Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.1011

(09/2016)

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 pour les solutions CA/DRM interchangeables; Architecture, définitions et vue d'ensemble

Recommandation UIT-T J.1011

Recommandation UIT-T J.1011

Interface commune intégrée pour les solutions CA/DRM interchangeables; Architecture, définitions et vue d'ensemble

Résumé

La Recommandation UIT-T J.1011 spécifie une architecture pour les solutions d'accès conditionnel et de gestion des droits numériques (CA/DRM) intégrées et interchangeables, qui permettent aux équipements de locaux d'abonnés (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 CA, 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 sur 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	UIT-T J.1011	02-09-2016	9	11.1002/1000/12773

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 oeuvre 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 oeuvre 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

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 réseaux 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 télévision utilisant le protocole Internet (TVIP) et les nouveaux services OTT (*over-the-top*) "emprisonnent" l'équipement CPE en le rattachant 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 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 pour l'essentiel pour la télévision par câble ou par satellite et ne peuvent 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 du contenu multimédia numérique. Les avancées technologiques permettent de mettre au point des solutions CA/DRM logicielles innovantes. Parce qu'elles offrent une interopérabilité maximum 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 adaptée. 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.1011

Interface commune intégrée pour les solutions CA/DRM interchangeables; Architecture, définitions et vue d'ensemble

1 Domaine d'application

La présente Recommandation vise à spécifier les entités fonctionnelles d'une architecture 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'équipement terminaux conformément aux droits acquis par l'utilisateur final concernant le contenu. La présente Recommandation fait partie d'une série de Recommandations qui spécifient l'ensemble de l'écosystème de l'interface commune intégrée (ECI).

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. 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.

[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 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 sécurité évoluée: fonction d'un équipement CPE conforme ECI qui fournit des fonctions de sécurité évoluée (matérielles et logicielles) pour un client ECI. Veuillez noter que les caractéristiques détaillées sont spécifiées dans [b-ETSI GS ECI 001-5].

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

3.2.3 client ECI (client d'une interface commune intégrée): mise en oeuvre d'un client CA/DRM qui est conforme aux spécifications d'interface commune intégrée. Veuillez noter 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.

3.2.4 chargeur de client ECI: partie du module logiciel de l'hôte ECI qui permet de télécharger, de vérifier et d'installer un nouveau logiciel client ECI dans un conteneur ECI de l'hôte ECI.

3.2.5 conteneur ECI (conteneur d'interface commune intégrée): concept abstrait qui fournit un environnement isolé comprenant une machine virtuelle et un client ECI unique.

3.2.6 hôte ECI: système matériel et logiciel d'un équipement CPE, qui couvre les fonctionnalités liées à l'interface ECI et comporte des interfaces vers un client ECI. Il est à noter que l'hôte ECI est une partie du micrologiciel d'un équipement CPE. L'hôte ECI est chargé de veiller à ce que chaque conteneur ECI soit isolé, et assure le chargement des clients ECI après authentification.

3.2.7 chargeur de l'hôte ECI: module logiciel qui permet de télécharger, de vérifier et d'installer un (nouveau) logiciel d'hôte ECI dans un équipement CPE. Il est à noter que dans une configuration de chargement à plusieurs étapes, ce terme est utilisé pour désigner toutes les fonctions de chargement essentielles à la sécurité associées au chargement de l'hôte ECI.

3.2.8 autorité de confiance (TA, *trust authority*): organisation régissant toutes les règles et tous les règlements qui s'appliquent aux mises en oeuvre d'une interface ECI. Il est à noter que l'autorité de confiance doit être une entité juridique pour pouvoir régler les réclamations fondées en droit. L'entité de confiance doit être impartiale envers tous les acteurs de l'écosystème des solutions CA/DRM téléchargeables.

3.2.9 tiers de confiance (TTP, *trusted third party*): fournisseur de services techniques qui délivre des certificats et des clés aux fabricants des composants pertinents d'un système ECI sous le contrôle de l'autorité de confiance (TA).

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

CA accès conditionnel (*conditional access*)

CENC chiffrement commun (*common encryption*)

CI interface commune (*common interface*)

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

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

DVB radiodiffusion vidéonumérique (*digital video broadcasting*)

ECI interface commune intégrée (*embedded comon inerface*)

HD haute définition (*high definition*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

iDTV téléviseur numérique intégré (*integrated digital TV*)

IP protocole Internet (*Internet protocol*)

LA accord de licence (*license agreement*)

MPEG Groupe d'experts pour les images animées (*motion picture experts group*)

OS système d'exploitation (*operating system*)

OSD affichage à l'écran (*on-screen display*)

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

PIN numéro personnel d'identification (*personal identification number*)

PVR enregistreur vidéo personnel (*personal video recorder*)

ROM mémoire morte (*read only memory*)

SI information relative au service (*service information*)

STB boîtier-décodeur (*set-top box*)

TA autorité de confiance (*trust authority*)

TTP tiers de confiance (*trusted third party*)

TV télévision

TVIP télévision utilisant le protocole Internet

UI interface d'utilisateur (*user interface*)

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 à la présente Recommandation.

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 à la présente Recommandation.

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 de la présente Recommandation 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 Architecture pour les solutions CA/DRM intégrées et interchangeables

6.1 Généralités

La présente Recommandation cadre, qui décrit l'architecture, les définitions et une vue d'ensemble concernant l'interface ECI est un élément d'une norme en plusieurs parties spécifiant une architecture pour des systèmes CA/DRM intégrés et interchangeables, fondés sur les logiciels et à vocation

générale, qui offrent 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 du contenu 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 plus bas coût possible pour les consommateurs, tout en imposant le moins de restrictions possibles aux fabricants de systèmes CA ou DRM en ce qui concerne l'élaboration de leurs produits cibles pour le marché de la télévision à péage. L'élément central d'une interface ECI consiste à spécifier l'interface entre le client CA/DRM logiciel et le système hôte. 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 vers 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 du contenu grâce aux techniques les plus récentes.
– Dispositions pour mettre à profit les fonctionnalités matérielles de sécurité.
– 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 client CA/DRM se situe dans le logiciel et non plus dans le matériel. Le changement d'un système CA ou DRM n'entraîne 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.

En conséquence, il est possible d'échanger un composant CA ou DRM bien plus facilement, ce qui permet à l'utilisateur final de changer d'opérateur ou d'obtenir des services auprès de différents opérateurs sur son équipement CPE, sans avoir à changer des modules coûteux.

Les différentes parties qui, ensemble, constituent la norme complète sont un groupe de spécifications, comprenant une spécification cadre, avec 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 001-21]
– Partie 3: Conteneur, chargeur, interfaces et révocation pour solutions CA/DRM [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 sécurisé [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 sur 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 [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 [b-ETSI GS ECI 001-4].

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

La présente Recommandation décrit une architecture et donne une vue d'ensemble des spécifications d'interface pertinentes pour 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 ultérieur du contenu qui est contrôlé par un système à accès conditionnel et/ou à gestion des droits numériques et a été embrouillé par le fournisseur de services. La présente Recommandation ne couvre pas le contenu qui n'est pas contrôlé par un système à accès conditionnel et/ou DRM.

La spécification de groupe ECI a pour vocation d'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 ([b-ETSI GS ECI 001-6]). Il est à noter que le travail de normalisation mené par le groupe ISG ECI ne porte pas sur le cadre contractuel (accord de licence), les règles de conformité et de robustesse et le processus de certification approprié.

6.2 Concept technique du système ECI

6.2.1 Considération de base

Associé aux parties 2 à 5 et 7 des spécifications ([ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4], [b-ETSI GS ECI 001-5] et [b-ETSI GS ECI 001-7]), la présente Recommandation spécifie une architecture permettant de télécharger, d'installer, de mettre à jour, de supprimer et de remplacer des clients ECI à tout moment, indépendamment des autres clients ECI fonctionnant sur le même hôte et du logiciel d'exploitation de l'équipement CPE hôte ou des applications fonctionnant sur cet hôte. Un hôte ECI doit être capable de prendre en charge et de fournir l'environnement d'exécution pour au moins deux ou le nombre maximal de clients ECI que ces ressources lui permettent de gérer. Les clients ECI sur un hôte doivent fonctionner en parallèle, en

permettant le déchiffrement ou le rechiffrement simultané de différents flux de contenus fournis par différents opérateurs.

Le concept technique décrit dans la présente Recommandation et spécifié dans [ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] et [b-ETSI GS ECI 001-5] s'applique à la fois aux systèmes de radiodiffusion vidéonumérique à accès conditionnel conformes Multicrypt et aux systèmes DRM conformes CENC (chiffrement commun).

L'équipement CPE héberge un chargeur spécial réservé aux clients ECI, qui a les fonctionnalités de sécurité nécessaires pour protéger l'intégrité et l'authenticité des clients ECI. Ce chargeur peut être appelé et utilisé à tout moment pour télécharger et vérifier un autre client ECI. Ce chargeur ainsi que ses dispositifs de sécurité associés sont spécifiés dans [b-ETSI GS ECI 001-3].

En ce qui concerne ce concept technique, chaque client ECI est installé dans un conteneur logiciel séparé, avec sa propre instance de machine virtuelle (instance VM), qui est spécifiée dans [b-ETSI GS ECI 001-4]. Le conteneur ECI est spécifié uniquement pour la fonctionnalité CA/DRM, présentée dans [b-ETSI GS ECI 001-3]. L'interface avec l'équipement CPE, décrite dans [b-ETSI GS ECI 001-3], permet de demander et d'échanger les données nécessaires pour les différentes fonctions CA/DRM. Ces demandes et échanges de données peuvent avoir lieu entre le client ECI et l'hôte, entre deux clients ECI dans le même hôte ou entre deux clients ECI dans des hôtes différents.

Les dispositifs conçus pour la télévision sont définis comme étant des dispositifs qui comprennent un mécanisme de traitement du flux de transport MPEG-2 à l'intérieur du jeu de puces. L'interface ECI exige que ces jeux de puces mettent en oeuvre des fonctionnalités de sécurité évoluée conformes ECI. La spécification [b-ETSI GS ECI 001-5] spécifie des dispositions pour mettre à profit des mécanismes de sécurité évoluée dans le jeu de puces, par exemple pour protéger la clé associée au contenu pendant son trajet dans le mécanisme de déchiffrement du contenu de la puce du processeur de l'équipement CPE. Ce concept de sécurité évoluée permet à tous les clients ECI qui utilisent le mécanisme, au besoin, de fonctionner simultanément et indépendamment les uns des autres.

Les dispositifs conçus pour d'autres environnements, en particulier les téléviseurs IP et les tablettes, les téléphones intelligents, etc., mettent généralement en oeuvre davantage de fonctionnalités dans les logiciels et assurent des communications IP bidirectionnelles, ce qui permet la prise en charge de nouveaux types spécifiques de mécanismes de renforcement de la sécurité. Etant donné que les jeux de puces utilisés dans ces dispositifs comprennent des éléments matériels pour différentes fonctions de traitement de la sécurité, l'interface ECI exige la mise en oeuvre de fonctionnalités matérielles dédiées de sécurité et de robustesse pour garantir la conformité ECI. Par conséquent, la spécification [b-ETSI GS ECI 001-3] comprend les méthodes permettant au client ECI d'obtenir les paramètres pertinents des capacités et fonctionnalités techniques de l'hôte, si elles présentent un intérêt, y compris la possible prise en charge de la sécurité évoluée comme définie dans [b-ETSI GS ECI 001-5].

Les fonctionnalités de sécurité évoluée sont disponibles simultanément pour tout client ECI actif dans un équipement CPE. Les clients ECI peuvent également être déployés dans des plates-formes dotées de systèmes à accès conditionnel conformes DVB ou de systèmes DRM conformes CENC fonctionnant en mode simulcrypt ou multicrypt, à condition que les extrémités serveurs de ces systèmes soient conformes aux normes d'extrémité DVB/CENC correspondantes.

6.2.2 Vue d'ensemble de l'architecture

L'interface ECI permet aux fournisseurs CA/DRM de mettre en oeuvre des solutions d'accès conditionnel (CA) et de gestion des droits numériques (DRM) dans le domaine d'un client particulier. La Figure 1 montre une configuration de référence qui est entièrement prise en charge par une mise en oeuvre ECI complète.

Pour permettre la prise en charge d'environnements multi-écrans à l'intérieur du domaine du consommateur particulier, les clients ECI à l'intérieur de ce domaine peuvent communiquer entre eux et utiliser un réseau bidirectionnel avec le fournisseur, en fonction de la disponibilité des réseaux

appropriés et des fonctionnalités de prise en charge dans les systèmes CA/DRM et dans leurs clients ECI. On trouvera plus de détails dans [b-ETSI GS ECI 001-3].

Un client ECI peut être mis en oeuvre de telle sorte qu'il soit également capable de jouer le rôle de passerelle vers des clients non conformes ECI. Les éléments de raccordement nécessaires sont par conséquent spécifiés dans [b-ETSI GS ECI 001-5]. Les protocoles et mises en oeuvre spécifiques des clients propriétaires ne relèvent pas des spécifications ECI.

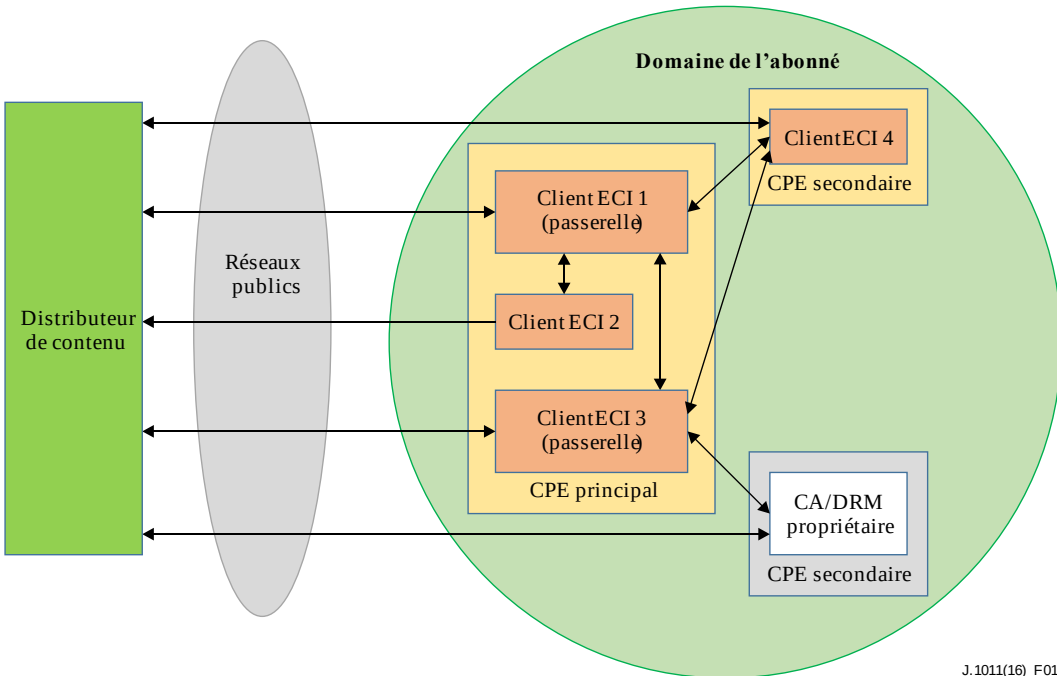


Figure 1 – Clients ECI à l'intérieur d'un domaine client unique

Les spécifications ECI définissent, entre autres choses, l'interface entre un conteneur ECI et l'hôte ECI. La Figure 2 illustre, sous la forme d'un schéma, un équipement CPE avec des conteneurs ECI et les autres fonctions à l'intérieur de l'hôte ECI avec lesquelles les conteneurs ECI communiquent ou peuvent communiquer. Certaines de ces fonctions sont facultatives. Pendant l'installation et le lancement d'un client ECI, l'hôte spécifie les fonctions pertinentes qu'il met à la disposition du client ECI.

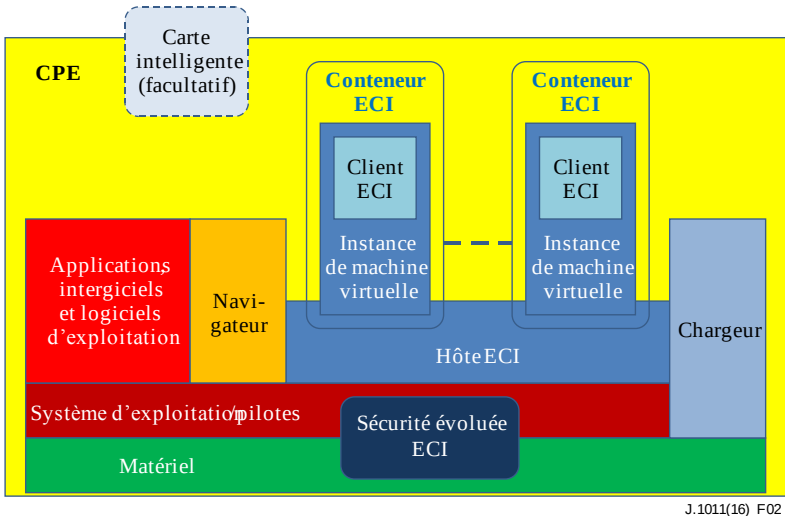


Figure 2 – Représentation d'un équipement CPE avec clients ECI intégrés, ayant chacun leur propre conteneur ECI et leur propre instance de machine virtuelle

Premier point, ce concept repose sur un concept de chargeur hiérarchique (voir la Figure 3) comprenant un chargeur à puce, le chargeur de logiciel d'exploitation et le chargeur de client ECI.

Le chargeur d'hôte ECI permet de charger le logiciel de l'hôte ECI. Il comprend entre autres éléments la machine virtuelle, l'accès aux composants de sécurité évoluée et le chargeur de client ECI. Un hôte ECI peut charger plusieurs clients ECI dans des instances de machine virtuelle séparées, qui fonctionnent de manière indépendante et sont isolées les unes des autres.

Lors du chargement d'un client ECI dans le système, une instance de machine virtuelle est créée, dans laquelle le client ECI est chargé. Cette instance VM sert de bac à sable entre le client ECI et l'hôte. L'interface entre le client ECI et l'instance VM est la principale interface définie par la spécification de groupe. L'interface spécifie en outre le flux d'information/protocole entre de multiples instances d'un client ECI de ce type et vers d'autres fonctionnalités à l'intérieur de l'équipement CPE, comme la sécurité évoluée, l'affichage, etc. Il est à noter que les autres clients ECI ne doivent pas nécessairement être dans le même hôte ECI. Ce protocole d'interface et de communication est spécifié dans [b-ETSI GS ECI 001-3].

L'hôte ECI lui-même dépend de la mise en oeuvre du fabricant.

Il assure l'interface vers le système d'exploitation et vers la couche pilote et fournit toutes les fonctionnalités définies par la spécification d'interface client ECI. L'hôte ECI n'est pas spécifié par l'interface ECI, mais il doit être certifié par l'autorité de confiance, afin de garantir la conformité à la spécification d'interface client ECI.

6.2.3 Fonctionnalités obligatoires des dispositifs conformes ECI

L'interface ECI permet de nombreux scénarios d'utilisation (voir la Figure 1). Par conséquent, elle doit pouvoir fonctionner avec un large éventail de dispositifs, par exemple des téléviseurs numériques intégrés, des décodeurs, des enregistreurs vidéo personnels, des téléviseurs IP, des tablettes, des téléphones intelligents, etc. Les capacités de ces dispositifs varient, alors que l'interface ECI fournit un cadre de sécurité harmonisé. L'interface ECI fait une distinction entre les dispositifs conçus pour la télévision et les dispositifs conçus pour d'autres environnements, notamment les téléviseurs IP et les tablettes.

Les dispositifs conçus pour la télévision sont définis comme étant des dispositifs qui comprennent un mécanisme de traitement du flux de transport MPEG-2 à l'intérieur du jeu de puces. L'interface ECI exige que ces jeux de puces mettent en oeuvre des fonctionnalités de sécurité évoluée conformes ECI. Les équipements CPE conformes ECI conçus pour la télévision doivent être compatibles avec les fonctions définies dans les spécifications [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] et [b-ETSI GS ECI 001-5].

Les dispositifs conçus pour d'autres environnements, en particulier les téléviseurs IP, les ordinateurs et les tablettes, mettent généralement en oeuvre davantage de fonctionnalités dans les logiciels et assurent des communications IP bidirectionnelles, ce qui permet la prise en charge de différents types de mécanismes de sécurité. Etant donné que les jeux de puces utilisés dans ces dispositifs comprennent des éléments matériels pour différentes fonctions de traitement de la sécurité, l'interface ECI exige la mise en oeuvre de fonctionnalités matérielles dédiées de sécurité et de robustesse dans les jeux de puces. [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] et [b-ETSI GS ECI 001-5] spécifient les mécanismes nécessaires pour mettre à profit ces fonctionnalités.

6.2.4 Interfaces nécessaires entre l'hôte ECI et le client ECI

Le conteneur ECI est un concept technique associant la machine virtuelle et le client ECI dans le but d'isoler la machine virtuelle et le client ECI et de les protéger du reste de l'équipement CPE. La machine virtuelle est une fonctionnalité de l'hôte ECI. En chargeant un client ECI, l'hôte ECI crée une instance de machine virtuelle. La machine virtuelle fournit les interfaces nécessaires vers les clients ECI et les raccorde à l'hôte ECI. La spécification ECI définit l'interface entre la machine virtuelle et le client ECI; voir également la Figure 2 qui présente une architecture de haut niveau sur

un dispositif conforme ECI. L'interface fournit certaines interfaces de programmation d'application (API) et établit en outre un canal de communication sécurisé.

Les interfaces logicielles ci-après sont importantes:

– Interface permettant de transmettre les informations sur la capacité du client ECI à l'hôte ECI, et inversement.
– Interface vers les fonctions de traitement des signaux d'entrée et de sortie de l'équipement CPE.
– Interface vers le bloc matériel/pilotes de sécurité évoluée.
– Interface vers les fonctionnalités de chargeur.
– Interface prenant en charge l'interaction avec l'utilisateur.
– Interface vers les fonctionnalités de chiffrement et de déchiffrement.
– Interface vers le lecteur de carte intelligente facultatif.
– Interface vers les fonctionnalités de sécurité spécifiques, comme la prise d'empreintes digitales et l'insertion de filigranes.
– Interface vers l'espace de stockage local.

Toutes les interfaces du client ECI sont fournies par l'intermédiaire de la machine virtuelle.

Des protocoles de communication viennent en outre au-dessus des interfaces pour permettre une communication sécurisée. En particulier, un protocole permettant d'établir des communications entre les clients ECI, qu'ils soient internes ou externes, est spécifié.

L'équipement CPE peut être raccordé simultanément à un type quelconque de réseau et à plusieurs réseaux, unidirectionnels ou bidirectionnels. Il n'est pas toujours nécessaire qu'il soit connecté à un réseau (contenus téléchargés/stockés).

6.2.5 Fonctionnalités minimales d'interface utilisateur et d'affichage

En ce qui concerne les communications avec l'utilisateur, une fonctionnalité minimum d'interface utilisateur et d'affichage à l'écran doit être disponible pour les conteneurs ECI. Elle est spécifiée dans [b-ETSI GS ECI 001-3]. Cette fonctionnalité est utilisée pour afficher les messages destinés à l'utilisateur qui ont été générés ou envoyés via le système CA/DRM. En outre, elle permet à l'utilisateur d'entrer des données, par exemple un numéro personnel d'identification (PIN). Des éléments détaillés sont également spécifiés dans [b-ETSI GS ECI 001-3].

L'utilisateur interagit au niveau local avec le système CA/DRM par l'intermédiaire du client ECI.

6.2.6 Machine virtuelle

Le client ECI fonctionne sur une machine virtuelle (VM) normalisée. Ce composant est spécifié dans [b-ETSI GS ECI 001-4]. Chaque client ECI installé doit posséder sa propre instance de machine virtuelle. Cette instance fournit un environnement sécurisé permettant d'exécuter les applications client de noyau d'accès conditionnel ou de gestion des droits numériques. Les interfaces API sont fournies par la machine virtuelle, l'accès aux ressources de l'environnement de l'hôte ECI se faisant de manière normalisée.

6.2.7 Fonction de sécurité évoluée

L'interface ECI définit des fonctionnalités de sécurité minimales requises pour construire un système de protection du contenu sécurisé. Elle exige des améliorations fondées sur des éléments matériels. Pour les dispositifs conçus pour la télévision, ces améliorations sont assurées par des fonctions de sécurité évoluée dédiées conçues spécialement pour la télévision. Elle spécifie ce que l'on appelle généralement un "bloc d'échelles de clés" (*key ladder block*) dans les systèmes sur puce. L'une des tâches essentielles du mécanisme de sécurité évoluée est de protéger les clés de protection du contenu

pendant leur transmission depuis le client ECI vers le mécanisme de déchiffrement du contenu dans un équipement CPE ou du transfert d'un contenu protégé depuis un client ECI vers un autre client ECI (voir la Figure 1). Le système de sécurité évoluée spécifié dans [b-ETSI GS ECI 001-5] prend en charge différent flux de mots de contrôle simultanés et différents clients ECI qui demandent en même temps ces services. En outre, le mécanisme de sécurité évoluée joue un rôle essentiel pour vérifier le téléchargement du logiciel pour l'hôte et les clients ECI.

Les dispositifs conçus pour d'autres environnements, en particulier les téléviseurs IP, les ordinateurs et les tablettes, mettent généralement en oeuvre davantage de fonctionnalités dans les logiciels et assurent des communications IP bidirectionnelles. L'interface ECI spécifie les mêmes concepts et mécanismes de sécurité évoluée, mais elle les associera de manière différente sur les architectures de sécurité des dispositifs [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] et [b-ETSI GS ECI 001-5].

La disponibilité de la sécurité évoluée dans l'équipement CPE est communiquée au client ECI lors de son installation et de son lancement.

6.2.8 Réembrouillage

Le contenu protégé, qui est reçu par un équipement CPE conforme ECI, n'est pas forcément consommé immédiatement. Les fonctionnalités ci-après sont disponibles avec les dispositifs conformes ECI:

– Stockage local:
  - sous le contrôle de l'équipement CPE;
  - sous le contrôle d'un client CA ou DRM.
– Passerelle:
  - fourniture d'un élément de contenu protégé à un dispositif externe sous le contrôle d'un client DRM;
  - fourniture d'un élément de contenu protégé à un autre client ECI situé à l'intérieur du même équipement CPE ou fonctionnant sur un autre équipement CPE conforme ECI.

Pour prendre en charge ces fonctionnalités, le dispositif conforme ECI est capable de réembrouiller le contenu. Le système ECI ne spécifie pas les mécanismes de transport, ni les fonctionnalités DRM disponibles pour le stockage du contenu protégé ou sa fourniture à d'autres dispositifs. La spécification [b-ETSI GS ECI 001-5] définit les interfaces nécessaires entre l'hôte ECI et le client ECI.

6.2.9 Fonctionnalités du chargeur ECI

Un équipement CPE conforme ECI doit fournir des fonctionnalités de chargeur, permettant de charger et d'installer les modules logiciels pertinents du système ECI, et de garantir leur intégrité et leur protection contre les substitutions.

Dans un premier temps, le chargeur intégré dans la puce charge le chargeur de logiciel d'exploitation. Le rôle de ce chargeur intégré est de garantir que seul un chargeur de logiciel d'exploitation certifié peut être installé et lancé. Le chargeur de logiciel d'exploitation comprend le chargeur d'hôte ECI et doit donc comporter la signature de l'autorité de confiance. Il peut comprendre des chargeurs pour d'autres logiciels d'exploitation qui ne concernent pas les fonctionnalités ECI et n'ont pas de relations avec les éléments de sécurité du système. Le logiciel de l'hôte ECI comprend le chargeur de client ECI, qui, sur demande, peut ensuite charger le client ECI.

Lors de son installation dans son conteneur ECI, ainsi que lors de son lancement, le client ECI est informé par l'hôte ECI des mécanismes que ce dernier propose (par exemple mécanismes d'enregistrement, mécanismes haute définition, lecteur de carte intelligente, mécanismes de prise d'empreintes digitales et d'insertion de filigranes) et des réseaux disponibles, ainsi que de la

conformité à la spécification cadre (la présente Recommandation), ainsi qu'à [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] et [b-ETSI GS ECI 001-5], et possiblement à [b-ETSI GS ECI 001-6].

Le chargeur ECI ainsi que les mécanismes de sécurité connexes sont spécifiés dans [b-ETSI GS ECI 001-3].

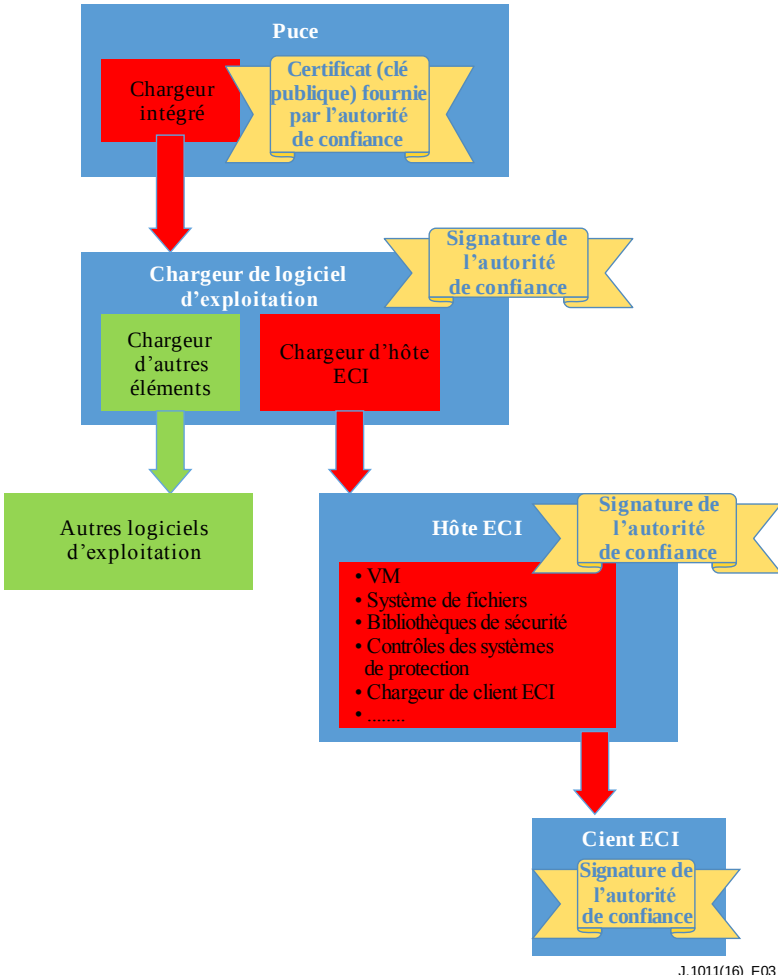


Figure 3 – Concept de chargeur hiérarchique

6.2.10 Révocation

L'autorité de confiance peut décider de mettre sur une liste noire un équipement CPE, une gamme d'équipements CPE, un type d'équipements CPE ou tous les équipements CPE d'un fabricant donné. Le fournisseur de contenu ou l'opérateur peut évoquer le ou les équipements CPE concernés de son point de distribution de service. Les méthodes utilisées permettent à d'autres opérateurs et distributeurs de contenu de continuer à desservir ces équipements CPE s'ils le souhaitent.

La révocation permet de bloquer la fourniture de tous les services de l'opérateur ou du fournisseur de contenu vers l'équipement CPE concerné ou un sous-ensemble de services. Ce point dépend de la fonctionnalité du système CA ou DRM pertinent et ne relève pas de la présente Recommandation.

Le processus de révocation est spécifié dans [b-ETSI GS ECI 001-3].

7 Environnement sécurisé

Pour pouvoir établir un système fondé sur une interface ECI, il faut mettre en place un environnement sécurisé. La présentation détaillée de l'environnement sécurisé ne relève pas des spécifications ECI. Toutefois, les principes définis dans [b-ETSI GS ECI 001-6] sont essentiels pour bien comprendre le fonctionnement de l'interface ECI.

L'autorité de confiance (TA) est une organisation régissant toutes les règles et tous les règlements qui s'appliquent aux mises en oeuvre de l'architecture ECI. L'autorité de confiance doit être une entité juridique pour pouvoir régler les réclamations fondées en droit. L'entité de confiance doit être impartiale envers tous les acteurs de l'écosystème des solutions CA/DRM téléchargeables. Ces acteurs sont les suivants:

– fabricants d'équipements CPE;
– fabricants de systèmes CA/DRM (clients ECI);
– fabricants de jeux de puces, qui comprennent notamment des clés et des certificats de processeur sécurisés non modifiables, nécessaires pour les interactions entre l'hôte et le système CA/DRM conforme;
– opérateurs de plate-forme: l'opérateur de plate-forme est la partie qui contrôle tous les éléments nécessaires d'un système CA/DRM. Il s'agit par exemple des fournisseurs de services ou d'opérateurs de réseaux;
– fournisseur d'applications, le cas échéant.

Un tiers de confiance (TTP) est un fournisseur de services techniques qui délivre des certificats et des clés aux fabricants des composants pertinents d'un système ECI. La confiance dans ces clés et certificats est garantie par l'autorité de confiance, qui détient la "racine de la confiance".

L'autorité de confiance et le tiers de confiance constituent la base de la chaîne de confiance et, par conséquent, doivent être associés à tous les processus allant de la production (puces et équipements CPE) aux mesures de contrôle (par exemple, révocation) en passant par les opérations (téléchargement et activation sécurisés du client ECI).

En sa qualité d'entité juridique, l'autorité de confiance veille au bon fonctionnement de l'environnement sécurisé grâce à un cadre contractuel, également appelé accord de licence, selon lequel les différentes parties concernées peuvent assumer leurs obligations et responsabilités. Dans le cadre de l'accord de licence, l'autorité de confiance/tiers de confiance génèrent et délivrent des paires de clés, des certificats, des justificatifs de test, des identifiants d'opérateurs, etc.

Une autorité de confiance établit la confiance entre tous les acteurs du marché. Il ne peut pas exister de seconde autorité de confiance afin d'établir la confiance "une deuxième fois" pour le même environnement. Toutefois, il peut y avoir de multiples autorités de confiance, par exemple en fonction du pays ou de la région, des segments, des écosystèmes.

Si de multiples autorités de confiance coexistent, l'autorité de confiance A et l'autorité de confiance B doivent se faire confiance mutuellement pour que les dispositifs enregistrés dans le domaine de l'autorité de confiance A puissent être utilisés dans le domaine de l'autorité de confiance B.

7.1 Flux opérationnels requis

Les paragraphes ci-après donnent un premier aperçu des flux opérationnels requis, qui répondent aux besoins des différents acteurs du marché, afin de mettre en oeuvre une activité économique reposant sur la technologie ECI. En outre, les flux mentionnés reposent sur les éléments techniques essentiels qui sont nécessaires pour la mise en oeuvre d'un système ECI. La Figure 4 montre ces interactions entre les composants techniques et les acteurs du marché concernés.

Remarque: Cette description est générique et n'a pas pour vocation de rendre compte de telle ou telle solution propriétaire existante ou de telle ou telle activité de normalisation effectivement en cours.

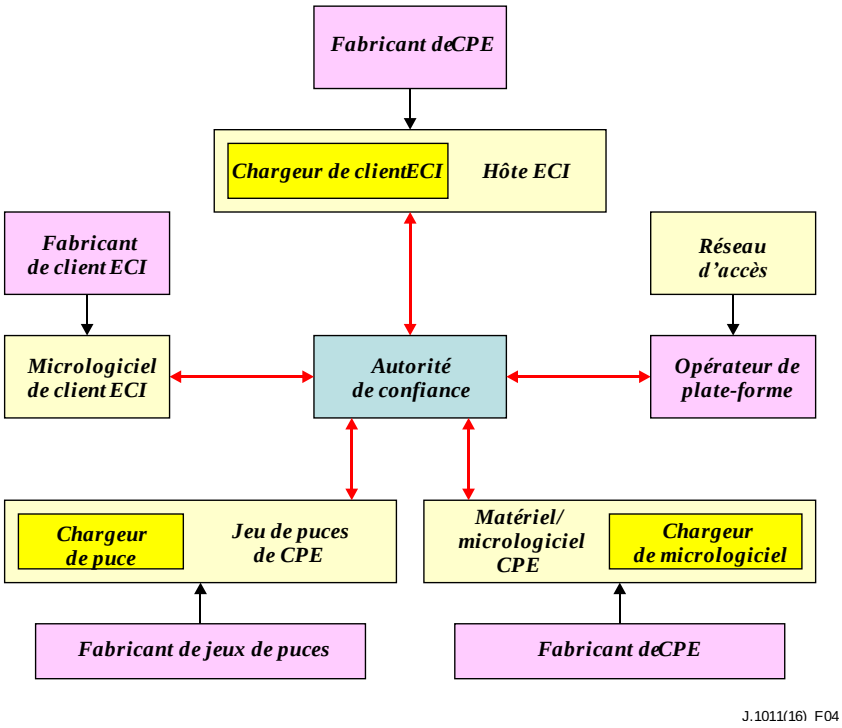


Figure 4 – Gestion de la confiance nécessaire entre l'autorité de confiance et les acteurs du marché concernés

Les questions opérationnelles et contractuelles connexes (voir les flèches en rouge dans la Figure 4) liées à l'environnement sécurisées sont les suivantes:

1) Intégrité

Par intégrité, on entend l'exigence qu'un acteur du marché puisse vérifier qu'un composant matériel/logiciel fourni par un autre acteur du marché n'a pas été modifié par une partie non autorisée et respecte les spécifications et les règles de robustesse. Cette exigence peut être satisfaite grâce à des justificatifs et à des signatures adaptées et à des procédures de test reposant sur des justificatifs de test fournis par l'autorité de confiance/le tiers de confiance.

2) Authenticité

L'authenticité signifie que tout composant matériel/logiciel qui provient d'un partenaire contractuel de l'autorité de confiance et qui a franchi avec succès les étapes de vérification et de certification requises peut clairement être associé au partenaire contractuel et, ainsi, différencié de tout composant "cloné". L'authenticité d'un composant matériel/logiciel pertinent est prouvée par un système ECI.

3) Cadre contractuel

Le cadre contractuel établi par l'autorité de confiance en sa qualité d'entité juridique doit préciser un régime de conformité et de robustesse, ainsi que des procédures de certification afin de fournir l'environnement propre à la mise en place de systèmes ECI.

4) Solutions correctives

Si des composants matériels/logiciels d'un système ECI ne sont plus conformes, l'autorité de confiance établit des procédures à l'intention du fournisseur de ce composant, en vue de rétablir l'intégrité de l'écosystème dans un délai raisonnable.

Les composants techniques essentiels (en jaune dans la Figure 4) sont les suivants:

1) Jeu de puces de l'équipement CPE

   Le jeu de puces de l'équipement CPE est le principal composant matériel de l'équipement CPE, qui comprend généralement un système sur puce en raison des exigences existantes des opérateurs de plate-forme et des fournisseurs de contenu. En outre, le chargeur de puce est généralement inclus dans la puce de l'équipement CPE.

2) Eléments matériels de l'équipement CPE

   La mise en oeuvre sécurisée du jeu de puces de l'équipement CPE, la prévention de tout accès non autorisé aux éléments de stockage (Flash, ROM) et la protection des interfaces sont essentielles.

3) Différents chargeurs

   Le chargeur de puce télécharge différents chargeurs supplémentaires, en fonction de la configuration matérielle/logicielle de l'équipement CPE.

4) Micrologiciel de l'équipement CPE

   Le micrologiciel de l'équipement CPE interagit sur de nombreux plans avec le client ECI et toutes les interfaces matérielles pertinentes de l'équipement CPE. La sécurité est assurée grâce à des spécifications détaillées et à des règles de conformité et de robustesse appropriées.

5) Client ECI

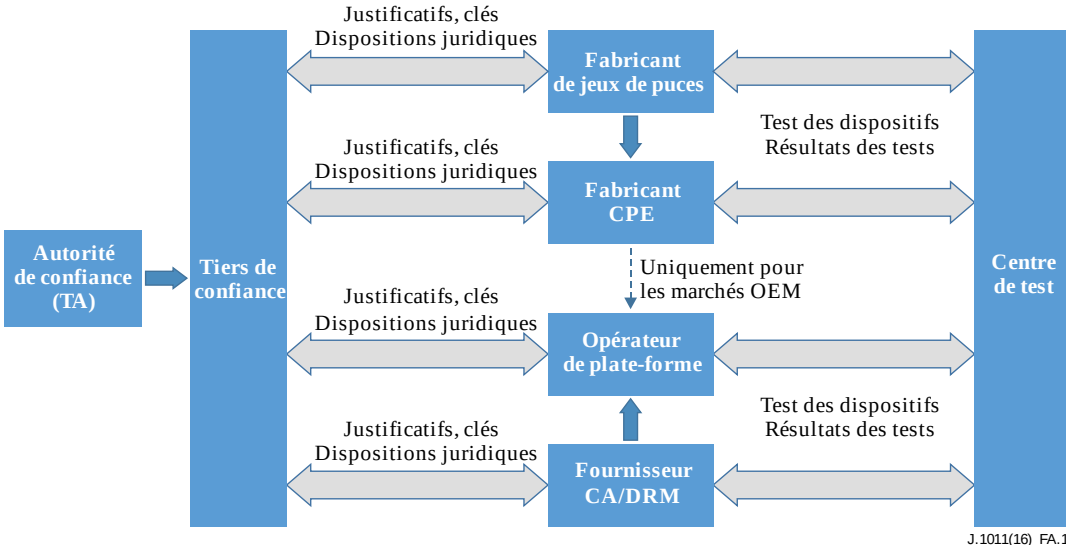
   Le client ECI extrait toutes les informations liées à l'accès conditionnel et à la gestion des droits numériques fournies par les extrémités avant de l'équipement CPE et lance le paramétrage correspondant à l'intérieur du dispositif CPE (désembrouillage, interfaces), ce qui nécessite incontestablement une interaction étroite et sécurisée avec le micrologiciel de l'équipement CPE.

Appendice I

Mise en oeuvre d'un système de confiance conforme ECI

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

L'Appendice I donne un premier aperçu des flux opérationnels requis, qui répondent aux besoins des différents acteurs du marché, afin de mettre en oeuvre une activité économique reposant sur la technologie ECI. La Figure I.1 donne un aperçu du flux général. En outre, les flux mentionnés reposent sur les éléments techniques essentiels qui sont nécessaires pour la mise en oeuvre d'un système ECI. La Figure 4 (§ 7.1) montre les interactions entre les composants techniques et les acteurs du marché concernés.



NOTE – Le tiers de confiance et le centre de test sont des partenaires contractuels de l'autorité de confiance en ce qui concerne les processus de certification et de délivrance de clés.

Figure I.1 – Aperçu du flux général

Cadre juridique/contractuel

La gestion sécurisée de la confiance ne peut avoir lieu que dans un cadre juridique et contractuel clairement défini, dont l'accord de licence est l'élément central. L'autorité de confiance fournit des accords de licence à toute entité cherchant à mettre en oeuvre les spécifications, qu'il s'agisse de fabricants d'équipements CPE, de fabricants de systèmes CA/DRM, de fabricants de puces, de fournisseurs d'autres technologies, d'opérateurs de plates-formes, etc.

Par conséquent, l'accord de licence est l'instrument essentiel grâce auquel l'autorité de confiance crée, maintient et met à la disposition du marché horizontal une méthode sécurisée mais conviviale pour recevoir et activer toutes les clés requises et tout autre élément et information de sécurité pertinent lorsqu'un utilisateur raccorde son équipement CPE à des fournisseurs de son choix, dans le respect des règles d'utilisation pertinentes. De même, le cadre d'accord de licence permet à l'autorité de confiance de procéder comme il convient à la révocation de tous les éléments de sécurité lorsqu'un consommateur est déconnecté par le fournisseur, dans la mesure où cela est possible sur les plans techniques et économiques.

L'accord de licence permet l'application coordonnée et cohérente des autres éléments du cadre contractuel, comme les spécifications techniques, les règles de conformité et de robustesse, les obligations et responsabilités, les procédures de test et de certification, les lignes directrices de mise en oeuvre, etc.

La Figure I.2 montre les éléments de l'accord de licence.

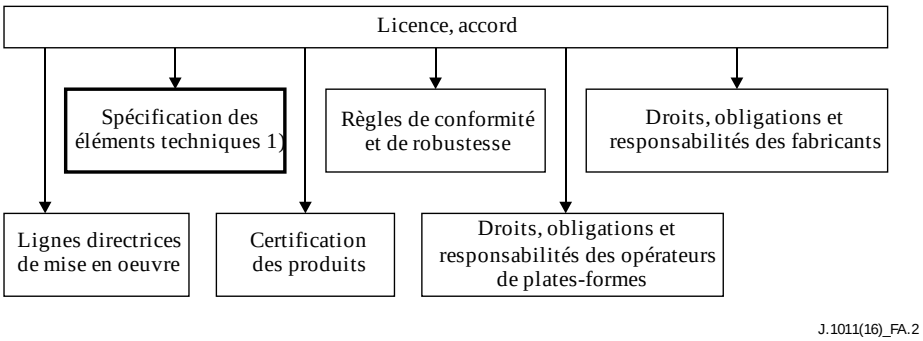


Figure I.2 – Eléments de l'accord de licence

Ces spécifications seront élaborées dans le cadre de l'ETSI ISG ECI en tant que spécifications de groupe.

Bibliographie

[b-UIT-T H.222.0] Recommandation UIT-T H.222.0 (2006) | ISO/CEI13818-1:2007, *Technologies de l'information – Codage générique des images animées et du son associé: Systèmes.*

[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 (ATTM); 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*.

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, 2018