Union internationale des télécommunications

UIT-T J.1015.1

(04/2020)

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 pour les solutions CA/DRM interchangeables; Système de sécurité évoluée – Bloc d'échelle de clés: authentification des informations sur les règles d'utilisation des mots de contrôle et des données associées 1

Recommandation UIT-T J.1015.1

Recommandation UIT-T J.1015.1

Interface commune intégrée pour les solutions CA/DRM interchangeables; Système de sécurité évoluée – Bloc d'échelle de clés: authentification des informations sur les règles d'utilisation des mots de contrôle et des données associées 1

Résumé

La Recommandation UIT-T J.1015.1, qui fait partie d'une publication en plusieurs parties sur l'interface commune intégrée pour les solutions de type accès conditionnel/gestion des droits numériques (CA/DRM) interchangeables, porte sur le bloc d'échelle de clés du système de sécurité évoluée.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T J.1015.1	23-04-2020	9	11.1002/1000/13837

Mots clés

Accès conditionnel, CA, gestion des droits numériques, DRM, échange.

* 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.

À 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/.

© UIT 2020

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

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	3
6	Authentification des informations sur les règles d'utilisation des mots de contrôle et des données associées 1	3
	6.1 Authentification des informations sur les règles d'utilisation des mots de contrôle	4
	6.2 Authentification des données associées 1	5
Appendice I – Domaines nécessitant des développements supplémentaires		6
Bibliographie		8

Introduction

L'objectif de la présente Recommandation[1] est de faciliter l'interopérabilité et la concurrence en matière de services de communications électroniques et, en particulier, sur le marché de la radiodiffusion et des appareils audiovisuels. Toutefois, d'autres technologies sont disponibles et peuvent également être appropriées et efficaces en fonction de la situation dans les États Membres.

Un fournisseur de contenus chiffre ses contenus numériques et emploie un **Système de protection des contenus**[2] pour bloquer tout accès non autorisé à ceux-ci. Un consommateur utilise un **Récepteur de contenus** pour accéder aux contenus protégés. À cette fin, le **Récepteur de contenus** comprend un microprocesseur qui effectue une ou plusieurs opérations de déchiffrement de contenus. Un protocole de création de clés de chiffrement est employé pour sécuriser le transport des clés de déchiffrement de contenus entre le **Système de protection des contenus** et le microprocesseur. Les étapes du protocole appliqué au sein du microprocesseur sont appelées "échelle de clés".

L'échelle de clés et le protocole peuvent aussi servir à sécuriser le transport de clés de chiffrement de contenus vers le microprocesseur. Ces clés sont nécessaires lorsque le microprocesseur doit rechiffrer des contenus, le microprocesseur pouvant effectuer à cette fin une ou plusieurs opérations de chiffrement de contenus. L'enregistrement de vidéos personnelles et l'exportation de contenus protégés vers un **Système de protection des contenus** différent sont des exemples classiques de cas dans lesquels les contenus doivent être rechiffrés. Dans l'ensemble de la présente Recommandation, les clés de chiffrement et de déchiffrement de contenus sont appelées **Mots de contrôle** (CW).

La présente Recommandation contient en outre les spécifications d'un mécanisme d'authentification. Celui-ci est étroitement lié à l'échelle de clés et peut servir à authentifier différentes entités, en particulier le microprocesseur.

L'échelle de clés et le mécanisme d'authentification décrits ci-après sont indépendants du **Système de protection des contenus** et du **Fournisseur de contenus**. Ce dernier peut donc utiliser n'importe quel **Système de protection des contenus** conforme aux spécifications; de même, le consommateur peut utiliser le **Récepteur de contenus** pour accéder aux contenus de n'importe quel fournisseur utilisant un **Système de protection de contenus** conforme.

Les mécanismes spécifiés dans la présente Recommandation prévoient qu'une **Autorité de certification** gère un certificat de clé publique pour chaque microprocesseur. Cette **Autorité de certification** a notamment pour rôle d'envoyer les informations sur les certifications et sur leur révocation aux **Fournisseurs de contenus** qui souhaitent employer l'échelle de clés et/ou le mécanisme d'authentification. Les **Fournisseurs de contenus** utilisent alors ces informations pour alimenter leur **Système de protection de contenus** conforme; comme nous allons le voir de manière détaillée dans le § 7 de la Recommandation [UIT-T J.1015], la clé publique du certificat d'un microprocesseur permet au **Système de protection de contenus** de produire les messages pertinents à passer en entrée à l'échelle de clés et au mécanisme d'authentification du microprocesseur.

---

[1] Plusieurs domaines nécessitant des développements supplémentaires ont été identifiés dans l'Appendice I.

[2] Dans le texte de la présente Recommandation, on utilise des caractères gras pour les termes dont la définition est propre au contexte de l'interface commune intégrée et peut différer de l'usage courant.

Recommandation UIT-T J.1015.1

Interface commune intégrée pour les solutions CA/DRM interchangeables; Système de sécurité évoluée – Bloc d'échelle de clés: authentification des informations sur les règles d'utilisation des mots de contrôle et des données associées 1

1 Domaine d'application

La présente Recommandation contient les spécifications d'un bloc d'échelle de clés destiné au microprocesseur d'un **Récepteur de contenus**. Ce bloc d'échelle de clés se compose d'une échelle de clés, qui permet de sécuriser le transport de **Mots de contrôle** (CW) vers le microprocesseur, et d'un mécanisme d'authentification. La présente Recommandation contient en outre des spécifications sur la personnalisation de certains éléments d'un microprocesseur conforme.

La présente Recommandation est destinée aux fabricants de microprocesseurs.

2 Références

La présente Recommandation se réfère à certaines dispositions de Recommandations UIT-T et autres textes 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 de Recommandation.

[UIT-T J.1015] Recommandation UIT-T J.1015 (2020), *Interface commune intégrée (ECI) pour les solutions CA/DRM interchangeables; Système de sécurité évoluée – Bloc d'échelle de clés.*

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 Autorité de certification: partie chargée de la gestion des certificats de clé publique dans un **Écosystème** d'interface commune intégrée (**ECI**). Toutes les autres parties du système font confiance à l'autorité de certification pour effectuer les opérations associées aux certificats.

3.2.2 ID du microprocesseur: dans un **Écosystème ECI**, numéro non secret employé comme identifiant d'un microprocesseur.

3.2.3 Système de protection des contenus: dans un **Écosystème ECI**, système employant des techniques de chiffrement pour gérer l'accès à des contenus et des services. L'expression "système de protection des services" est aussi souvent employée dans le même sens. En général, il s'agit soit de systèmes d'accès conditionnel (CAS), soit de systèmes de gestion des droits numériques (DRM).

3.2.4 Fournisseur de contenus: dans un **Écosystème ECI**, partie qui distribue des contenus numériques à un **Récepteur de contenus**.

3.2.5 Récepteur de contenus: dans un **Écosystème ECI**, dispositif employé pour accéder à des contenus numériques. Un **Récepteur de contenus** contient un microprocesseur doté d'un **Désembrouilleur de contenus**.

3.2.6 Désembrouilleur de contenus: dans un **Écosystème ECI**, élément du microprocesseur capable de déchiffrer des contenus. Un désembrouilleur de contenus peut également être en mesure de chiffrer des contenus (aux fins du rechiffrement de contenus). Dans la présente Recommandation, le chiffrement/déchiffrement de contenus utilise un **Système de chiffrement symétrique**. Pour les contenus MPEG-2, le chiffrement et le déchiffrement de contenus sont également appelés respectivement embrouillage et désembrouillage.

3.2.7 Mot de contrôle: dans un **Écosystème ECI**, clé secrète utilisée pour chiffrer et déchiffrer des contenus. Dans les systèmes de gestion des droits numériques, un mot de contrôle est généralement appelé clé de contenu.

3.2.8 Fonction de hachage cryptographique: dans un **Écosystème ECI**, fonction de chiffrement sans clé qui reçoit en entrée des données de taille arbitraire, appelées message, et qui produit un bloc de données de sortie de taille fixe, appelé condensé du message. Dans la présente Recommandation, on suppose que la **fonction de hachage cryptographique** se comporte comme une fonction aléatoire et qu'elle est résistante à la seconde préimage.

3.2.9 Système de signature numérique: dans un **Écosystème ECI**, système de chiffrement asymétrique par clé qui est utilisé pour protéger l'authenticité des données. Un **Système de signature numérique** se compose d'un algorithme de création de clé, d'une opération de création de signature et d'une opération de vérification de signature. Les clés sont créées sous forme de paires (clé secrète/privée, clé publique). Les données sont signées à l'aide d'une clé secrète/privée et la clé publique correspondante sert à vérifier la signature. Le **Système de signature numérique** spécifié dans la présente Recommandation est utilisé pour protéger l'authenticité des messages comme défini dans le document [b-ROEL]; en particulier, le système n'est pas utilisé pour assurer la non-répudiation ou l'authentification de la source dans la présente Recommandation.

3.2.10 Écosystème ECI: opération commerciale fondée sur une autorité de confiance et sur plusieurs plates-formes et équipements de locaux d'abonnés conformes à l'interface **ECI** qui sont déployés sur le terrain.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AD1 données associées 1 (*associated data 1*)

AK clé d'authentification (*authentication key*)

CA accès conditionnel (*conditional access*)

CW mot de contrôle (*control word*)

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

ECI interface commune intégrée (*embedded common interface*)

ID identifiant/identificateur (*Identifier*)

LK clé de liaison (*link key*)

SHA algorithme de hachage sûr (*secure hash algorithm*)

SPK clé publique de l'expéditeur (*sender public key*)

SSK clé secrète/privée de l'expéditeur (*sender secret/private key*)

T étiquette (*tag*)

URI informations sur les règles d'utilisation (*usage rules information*)

5 Conventions

Dans le texte de la présente Recommandation, on utilise des caractères gras pour les termes dont la définition est propre au contexte de l'interface commune intégrée et peut différer de l'usage courant.

6 Authentification des informations sur les règles d'utilisation des mots de contrôle et des données associées 1

Concernant les spécifications détaillées figurant dans le § 7 de la Recommandation [UIT-T J.1015], plusieurs entrées du bloc d'échelle de clés sont définies, notamment: CW-URI, AD1, τ_b, SPK-URI, SPK_i, une clé LK chiffrée ainsi qu'un identifiant de microprocesseur signé. Certaines de ces entrées, par exemple la clé LK et l'identifiant de microprocesseur, sont chiffrées et une procédure de signature numérique leur est appliquée. En revanche, les entrées CW-URI, AD1, τ_b, SPK-URI et SPK_i sont envoyées sans qu'aucune procédure de chiffrement ne leur soit appliquée. L'authentification de ces entrées est implicite; si une valeur non authentique est fournie pour l'une des entrées de l'échelle de clés, une valeur non valable de CW est calculée et le contenu ne peut être désembrouillé.

La possibilité d'envoyer en clair SPK_i, SPK-URI et τ_b s'explique par la nature des caractéristiques de ces entrées. En particulier, on peut vérifier τ_b au moyen des routines de vérification des données associées et il n'est donc pas nécessaire d'appliquer un système d'authentification explicite.

Si des prestataires de services le souhaitent, ils peuvent mettre en place une méthode d'authentification explicite supplémentaire pour les entrées CW-URI et AD1 du bloc d'échelle de clés. Une telle fonctionnalité pourrait apporter plus de commodité aux utilisateurs et offrir des avantages opérationnels aux prestataires de services.

La présente Recommandation contient les spécifications d'une méthode permettant de mettre en œuvre un tel système d'authentification pour les chaînes de bits CW-URI et AD1 lorsque celles-ci sont passées en entrée d'un bloc d'échelle de clés. Pour ce faire, on utilise un système de signature numérique déjà employé avec une clé SSK pour authentifier l'ensemble Chipset-ID || E(SPK, LK). Les prestataires de services peuvent authentifier CW-URI ou AD1, ou les deux en même temps.

Si des prestataires de services souhaitent protéger CW-URI ou AD1, ils doivent obligatoirement employer le système défini dans la présente Recommandation.

Voir la Figure 1.

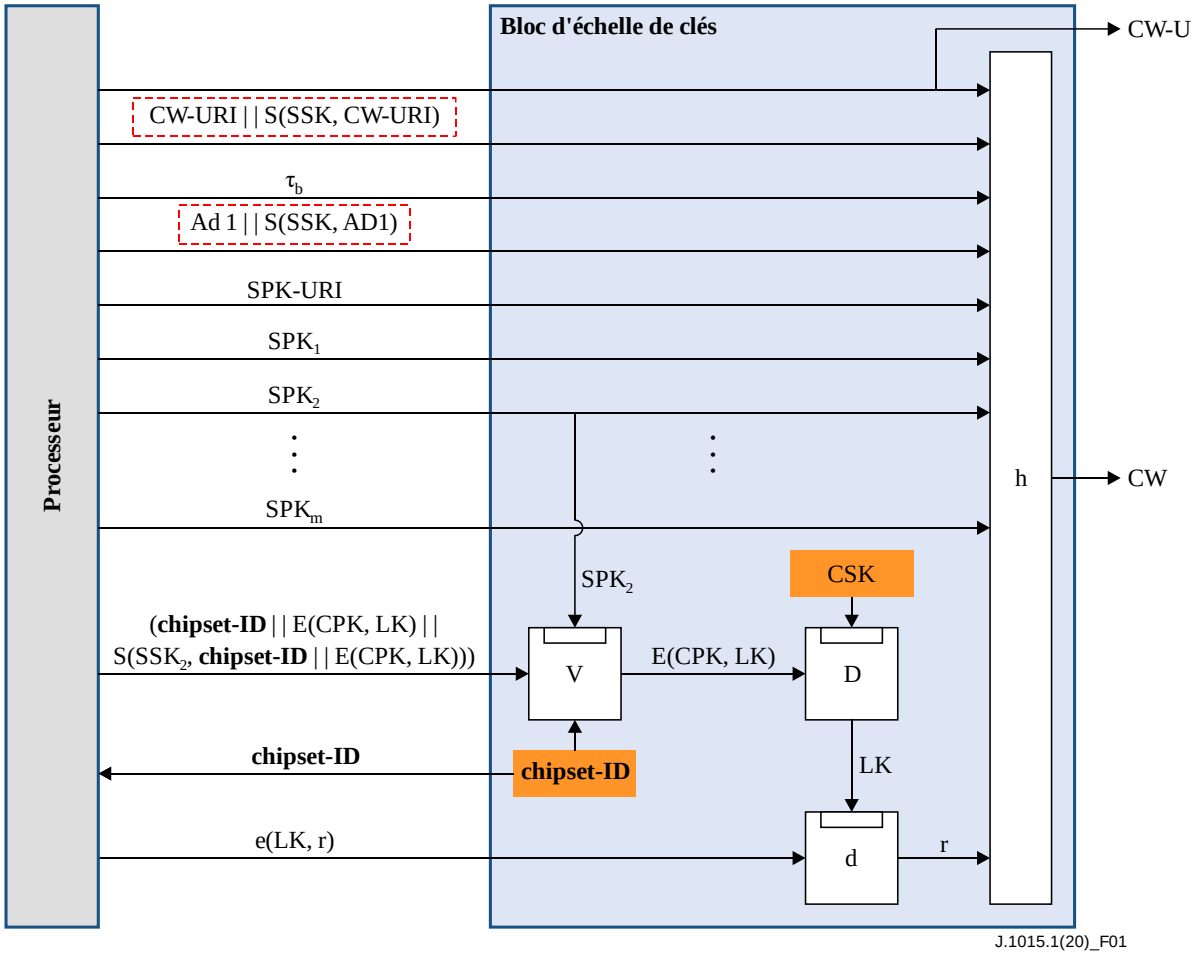

Figure 1 – Authentification des informations sur les règles d'utilisation des mots de contrôle et des données associées 1

6.1 Authentification des informations sur les règles d'utilisation des mots de contrôle

Calcul de CW-URI ||signature (expéditeur):

1) Signer la chaîne de bits CW-URI au moyen de la clé SSK_i; la signature est désignée par $S(SSK_i, CW\text{-}URI)$.

2) Ajouter cette signature en suffixe à la chaîne de bits CW-URI.

Extraction de CW-URI (bloc d'échelle de clés):

1) Vérifier la longueur des données d'entrée. Si CW-URI a une longueur de 64 bits, le bloc d'échelle de clés effectue la procédure normale définie dans le § 7.3.1 de la Recommandation [UIT-T J.1015] et arrête la procédure d'authentification de CW-URI. Dans le cas contraire, c'est-à-dire si la longueur est supérieure à 64 bits, la procédure d'authentification de CW-URI est appliquée et le système passe à l'étape suivante.

2) Vérifier si la chaîne SPK-URI et la règle d'utilisation définies dans le § 7.3.2 de la Recommandation [UIT-T J.1015] autorisent l'opération de vérification V à utiliser la clé SPK_i pour vérifier la signature. Si tel n'est pas le cas, le bloc d'échelle de clés arrête les calculs.

3) Utiliser le couple (CW-URI ||signature) et la clé SPK_i reçus pour vérifier la signature. Si celle-ci n'est pas valable, le bloc d'échelle de clés arrête les calculs.

4) Extraire CW-URI.

6.2 Authentification des données associées 1

Calcul de AD1 ||signature (expéditeur):

1) Signer la chaîne de bits AD1 au moyen de la clé SSK_i; la signature est désignée par $S(SSK_i, AD1)$.
2) Ajouter cette signature en suffixe à la chaîne de bits AD1.

Extraction des données associées 1 (bloc d'échelle de clés):

1) Vérifier la longueur des données d'entrée. Si AD1a une longueur de 256 bits, le bloc d'échelle de clés effectue la procédure normale définie dans le § 7.3.1 de la Recommandation [UIT-T J.1015] et arrête la procédure d'authentification d'AD1. Dans le cas contraire, c'est-à-dire si la longueur est supérieure à 256 bits, la procédure d'authentification d'AD1 est appliquée et le système passe à l'étape suivante.
2) Vérifier si la chaîne SPK-URI et la règle d'utilisation définies dans le § 7.3.2 de la Recommandation [UIT-T J.1015] autorisent l'opération de vérification V à utiliser la clé SPK_i pour vérifier la signature. Si tel n'est pas le cas, le bloc d'échelle de clés arrête les calculs.
3) Utiliser le couple (AD1 ||signature) et la clé SPK_i reçus pour vérifier la signature. Si celle-ci n'est pas valable, le bloc d'échelle de clés arrête les calculs.
4) Extraire AD1.

Appendice I

Domaines nécessitant des développements supplémentaires

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

Il a été établi que la présente Recommandation nécessite des développements et une validation supplémentaires afin de répondre aux exigences énoncées dans la Recommandation [b-UIT-T J.1010], et que la Recommandation [b-UIT-T J.1010] doit être mise à jour pour refléter les exigences de la spécification Enhanced Content Protection (ECP) de MovieLabs [b-ECP]. Les Recommandations [b-UIT-T J.1011], [b-UIT-T J.1012], [b-UIT-T J.1013], [b-UIT-T J.1014], [UIT-T J.1015] et UIT-T J.1015.1 devront à l'avenir être mises à jour pour refléter ces mises à jour de la Recommandation [b-UIT-T J.1010].

Plusieurs États Membres de l'UIT ainsi que des parties prenantes de divers secteurs – notamment des fabricants d'appareils et de composants électroniques, des propriétaires et des titulaires de licences de contenus protégés par le droit d'auteur, des fournisseurs de services over-the-top (OTT) et de télévision linéaire, et des fournisseurs de solutions de système d'accès conditionnel (CAS) et de gestion des droits numériques (DRM) – basées dans le monde entier se sont déclarés préoccupés par le fait que l'interface commune intégrée (ECI) ne répond pas pleinement aux exigences de la spécification ECP, ni aux exigences plus larges du secteur en matière de protection des contenus.

Plus précisément, leurs préoccupations ont été exprimées dans des contributions soumises à la réunion de la Commission d'étude 9 (CE 9) de l'UIT-T tenue du 16 au 23 avril 2020. Dans leurs contributions, Israël, l'Australie, Samsung (Membre de secteur de l'UIT-T) ainsi que Sky Group et MovieLabs (Associés de la CE 9) ont proposé d'apporter plusieurs modifications aux Recommandations relatives à l'interface ECI, mais aucun accord n'a été trouvé à leur sujet. Ces points sont répertoriés dans le document [b-CE 9 Rapport 17 Ann.1].

Les propositions visent à:

1) simplifier le système ECI en réduisant son champ d'application;
2) supprimer la gestion DRM;
3) supprimer le rechiffrement de contenu;
4) supprimer la gestion des logiciels;
5) ajouter des API pour les opérations de stockage et de chiffrement sécurisées;
6) autoriser des échelles de clés propres aux fournisseurs;
7) utiliser les exigences TEE UIT-T J.1207;
8) inclure l'implémentation TEE pour les machines virtuelles;
9) augmenter la puissance des algorithmes de chiffrement, par exemple en utilisant SHA-384;
10) utiliser des certificats standard, comme UIT-T X.509;
11) revoir les communications entre clients;
12) mener des échanges supplémentaires avec l'ETSI;
13) effectuer une évaluation par les pairs supplémentaire;
14) envisager des alternatives au modèle de l'autorité de confiance;
15) définir plus précisément les aspects techniques des règles de conformité et de robustesse de l'interface ECI;
16) ajouter des exigences en matière de diversité, par exemple la randomisation de l'espace d'adresses;
17) ajouter des exigences relatives à la vérification de l'intégrité de l'exécution.

Ces propositions reflètent le fait que la protection des contenus et les menaces de compromission de contenu sont en constante évolution. L'interface ECI a été conçue initialement près de dix ans avant l'approbation de la présente Recommandation UIT-T. Des systèmes comme l'interface ECI doivent être évalués régulièrement en fonction à la fois des techniques d'attaque et des exigences de protection du secteur les plus récentes.

D'autres mécanismes existent pour assurer l'interopérabilité. En particulier, s'agissant de la gestion DRM, la plupart des services vidéo sur l'Internet ont déployé d'autres solutions pour assurer l'interopérabilité et répondre à leurs besoins.

Il est important d'apporter davantage de clarté, car de nombreux États Membres considèrent les normes de l'UIT comme des guides importants pour le développement de leurs marchés et de leurs secteurs. La liste de préoccupations vise à faire en sorte que la mise en œuvre de l'interface ICE sur les marchés nationaux puisse reposer sur une compréhension parfaite des conséquences de la présente Recommandation de l'UIT-T et que les questions soient prises en compte au moment d'examiner une législation, une réglementation ou des besoins du marché exigeant que les équipements de télévision numérique grand public soient interopérables. Elle vise également à faire en sorte que les fabricants d'équipements techniques, qui peuvent préférer utiliser un ensemble unique d'exigences ou d'autres normes pour concevoir les produits, puissent prendre en compte ces questions lors du développement de produits pour des marchés différents.

Bibliographie

[b-UIT-T J.1010] Recommandation UIT-T J.1010 (2016), *Interface commune intégrée pour les solutions CA/DRM interchangeables; Cas d'utilisation et exigences*.

[b-UIT-T J.1011] Recommandation UIT-T J.1011 (2016), *Interface commune intégrée pour les solutions CA/DRM interchangeables; Architecture, définitions et vue d'ensemble*.

[b-UIT-T J.1012] Recommandation UIT-T J.1012 (2020), *Interface commune intégrée pour les solutions CA/DRM interchangeables; Conteneur CA/DRM, chargeur, interfaces et révocation*.

[b-UIT-T J.1013] Recommandation UIT-T J.1013 (2020), *Interface commune intégrée pour les solutions CA/DRM interchangeables; Machine virtuelle*.

[b-UIT-T J.1014] Recommandation UIT-T J.1014 (2020), *Interface commune intégrée pour les solutions CA/DRM interchangeables; Sécurité évoluée – Fonctionnalités propres aux interfaces ECI*.

[b-CE 9 Rapport 17 Ann.1] Rapport de la réunion de la CE 9 de l'UIT-T, SG9-R17-Annexe 1 (2020), Annexe 1 au Rapport 17 de la réunion de la CE 9 organisée de manière entièrement virtuelle du 16 au 23 avril 2020. https://www.itu.int/md/T17-SG09-R-0017/en

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 Available at: https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

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	Équipements 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, 2020