Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.197
(11/2005)

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

Câblo-modems

Prescriptions de haut niveau pour un pont de gestion des droits numériques (DRM) à partir d'un réseau d'accès par câble à un réseau domestique

Recommandation UIT-T J.197

Recommandation UIT-T J.197

Prescriptions de haut niveau pour un pont de gestion des droits numériques (DRM) à partir d'un réseau d'accès par câble à un réseau domestique

Résumé

La présente Recommandation établit les prescriptions d'un pont de gestion des droits numériques à partir d'un réseau d'accès par câble à un réseau domestique, auquel de nombreux types de contenu (p. ex. vidéo, audio, etc.) peuvent être transférés par l'opérateur de réseau avec l'assurance que ce contenu ne sera pas utilisé de façon à constituer une violation d'éventuelles conventions de service ou exigences légales.

Source

La Recommandation UIT-T J.197 a été approuvée le 29 novembre 2005 par la Commission d'études 9 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) 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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T J.197

Prescriptions de haut niveau pour un pont de gestion des droits numériques (DRM) à partir d'un réseau d'accès par câble à un réseau domestique

1 Domaine d'application

La présente Recommandation définit les prescriptions d'un pont de gestion des droits numériques à partir d'un réseau d'accès par câble à un réseau domestique, auquel de nombreux types de contenu (p. ex. vidéo, audio, etc.) peuvent être transférés par l'opérateur de réseau avec l'assurance que ce contenu ne sera pas utilisé de façon à constituer une violation d'éventuelles conventions de service ou exigences légales.

2 Références

2.1 Références normatives

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.

– NIST FIPS 140-2 (2002), *Security requirements for cryptographic modules* (Exigences de sécurité pour modules cryptographiques).

2.2 Références informatives

– Recommandation UIT-T J.192 (2005), *Passerelle résidentielle assurant la remise des services de données par câble*.

– DTCP (2005), *Digital transmission content protection specification volume 1 (information version)*.

– Intel (2005), *High-bandwidth digital content protection system, revision 1.1*.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 bits du système de protection analogique (bits APS): bits 3 et 2 des informations CCI, désignant l'état de protection analogique pour un terminal adaptateur.

3.2 règles de conformité: règles qui s'appliquent aux terminaux adaptateurs et qui visent à empêcher la copie non autorisée d'un contenu contrôlé.

3.3 filigrane numérique consensuel: filigrane numérique qui a été développé pour utilisation dans un système de gestion DRM.

3.4 contrainte d'image: équivalent visuel d'un maximum de 520 000 pixels par trame (p. ex. une image avec résolution de 540 verticalement par 960 horizontalement pour le format 16:9). Une image contrainte peut être extraite ou affichée au moyen de techniques de traitement des signaux vidéo telles que le doublement de ligne ou le renforcement des contours afin d'améliorer la qualité perçue de l'image.

3.5 déclencheur de contrainte d'image (CIT, ***constrained image trigger*****)**: champ ou bits servant à déclencher l'extraction d'une "image contrainte" dans le signal de sortie analogique à haute définition de terminaux adaptateurs.

3.6 protection du contenu: application de sauvegardes techniques empêchant la copie et/ou la redistribution sans autorisation d'un contenu acheminé par le réseau.

3.7 contenu contrôlé: contenu transmis à partir d'un réseau de fournisseur de service vidéo avec les bits de l'indicateur de mode de chiffrement ("EMI") réglés à une valeur autre que "zéro, zéro" (0,0) (signifiant "copie non restreinte").

3.8 informations de commande de copie (CCI, *copy control information*): champ d'un seul octet qui contient des informations que les terminaux adaptateurs utilisent afin de commander la copie d'un contenu. Voir l'Annexe A pour de plus amples détails.

3.9 gestion des droits numériques (DRM, *digital rights management*): définition, gestion et mise en application d'un ensemble de règles d'usage de contenu. Ces règles d'usage indiqueront des éléments tels que le droit de copier, de voir, ou de distribuer un fragment particulier de contenu.

3.10 protection du contenu d'une transmission numérique (DTCP, *digital transmission content protection*): méthode de chiffrement, de déchiffrement, d'échange des clés et de renouvelabilité qui est décrite dans la spécification intitulée "5C Digital Transmission Content Protection – Release 1.0" (Protection du contenu d'une transmission numérique 5C – Version 1.0).

3.11 pont de gestion DRM: infrastructure et techniques de distribution et de réseau domestique, mises en place afin de permettre la protection d'un contenu et la gestion des droits numériques du contenu acheminé par le réseau puis mémorisé et distribué dans un réseau domestique.

3.12 bits d'indicateur de mode de chiffrement (bits EMI): deux bits, associés au contenu protégé, qui spécifient les opérations de copie et qui sont permissibles pour le contenu associé.

3.13 forme [ou] sortie analogique à haute définition: format ou sortie qui n'est pas numérique et qui a une résolution supérieure à la forme ou sortie analogique à définition normale.

3.14 système de protection d'un contenu numérique à grande largeur de bande (HDCP, *high-bandwidth digital content protection*): méthode d'authentification, de chiffrement, de déchiffrement et de renouvelabilité qui est décrite dans la spécification intitulée "High-Bandwidth Digital Content Protection System, Rev. 1.1" (Système de protection d'un contenu numérique à grande largeur de bande, Rév.1.1).

3.15 produit: dispositif et/ou technique qui reçoit et éventuellement distribue un contenu avec contrôle de redistribution et/ou de copie.

3.16 règles de robustesse: règles décrites dans le § 6, qui s'appliquent aux terminaux adaptateurs et qui visent à résister aux tentatives de modifier des terminaux adaptateurs afin de déjouer les fonctions des règles de conformité.

3.17 service: signaux vidéo, audio, ou de données, de format analogique ou numérique, transmis sur le réseau vidéo du fournisseur de service jusqu'au terminal adaptateur (ou à partir de celui-ci), afin d'assurer la réception ou la transmission d'un contenu informationnel, ludique ou relationnel.

3.18 terminal adaptateur (STB, *set top box*): tout dispositif qui reçoit un contenu issu directement d'un fournisseur de service vidéo, ce qui inclut à la fois les dispositifs qui sont distincts du dispositif d'affichage et les dispositifs d'affichage qui ont la fonctionnalité intégrée appropriée. Le terminal adaptateur STB joue le rôle de passerelle de service pour le réseau domestique. Il contient le système d'accès conditionnel et un système de gestion des droits numériques (DRM).

3.19 forme [ou] sortie analogique à définition normale: signal ou sortie qui n'est pas numérique, (p. ex. RF PAL, RF NTSC, composite, S-Vidéo, YUV, Y,R-Y,B-Y ou RGB) et qui n'a pas plus de 483 lignes de balayage actif, entrelacées ou progressives.

3.20 système de protection du contenu vidéo (VCPS, *video content protection system*): pour l'enregistrement d'un contenu chiffré sur support optonumérique (DVD+RW et DVD+R) protégé par la technique du système VCPS.

3.21 fournisseur de service vidéo (VSP, *video service provider*): fournisseur de service offrant un "service" comme défini dans la présente Recommandation.

4 Abréviations, acronymes et conventions

4.1 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

AES	norme de chiffrement évolué (*advanced encryption standard*)
AMNT	Assemblée mondiale de normalisation des télécommunications
APS	système de protection analogique (*analogue protection system*)
CCI	informations de commande de copie (*copy control information*)
CGMS-A	copy generation management system analogue
CIT	déclencheur de contrainte d'image (*constrained image trigger*)
DRM	gestion des droits numériques (*digital rights management*)
DTCP	protection du contenu d'une transmission numérique (*digital transmission content protection*)
DVD-RW	disque numérique versatile – à réécriture (*digital versatile disk – re-writable*)
DVD+R	disque numérique versatile – enregistrable (*digital versatile disk + recordable*)
DOCSIS	spécification d'interface du service de transmission de données par câble (*data over cable service interface specification*)
DVI	interface visuelle numérique (*digital visual interface*)
EEPROM	mémoire ROM reprogrammable (*electrically erasable programmable read-only memory*)
EMI	indicateur de mode de chiffrement (*encryption mode indicator*)
HDCP	système de protection d'un contenu numérique à grande largeur de bande (*high-bandwidth digital content protection*)
HDMI	interface multimédia à haute définition (*high-definition multimedia interface*)
IP	protocole Internet (*Internet protocol*)
LSB	bit de plus faible poids (*least significant bit*)
MPEG	groupe d'experts pour les images animées (*moving picture experts group*)
NTSC RF	national television system committee radio frequency
OOB	hors bande (*out of band*)
PAL	phase alternate line
PCI	interface de composant périphérique (*peripheral component interface*)
PCMCIA	personal computer memory card international association
QS	qualité de service
RF	radiofréquence

RVB	rouge vert bleu (*red, green, blue*)
SRM	message de renouvelabilité du système (*system renewability message*)
STB	terminal adaptateur (*set top box*)
S-Video	super-vidéo
VCPS	système de protection d'un contenu vidéo (*video content protection system*)
VSP	fournisseur de système vidéo (*video service provider*)

5 Aperçu général

La technique d'implantation de réseaux domestiques et son acceptation ont évolué au point qu'un réseau domestique peut servir de réseau récréatif incontournable, permettant à un utilisateur de mémoriser et de distribuer un contenu entre divers dispositifs intégrés au réseau domestique. L'industrie a intérêt à déployer cet environnement en étendant l'acheminement des services récréatifs jusqu'au réseau domestique. Etant donné que les services par câble impliquent souvent un contenu de haute qualité soumis à des droits de propriété intellectuelle, la nécessité apparaît de définir des mécanismes visant à protéger ce contenu et à appliquer les règles d'usage associées, pour une variété de raisons d'ordre légal et commercial. La présente Recommandation établit les exigences d'un pont de gestion des droits numériques à partir d'un réseau d'accès par câble à un réseau domestique, auquel un contenu peut être transféré par l'opérateur de réseau avec l'assurance que ce contenu ne sera pas utilisé de façon à constituer une violation d'éventuelles conventions de service ou exigences légales.

5.1 Objectifs essentiels

Les objectifs essentiels pour l'implémentation du pont de gestion DRM sont les suivants:

- robustesse suffisante du point de vue du fournisseur de contenu;
- absence d'intrusion du point de vue de l'abonné;
- conformité à l'environnement réglementaire et législatif.

5.2 Caractéristiques essentielles

Les caractéristiques essentielles d'un pont de gestion DRM sont les suivantes:

- authentification de tous les dispositifs participant à la transmission et/ou à la consommation d'un contenu vidéo;
- extension d'un riche ensemble de règles commerciales de protection d'un contenu par gestion des droits numériques (restrictions de copie, nombre de reproductions, limites temporelles, etc.) qui ont été établis dans le cadre du terminal STB;
- chiffrement/déchiffrement de contenu vidéo pour transmission/consommation.

5.3 Aspects techniques essentiels

L'on trouvera ci-dessous un certain nombre d'aspects techniques essentiels pour le pont de gestion DRM:

- le pont de gestion DRM étend des éléments essentiels de la gestion DRM jusqu'à des points situés à l'extérieur du terminal STB;
- le pont de gestion DRM prend en charge la transmission et le stockage du contenu acheminé aussi bien par l'opérateur de réseau par câble que par l'opérateur d'un autre réseau;
- le contenu avec contrôle de redistribution ou de copie ne peut sortir du terminal adaptateur STB ou d'éléments du flux aval qu'au moyen de sorties homologuées;

- le contenu sans contrôle de redistribution ou de copie peut être consommé et mémorisé dans le terminal adaptateur STB ou dans des éléments du flux aval;
- le contenu sans contrôle de redistribution ou de copie peut librement sortir du terminal adaptateur STB ou des éléments du flux aval.

5.4 Prescriptions générales concernant le pont de gestion DRM

G-1	**convivialité avec l'abonné**: le pont de gestion DRM doit être transparent à l'abonné, permettant une consommation pratique du contenu et ne présentant aucune barrière à l'emploi.
G-2	**modèle d'usage simple**: le pont de gestion DRM fera appel à un modèle d'usage simple, permettant d'utiliser dans le réseau domestique le contenu acheté à l'opérateur du réseau et acheminé par lui, conformément aux droits conférés à ce contenu.
G-3	**protection du contenu**: le pont de gestion DRM doit empêcher une transmission et une copie non autorisées d'un contenu protégé, à l'extérieur du réseau domestique.
G-4	**blocage du vol de service**: le pont de gestion DRM doit empêcher le vol de service et protéger les règles d'utilisation de contenu (par exemple le vol de contenu sur un réseau sans fil dans un habitat collectif résidentiel).
G-5	**compatibilité avec d'autres techniques de gestion DRM**: le pont de gestion DRM ne doit pas exclure l'utilisation d'autres techniques de protection d'un contenu acheminé par un opérateur de réseau autre que le câble.
G-6	**indépendance de la technique de transport**: la technique servant à implémenter le pont de gestion DRM doit être indépendante de la technique d'implantation des réseaux domestiques.
G-7	**rétrocompatibilité**: la technologie du pont de gestion DRM ne doit pas affecter les contrats de vidéodistribution existants.
G-8	**indépendance de la technique de distribution**: le pont de gestion DRM doit impérativement prendre en charge diverses techniques de distribution, y compris la diffusion d'images MPEG, les flux IP en temps réel et le transfert de fichiers (FTP).
G-9	**protection en temps réel**: la technique servant à implémenter le pont de gestion DRM doit être applicable aux médias en temps réel (par exemple pour la diffusion d'images MPEG et pour les sources de flux IP en temps réel)
G-10	**intégration**: les techniques et les processus du pont de gestion DRM devraient être compatibles avec d'autres initiatives industrielles pertinentes, telles que DOCSIS (Recommandations UIT-T J.112/122), IPCablecom (Recommandations UIT-T de la série J.16.x et J.17.x) et IPCable2Home (Recommandations UIT-T de la série J.19.x).
G-11	**spécification ouverte**: la spécification du pont de gestion DRM doit permettre l'interopérabilité entre équipements issus de divers vendeurs.
G-12	**faisabilité économique**: le coût de l'implémentation, de la maintenance, de la validation et de la mise en vigueur des techniques et processus de pont de gestion DRM devrait permettre de réaliser des modèles commerciaux viables.
G-13	**gérabilité dynamique**: les informations servant à protéger le contenu doivent être configurables et gérables dynamiquement.
G-14	**renouvelabilité**: le logiciel de sécurité du pont de gestion DRM doit être renouvelable.
G-15	**maintien du fonctionnement pendant un délestage**: la distribution de contenu contrôlé et non contrôlé jusqu'au réseau domestique doit être prise en charge quand l'accès au système d'accès conditionnel est défectueux.
G-16	**contenu non protégé**: le pont de gestion DRM ne devrait avoir aucune influence sur l'utilisation d'un contenu non protégé.
G-17	**étendue de la protection d'un contenu**: la protection d'un contenu doit être disponible, comme établi par un ensemble de règles de système de gestion DRM, pour toutes les vidéotransmissions dans le réseau domestique.

G-18	**extension de l'ensemble de règles de gestion DRM**: un riche ensemble de règles de gestion DRM (copie, reproduction, heure de visionnement, etc.) est fourni dans le système de gestion DRM et doit impérativement être géré par le terminal adaptateur STB puis être étendu aux éléments de flux aval.
G-19	**authentification du client**: l'authentification doit être prise en charge pour tous les éléments intégrés au réseau domestique qui participent à la transmission et/ou à la consommation d'un contenu vidéo.
G-20	**chiffrement**: le chiffrement du contenu doit être fourni pour les vidéotransmissions dans le réseau domestique.
G-21	**révocation du dispositif**: la capacité de refuser l'accessibilité d'un contenu à un dispositif particulier doit être assurée, même si ce dispositif a été à un moment un élément de réseau valide du pont de gestion DRM.

5.5 Historique

Lors du traitement de l'acheminement d'un contenu protégé via un réseau de distribution sécurisé, il est critique qu'une technique soit en place afin de protéger le contenu contre une copie ou une redistribution non autorisée. En outre, le dispositif proprement dit doit impérativement être robuste et résistant à la compromission de la sécurité. La présente Recommandation détaille les exigences relatives à la technique de protection d'un contenu et les exigences de robustesse et de conformité pour les dispositifs qui manipulent un contenu protégé. Ces exigences relatives à la technique et à la robustesse d'un contenu sont rédigées du point de vue d'un dispositif de réception (c'est-à-dire un terminal adaptateur) chez un client qui reçoit un contenu issu d'un fournisseur de service vidéo dans le cadre d'un réseau de distribution par câble qui doit impérativement protéger un contenu à haute valeur ajoutée. Le contenu est chiffré à la source et est protégé dans tout le réseau du fournisseur de service. L'objet de la présente Recommandation consiste à garantir qu'un niveau comparable de sécurité est disponible dans les réseaux domestiques. L'insertion de ce flux de contenu par routage dans les environnements de flux aval de façon robuste et sécurisée constitue l'objet principal de la présente Recommandation.

Les techniques numériques de protection et d'extraction de contenu, qui permettent au contenu issu du fournisseur de service de sortir d'un terminal adaptateur, doivent impérativement garantir que ce fournisseur de service continue à conserver le contrôle de la copie et de la redistribution de ce contenu, même après que celui-ci est sorti du terminal adaptateur vers d'autres dispositifs. Les dispositifs situés en aval du terminal adaptateur, qui contiennent une quelconque sortie numérique, gestion DRM, ou technique de protection de contenu, doivent également être conformes aux règles de robustesse et de conformité établies pour le terminal adaptateur par la présente Recommandation. Les règles de robustesse et de conformité établies pour le terminal adaptateur vont contrôler l'ensemble de l'écosystème du flux aval.

6 Exigences relatives à la robustesse

Les dispositifs qui reçoivent et éventuellement distribuent un contenu protégé doivent impérativement être conformes à un certain nombre d'exigences relatives à la robustesse afin de garantir une protection suffisante du contenu. Il est reconnu que la robustesse peut varier selon le contenu disponible dans le dispositif et que cette robustesse peut nécessiter des changements dans le temps, au fur et à mesure de l'évolution de la technique de sécurisation et de celle de son piratage. Le présent paragraphe décrit un ensemble générique recommandé d'exigences relatives à la robustesse des dispositifs.

6.1 Construction

6.1.1 Généralités

Les produits doivent répondre aux règles de conformité et doivent être conçus et fabriqués de façon à déjouer effectivement les tentatives de modifier de tels produits afin de contourner les règles de conformité.

6.1.2 Fonctions de mise en échec

Les produits ne doivent pas comprendre:

i) d'interrupteurs, de boutons, de cavaliers, ni de traces spécifiques pouvant être coupées, ni des équivalents logiciels de l'un quelconque des éléments précédents;

ii) de menus ou fonctions de service (y compris les fonctions de télécommande),

permettant dans chaque cas de mettre en échec les techniques de protection du contenu, les systèmes de protection analogiques, la reprotection, les restrictions de sortie, les limitations d'enregistrement, ou autres dispositions obligatoires des règles de conformité ou permettant qu'un contenu contrôlé soit exposé à une copie non autorisée. Aux fins de la présente Recommandation, le terme "reprotection" signifie l'application d'une technique de protection homologuée, quand cela est nécessaire, à un contenu contrôlé reçu d'un réseau de vidéodistribution, ce contenu devant être extrait du terminal adaptateur. Ce terme doit également désigner l'intégrité du système et les méthodes par lesquelles une telle application est assurée.

6.1.3 Conservation des secrets

De façon à déjouer les tentatives, faites par des parties non autorisées, de compromettre la sécurité, les produits doivent être conçus et fabriqués de façon à déjouer effectivement les tentatives de découvrir ou révéler:

i) le numéro unique, d'une longueur binaire spécifiée, attribué à chaque terminal adaptateur, ou les nombres utilisés dans le traitement de chiffrement ou déchiffrement d'un contenu contrôlé (nombres désignés collectivement par le terme de "clés");

ii) les méthodes et algorithmes cryptographiques servant à produire de telles clés.

6.2 Chemins de contenu contrôlé

Un contenu ne doit pas être disponible à des sorties autres que celles qui sont spécifiées dans les règles de conformité et, dans de tels produits, un contenu contrôlé ne doit pas être présent sur d'éventuels bus accessibles à l'utilisateur (comme défini ci-dessous) sous une forme non chiffrée et comprimée. De même, des clés non chiffrées servant à prendre en charge un quelconque chiffrement et/ou déchiffrement du contenu dans les données du produit ne doivent pas être présentes sur d'éventuels bus accessibles à l'utilisateur. Un "bus accessible à l'utilisateur" est un bus de données conçu pour des mises à jour par l'utilisateur final ou pour un accès tel qu'un bus *PCI* qui possède des interfaces de connexion ou qui est autrement accessible à l'utilisateur, ou qui peut recevoir une carte de type *SmartCard*, *PCMCIA* ou *Cardbus*.

6.3 Méthodes permettant d'augmenter la robustesse des fonctions

Les produits doivent utiliser au moins les techniques suivantes afin d'augmenter la robustesse des fonctions et des protections spécifiées dans la présente Recommandation:

6.3.1 Fonctions réparties

Les portions du produit qui exécutent l'authentification et le déchiffrement, ainsi que le décodeur MPEG (ou dispositif semblable), doivent être conçus et fabriqués en association sinon en intégration les uns avec les autres de façon qu'un contenu contrôlé, dont le flux s'écoule sous toute

forme utilisable entre ces portions du produit, soit sécurisé au niveau de protection décrit dans le § 6.3.5 ci-dessous contre toute interception ou copie.

6.3.2 Logiciel

Toute portion du produit qui implémente dans un logiciel une partie de la technique de protection d'un contenu doit comprendre toutes les caractéristiques exposées dans les § 6.1 et 6.2. Aux fins de la présente Recommandation, le terme "logiciel" doit signifier l'implémentation des fonctions selon les exigences établies par la présente Recommandation au moyen de tout code de programmation informatique composé d'instructions ou de données, autre que les instructions ou données qui sont incluses dans le matériel. De telles implémentations doivent:

a) être conformes au § 6.1.3 par toute méthode raisonnable y compris mais sans exhaustivité: le chiffrement, l'exécution d'une portion de l'implémentation en mode superviseur (anneau de niveau zéro) et/ou implantation dans une sécurisation d'implémentation physique; et dans chaque cas d'implémentation sous forme logicielle, utilisation des techniques efficaces d'obscurcissement afin d'interdire ou de restreindre les tentatives de découvrir les approches utilisées;

b) être conçues de façon à exécuter un autocontrôle de l'intégrité de leurs éléments constituants de telle sorte que des modifications non autorisées soient censées se traduire par une défaillance de l'implémentation à offrir la fonction autorisée d'authentification et/ou de déchiffrement. Aux fins de cette disposition, une "modification" contient tout changement, perturbation ou invasion d'éléments de service ou de caractéristiques, ou interruption de traitement, relevant des § 6.1 et 6.2. Cette disposition nécessite au minimum l'utilisation d'un code avec contrôle de redondance cyclique qui est ensuite chiffré avec une clé privée ou un algorithme de hachage sécurisé;

c) répondre au niveau de protection décrit dans le § 6.3.5 ci-dessous;

d) être conçues de façon à offrir des mécanismes de protection contre des attaques logicielles non autorisées.

6.3.3 Matériel

Toute portion du produit qui implémente les exigences de la présente Recommandation dans le matériel doit comprendre toutes les caractéristiques exposées dans les § 6.1 et 6.2. Aux fins des présentes règles de robustesse, le terme "matériel" doit désigner un dispositif physique, y compris un composant, qui implémente l'une quelconque des exigences de protection d'un contenu auxquelles la présente Recommandation exige qu'un produit soit conforme et qui:

i) ne comprend pas d'instructions ou de données autres que celles qui sont constamment intégrées dans de tels dispositifs ou composants;

ii) qui contient des instructions ou données qui ne sont pas constamment intégrées dans des dispositifs ou composants lorsque de telles instructions ou données ont été individualisées pour de tels produits ou composants et lorsque de telles instructions ou données ne sont pas accessibles à l'utilisateur final au moyen de ces produits ou composants.

De telles implémentations doivent:

a) être conformes au § 6.1.3 par toute méthode raisonnable y compris mais sans exhaustivité: clés d'imbrication, méthodes de production des clés et algorithmes cryptographiques intégrés dans les circuits intégrés ou dans la logique câblée qui ne peuvent raisonnablement pas être lus, ou les techniques décrites ci-dessus pour les logiciels;

b) être conçues de façon que les tentatives de reprogrammation, de retrait ou de remplacement d'éléments matériels, d'une façon qui compromettrait la sécurité ou des caractéristiques de protection du contenu faisant partie de la technique en évaluation ou du terminal adaptateur, poseraient un risque sérieux d'endommagement du produit au point que celui-ci ne serait

plus en mesure de recevoir, de déchiffrer ou de décoder le contenu contrôlé. A titre d'exemple, un composant qui est soudé plutôt qu'enfiché dans un socle peut être approprié à cette fin;

c) répondre au niveau de protection décrit dans le § 6.3.5 ci-dessous.

6.3.4 Matériel hybride

Les interfaces entre portions matérielles et logicielles d'un produit doivent être conçues de façon qu'elles offrent un niveau de protection similaire à celui qui serait fourni par une implémentation purement matérielle ou purement logicielle, comme décrit ci-dessus.

6.3.5 Niveau de protection

Les fonctions essentielles de chiffrement (maintien de la confidentialité des clés, méthodes de production des clés et des algorithmes cryptographiques, conformité aux règles de conformité et prévention de la copie ou du visionnement sans autorisation d'un contenu contrôlé qui a été déchiffré) doivent être implémentées conformément aux exigences de "niveau 2" de la spécification FIPS PUB 140-2 "Exigences de sécurité pour modules cryptographiques" et, au minimum, de façon:

a) qu'on ne puisse raisonnablement pas prévoir qu'elles soient déjouées ou contournées au seul moyen d'outils ou d'équipements à usage général qui sont largement disponibles à un prix raisonnable tels que tournevis, cavaliers, pinces crocodiles et fers à souder ("outils largement disponibles"), ou au moyen d'outils électroniques spécialisés ou d'utilitaires logiciels spécialisés qui sont largement disponibles à un prix raisonnable, tels que lecteurs et enregistreurs de mémoire programmable en lecture seulement et effaçable électriquement (EPROM), débogueurs ou décompileurs ou outils de développement logiciel analogues ("outils spécialisés"), autres que les dispositifs ou techniques aussi bien matériels que logiciels qui sont conçus et mis à disposition dans l'intention spécifique de contourner ou de circonvenir les techniques de protection requises ("dispositifs de contournement"); et

b) qu'elles ne puissent être déjouées ou contournées qu'avec difficulté au moyen d'outils ou d'équipements professionnels (à l'exclusion des dispositifs de contournement et des outils ou équipements professionnels qui ne sont mis à disposition que sur la base d'un accord de non-divulgation), tels que les analyseurs logiques, les systèmes de désassemblage de circuits intégrés, ou les émulateurs en circuit ou autres outils, équipements, méthodes ou techniques non inclus dans la définition des outils largement disponibles et des outils spécialisés sous lettre a ci-dessus.

7 Règles de conformité

7.1 Introduction

De façon à être accepté pour rattachement au réseau d'un fournisseur de service vidéo en vue de la réception de contenus protégés, un dispositif doit impérativement être conforme à un certain nombre de conditions.

7.2 Sorties

7.2.1 Généralités

Un produit ne doit ni extraire ni transmettre un contenu reçu au moyen du Service, à destination d'une quelconque sortie sauf si cela est autorisé dans la présente Recommandation, aux fins de laquelle une sortie doit être considérée comme incluant, mais sans y être limitée, toutes les transmissions vers un quelconque dispositif interne de copie, d'enregistrement ou de stockage, mais à l'exclusion des transmissions internes non persistantes ou transitoires qui satisfont par ailleurs aux présentes règles de conformité et de robustesse.

7.2.2 Sorties analogiques à définition normale

Les produits comportant d'éventuelles sorties analogiques à définition normale ne doivent extraire un contenu reçu au moyen du service, ou transmettre un contenu reçu au moyen du service, que si ce contenu est convenablement protégé en conformité avec les normes nationales ou régionales appropriées à la protection contre la copie de contenu analogique.

7.2.3 Sorties analogiques à haute définition

Le produit doit être en mesure de limiter à une image contrainte, quand cela est rendu nécessaire par le bit CIT des informations CCI, la résolution d'un contenu à haute définition qui doit être extrait au moyen d'une connexion capable de transmettre un contenu sous une forme analogique à haute définition. Le produit doit comprendre une ou plusieurs sorties numériques homologuées. Tous les produits doivent émettre et propager des signaux CGMS-A pour toutes les sorties analogiques à haute définition; mais ils ne doivent pas être tenus de respecter le déclenchement CGMS-A sauf prescription contraire de la législation ou réglementation appropriée.

7.2.4 Sorties numériques

Un produit possédant éventuellement des sorties numériques ne doit extraire ou transmettre le contenu reçu au moyen du service que conformément aux règles d'autorisation de la présente Recommandation. Une liste des techniques dont la conformité à la présente Recommandation a été contrôlée par des essais est contenue dans l'Appendice I.

7.2.5 Non-brouillage du filigrane numérique

Les produits et composants DOIVENT IMPÉRATIVEMENT NE PAS enlever, obscurcir ou brouiller le filigrane numérique consensuel dans un contenu contrôlé qui a été déchiffré.

7.3 Copie, enregistrement et stockage d'un contenu contrôlé

7.3.1 Généralités

Les produits, y compris sans limitation, ceux qui possèdent une capacité intrinsèque ou intégrée de copie, d'enregistrement ou de stockage, ne doivent pas copier, enregistrer, ou mémoriser de contenu contrôlé, sauf si cela est autorisé dans le présent paragraphe.

7.3.2 Simple tampon d'affichage

Les produits peuvent mémoriser temporairement un contenu contrôlé à seule fin de permettre l'affichage immédiat de ce contenu contrôlé, à condition que:

a) un tel stockage ne persiste pas après que le contenu a été affiché;

b) les données ne soient pas mémorisées de façon à prendre en charge la copie, l'enregistrement, ou le stockage de telles données à d'autres fins.

7.3.3 Plus aucune copie

Les produits ne doivent pas dupliquer, enregistrer ou mémoriser un contenu contrôlé qui est désigné dans les bits EMI comme ayant été copié mais qui ne doit plus être copié désormais ("plus aucune copie"), sauf si cela est autorisé dans le § 7.3.2 ou 7.3.5.2.

7.3.4 Jamais de copie

Les produits, y compris (sans limitation) un dispositif avec capacité d'enregistrement intégrée tel que l'appareil communément appelé "magnétoscope personnel", ne doivent pas copier un contenu contrôlé qui est désigné dans les bits EMI comme ne devant jamais être copié ("jamais de copie") sauf si cela est autorisé dans le § 7.3.2 ou par ce qui suit.

Un tel dispositif peut stocker en mémoire interne un tel contenu, y compris afin de mettre en pause le programme, si le contenu mémorisé est rattaché de façon sûre au produit effectuant

l'enregistrement au point qu'il n'en soit pas effaçable et qu'il ne soit pas lui-même exposé ultérieurement à un enregistrement temporaire ou autre dans le produit avant d'être rendu inutilisable; à condition que le dispositif soit réalisé conformément aux exigences spécifiées au sujet de la robustesse afin d'éviter le contournement de telles restrictions. Lors du stockage interne d'un tel contenu, y compris aux fins de l'implémentation d'une pause comme autorisé dans le présent paragraphe, le contenu doit être mémorisé de façon à être chiffré et à ne pas offrir de sécurité inférieure à la norme de chiffrement évolué (AES, *advanced encryption standard*) de 128 bits.

Les produits doivent être conçus et fabriqués de façon à être en mesure de masquer le contenu mémorisé ou à le rendre inutilisable après un intervalle de temps défini, trame par trame, minute par minute, méga-octet par méga-octet.

7.3.5 Copie de première génération

7.3.5.1 Fonction de copie

Les produits peuvent faire une copie d'un contenu contrôlé qui est désigné dans les bits EMI comme pouvant être copié sur une seule génération ("copie de première génération"), comme décrit dans le § 7.3.2 ou 7.3.4 ou à condition que la copie

a) soit brouillée, chiffrée ou rattachée de façon unique à ce dispositif, dans chaque cas avec utilisation d'une forme de protection contre la copie qui est identifiée par un amendement au § 7.3.5, le cas échéant;

b) soit marquée comme ne devant plus être copiée ("plus aucune copie") d'une façon qui sera identifiée par un amendement au § 7.3.5, le cas échéant, et qui permettra d'empêcher efficacement que de telles nouvelles copies soient effectuées par des dispositifs capables de recevoir la transmission de telles données marquées, par l'intermédiaire des sorties identifiées dans le § 7.2.4. En l'absence de l'un ou l'autre de ces deux amendements au § 7.3.5, aucune copie d'un tel contenu contrôlé, autre que conformément aux règles d'autorisation indiquées dans le § 7.3.2 ou 7.3.4, ne pourra être effectuée, sauf comme prévu dans le § 7.3.5.2.

7.3.5.2 Fonction de transfert

Un produit qui fait une copie de contenu marquée dans les informations CCI comme étant une "copie de première génération" conformément au § 7.3.5 ne peut transférer un tel contenu vers un unique support d'enregistrement effaçable ou vers un unique dispositif d'enregistrement externe, que quand :

a) le dispositif d'enregistrement externe indique qu'il est autorisé à exécuter cette fonction de transfert conformément aux exigences du présent paragraphe et à copier un tel contenu contrôlé conformément aux exigences du § 7.3.5;

b) un tel contenu contrôlé est marqué pour transmission par le produit de départ comme étant une "copie de première génération";

c) le contenu contrôlé est extrait vers une sortie protégée conformément aux § 7.2.2, § 7.2.3 ou § 7.2.4;

d) avant que le transfert soit effectué, l'enregistrement initial par le produit est rendu inutilisable et le contenu contrôlé faisant l'objet du transfert est marqué "Plus aucune copie";

e) le dispositif vers lequel le support d'enregistrement effaçable est transféré est incapable ou rendu incapable d'extraire le contenu contrôlé, sauf au moyen de sorties autorisées par les présentes règles de conformité;

f) la copie est mémorisée:

i) au moyen d'un protocole de chiffrement homologué par amendement des présentes règles de conformité, qui associe de façon univoque de telles copies à un unique dispositif de façon qu'elles ne puissent pas être reproduites sur un autre dispositif ou, si elles sont mémorisées sur un support effaçable, de façon qu'aucune copie encore utilisable ne puisse en être effectuée;

ii) même en utilisant par ailleurs les méthodes citées en référence dans le § 7.3.5.1.

L'implémentation actuelle limite les transferts à un transfert unique. Des moyens supplémentaires de contrôler le contenu sont à l'étude et pourraient être appliqués quand le système de gestion DRM de prochaine génération sera défini.

8 Commande de changement

Toute modification matérielle ou substantielle à la technique devra être réévaluée au moyen des critères et processus ici décrits. Ces modifications matérielles ou substantielles comprennent ce qui suit mais n'y sont pas limitées:

1) mappage sur un nouveau transport ou média;

2) modifications dans le codage ou dans le traitement d'un contenu;

3) modifications qui peuvent avoir un effet matériel et défavorable sur l'intégrité ou la sécurité de la technique;

4) modifications dans la méthode cryptographique utilisée (sauf si l'algorithme n'est pas modifié et si seule la longueur de clé est augmentée);

5) modifications du domaine d'application de la redistribution;

6) tout changement fondamental dans la nature de la technique.

Annexe A

Informations de commande de copie

Les informations de commande de copie (CCI, *copy control information*) sont transmises à partir du fournisseur de service vidéo sur le canal de données afin d'informer le terminal adaptateur du niveau requis de protection contre la copie. Les informations CCI sont envoyées sans codage au terminal adaptateur, mais l'intégrité des informations est conservée par authentification des informations CCI au moyen d'un simple protocole. Ce traitement est réitéré pour chaque élément du flux aval à partir du terminal adaptateur.

L'unique octet du champ d'informations CCI contient des informations que le terminal adaptateur et les éléments du flux aval utilisent afin de commander la copie d'un contenu. Deux bits EMI commandent la copie sur sorties numériques de terminal adaptateur, deux bits APS commandent la copie sur sorties analogiques, un seul bit commande un déclenchement de contrainte d'image et trois bits sont réservés.

A.1 Changement de canal

Quand un changement de canal se produit, le terminal adaptateur doit traiter tous les contenus à protection (CP, *content protection*) par brouillage comme si les bits EMI étaient réglés à "jamais de copie", mais ne doit pas appliquer de contrainte d'image avant que le nouveau message CCI soit reçu. Le terminal adaptateur doit immédiatement commencer à utiliser les valeurs du message CCI quand celui-ci est reçu du fournisseur de service vidéo. Si un nouveau message CCI n'est pas reçu dans les 10 s, le terminal adaptateur doit appliquer la contrainte d'image comme si le bit CIT avait été réglé à 1. Un changement de canal ne doit pas provoquer l'apparition d'un rafraîchissement de clé.

A.2 Définition des informations CCI

Les informations CCI forment un champ d'un octet (8 bits) transporté du terminal adaptateur aux éléments de réseau du flux aval. Cinq de ces 8 bits sont définis. Les trois autres sont réservés. Les bits réservés doivent être réglés à zéro comme représenté dans le Tableau A.1. L'élément du flux aval ne doit utiliser les valeurs de bit réservé reçues du terminal adaptateur vidéo que pour l'exécution du protocole de tunnel authentifié qui est décrit ci-dessous. Le terminal adaptateur doit ignorer les valeurs suivantes du bit réservé.

Tableau A.1/J.197 – Affectation des bits d'informations CCI

Bits CCI n°	7	6	5	4	3	2	1	0
Le VSP met à:	0	0	0	CIT	APS1	APS0	EMI1	EMI0
Le STB interprète par:	rsvd	rsvd	rsvd	CIT	APS1	APS0	EMI1	EMI0

A.3 Bits EMI de commande DE copie numérique

Les deux bits de plus faible poids de l'octet du message CCI sont les bits EMI. Ils doivent commander les autorisations de copie pour les copies numériques. Les bits EMI doivent être fournis à tout accès numérique d'une sortie de terminal adaptateur pour la commande des copies effectuées à partir de ces sorties. Les bits EMI sont définis dans le Tableau A.2.

Tableau A.2/J197 – Valeurs et contenu des bits EMI

Valeur EMI	Autorisation de copie numérique	Type de contenu
00	Copie non restreinte	Pas de "Valeur haute"
01	Plus aucune copie autorisée	Valeur haute
10	Copie de première génération autorisée	Valeur haute
11	Copie interdite	Valeur haute

A.4 APS – Système de protection analogique

Les bits 3 et 2 des informations CCI, comme représenté dans le Tableau A.1, sont respectivement les bits APS 1 et 0. Le terminal adaptateur doit utiliser les bits APS afin de commander le codage de protection contre la copie aux sorties analogiques composites comme décrit dans le Tableau A.3.

Tableau A.3/J.197 – Définition des valeurs du système APS

APS	Description
00	Codage de protection contre la copie désactivé
01	Traitement AGC activé, rafale de signaux chromatiques modulés désactivée
10	Traitement AGC activé, rafale de signaux chromatiques modulés activée sur une paire de lignes
11	Traitement AGC activé, rafale de signaux chromatiques modulés activée sur un bloc de 4 lignes

A.5 CIT – déclenchement de contrainte d'image

Le bit 4 des informations CCI est, comme représenté dans le Tableau A.4, le bit CIT. Le terminal adaptateur doit utiliser le bit CIT afin de commander la contrainte d'image des sorties analogiques à composantes de haute définition.

Tableau A.4/J.197 – Valeurs et application du bit CIT

Valeur du bit CIT	Application de contrainte d'image
0	Aucune contrainte d'image validée
1	Contrainte d'image requise

A.6 Protocole de tunnel authentifié

Le terminal adaptateur calcule la valeur CCI_auth au moyen de la valeur d'informations CCI reçue et la compare à la valeur CCI_auth reçue du fournisseur de service vidéo. L'échec d'équivalence produit une condition d'erreur et le terminal adaptateur met les bits EMI à 11 puis applique la contrainte d'image comme si la valeur avait été égale à 1.

Annexe B

Liste de contrôle de la robustesse

Avant de commercialiser un produit quelconque, le réalisateur de la technique doit impérativement exécuter des essais et analyses afin de garantir la robustesse de l'implémentation. La liste de contrôle de la robustesse ci-dessous peut être utilisée afin d'aider le réalisateur à effectuer des essais couvrant certains aspects importants de la robustesse. Etant donné que la liste de contrôle de la robustesse ne vise pas tous les éléments requis pour la fabrication d'un produit conforme, le réalisateur est instamment prié d'évaluer sous tous les angles, aussi bien ses procédures d'essai que la conformité de ses produits.

Questions générales relatives à l'implémentation

1) Est-ce que le produit a été conçu et fabriqué de façon qu'il n'y ait aucun interrupteur, bouton, cavalier, ou équivalent logiciel de ce qui précède, ni de trace spécifique qui puisse être coupée, par lequel les techniques de protection du contenu, les mesures de protection analogiques, les restrictions de sortie, les limitations d'enregistrement ou autres dispositions obligatoires des règles de conformité pourraient être déjouées ou par lequel un contenu contrôlé pourrait être exposé à une copie non autorisée?

2) Est-ce que le produit a été conçu et fabriqué de façon qu'il n'y ait aucun menu de service ni aucune fonction (telle que fonction de télécommande, interrupteur, case à cocher ou autre dispositif) qui pourrait intercepter le flux d'un contenu contrôlé ou l'exposer à une copie non autorisée?

3) Est-ce que le produit a été conçu et fabriqué de façon qu'il n'y ait aucun menu de service ni aucune fonction (telle que fonction de télécommande, interrupteur, case à cocher ou autre dispositif) qui pourrait désactiver tous les systèmes de protection analogiques, les restrictions de sortie, les limitations d'enregistrement, ou autres dispositions obligatoires des règles de conformité?

4) Est-ce que le produit possède un menu de service, des fonctions de service, ou des utilitaires de service qui pourraient altérer ou révéler le flux d'un contenu contrôlé dans le dispositif?

   Si oui, veuillez décrire ce menu de service, ces fonctions de service, ou ces utilitaires de service ainsi que les mesures qui sont prises afin de garantir que ces utilitaires de service ne serviront pas à révéler ou à dévier le contenu contrôlé.

5) Est-ce que le produit possède un menu de service, des fonctions de service, ou des utilitaires de service qui pourraient désactiver tous les systèmes de protection analogiques, les restrictions de sortie, les limitations d'enregistrement, ou autres dispositions des règles de conformité?

   Si oui, veuillez décrire ces menus, fonctions ou utilitaires de service et les mesures qui sont prises afin de garantir que ces utilitaires de service ne serviront pas à déjouer les éléments du service de chiffrement du produit (y compris l'observation des présentes règles de conformité).

6) Est-ce que le produit possède des bus accessibles à l'utilisateur (comme défini dans le § 6.2 des Règles de robustesse)?

   Si tel est le cas, est-ce qu'un contenu contrôlé est acheminé sur ce bus?

   Si tel est le cas, alors:

   identifier et décrire le bus et indiquer si le contenu contrôlé est comprimé ou non comprimé. Si ces données sont comprimées, alors expliquer en détail comment et par quels

moyens les données vont être rechiffrées comme requis par le § 6.2 des règles de robustesse.

7) Expliquer en détail comment le produit protège la confidentialité de toutes les clés.

8) Expliquer en détail comment le produit protège la confidentialité des algorithmes cryptographiques confidentiels qui sont utilisés dans le produit.

9) Si le produit achemine un contenu contrôlé d'une partie à une autre de ce produit, que ce soit entre modules logiciels, entre circuits intégrés ou entre leurs combinaisons, expliquer comment les portions du produit qui exécutent l'authentification et le déchiffrement, ainsi que le décodeur MPEG (ou dispositif semblable) ont été conçues, associées et intégrées les unes avec les autres au point qu'un contenu contrôlé soit protégé contre l'interception et la copie conformément au § 6.3.1 des règles de robustesse.

10) Est-ce que des fonctions de protection d'un contenu sont implémentées dans le matériel?

Si oui, répondre aux questions relatives à l'implémentation matérielle.

11) Est-ce que des fonctions de protection d'un contenu sont implémentées dans le logiciel?

Si oui, répondre aux questions relatives à l'implémentation logicielle.

Questions relatives à l'implémentation logicielle

12) Dans le produit, décrire la méthode par laquelle toutes les clés sont mémorisées de façon protégée.

13) Au moyen de l'utilitaire d'impression grep ou équivalent, êtes-vous incapable de découvrir d'éventuelles clés dans les images binaires d'éventuels dispositifs à mémoire persistante?

14) Dans le produit, décrire la méthode servant à obscurcir les algorithmes cryptographiques confidentiels et les clés confidentielles dont l'implémentation est logicielle.

15) Décrire la méthode par laquelle les valeurs cryptographiques intermédiaires (par exemple les valeurs créées pendant le traitement d'authentification entre modules ou dispositifs dans un produit) sont créées et conservées de façon protégée dans le produit.

16) Décrire la méthode utilisée afin d'empêcher l'utilisation d'utilitaires communément disponibles de débogage ou décompilation (par exemple, *Softice*) afin de décomposer en étapes, de décompiler, ou d'examiner l'application des fonctions de protection d'un contenu implémentées dans le logiciel.

17) Décrire la méthode par laquelle le produit autocontrôle l'intégrité d'éléments constituants de telle façon que d'éventuelles modifications provoqueraient un défaut d'autorisation ou de déchiffrement comme décrit dans le § 6.3.2b des règles de robustesse. Décrire ce qui se passe quand l'intégrité est violée.

18) Afin de garantir que l'autocontrôle d'intégrité est bien effectué, exécuter un essai et s'assurer que l'exécutable ne parviendra pas à fonctionner dès qu'un éditeur binaire est utilisé afin de modifier un octet aléatoire de l'image exécutable contenant des fonctions de protection d'un contenu; décrire la méthode et les résultats de cet essai.

Questions relatives à l'implémentation du matériel

19) Dans le produit, décrire la méthode par laquelle toutes les clés sont mémorisées de façon protégée et comment leur confidentialité est conservée.

20) Au moyen de l'utilitaire d'impression grep ou équivalent, êtes-vous incapable de découvrir d'éventuelles clés dans les images binaires d'éventuels dispositifs à mémoire persistante?

21) Dans le produit, décrire comment les algorithmes cryptographiques confidentiels et les clés confidentielles utilisés ont été implémentés dans les circuits intégrés ou dans la logique câblée de façon qu'ils ne puissent pas être lus.

22) Décrire la méthode par laquelle les valeurs cryptographiques intermédiaires (par exemple les valeurs créées pendant le traitement d'authentification entre modules ou dispositifs dans un produit) sont créées et conservées de façon protégée dans le produit.

23) Décrire les moyens utilisés afin d'empêcher les tentatives de remplacer, de supprimer, ou d'altérer des éléments ou modules matériels servant à implémenter des fonctions de protection d'un contenu?

24) Dans le produit, est-ce que la suppression ou le remplacement d'éléments ou modules matériels qui compromettraient les éléments de service de protection du contenu du produit (y compris les règles de conformité et les règles de robustesse) endommage le produit au point de rendre le produit incapable de recevoir, de déchiffrer, ou de décoder un contenu contrôlé?

Appendice I

Sorties numériques

Il sera nécessaire de vérifier la conformité des sorties numériques aux exigences établies dans la présente Recommandation. Les sorties numériques énumérées ci-dessous ont été vérifiées quant à leur conformité à la présente Recommandation et sont indiquées pour information. Il est attendu que d'autres sorties seront ultérieurement conformes aux exigences de la présente Recommandation.

I.1 La compagnie *Cable Television Laboratories* a essayé la sortie suivante et constate qu'elle est conforme à la présente Recommandation:

- **1394 avec DTCP**: le produit peut extraire un contenu contrôlé et le transmettre à une sortie sous forme numérique sur des interfaces IEEE 1394, où une telle sortie est protégée par le système DTCP. Le produit doit impérativement prendre en charge la valeur DTCP "authentification complète"; il peut également prendre en charge la valeur DTCP "authentification restreinte". Si cela est prescrit par la licence applicable à la protection DTCP, un contenu qui n'est pas contrôlé doit être extrait sur la sortie IEEE 1394 sans protection DTCP.

I.2 La compagnie *Cable Television Laboratories* a essayé la sortie suivante et constate qu'elle est conforme à la présente Recommandation:

- **Sortie DVI/HDMI avec HDCP**: le produit peut extraire le contenu reçu au moyen du service et le transmettre au moyen du service à une sortie, sous forme numérique sur les interfaces DVI y compris HDMI et lorsque la sortie a une protection HDCP toujours active. Le produit doit impérativement transmettre à la fonction HDCP tous les messages SRM reçus légalement.

Appendice II

Critères d'évaluation

Selon la sortie spécifique ou la technique soumise, les critères d'évaluation devraient comprendre ce qui suit:

II.1 Transport des signaux vidéo

Est-ce que les méthodes de conversion et d'acheminement des informations CCI jusqu'au terminal adaptateur sont définies dans l'environnement ou profil du dispositif proposé?

i) *Sorties numériques à compression*

- Est-ce que le système de compression numérique original est utilisé à l'interface, ou est-ce que le signal est recomprimé?
- Si le signal est recomprimé, quels système, profil, résolution et débit binaire sont requis?
- Si la compression originale est préservée, est-ce que le multiplex de transport est envoyé entier à l'interface, ou est-ce que celle-ci est limitée à unique flux de programme envoyé après le démultiplexage?
- Si la sortie transporte le flux de transport entier, comment est-ce que les informations du système (par exemple les données hors bande) vont-elle être transportées?
- Quelles méthodes utilise-t-on afin de garantir un flux ininterrompu de programmes à travers cette interface, sans considération d'un autre trafic (QS) pouvant être présent à cette interface?
- Quel est le débit utile de données minimal qui est garanti à l'interface?
- Quelles méthodes utilise-t-on afin de permettre l'acheminement, le décodage, ou l'affichage des données analogiques ou numériques à sous-titrage codé, des niveaux consultatifs de contenu et des messages dans la bande du système d'alerte d'urgence?
- Comment les services de programmation analogiques sont-ils préservés en transparence à cette interface?

ii) *Sorties numériques sans compression*

- quel est le débit utile de données minimal qui est garanti à l'interface?
- Comment les services de programmation analogiques sont-ils préservés en transparence à cette interface?
- Quelles méthodes utilise-t-on afin de permettre l'acheminement, le décodage, ou l'affichage de données analogiques ou numériques à sous-titrage codé, des niveaux consultatifs de contenu et des messages dans la bande du système d'alerte d'urgence?

II.2 Interfaces de sécurité

- Comment est-ce que la sécurité est utilisée lors du transport des signaux vidéo et comment est-ce que ce transport est associé aux profils de protection du contenu et aux méthodes d'authentification et de protection des profils de protection du contenu?
- Quelles sont les méthodes utilisées pour la construction, la protection et l'échange des clés?
- Y a-t-il des zones apparentes où le contenu est sans codage?

II.3 Points d'attaque et vulnérabilités du système

- Est-ce que la technique peut être contournée quelque part?
- Où se trouvent les plus faibles barrières qui peuvent être attaquées?

- Où le pirate attaquera-t-il et quelles ressources seront-elles requises?
- Quelles sont les possibles vulnérabilités/menaces et quel est le compromis de sécurité en fonction des coûts appliqués?

II.4 Efficacité de la technique proposée

- Est-ce que la technique proposée protège adéquatement le contenu lors de son passage par la sortie numérique ou lors de son enregistrement ou stockage sécurisé pour reproduction ultérieure?
- Quel est le domaine d'application de la redistribution du contenu? Est-ce que la technique de sortie numérique ou de gestion DRM protège effectivement le contenu contre une redistribution non autorisée, au moyen d'un contrôle de localisation ou d'autres restrictions d'ordre géographique ou propres à l'utilisateur?

II.5 Traitement de sécurité

- Est-ce que les clés et les secrets sont protégés contre la lecture et l'écriture pendant les calculs cryptographiques?
- Est-ce que les informations CCI, la contrainte d'image et d'autres commandes sont protégées dans toute la conception du système?

II.6 Révocation et renouvelabilité des clés

- Est-ce que le produit offre une solution de révocation des clés au niveau du système?
- Est-ce que le produit offre une solution de renouvelabilité des clés au niveau du système?
- Quels critères et processus sont utilisés pour la révocation et la renouvelabilité? Qui sont les participants à ce processus?
- Quelle sont les longueurs minimale et maximale du message de renouvelabilité du système (SRM, *system renewability message*) et dans quel format ce message est-il acheminé?
- Comment le message SRM est-il généralement acheminé? Quelles conséquences opérationnelles et infrastructurelles la solution de révocation/renouvelabilité aurait-elle sur un réseau de fournisseur de service vidéo (y compris les biens d'équipement ou les mises à jour du réseau qui peuvent être requis)? Que doit impérativement faire un fournisseur de service vidéo afin d'adopter les solutions proposées de révocation et de renouvelabilité?

II.7 Nouveaux algorithmes

- Quelle est la résistance relative de l'algorithme?
- Quelle est la résistance relative d'authentification par rapport à d'autres techniques?

II.8 Préservation de l'intégrité du service

- Est-ce que la sortie/technique proposée proposée interfère avec l'observation – par un dispositif tel qu'un terminal adaptateur – de ses autres obligations de licence ou d'essais? Est-ce que la commutation de source analogique ou le transfert à haute définition est nécessaire pour la sortie numérique proposée?
- Est-ce que la sortie permet de préserver les applications de navigation et de service du fournisseur de service?
- Est-ce que la sortie/technique proposée interfère avec d'autres dispositifs et interfaces disponibles dans le commerce?
- Est-ce que la sortie/technique proposée pose des problèmes d'interopérabilité avec d'autres dispositifs et interfaces disponibles dans le commerce?

- L'interface proposée est-elle interopérable avec des produits issus d'autres constructeurs, ou constitue-t-elle une solution soumise à droits intellectuels ou autrement exclusive?
- Est-ce que l'interopérabilité est définie par des normes industrielles (lesquelles?) ou par une licence, ou par les deux?
- Est-ce que la technique nécessite des essais de conformité ou de compatibilité afin d'assurer l'interopérabilité?

II.9 Conditions d'octroi de licences

- Les conditions d'octroi de licences devraient être conformes à la pratique de l'UIT et aux prescriptions nationales.

II.10 Impact global sur le réseau de vidéodistribution

- Quels impacts opérationnels et infrastructurels la technique proposée aura-t-elle sur un réseau de vidéodistribution (y compris les biens d'équipement ou les mises à jour du réseau qui pourront être requis)?
- Que doit impérativement faire un fournisseur de service vidéo afin d'adopter la solution technique proposée?

Appendice III

Revue des éléments de solution technique en vue de leur soumission

Les techniques faisant l'objet du présent processus d'évaluation recommandé comprennent les interfaces numériques protégées, l'enregistrement et le stockage sécurisés du contenu, la reproduction de celui-ci et la gestion des droits numériques. Les mesures de sécurité spécifiquement utilisées par ces techniques peuvent varier. Par ailleurs, différentes techniques de sortie peuvent faire appel à des mécanismes et protocoles de transport qui nécessitent certaines limitations ou restrictions d'implémentation. Le présent appendice identifie plusieurs éléments essentiels qui devraient être communs à toutes les techniques dont l'application est en cours d'étude, mais il ne constitue pas une liste exhaustive qui exclurait d'autres types d'informations pouvant être nécessaires afin d'évaluer complètement une technique particulière. Les appels d'offres doivent impérativement éviter toute omission ou fausse déclaration concernant les spécifications des matériels, les faits, ou d'autres détails nécessaires afin de conduire une analyse approfondie et précise de la technique.

Les techniques considérées peuvent comporter un mélange d'éléments relatifs aux interfaces numériques protégées, à l'enregistrement et au stockage sécurisés du contenu et aux techniques de gestion des droits numériques. Les paragraphes suivants décrivent les éléments recommandés qui devraient être soumis en vue de l'analyse approfondie des techniques envisagées.

III.1 Conditions d'octroi de licence

Les conditions d'octroi de licence devraient être conformes à la pratique de l'UIT et aux prescriptions nationales.

Note sur les règles de robustesse et de conformité – Les dispositifs en flux aval du terminal adaptateur, qui contiennent éventuellement une technique de sortie numérique, de gestion DRM, ou de protection du contenu doivent impérativement être également conformes aux règles de robustesse et de conformité établies par la présente Recommandation pour le terminal adaptateur. Les règles de robustesse et de conformité établies pour le terminal adaptateur contrôleront l'ensemble de l'écosystème du flux aval. En conséquence, les règles de robustesse et de conformité revendiquées dans toute licence technologique d'un constructeur doivent impérativement ne pas être en contradiction avec les règles de robustesse et de conformité détaillées dans la présente Recommandation.

III.2 Aperçu général de la sécurité

La spécification et la documentation de la sécurité devraient comprendre une introduction et un aperçu général de la sécurité comportant:

1) Un aperçu général de l'architecture de sécurité, de ses composants (par exemple serveur de mise en paquets, serveur de licence, client, etc.), de leurs fonctions et des interfaces essentielles, des exigences de connexité pour la sortie/sécurité.
2) Un schéma détaillé de l'architecture de sécurité indiquant les composants et interfaces essentiels qui sont nécessaires afin d'implémenter la solution de bout en bout, y compris le récepteur et les autres éléments de média (ordinateurs, mémoires, écrans, etc.).
3) Cet aperçu général devrait également identifier clairement les options de transport des signaux vidéo lorsqu'il y a des options d'implémentation. Par exemple, les algorithmes de chiffrement pour le transport des signaux vidéo (AES, 3-DES, etc.) et les algorithmes d'échange de clés (Diffie-Hellman, RSA, etc.).
4) Une description détaillée du mappage des règles ou des licences de protection du contenu d'un terminal adaptateur sur la technique proposée de protection du contenu qui doit être intégrée dans les dispositifs "en flux aval", en analysant spécifiquement la question du

maintien global de la sécurité et de la protection du contenu dans tout l'écosystème de distribution.

III.3 Transport des signaux vidéo

La spécification de sécurité devrait comprendre des détails concernant la méthode de transport des signaux vidéo et les spécificités de la façon dont les informations de commande de copie (CCI) présentées par le terminal adaptateur sont converties dans l'environnement ou profil proposé. La spécification devrait également préciser comment le transport des signaux vidéo est associé à d'éventuels profils de protection du contenu et indiquer les méthodes d'authentification et de protection des profils de protection du contenu.

Par ailleurs, des spécifications ou d'autres descriptions techniques doivent impérativement être fournies afin d'expliquer complètement comment la sortie numérique proposée prend en charge un ou plusieurs protocoles de transport de signaux vidéo capables d'acheminer tous les services audiovisuels définis[1] et associés à un terminal adaptateur sans interrompre, empêcher ni dégrader l'acheminement de tels services jusqu'au dispositif d'affichage final. De tels services comprennent également, mais sans y être limités, l'acheminement, le décodage, ou l'affichage de données analogiques ou numériques à sous-titrage codé, les niveaux consultatifs de contenu et les messages du système d'alerte d'urgence.

L'analyse technologique devrait être conduite pour chaque mécanisme et chaque protocole de transport englobé dans la technique de protection d'un contenu. De telles analyses devraient être effectuées transport par transport, ou média par média. Si une technique particulière satisfait correctement aux critères ici définis, cette technique ne devrait pas être considérée comme bénéficiant d'une "approbation générale" pour un quelconque transport ou protocole.

III.4 Profils de protection du contenu

La spécification de sécurité devrait comprendre des détails concernant le format et utiliser les éventuels profils de protection du contenu, signés numériquement, qui existent dans le système. La spécification de sécurité devrait également définir la structure et les options qui sont employées dans ce système et toutes les fonctions de messagerie et de signalisation nécessaires pour l'implémentation.

III.5 Algorithmes d'échange des clés

La spécification de sécurité devrait comprendre des détails concernant l'authentification des dispositifs de réception, des dispositifs de stockage et de tout dispositif connecté. La spécification de sécurité devrait également comprendre les méthodes d'authentification du serveur de licence, du serveur de mise en paquets et du client. Toutes les clés de session échangées et les protocoles cryptographiques utilisés devraient être bien définis pour une analyse complète. Des options sans chiffrement peuvent également être employées, mais elles devraient être expliquées sous tous les angles.

III.6 Interfaces de sécurité

La spécification devrait comprendre des détails qui définissent complètement les interfaces de sécurité du système global ainsi que la création et la protection de clés symétriques et asymétriques. Des définitions détaillées des composants de sécurité implémentés dans le matériel et dans le logiciel ont besoin d'être établies afin que ces interfaces de sécurité puissent être analysées.

---

[1] Voir par exemple la référence ANSI/SCTE-40-2004, § 8.1.

III.7 Traitement de sécurité

La spécification devrait comprendre des détails qui démontrent comment les clés et secrets sont protégés contre la lecture et l'écriture pendant les calculs cryptographiques et comment les informations CCI, la contrainte d'image et d'autres paramètres sont protégés dans tout le système.

III.8 Gestion des certificats

La spécification devrait comprendre des détails définissant complètement l'usage des certificats, les méthodes de protection de clé privées, les méthodes de révocation et la façon dont les certificats se rapportent à un contenu ainsi qu'aux serveurs distants de paquets/licences. Des détails relatifs à l'installation, à la signature, à l'enchaînement jusqu'à la racine, ainsi qu'à la structure globale, à la validation de sécurité et à la protection contre le clonage de certificats devraient être inclus.

III.9 Révocation/renouvelabilité de clé

La spécification devrait comprendre des détails sur la façon dont la révocation et la renouvelabilité des clés du système sont accomplies.

III.10 Points d'attaque/vulnérabilités possibles

La spécification devrait comprendre des revues ou analyses de menace pouvant être mises à disposition afin d'examiner les possibles vulnérabilités/menaces et le compromis avec les coûts appliqués. Des analyses de sécurité indépendantes devraient également être effectuées. Selon le cas, des restrictions à la non-divulgation pourront être mises en place afin de couvrir ces analyses.

III.11 Usage commercial

La soumission devrait comprendre toute utilisation commerciale connue de la sortie ou technique proposée, ainsi que toutes incidences connues sur la performance de dispositifs, ainsi que les questions d'interopérabilité. Le soumissionnaire devrait offrir une liste d'adopteurs (réalisateurs) et de supporteurs (propriétaires, développeurs de contenu, etc.) et devrait indiquer toutes relations commerciales entre le soumissionnaire de la technique et d'éventuels propriétaires de contenu.

III.12 Informations de contact

La soumission devrait comprendre les coordonnées nominatives de contact avec le spécialiste de la sécurité et avec d'autres personnes pouvant être approchées pour des questions concernant la soumission.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
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	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
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 et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006