cryptage évoluée) et l'hôte doit au minimum prendre en charge le flux de transport MPEG (norme ISO/CEI 13818-1 [b-UIT-T H.222.0]) et le format ISOBMFF (norme ISO/CEI 14496-12 [b-ISO/CEI 14496-12:2012], y compris l'Amendement 3 et la conformité avec la signalisation définie via le système d'encryptage commun décrit dans la norme ISO/CEI 23001-7 [b-ISO/CEI 23001-7:2011], mais avec éventuellement un algorithme de cryptage différent). On notera que la mise en oeuvre de cette exigence serait compatible avec les systèmes DRM utilisés dans l'écosystème de contenus de divertissement numériques (DECE) actuel et fournirait aux autres systèmes DRM un format normalisé à adopter pour la prise en charge de l'**interface ECI**.

[R 30] L'**interface ECI** doit prendre en charge un large éventail de droits d'utilisateur en fournissant les fonctionnalités appropriées pour l'interface entre le conteneur ECI et l'hôte.

[R 31] L'**interface ECI** doit être capable de décrire des droits d'utilisation et des fonctionnalités d'utilisation à un client ECI ou d'un client ECI à un autre.

[R 32] L'**interface ECI** doit fournir une voie de communication sécurisée entre les clients ECI, soit sur le même dispositif soit sur des dispositifs différents.

Annexe A

Cas d'utilisation

(Cette Annexe fait partie intégrante de la présente Recommandation.)

Les cas d'utilisation présentés dans l'Annexe A ne sont pas exhaustifs.

A.1 Cas d'utilisation 1

Dans l'environnement de la télévision numérique commerciale, le besoin de changer le système CA/DRM des équipements CPE peut intervenir pour différentes raisons.

- Un fournisseur de contenus medias numériques peut décider de changer le système CA/DRM des équipements CPE de ses clients, par exemple pour les motifs suivants:
  - Différentes raisons d'ordre technique ou commercial, telles que des exigences liées à une amélioration des fonctionnalités CA/DRM, à des niveaux de sécurité plus élevés ou à une meilleure qualité de fonctionnement du système, ou en cas de piratage de grande ampleur du système existant.
  - Acquisition, dans un certain réseau, de nouveaux clients qui utilisaient auparavant les services d'un concurrent.
- Un opérateur de plate-forme peut décider de changer le système CA/DRM des équipements CPE de sa plate-forme, par exemple pour les motifs suivants:
  - Différentes raisons d'ordre technique ou commercial, telles que des exigences liées à une amélioration des fonctionnalités CA/DRM, à des niveaux de sécurité plus élevés ou à une meilleure qualité de fonctionnement du système, ou en cas de piratage de grande ampleur du système existant.
  - Harmonisation de technologies après l'acquisition d'un réseau.
- Un fabricant de systèmes CA/DRM acquiert un nouveau client qui exploite une plate-forme sur laquelle un concurrent avait déjà établi son système CA, ou un fabricant de systèmes CA/DRM prend le contrôle d'un autre fabricant de systèmes CA/DRM et souhaite harmoniser les technologies de sécurité.
- Un utilisateur final a acheté un équipement CPE dans un magasin quelconque et le connecte au réseau d'un fournisseur de réseau d'accès A. Un ou plusieurs fournisseurs de services offrent leurs services sur ce réseau. L'utilisateur final peut choisir n'importe lequel de ces services et télécharger le système CA/DRM qui lui correspond, s'il est enregistré (y compris pour ce qui est de l'authentification et de l'autorisation) auprès du fournisseur de services correspondant.

  Après quelque temps, le même utilisateur final décide de se connecter au réseau d'un fournisseur de réseau d'accès B. Il connecte son équipement CPE à ce réseau. Si son équipement CPE prend en charge les technologies de réception nécessaires (par exemple, DVB-C/C2, -S/S2, -T/T2, Ethernet, xDSL), étant donné qu'un ou plusieurs fournisseurs de services offrent leurs services sur ce réseau, l'utilisateur final peut choisir n'importe lequel de ces services et échanger les systèmes CA/DRM en conséquence, s'il est enregistré (y compris pour ce qui est de l'authentification et de l'autorisation) auprès du fournisseur de services correspondant.

- Un fabricant d'électronique grand public souhaite introduire sur le marché de détail des équipements CPE prenant en charge à la fois la télévision gratuite et la télévision à péage. Il est toutefois possible, avec l'accord de l'utilisateur final, d'adapter les équipements CPE de sorte qu'ils puissent être utilisés avec des services de télévision à péage particuliers, à l'aide d'une mise à niveau de logiciel.

A.2 Cas d'utilisation 2

A l'heure actuelle, s'il est nécessaire de changer (pour quelque raison que ce soit) le système CA d'une base d'équipements CPE existante d'une plate-forme CA opérationnelle, il y a toujours quatre acteurs concernés:

- Le fournisseur d'accès conditionnel existant.
- L'opérateur de la plate-forme ou le fournisseur de contenus médias numériques.
- Le fabricant d'équipements CPE.
- Le nouveau fournisseur d'accès conditionnel.

Le fournisseur d'accès conditionnel existant doit fournir au nouveau fournisseur les informations techniques dont celui-ci a besoin pour accéder à la base d'équipements CPE existante, ainsi qu'une licence pour l'utilisation de certains composants matériels, protocoles ou éléments logiciels utilisés dans ces équipements CPE. Dans tous les cas, le nouveau fournisseur d'accès conditionnel doit adapter son système CA aux fonctionnalités, aux limites de matériel/logiciel et aux protocoles des équipements CPE sur le terrain. Les fabricants d'équipements CPE doivent intégrer le nouveau système CA dans le logiciel des différents équipements CPE installés. Dans le cas le plus défavorable, le changement de système CA/DRM peut ne même pas constituer une solution viable sur le plan technique ou commercial. Il convient de remédier à cette situation afin d'assurer une plus grande interopérabilité.

Etant donné que les modules de sécurité propriétaires font aujourd'hui partie intégrante de la plupart des systèmes CA de technologie récente, les équipements CPE sont fabriqués principalement pour des systèmes CA dédiés. Il peut en résulter une limitation du niveau de sécurité qu'un nouveau système CA peut assurer pour des équipements CPE sur le terrain après un changement de système CA. Il convient de remédier à cette situation de manière à faire en sorte que tout renforcement de la sécurité soit entièrement transférable.

A.3 Cas d'utilisation 3

Le système ECI doit prendre en charge les applications servant uniquement à utiliser des contenus, mais aussi la fourniture de **contenus protégés** à des dispositifs secondaires. Deux cas d'utilisation peuvent se présenter concernant la prise en charge d'applications pour dispositifs secondaires:

- Application centralisée: l'équipement CPE de type passerelle conforme aux spécifications ECI transmet des informations relatives aux droits d'utilisation (URI) et des contenus chiffrés au dispositif secondaire.
- Application décentralisée: l'équipement CPE de type passerelle conforme aux spécifications ECI transmet uniquement des informations URI au dispositif secondaire, qui obtient les contenus cryptés à partir du réseau. On notera qu'il n'y a pas d'exigences pour le système ECI concernant la mise en oeuvre d'un client DRM dans un dispositif secondaire. La transmission de contenus protégés d'une passerelle à un dispositif secondaire nécessite seulement que les deux clients DRM puissent communiquer entre eux d'une manière sécurisée et que le propriétaire des contenus prenne en charge le système DRM mis en oeuvre.

A.4 Cas d'utilisation 4 (tiers de confiance (TTP))

A l'heure actuelle, les identifiants uniques ou certificats requis sont intégrés dans l'équipement CPE selon une méthode exclusive, définie par le fournisseur du système CA/DRM. Cette solution n'est pas appropriée du point de vue de l'interopérabilité, étant donné qu'il est très peu probable que les fabricants divulguent les mécanismes d'accès à leurs identifiants uniques ou à leurs certificats. Par exemple, le consortium CI-Plus a démontré qu'il était possible de transférer le traitement sécurisé des certificats à un "tiers de confiance". Des solutions similaires seront nécessaires pour assurer l'interopérabilité des systèmes CA/DRM.

Bibliographie

[b-ITU-T H.222.0] Recommandation UIT-T H.222.0 (2006) | ISO/IEC 13818-1 (2007), *Technologies de l'information – Codage générique des images animées et du son associé: systèmes*.

[b-ETSI GS ECI 001-3] ETSI GS ECI 001-3, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation*.

[b-ETSI GS ECI 001-4] ETSI GS ECI 001-4, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 4: The Virtual Machine*.

[b-ETSI GS ECI 001-5] ETSI GS ECI 001-5, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System*.

[b-ETSI GS ECI 001-6] ETSI GS ECI 001-6, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment*.

[b-ETSI GS ECI 001-7] ETSI GS ECI 001-7, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 7: Extended Requirements*.

[b-ETSI ISG ECI] ETSI ISG ECI White Paper-v1_20 (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*.

[b-ISO/CEI 14496-12] ISO/CEI 14496-12:2012, *Technologies de l'information – Codage des objets audiovisuels – Partie 12: Format ISO de base pour les fichiers médias*.

[b-ISO/CEI 23001-7] ISO/CEI 23001-7:2011, *Technologies de l'information – Technologies des systèmes MPEG – Partie 7: Cryptage commun des fichiers au format de fichier de médias de la base ISO*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2017