

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1191

(02/2009)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés – Sécurité de la
télévision par réseau IP

**Spécifications fonctionnelles et architecture
pour les aspects de sécurité de la TVIP**

Recommandation UIT-T X.1191



RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1191

Spécifications fonctionnelles et architecture pour les aspects de sécurité de la TVIP

Résumé

La Recommandation UIT-T X.1191 traite des spécifications fonctionnelles, de l'architecture et des mécanismes relatifs aux aspects de sécurité du contenu, des services, des réseaux, des dispositifs terminaux et des abonnés (utilisateurs finals) de TVIP.

Source

La Recommandation UIT-T X.1191 a été approuvée le 20 février 2009 par la Commission d'études 17 (2009-2012) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Architecture de sécurité, authentification, autorisation, chiffrement, embrouillage, protection de la vie privée, protection de service et de contenu, sécurité, TVIP.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT [avait/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 2009

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	Termes et définitions 1
3.1	Termes définis ailleurs 1
3.2	Termes définis dans la présente Recommandation 3
4	Abréviations et acronymes 5
5	Conventions 6
6	Spécifications de sécurité 6
6.1	Spécifications de sécurité générales 6
6.2	Spécifications de sécurité du contenu..... 6
6.3	Spécifications de sécurité des services 9
6.4	Spécifications de sécurité des réseaux..... 11
6.5	Spécifications de sécurité des terminaux..... 12
6.6	Spécifications de sécurité des abonnés..... 13
7	Architecture de sécurité 14
7.1	Architecture de sécurité générale 14
7.2	Architecture de protection de contenu..... 16
7.3	Architecture de protection de service 19
7.4	Description des fonctions et blocs fonctionnels des architectures de sécurité de la TVIP 20
8	Mécanismes de sécurité 23
8.1	Mécanismes de sécurité pour la protection de contenu 23
8.2	Mécanismes de sécurité pour la protection de service 24
8.3	Mécanismes de sécurité pour la protection de réseau 25
8.4	Mécanismes de sécurité pour la protection de dispositif terminal 25
8.5	Mécanismes de sécurité pour les abonnés ou les utilisateurs finals 25
Annexe A	– Protection de la sécurité des abonnés 26
A.1	Protection des données des utilisateurs 26
A.2	Contrôle parental, protection des mineurs légaux, contrôle d'accès..... 27
Appendice I	– Menaces de sécurité..... 28
I.1	Modèle des menaces de sécurité..... 28
Appendice II	– Interopérabilité SCP..... 32
II.1	Aperçu de l'interopérabilité SCP 32
II.2	Scénarios d'interopérabilité SCP 32
II.3	Domaines techniques d'interopérabilité SCP 33
II.4	Architectures d'interopérabilité SCP 34
II.5	Scénarios de déploiement des modes SCP-B et SCP-IX dans des dispositifs terminaux 36

	Page
Appendice III – Exemple de processus de protection de contenu de TVIP.....	38
Appendice IV– Protection du contenu et gestion des copies de DVB.....	39
IV.1 Introduction	39
IV.2 Définitions	39
IV.3 Abréviations et acronymes	41
IV.4 Architecture CPCM.....	41
IV.5 Modèle de référence et entités fonctionnelles CPCM.....	43
IV.6 Domaine autorisé CPCM.....	43
IV.7 Règles d'utilisation du contenu CPCM.....	43
IV.8 Informations d'état d'utilisation	43
IV.9 Contenu CPCM	44
IV.10 Dispositif CPCM	44
IV.11 Règle d'utilisation et informations d'état d'utilisation	44
Appendice V – Mécanisme transcodable sécurisé.....	45
V.1 Aperçu du mécanisme transcodable sécurisé	45
Bibliographie.....	46

Introduction

Les services de TVIP, le contenu fourni grâce à ces services, les dispositifs terminaux utilisés pour le traitement, et la fourniture de ces services nécessitent la prise en compte de nombreux aspects de sécurité. Cette Recommandation porte sur les spécifications, les modèles architecturaux, les entités fonctionnelles, les interfaces et les mécanismes et contient aussi des textes de référence donnés à titre d'information qui décrivent et examinent ces aspects de sécurité.

Recommandation UIT-T X.1191

Spécifications fonctionnelles et architecture pour les aspects de sécurité de la TVIP

1 Domaine d'application

La présente Recommandation traite des spécifications fonctionnelles, de l'architecture et des mécanismes relatifs aux aspects de sécurité et de protection du contenu, des services, des réseaux, des dispositifs terminaux et des abonnés de TVIP. Le but est que les spécifications et fonctions pertinentes décrites dans la présente Recommandation puissent être appliquées de façon appropriée en fonction du service de TVIP et des modèles d'activité, qui peuvent exiger différents niveaux pour les capacités de sécurité.

2 Références

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

[UIT-T X.509] Recommandation UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[UIT-T Y.1910] Recommandation UIT-T Y.1910 (2008), *Architecture fonctionnelle de la TVIP.*

3 Termes et définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [b-UIT-T X.800]: précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

3.1.2 application [b-UIT-T Y.101]: ensemble structuré de capacités qui assure des fonctions à valeur ajoutée prises en charge par un ou plusieurs services.

3.1.3 authentification [b-UIT-T X.800]: voir authentification de l'origine des données et authentification d'entité homologue.

3.1.4 autorisation [b-UIT-T X.800]: attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.1.5 disponibilité [b-UIT-T X.800]: propriété d'être accessible et utilisable sur demande par une entité autorisée.

3.1.6 confidentialité [b-UIT-T X.800]: propriété d'une information qui en interdit l'accès à des personnes, des entités ou des processus non autorisés.

3.1.7 authentification de l'origine des données [b-UIT-T X.800]: confirmation que la source des données reçues est telle que déclarée.

3.1.8 déni de service [b-UIT-T X.800]: impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.

3.1.9 signature numérique [b-UIT-T X.800]: données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et de la protéger contre la contrefaçon (par le destinataire, par exemple).

3.1.10 flux élémentaire [b-UIT-T H.220.0]: terme générique désignant un flux binaire de données codées, de type vidéo, audio ou autre contenues dans des paquets PES.

NOTE – PES signifie flux élémentaire mis en paquets (*packetized elementary stream*).

3.1.11 architecture fonctionnelle [b-UIT-T Y.2012]: ensemble d'entités fonctionnelles et de points de référence entre celles-ci, utilisé pour décrire la structure d'un NGN. Ces entités fonctionnelles sont séparées par des points de référence et définissent de ce fait la répartition des fonctions.

3.1.12 entité fonctionnelle [b-UIT-T Y.2012]: entité comportant un ensemble indivisible de fonctions déterminées. Les entités fonctionnelles sont des concepts logiques, alors que les groupements d'entités fonctionnelles sont utilisés pour décrire des implémentations physiques ou concrètes.

3.1.13 intégrité [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.14 clé [b-UIT-T X.800]: série de symboles commandant les opérations de chiffrement et de déchiffrement.

3.1.15 gestion de clés [b-UIT-T X.800]: production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité.

3.1.16 usurpation d'identité [b-UIT-T X.800]: prétention qu'a une entité d'en être une autre.

3.1.17 fournisseur de réseau [b-UIT-T Q.1290]: organisation qui assure la maintenance et l'exploitation des éléments de réseau nécessaires pour la fonctionnalité de TVIP.

NOTE 1 – Un fournisseur de réseau peut optionnellement aussi faire office de fournisseur de service.

NOTE 2 – Bien qu'ils soient considérés comme étant deux entités distinctes, le fournisseur de service et le fournisseur de réseau peuvent optionnellement constituer une seule entité organisationnelle.

3.1.18 authentification d'entité homologue [b-UIT-T X.800]: confirmation qu'une entité homologue d'une association est bien l'entité déclarée.

3.1.19 respect de la vie privée [b-UIT-T X.800]: droit des individus de contrôler ou d'agir sur les informations les concernant qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées.

3.1.20 répudiation [b-UIT-T X.800]: le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie.

3.1.21 étiquette de sécurité [b-UIT-T X.800]: marque liée à une ressource dénommant ou désignant les attributs de sécurité de cette ressource (cette ressource peut être une unité de données).

NOTE – La marque et/ou l'association de la marque à la ressource peuvent être implicites ou explicites.

3.1.22 politique de sécurité [b-UIT-T X.800]: ensemble de critères pour la fourniture de services de sécurité.

3.1.23 fournisseur de service [b-UIT-T M.1400]: terme général désignant une entité qui fournit des services de télécommunication à des clients ou à d'autres usagers sur la base d'un tarif ou par

contrat. Un fournisseur de service peut ou non exploiter un réseau. Il peut ou non être le client d'un autre fournisseur de service.

3.1.24 menace [b-UIT-T X.800]: violation potentielle de la sécurité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 acquisition: processus d'obtention d'un contenu par l'utilisateur final.

3.2.2 exportation de contenu: processus d'exportation sécurisée d'un contenu de TVIP d'un terminal de TVIP à un autre terminal détenu par l'utilisateur habilité à l'utiliser.

3.2.3 protection de contenu: fait de garantir qu'un utilisateur final ne peut utiliser que le contenu qu'il a déjà acquis conformément aux droits que lui a accordés le détenteur des droits; la protection de contenu consiste à protéger le contenu contre la copie et la distribution illégales, l'interception, l'altération, l'utilisation non autorisée, etc.

3.2.4 traçage de contenu: processus permettant d'identifier l'origine (arbitraire) d'un contenu et/ou l'entité responsable (par exemple l'utilisateur final) afin de faciliter les investigations ultérieures en cas d'utilisation non autorisée du contenu (par exemple copie ou redistribution de contenu).

NOTE – Les informations de traçage de contenu peuvent être jointes au contenu sous forme de métadonnées ou de filigranes numériques.

3.2.5 habilitations: désignent les niveaux d'autorisation, y compris les informations d'accès conditionnel, qu'un abonné peut utiliser pour accéder à certains services de TVIP dans son dispositif terminal de TVIP.

3.2.6 protection de dispositif terminal de TVIP: fait de garantir que le dispositif terminal employé par un utilisateur final pour la réception d'un service peut utiliser de façon fiable et sécurisée le contenu conformément aux droits d'utilisation accordés pour ce contenu tout en protégeant physiquement et électroniquement l'intégrité du dispositif terminal et la confidentialité du contenu ainsi que les paramètres de sécurité critiques (par exemple clés sauvegardées) qui ne sont pas protégés.

3.2.7 télévision linéaire: service de radiodiffusion télévisuelle analogue à la forme classique des services de télévision fournis par les câblo-opérateurs, les opérateurs de services de Terre et les opérateurs de services de diffusion individuelle par satellite; ici, le contenu du programme est transmis selon un horaire défini et destiné à être consommé en temps réel par l'utilisateur final.

3.2.8 métadonnées pour faciliter le filigranage: métadonnées créées pour faciliter l'insertion ultérieure de filigranes par des dispositifs situés en aval.

3.2.9 hameçonnage: acquisition d'informations sensibles ou personnelles telles qu'un nom d'utilisateur, une date de naissance, ou des relevés de carte de crédit en se faisant passer pour une entité de confiance.

3.2.10 droits: désignent la capacité à réaliser un ensemble prédéfini de fonctions d'utilisation pour un élément de contenu; ces fonctions d'utilisation incluent des permissions (par exemple visionner/écouter, copier, modifier, enregistrer, extraire, échantillonner, garder pendant un certain temps, distribuer), des restrictions (par exemple passer/visionner/écouter un certain nombre de fois, passer/visionner/écouter un certain nombre d'heures) et des obligations (par exemple, paiement, traçage de contenu) qui s'appliquent au contenu et permettent à l'utilisateur final de faire l'usage qui lui a été accordé.

3.2.11 expression des droits: représentation syntaxique des droits sous forme concrète et officielle.

3.2.12 SCP de bout en bout: mode de fonctionnement de la protection de service et de contenu dans lequel le contenu est consulté ou échangé par les dispositifs d'extrémité suivant les droits accordés, en utilisant un seul système de protection de service et de contenu.

3.2.13 SCP avec pontage: mode de fonctionnement de la protection de service et de contenu dans lequel deux systèmes de protection de service et de contenu ou plus sont opérationnels sur un même dispositif faisant office de pont entre ces systèmes; le contenu acquis via l'un des systèmes de protection de service et de contenu peut être consulté via un autre système de protection de service et de contenu sur le pont suivant les droits accordés.

3.2.14 SCP avec échange: mode de fonctionnement de la protection de service et de contenu plus général faisant intervenir deux dispositifs ou plus, chaque dispositif ayant un ou plusieurs systèmes de protection de service et de contenu opérationnels; le contenu acquis par l'un des dispositifs par le biais de l'un de ses systèmes de protection de service et de contenu peut être transféré en toute sécurité et consulté sur un autre dispositif par le biais d'un système de protection de service et de contenu différent suivant les droits accordés.

3.2.15 embrouillage: processus conçu pour protéger le contenu multimédia; l'embrouillage utilise généralement une technique de chiffrement pour protéger le contenu.

3.2.16 algorithme d'embrouillage: algorithme utilisé dans les processus d'embrouillage et de désembrouillage.

3.2.17 mécanisme transcodable sécurisé: type de mécanisme de sécurité permettant à un nœud de réseau intermédiaire d'effectuer un transcodage sans déchiffrement tout en préservant la sécurité de bout en bout; pour exécuter ce mécanisme, on peut combiner un codage modulable, un chiffrement progressif et une mise en paquets. Le mécanisme transcodable sécurisé peut assurer à la fois la confidentialité et l'intégrité/authentification des messages.

3.2.18 protection de service: fait de garantir qu'un utilisateur final ne peut acquérir qu'un service et, par extension, le contenu associé qu'il est habilité à recevoir; comprend aussi la protection du service contre tout accès non autorisé lorsque le contenu de TVIP passe par les connexions de service de TVIP.

3.2.19 protection de service et de contenu: combinaison de la protection de service et de la protection de contenu ou système qui la met en œuvre.

3.2.20 usurpation d'identité: activité dans laquelle une fausse source (par exemple une personne ou un programme informatique) se fait passer avec succès pour une source légitime en falsifiant des données et ce, dans le but d'obtenir des informations et/ou d'occulter la source réelle de sorte que la fausse source puisse réaliser des activités non autorisées telles que la diffusion de logiciels malveillants (par exemple des virus), etc.

3.2.21 résistant aux altérations: résistance aux altérations commises par les utilisateurs personnels ou les attaquants d'un produit, paquetage ou système avec accès physique ou logiciel à ces derniers.

3.2.22 transcodage: processus de transformation du format d'origine d'un contenu multimédia (par exemple images, texte, signaux audio et signaux vidéo) en un format différent ou en une qualité différente.

3.2.23 protection de la vie privée de l'utilisateur: fait de garantir que les informations considérées comme étant privées (ou confidentielles) par un utilisateur final sont gardées confidentielles tout en restant assujetties à une divulgation obligatoire si des processus juridiques l'exigent.

3.2.24 signature vidéo: métadonnées (ou caractéristique visuelle) permettant d'identifier un contenu vidéo; contrairement au filigrane qui est inséré en manipulant le contenu vidéo d'origine, la signature vidéo est extraite d'un contenu vidéo sans risque de détérioration de la qualité.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AAA	authentification, autorisation et comptabilité (<i>authentication, authorization and accounting</i>)
AD	domaine autorisé (<i>authorized domain</i>)
CBC	enchaînement de blocs chiffrés (<i>cipher block chaining</i>)
CDN	réseau de fourniture du contenu (<i>content delivery network</i>)
DNG	passerelle de réseau de fourniture (<i>delivery network gateway</i>)
DNGF	fonction de passerelle de réseau de fourniture (<i>delivery network gateway function</i>)
DoS	déni de service (<i>denial of service</i>)
ECB	dictionnaire de codes (<i>electronic code book</i>)
ECM	message de contrôle d'habilitation (<i>entitlement control message</i>)
EMM	message de gestion d'habilitation (<i>entitlement management message</i>)
EPG	guide de programme électronique (<i>electronic program guide</i>)
HN	réseau domestique (<i>home network</i>)
HN-TD	dispositif terminal de réseau domestique (<i>home network terminal device</i>)
ID	identifiant
MIKEY	calcul de clé Internet multimédia (<i>multimedia internet KEYing</i>)
NAT	traduction d'adresse réseau (<i>network address translation</i>)
OFB	rebouclage de la sortie (<i>output feedback</i>)
P2P	homologue à homologue (<i>peer to peer</i>)
PDA	assistant numérique personnel (<i>personal digital assistant</i>)
PIN	numéro d'identification personnel (<i>personal identification number</i>)
PKI	infrastructure de clé publique (<i>public key infrastructure</i>)
PVR	enregistreur vidéo personnel (<i>personal video recorder</i>)
QoE	qualité d'expérience (<i>quality of experience</i>)
QoS	qualité de service (<i>quality of service</i>)
REL	langage d'expression des droits (<i>rights expression language</i>)
SCP	protection de service et de contenu (<i>service and content protection</i>)
SCP-B	SCP avec pontage (<i>SCP bridge</i>)
SCP-EE	SCP de bout en bout (<i>SCP end-to-end</i>)
SCP-IX	SCP avec échange (<i>SCP interchange</i>)
STS	mécanisme transcodable sécurisé (<i>secure transcodable scheme</i>)
TD	dispositif terminal compatible TVIP (<i>IPTV-compliant terminal device</i>)
TVIP	télévision utilisant le protocole Internet
USB	bus série universel (<i>universal serial bus</i>)
VoD	vidéo à la demande (<i>video on demand</i>)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une spécification qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

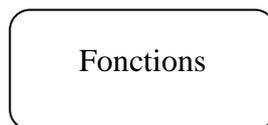
L'expression "**il est recommandé**" indique une spécification qui est recommandée mais qui n'est pas absolument nécessaire. Cette disposition n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une spécification qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

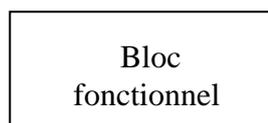
L'expression "**peut, à titre d'option**" indique une spécification optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou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

Dans le contexte de l'architecture de sécurité de TVIP de la présente Recommandation:

Les "**fonctions**" sont définies comme un ensemble de fonctionnalités. Elles sont représentées par le symbole suivant:



Le "**bloc fonctionnel**" est défini comme un groupe de fonctionnalités considéré comme un tout dans la présente Recommandation. Il est représenté par le symbole suivant:



6 Spécifications de sécurité

6.1 Spécifications de sécurité générales

- Il est recommandé que l'architecture de TVIP tienne compte de l'incidence du déploiement de la sécurité en termes de qualité de fonctionnement, de qualité de service, d'utilisabilité, de modularité et de coûts.
- L'architecture de TVIP peut, à titre d'option, prendre en charge la protection du contenu partagé par des utilisateurs finals.

6.2 Spécifications de sécurité du contenu

Le présent paragraphe contient les spécifications qui, séparément ou ensemble, se rapportent au contenu et à sa protection.

Obligations pour l'architecture

- Il est obligatoire que l'architecture de TVIP prenne en charge la protection de contenu telle qu'elle est définie au § 3.
- Il est obligatoire que l'architecture de TVIP prenne en charge l'association des métadonnées de protection et de gestion de contenu.
- Il est obligatoire que l'architecture de TVIP prenne en charge la fourniture sécurisée des métadonnées de protection et de gestion de contenu, y compris les métadonnées relatives aux droits d'utilisation.
- Il est obligatoire que l'architecture de TVIP prenne en charge des métadonnées relatives aux droits d'utilisation du contenu qui fassent la distinction entre les droits d'utilisation, notamment la restitution (visionnage), le stockage, la (re)distribution et des combinaisons de ces derniers.
- Il est obligatoire que l'architecture de TVIP prenne en charge la protection du contenu distribué simultanément à un très grand nombre d'abonnés (modulabilité).
- Il est obligatoire que l'architecture de TVIP prenne en charge la protection du contenu diffusé en continu en multidiffusion et/ou en monodiffusion.
- Il est obligatoire que l'architecture de TVIP prenne en charge la récupération du contenu stocké conformément au droit d'utilisation accordé.
- Si le traçage de contenu est installé, il est obligatoire que l'architecture de TVIP prenne en charge un traçage de contenu robuste en différé (pas en temps réel) (par exemple contenu de VoD).
- Il est interdit que l'architecture de TVIP empêche la prise en charge de moyens de transmission des informations de traçage de contenu (par exemple métadonnées pour faciliter le filigranage).
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'application d'une technologie de traçage de contenu à la sortie du dispositif terminal dans le but d'identifier de façon univoque une session (par exemple chaîne, date/heure), un dispositif terminal et/ou un opérateur de réseau. Une technologie de traçage de contenu peut par exemple inclure des informations visibles et des informations invisibles en option.
- Il est interdit que l'architecture de TVIP empêche la récupération, dans le contenu, de l'ensemble des informations de traçage de contenu.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu dans laquelle seuls les utilisateurs et dispositifs autorisés peuvent utiliser le contenu de TVIP, y compris après le transfert vers un autre système de sécurité.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu afin de conserver les informations d'identification de sorte que le contenu de TVIP puisse être identifié systématiquement, quel que soit le mécanisme d'identification utilisé et quel que soit le système de sécurité vers lequel le contenu est transféré.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu afin d'éviter de passer à un niveau de sécurité inférieur lorsque le contenu est transféré vers un autre système de sécurité.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu dans laquelle des droits ne sont accordés qu'aux dispositifs fiables.

- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu afin de disposer d'un environnement sécurisé pour l'échange de données relatives à cette interopérabilité (par exemple informations d'authentification, métadonnées, informations relatives aux clés, etc.).
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu de sorte que l'interopérabilité ne dépende d'aucun logiciel ou matériel spécifique.
- Il est interdit que l'architecture de TVIP exige que le mécanisme de protection de service et de contenu de l'un ou l'autre de deux systèmes SCP en interfonctionnement soit spécifié de façon ouverte pour tenter de parvenir à une interopérabilité.
- Il est interdit que l'architecture de TVIP empêche la prise en charge d'une interopérabilité de la protection de service et de contenu qui soit souple et extensible afin de prendre en charge divers modèles d'activité.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu entre plusieurs systèmes de sécurité utilisant différents mécanismes de sécurité dans le but de prendre en charge de façon transparente le changement de temps (les abonnés peuvent stocker le contenu et le récupérer ultérieurement) et le changement de lieu (les abonnés peuvent visionner le contenu n'importe où) y compris avec des mécanismes de sécurité différents.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'interopérabilité de la protection de service et de contenu afin de maintenir la transparence pour les utilisateurs.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de plusieurs mécanismes de protection de service et de contenu, quelles que soient les spécifications logicielles ou matérielles spécifiques.

Recommandations pour l'architecture

- Si le contenu de TVIP emploie une technologie de traçage de contenu, il est recommandé que cette technologie soit imperceptible.
- Il est recommandé que l'architecture de TVIP prenne en charge un traçage de contenu robuste en temps réel (par exemple contenu de radiodiffusion).
- Il est recommandé que l'architecture de TVIP prenne en charge la capacité d'authentifier et d'autoriser les utilisateurs finals pour les services de partage de contenu (par exemple exportation de contenu et redistribution de contenu), si le partage de contenu est pris en charge.
- Si la mise en œuvre de l'architecture de TVIP utilise une technologie de traçage de contenu basée sur des métadonnées pour faciliter le filigrane, il est recommandé d'insérer les métadonnées pertinentes dans le flux élémentaire de contenu en se basant, pour les "données d'utilisateur", sur le mécanisme de codage spécifique.
- Si un seul dispositif terminal ou dispositif terminal de réseau domestique (HN-TD) d'une architecture de TVIP prend en charge plusieurs mécanismes de protection de service et de contenu, il est recommandé d'utiliser une seule fonction de conversion normalisée, ce qui permet de relier plusieurs systèmes SCP ensemble, d'effectuer des conversions entre eux de manière cohérente et de garantir l'interopérabilité pour tout dispositif terminal ou HN-TD connecté qui participe à ce mécanisme de conversion.

Options pour l'architecture

- L'architecture de TVIP peut, à titre d'option, prendre en charge l'inclusion d'informations de traçage de contenu. Ces informations peuvent comprendre l'identité de l'opérateur, l'identité du propriétaire du contenu, l'identité du dispositif terminal, etc.

Obligations pour les algorithmes d'embrouillage

- Il est obligatoire que les algorithmes d'embrouillage des flux de radiodiffusion prennent en charge la mise à jour périodique des clés cryptographiques nécessaires.
- Il est obligatoire que les algorithmes d'embrouillage de la TVIP soient élaborés à partir d'algorithmes cryptographiques normalisés et accessibles publiquement.

Recommandations pour les algorithmes d'embrouillage

- Il est recommandé que les algorithmes d'embrouillage de la TVIP aient une entropie de clé suffisamment grande pour protéger efficacement le contenu contre l'analyse cryptographique.
- Il n'est pas interdit que l'architecture de TVIP empêche la prise en charge d'algorithmes d'embrouillage largement utilisés.
- Il est recommandé que l'architecture de TVIP n'empêche pas la prise en charge de plusieurs systèmes d'embrouillage.
- Il est recommandé que les algorithmes d'embrouillage de la TVIP puissent être implémentés efficacement en termes de matériels et/ou de logiciels.
- Il est recommandé que les algorithmes d'embrouillage de la TVIP soient modulables et à l'abri de l'obsolescence (paramètres cryptographiques (par exemple longueur de clé, périodes cryptographiques, etc.) et mode cryptographique (par exemple CBC, OFB, ECB, etc.)).

Options pour les algorithmes d'embrouillage

- Les algorithmes d'embrouillage de la TVIP peuvent, à titre d'option, appliquer des algorithmes cryptographiques de forces différentes à des types de contenu différents.

6.3 Spécifications de sécurité des services

Le présent paragraphe contient les spécifications qui, séparément ou ensemble, se rapportent aux services et à leur protection.

Obligations pour l'architecture

- Il est obligatoire que l'architecture de TVIP prenne en charge la protection de service telle qu'elle est définie au § 3.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de la mise à jour ou du remplacement de la SCP dans le dispositif terminal depuis le côté serveur.
- Il est obligatoire que l'architecture de TVIP prenne en charge l'autorisation et l'authentification de l'utilisateur final (abonné).
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme pour signaler au dispositif terminal qu'il doit utiliser un certain algorithme d'embrouillage basé sur un cadre normalisé.
- Il est obligatoire que l'architecture de TVIP puisse utiliser les systèmes standard de gestion de clé (par exemple MIKEY, EMM/ECM) nécessaires pour l'interopérabilité.
- Il est obligatoire que l'architecture de TVIP prenne en charge la capacité de mettre à jour et d'interroger le système SCP concernant les algorithmes d'embrouillage de la TVIP et tout autre algorithme d'embrouillage choisi par l'opérateur côté serveur via des interfaces SCP.
- Il est obligatoire que l'architecture de TVIP prenne en charge des mécanismes SCP qui soient indépendants des formats de contenu spécifiques.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme de protection de l'intégrité et d'authentification de l'origine des données concernant les métadonnées sensibles.

- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme de fourniture sécurisée aux dispositifs terminaux des droits et des informations de contrôle d'accès au contenu.
- Il est obligatoire que l'architecture de TVIP prenne en charge un contrôle d'utilisation du contenu (par exemple lecture répétée).
- Il est obligatoire que l'architecture de TVIP prenne en charge différents modes pour les lectures répétées, par exemple limitation du nombre de lectures, limitation de la durée de lecture, restriction concernant l'avance ou le retour rapide.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme capable de maintenir la confidentialité des messages de signalisation entre le serveur SCP et le client SCP.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme capable de maintenir l'authenticité des messages de signalisation entre le serveur SCP et le client SCP.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme capable de maintenir l'intégrité des messages de signalisation entre le serveur SCP et le client SCP.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme de récupération sécurisée des paramètres SCP de dispositif terminal (par exemple configuration, statut).
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme de mise à jour sécurisée des paramètres SCP de dispositif terminal (par exemple configuration).
- Il est interdit que l'architecture de TVIP empêche la prise en charge d'une capacité d'activation et de désactivation de la fonction de traçage du contenu de manière programmée (par exemple, en fonction du temps, de l'événement, du contenu ou de la chaîne).
- Si un système de gestion de clés est employé, il doit être conçu pour être évolutif, fiable et interopérable.
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'installation et de l'exploitation de plusieurs solutions de protection de service sans matériels de remplacement à l'exception des dispositifs amovibles (par exemple clés USB et cartes SIM).
- Il est interdit que l'architecture de TVIP empêche la prise en charge d'un mécanisme d'identification des solutions de protection de service disponibles qui soient capables de satisfaire les dispositions spécifiées pour la protection de contenu associée.
- Il est interdit que l'architecture de TVIP empêche la prise en charge d'un mécanisme de découverte de système SCP qui puisse prendre en charge une méthode de découverte et s'y adapter chaque fois qu'un contenu spécifique nécessite un système de protection de service spécifique.
- Il est interdit que l'architecture de TVIP empêche la prise en charge d'un mécanisme de sélection d'un système SCP parmi les systèmes SCP disponibles sans matériels de remplacement à l'exception des dispositifs amovibles.
- Il est interdit que l'architecture de TVIP empêche la prise en charge du téléchargement sécurisé d'un système SCP. Le système SCP téléchargé peut, à titre d'option, dépendre des spécifications de protection de service particulières.
- Si un système SCP téléchargeable est déployé, il est obligatoire que l'architecture de TVIP assure la protection de l'intégrité et l'authentification de l'origine des données pour le système SCP téléchargé.

- Si le téléchargement sécurisé d'un programme applicatif vers des dispositifs terminaux est pris en charge, il est obligatoire que l'architecture de TVIP assure la protection de l'intégrité et l'authentification de l'origine des données pour les applications téléchargées.

Recommandations pour l'architecture

- Il est recommandé que l'architecture de TVIP assure la confidentialité du contenu.
- Il est recommandé que l'architecture de TVIP prenne en charge plusieurs algorithmes d'embrouillage.
- Il est recommandé que l'architecture de TVIP prenne en charge la capacité d'authentifier et d'autoriser les utilisateurs finals pour les services de partage de contenu (par exemple exportation de contenu et redistribution de contenu).
- Si l'architecture de TVIP emploie un système de gestion de clés, il est recommandé d'envisager une gestion de clés hiérarchique afin de prendre en charge l'évolutivité.
- Si l'architecture de TVIP emploie un système de gestion de clés qui utilise un protocole de gestion de clés de groupe, il est recommandé d'envisager une gestion de clés hiérarchique et un algorithme de gestion de clés de remplacement afin de prendre en charge l'évolutivité.
- Si l'architecture de TVIP emploie un système de gestion de clés qui utilise des clés temporaires, il est recommandé de configurer le trajet de média de sorte que la traversée de dispositifs NAT et les contraintes de largeur de bande ne limitent pas l'échange de clés.
- Il est recommandé que l'architecture de TVIP prenne en charge au moins le même degré de protection (aux fins de contrôle des accès non autorisés) pour les informations de traçage de contenu que celui qui est appliqué au contenu tracé correspondant.
- Il est recommandé que l'architecture de TVIP prenne en charge la transmission conjointe du contenu et des informations de traçage de contenu tout en conservant la synchronisation du contenu et des informations de traçage de contenu pendant le transport.
- Si l'architecture de TVIP emploie une infrastructure PKI pour authentifier le dispositif terminal ou le service ou le fournisseur de contenu, il est recommandé d'envisager une hiérarchie multicouches de l'infrastructure PKI afin de prendre en charge l'évolutivité, la fiabilité et l'interopérabilité.
- Si l'architecture de TVIP emploie une infrastructure PKI pour le service de TVIP, il est recommandé d'utiliser un format de certificat, une liste de révocation de certificats ou un protocole de statut de certificat en ligne normalisé, accessible publiquement.
- Il est recommandé que l'architecture de TVIP prenne en charge le téléchargement sécurisé de programmes applicatifs vers les dispositifs terminaux.
- Il est recommandé que l'architecture de TVIP prenne en charge un mécanisme de limitation des droits de visionnage de certains programmes à certains groupes d'abonnés (par exemple visionnage en bloc par les résidents d'une zone spécifique, ce qui peut, par exemple, être utile pour des manifestations sportives).

Options pour l'architecture

- Afin d'offrir un service de TVIP évolutif pour le terminal possédé par l'utilisateur dont la résolution est différente de celle du terminal de l'utilisateur, l'architecture de TVIP peut, à titre d'option, prendre en charge un mécanisme transcodable sécurisé comme défini au § 3.

6.4 Spécifications de sécurité des réseaux

Le présent paragraphe contient les spécifications qui, séparément ou ensemble, se rapportent aux réseaux ou à leur protection.

Obligations pour l'architecture

- Il est obligatoire que l'architecture de TVIP prenne en charge la capacité de réduire les effets d'une attaque DoS.
- Il est obligatoire que l'architecture de TVIP prenne en charge la mise en place de mesures de sécurité pour bloquer le trafic illégal ou non désiré.
- Il est obligatoire que l'architecture de TVIP soit résistante aux attaques visant les capacités de multidiffusion.
- Il est recommandé que l'architecture de multidiffusion prenne en charge la capacité d'authentifier un homologue dans l'environnement de multidiffusion général ou superposé (entre homologues).
- Il est obligatoire que la liaison de communication entre dispositifs terminaux du réseau domestique bénéficie d'une protection de sécurité du contenu lorsqu'elle achemine un contenu à tarif majoré, par exemple payé par le consommateur, qui n'est pas protégé.
- Il est obligatoire que l'architecture de TVIP prenne en charge l'authentification de la passerelle DNG par la fonction de gestion de la TVIP.
- Il est obligatoire que l'architecture de TVIP prenne en charge l'authentification de la fonction de gestion de la TVIP par la passerelle DNG.

Recommandations pour l'architecture

- Afin de protéger le réseau domestique contre les accès malveillants ou non autorisés, il est recommandé que l'architecture de TVIP prenne en charge la capacité pour la fonction de passerelle de réseau de fourniture (DNGF) d'établir un pare-feu configurable à distance avec plusieurs niveaux de sécurité et des passerelles appropriées au niveau application.
- Il est recommandé que l'architecture de TVIP prenne en charge la capacité pour la gestion de la TVIP de configurer à distance une fonction NAT et une fonction de protection de la passerelle DNG contre les intrusions.
- Il est recommandé que l'architecture de TVIP prenne en charge la capacité pour la fonction de télégestion de la TVIP de configurer à distance la fonction NAT et la fonction de protection de la passerelle DNG contre les intrusions.
- Il est recommandé que l'architecture de TVIP protège la télégestion des dispositifs terminaux lorsque cette télégestion est prise en charge.
- Il est recommandé que l'architecture de TVIP protège en charge l'utilisation des informations relatives aux étiquettes de contenu pour commander la fourniture de contenu.

6.5 Spécifications de sécurité des terminaux

Le présent paragraphe contient les spécifications qui, séparément ou ensemble, se rapportent aux dispositifs terminaux ou à leur protection.

Obligations pour l'architecture

- Il est obligatoire que l'architecture de TVIP prenne en charge la protection de dispositif terminal telle qu'elle est définie au § 3.
- Il est obligatoire que l'architecture de TVIP prenne en charge l'authentification des dispositifs terminaux.
- Il est obligatoire que l'architecture de TVIP prenne en charge la résistance aux altérations physiques des dispositifs terminaux.
- Il est obligatoire que l'architecture de TVIP prenne en charge un moyen de détection des altérations physiques des dispositifs terminaux.

- Si un système SCP téléchargeable est déployé, il est obligatoire que l'architecture de TVIP prenne en charge le téléchargement et l'installation sécurisés du code de fonctionnement du système SCP dans les dispositifs terminaux.
- Il est obligatoire que l'architecture de TVIP prenne en charge un moyen sécurisé de réalisation des processus critiques en termes de sécurité dans les dispositifs terminaux comme la gestion de clés et la sérialisation de média afin d'interrompre la lecture en différé de contenu en cas de dysfonctionnement lié à la sécurité, de détection d'altération, ou d'une autre indication d'utilisation abusive.
- Il est obligatoire que l'architecture de TVIP assure une protection physique des processus sensibles du point de vue de la sécurité et des composants intervenant dans le traitement, la transmission et le stockage de contenu de valeur dans les dispositifs terminaux en l'absence de protection logique (par exemple chiffrement ou filigranes de sérialisation). Ces processus comprennent le désembrouillage et la sérialisation de média.
- Il est obligatoire que l'architecture de TVIP reconnaisse qu'il est nécessaire de protéger physiquement (contre l'exploration ou l'altération du système SCP dans les dispositifs terminaux) les processus sensibles du point de vue de la sécurité dans les dispositifs terminaux, y compris le désembrouillage et la sérialisation de média (traçage de contenu), et les données critiques servant pour ces processus ainsi que tous les composants intervenant dans le traitement, la transmission et le stockage de tout contenu de valeur ne bénéficiant pas de protections logiques (par exemple chiffrement ou filigranes de traçage de contenu).
- Il est interdit que l'architecture de TVIP empêche la prise en charge de l'échange de contenu entre un dispositif terminal et d'autres dispositifs (physiques ou logiques), sous réserve que les utilisations permises pour ce contenu comprennent cet échange.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme permettant à un dispositif terminal d'authentifier les serveurs SCP.
- Il est interdit que l'architecture de TVIP empêche la prise en charge du remplacement de la SCP dans le dispositif terminal.
- Il est obligatoire que l'architecture de TVIP assure la protection de la sortie numérique ou analogique telle qu'elle est requise par le client SCP pour un stockage en dehors du dispositif lorsqu'une sortie vidéo/audio numérique ou analogique est disponible sur le dispositif terminal.

Recommandations pour l'architecture

- Il est recommandé que l'architecture de TVIP assure l'exportation de contenu dans les dispositifs terminaux en permettant un transfert sécurisé du contenu de TVIP du terminal de TVIP à un autre terminal détenu par l'utilisateur habilité à l'utiliser.

6.6 Spécifications de sécurité des abonnés

Le présent paragraphe contient les spécifications qui, séparément ou ensemble, se rapportent aux abonnés et aux utilisateurs finals ou à leur protection.

Obligations pour l'architecture

- Il est obligatoire que l'architecture de TVIP prenne en charge la protection de la vie privée de l'utilisateur telle qu'elle est définie au § 3.
- Il est obligatoire que l'architecture de TVIP autorise un abonné à mettre en place un mécanisme de contrôle d'accès (par exemple utilisation d'un mot de passe) pour restreindre l'accès au contenu et/ou aux services.

- Il est obligatoire que l'architecture de TVIP puisse indiquer la raison pour laquelle l'accès au contenu a été refusé à un utilisateur.
- Il est obligatoire que l'architecture de TVIP prenne en charge un mécanisme permettant à un abonné de demander des extensions (par exemple un plus grand nombre de lectures, une durée de lecture plus longue) relatives aux droits d'utilisation associés à des instances de contenu particulières.

Recommandations pour l'architecture

- Il est recommandé que l'architecture de TVIP permette à l'utilisateur final (tel qu'autorisé par des droits) de remplacer un dispositif terminal sans affecter intrinsèquement les droits afférents à la consommation du contenu.
- Il est recommandé que l'architecture de TVIP prenne en charge un mécanisme de classement des programmes en fonction du contenu.

NOTE – Les informations de classement peuvent être utilisées pour le contrôle d'accès, par exemple le contrôle parental.

7 Architecture de sécurité

Le présent paragraphe définit une architecture de sécurité de la TVIP sous la forme d'une architecture de sécurité générale, d'une architecture de protection de contenu et d'une architecture de protection de service ainsi que d'entités fonctionnelles de sécurité pour respecter les spécifications décrites dans les paragraphes précédents.

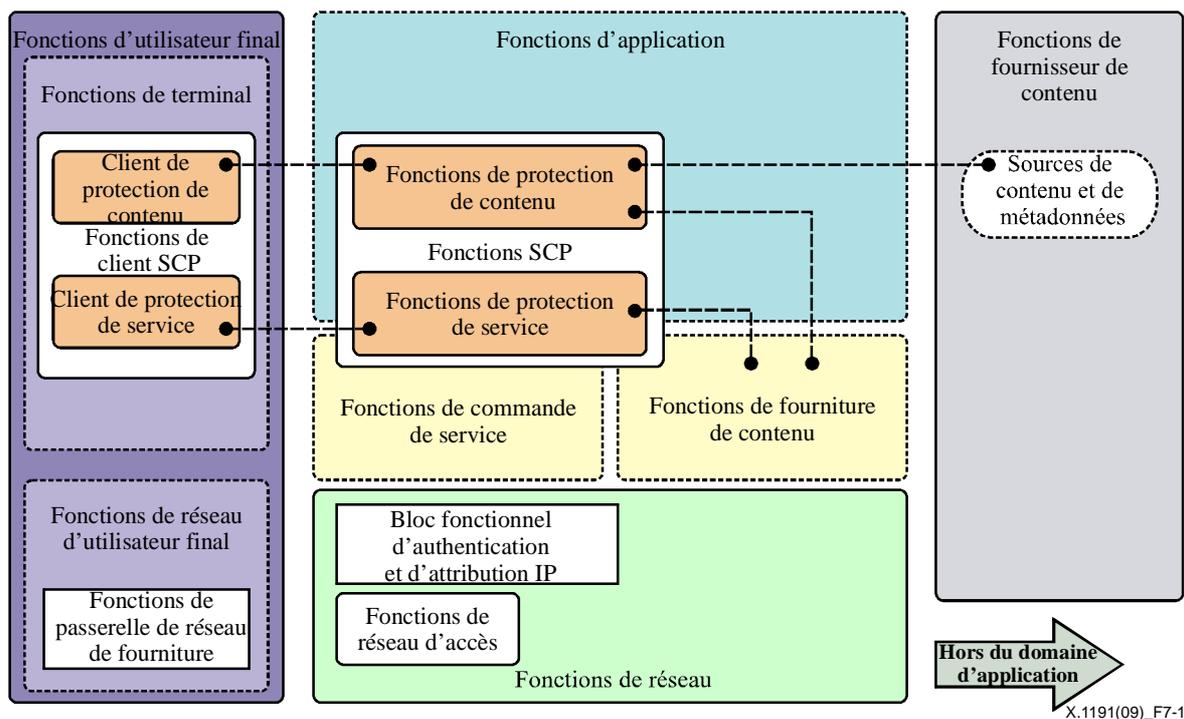
L'architecture de sécurité de la TVIP décrite ci-dessous est supposée et censée être utilisée dans le contexte des domaines fonctionnels de la TVIP et du cadre architectural fonctionnel de la TVIP définis respectivement aux § 6 et 8 de [UIT-T Y.1910].

7.1 Architecture de sécurité générale

Une architecture de sécurité générale de la TVIP est illustrée sur la Figure 7-1 ci-dessous. Elle est subdivisée en deux zones principales – l'une étant considérée comme faisant partie du domaine d'application de la présente Recommandation, et l'autre comme n'en faisant pas partie. La première zone comprend les domaines de l'utilisateur final, du fournisseur de réseau et du fournisseur de service, tandis que la deuxième correspond au domaine du fournisseur de contenu.

Dans la deuxième zone, tous les aspects de sécurité au sein du domaine des fournisseurs de contenu et l'interconnexion entre les fournisseurs de contenu et les fournisseurs de service font l'objet d'accords privés entre les parties prenantes actives dans ces domaines et sont donc considérés comme ne faisant pas partie du domaine d'application de la présente Recommandation.

Même si le domaine du fournisseur de contenu et son interconnexion avec le domaine du fournisseur de service sont considérés comme ne faisant pas partie du domaine d'application du présent document, le domaine du fournisseur de contenu est inclus dans les figures et descriptions qui suivent dans un souci d'exhaustivité. A cet égard, tout ce qui est énoncé ici concernant ces domaines est donné à titre d'information ou d'explication.



X.1191(09)_F7-1

NOTE 1 – Les fonctions de protection de contenu et les fonctions de protection de service représentées sur cette figure sont les parties les plus importantes de l'architecture de sécurité de la TVIP. Ces fonctions sont détaillées sur les Figures 7-2 (*Architecture de protection de contenu*) et 7-3 (*Architecture de protection de service*).

NOTE 2 – Pour l'architecture de la TVIP, certaines fonctions et certains blocs fonctionnels n'ayant pas de relation directe avec la sécurité de la TVIP sont omis sur cette figure afin de la simplifier.

Figure 7-1 – Architecture de sécurité générale de la TVIP

L'architecture de sécurité générale est subdivisée schématiquement en quatre domaines fonctionnels, à savoir:

- Fonctions de fournisseur de contenu (techniquement en dehors du domaine d'application)

Les fournisseurs de contenu sont supposés offrir un accès au contenu aux fournisseurs de service qui ont établi des relations avec les fournisseurs de contenu. Dans certains cas, un fournisseur de contenu peut lui-même servir de fournisseur de service, auquel cas cette relation est considérée comme interne.

Pour offrir aux fournisseurs de service un accès au contenu, un fournisseur de contenu peut utiliser des mécanismes normalisés ou privés pour contrôler et permettre l'accès au contenu; il est toutefois à noter que ces mécanismes sont considérés comme ne faisant pas partie du domaine d'application de la présente Recommandation et qu'ils font simplement l'objet d'un accord privé entre les parties prenantes.
- Fonctions de protection de service et de contenu (SCP) (chevauchement avec certaines parties des fonctions d'application, des fonctions de commande de service et des fonctions de fourniture de contenu)

Les fonctions SCP jouent un rôle central dans l'architecture de sécurité générale de la TVIP, en particulier dans le domaine du fournisseur de service. Plus précisément, les fonctions de protection de service permettent de protéger l'infrastructure des services et de contrôler l'accès aux services et au contenu associé. Quant aux fonctions de protection de contenu, elles permettent de contrôler l'utilisation des services et du contenu en fonction des licences accordées. Les fonctions et blocs fonctionnels spécifiques des fonctions SCP sont subdivisés en trois sous-domaines: fonctions d'application, fonctions de commande de service et fonctions de fourniture de contenu.

Les licences des fournisseurs de contenu obligent le fournisseur de service à ne donner accès au contenu que dans certaines conditions d'utilisation, par exemple un seul visionnage sans enregistrement, un seul enregistrement avec plusieurs visionnages, un seul enregistrement avec transfert des droits d'enregistrement, etc. Le principal objectif des aspects de protection de contenu des fonctions SCP est de permettre à un fournisseur de service de satisfaire à ces obligations d'une manière qui soit vérifiable objectivement.

Le principal objectif des aspects de protection de service des fonctions SCP est d'éviter tout accès non autorisé aux ressources de services et aux informations considérées comme confidentielles par les entités dans différents domaines: service, réseau, dispositif terminal et utilisateur final (abonné).

Un objectif secondaire des aspects de protection de service des fonctions SCP est de protéger l'infrastructure des services contre les préjudices dus aux utilisations abusives de ressources, qu'elles soient délibérées ou involontaires.

Les blocs fonctionnels détaillés des fonctions de protection de contenu et des fonctions de protection de service sont illustrés respectivement sur les Figures 7-2 (*Architecture de protection de contenu*) et 7-3 (*Architecture de protection de service*).

- Fonctions de réseau

Les fonctions de sécurité concernant le domaine du réseau visent principalement à authentifier les entités et à autoriser l'accès aux réseaux par l'intermédiaire desquels les services de TVIP sont ou seront fournis. Elles visent secondairement à protéger l'intégrité du réseau proprement dit – sur les plans physique, électronique et opérationnel (par exemple en détectant et en contrecarrant les attaques par déni de service sur le réseau d'accès ou support).

- Fonctions d'utilisateur final

Les aspects de sécurité applicables à l'utilisateur final (abonné) comprennent la protection de l'intégrité du dispositif terminal fonctionnant dans les locaux de l'abonné et la protection de la vie privée de l'utilisateur final.

Dans certains cas, on peut envisager qu'une passerelle DNG entre un dispositif terminal et un domaine de réseau soit installée dans le domaine de l'utilisateur final et qu'elle fasse l'objet de mesures de sécurité prises par l'utilisateur final.

Enfin, il est recommandé d'appliquer des mécanismes afin de garantir l'intégrité du contenu reçu par un dispositif terminal puis redistribué à d'autres dispositifs à l'intérieur du réseau domestique ou en dehors. (Il en résulte un chevauchement entre les aspects de sécurité de l'utilisateur final et les aspects de sécurité du contenu.)

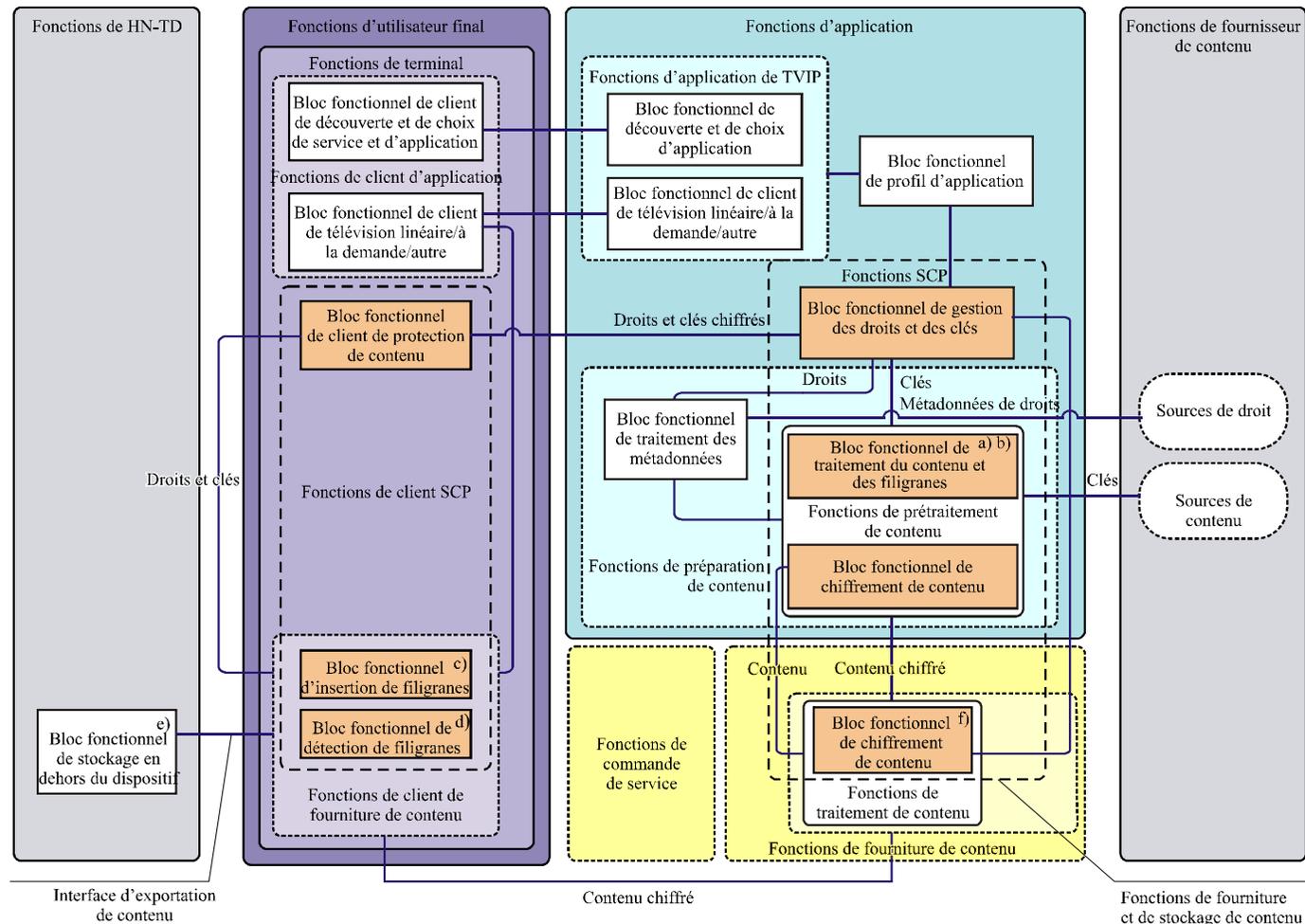
Le § 7.4.1 contient des descriptions plus détaillées des fonctions et blocs fonctionnels représentés sur la Figure 7-1.

7.2 Architecture de protection de contenu

Une architecture de protection de contenu pour la TVIP est illustrée sur la Figure 7-2 ci-dessous.

La principale fonction de l'architecture de protection de contenu est de délimiter le flux et le traitement des informations relatives aux droits d'utilisation du contenu et des informations nécessaires pour gérer et faciliter ces droits.

Les droits d'utilisation du contenu sont fixés au départ par les fournisseurs de contenu; il est toutefois à noter que ces droits peuvent être modifiés (par exemple réduits, voire étendus) par les fournisseurs de service en fonction des accords qu'ils ont conclus avec les fournisseurs de contenu et des politiques opérationnelles et commerciales.



- ^{a)} Production optionnelle de métadonnées de filigranes pour faciliter l'insertion de filigranes en aval.
^{b)} Insertion optionnelle de filigranes pour singulariser le contenu pour les réseaux, les serveurs et l'unidiffusion.
^{c)} Insertion optionnelle de filigranes pour singulariser les instances de contenu de multidiffusion.
^{d)} Détecteur optionnel des filigranes de protection contre les copies.
^{e)} Stockage optionnel en dehors du dispositif: dispositif de stockage à l'intérieur du HN-TD.
^{f)} Le bloc fonctionnel de chiffrement de contenu situé dans les fonctions de fourniture et de stockage de contenu est optionnel.

X.1191(09)_F7-2

NOTE – Sur cette figure, les blocs fonctionnels de protection de contenu comprennent les fonctions de protection de contenu et les fonctions de client de protection de contenu.

Figure 7-2 – Architecture de protection de contenu de la TVIP

L'architecture de protection de contenu représentée ci-dessus est constituée de fonctions résidant essentiellement dans deux domaines fonctionnels:

- Fonctions de protection de service et de contenu (chevauchement avec les fonctions d'application et les fonctions de fourniture de contenu)

Le contenu et les droits qui lui sont associés sont collectés auprès des fournisseurs de contenu, rassemblés et traités en vue de leur fourniture à l'utilisateur final, au niveau duquel l'ensemble du processus est géré par plusieurs fonctions telles que les fonctions de préparation de contenu, qui utilisent les données décrivant les droits de l'utilisateur final et les conditions associées.

Les informations relatives au contenu, aux droits et aux clés (utilisées pour autoriser l'accès au contenu et permettre son utilisation) sont organisées sous une forme adaptée à l'application considérée (par exemple visionnage de télévision linéaire). Les informations relatives aux droits et aux clés sont fournies au bloc fonctionnel de client de protection de contenu du dispositif terminal sous forme d'habilitation (par exemple message EMM) par le bloc fonctionnel de gestion des droits et des clés; le contenu est traité afin d'y insérer, à titre d'option, des métadonnées de traçage de contenu (par exemple filigranes) puis chiffré dans les fonctions de préparation de contenu avant fourniture. Dans certains cas (par exemple services IP en temps réel), le contenu peut aussi, à titre d'option, être chiffré par les fonctions de fourniture de contenu.

Dans le contexte de l'architecture de protection de contenu de la TVIP (par opposition à l'architecture de protection de service de la TVIP qui sera décrite plus loin), l'accent est mis sur la gestion, le traitement et la fourniture des droits et des clés, et non sur le chiffrement de ces informations ou du contenu faisant l'objet de ces droits.

- Fonctions d'utilisateur final

Les fonctions de terminal dans le domaine de l'utilisateur final sont chargées d'appliquer les règles d'utilisation du contenu associées aux informations relatives aux droits (également appelées métadonnées de protection de contenu). Cette entité fonctionnelle interprète les droits et clés associés au contenu transmis par le bloc fonctionnel de gestion des droits et des clés puis, sur la base de cette interprétation, commande le traitement du contenu et sa présentation à l'utilisateur final soit par le biais de dispositifs de présentation intégrés (par exemple écran ou système de restitution audio) soit par le biais d'interconnexions physiques avec des dispositifs externes.

Dans les cas où le dispositif terminal transmet un contenu protégé à un dispositif externe (par exemple un dispositif d'affichage), les droits afférents au contenu peuvent être convertis sous d'autres formes; le contenu auquel cette utilisation s'applique peut subir un traitement supplémentaire afin d'insérer, à titre d'option, des informations de traçage de contenu côté client (par exemple filigranes) ou de chiffrer à nouveau le contenu pour exécuter un contrôle d'accès en aval.

Le § 7.4 contient des descriptions plus détaillées des blocs architecturaux représentés sur la Figure 7-2.

Sur la Figure 7-2, l'interface d'exportation de contenu est une interface logique raccordant le dispositif terminal de TVIP et le dispositif terminal de réseau domestique (HN-TD). Le HN-TD peut consommer le contenu ou l'exporter vers d'autres HN-TD. Les fonctions de client de fourniture de contenu peuvent modifier l'étiquette de sécurité correspondante pour faire en sorte que seul le HN-TD autorisé puisse consommer et exporter le contenu.

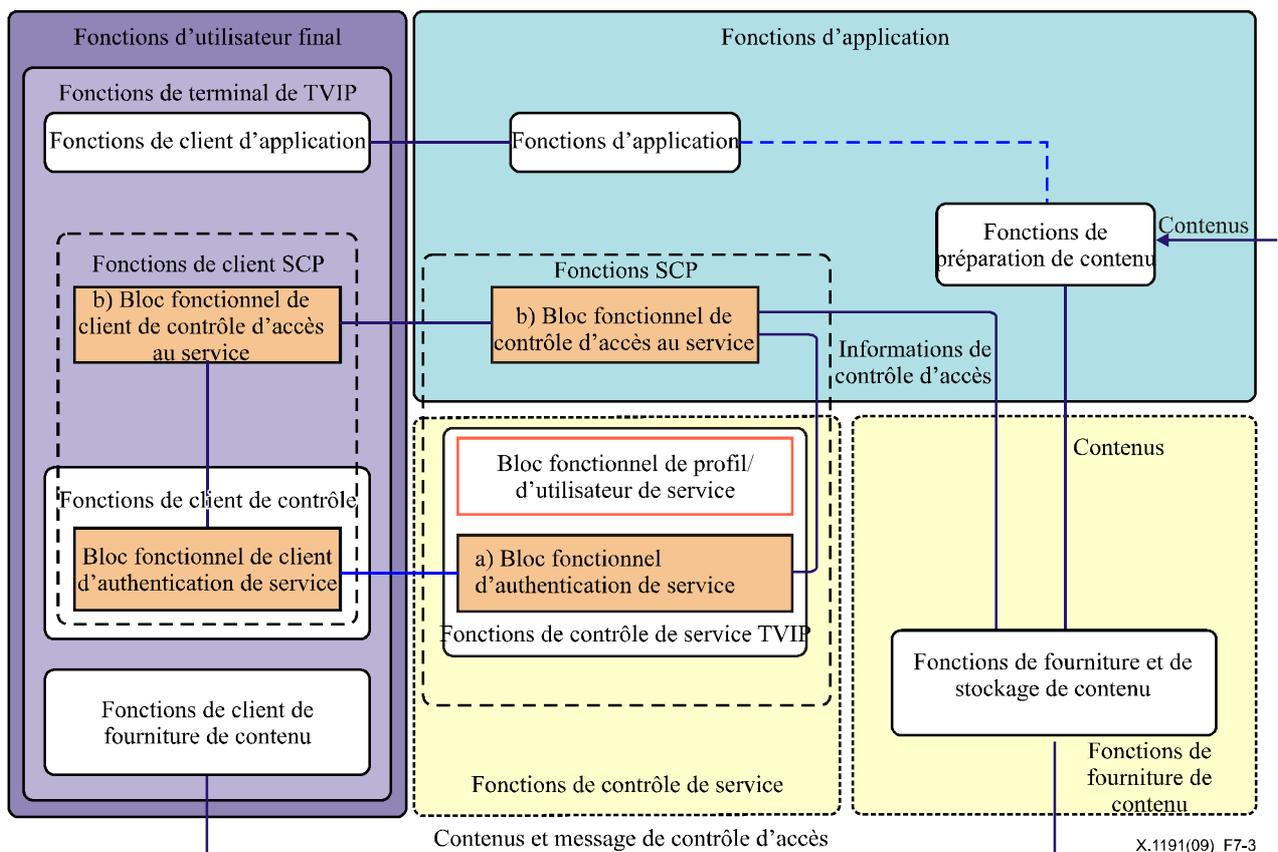
7.3 Architecture de protection de service

Pour les services gérés faisant intervenir un contenu protégé, l'utilisateur final (l'abonné) et le dispositif terminal doivent généralement être authentifiés puis autorisés avant qu'il soit possible d'accéder aux services et au contenu associé.

Suivant les cas, les fonctions d'authentification et d'autorisation peuvent être exécutées séparément au niveau du dispositif terminal et de l'utilisateur final. Dans d'autres cas, des dispositifs complémentaires situés dans les locaux de l'utilisateur final (par exemple une passerelle de réseau de fourniture et d'autres dispositifs d'utilisateur final) peuvent nécessiter une authentification avant que l'accès au service soit autorisé.

On peut utiliser une combinaison authentification-autorisation pour contrôler l'accès au service de TVIP et au dispositif terminal aux fins d'acquisition de service et de contenu avant utilisation.

Une architecture de protection de service pour la TVIP est illustrée sur la Figure 7-3 ci-dessous.



a) Authentification: permet de déterminer le nom de l'abonné et son identifiant avec le privilège attribué.

b) Contrôle d'accès au service: permet de protéger un service contre tout accès non autorisé et illégal.

NOTE – Sur cette figure, les blocs fonctionnels de protection de service comprennent des fonctions de protection de service et des fonctions de client de protection de service.

Figure 7-3 – Architecture de protection de service de la TVIP

Les principales fonctions de l'architecture de protection de service sont les suivantes:

- Authentification de l'abonné et du dispositif terminal:
 Cette fonction est chargée de l'authentification de l'abonné et du dispositif terminal.
 - Authentification de l'abonné: vérification de l'authenticité de l'utilisateur
 - Authentification du dispositif terminal: vérification de l'authenticité du dispositif terminal

Lorsqu'on utilise des certificats de base X.509 comme justificatifs d'identité pour l'authentification, une fonction de révocation est nécessaire.

- Authentification du serveur:
 - Dans le dispositif terminal, fonction permettant d'authentifier le serveur pour une authentification mutuelle
- Contrôle d'accès au service:
 - Fonction permettant de restreindre l'acquisition de services et l'accès à ces services aux utilisateurs autorisés en utilisant des mécanismes de sécurité tels que l'embrouillage et le chiffrement

Le § 7.4 contient des descriptions plus détaillées des blocs architecturaux représentés sur la Figure 7-3.

7.4 Description des fonctions et blocs fonctionnels des architectures de sécurité de la TVIP

Le présent paragraphe décrit plus en détail les fonctions et blocs fonctionnels des modèles architecturaux illustrés au § 7.1 (*Architecture de sécurité générale*), au § 7.2 (*Architecture de protection de contenu*) et au § 7.3 (*Architecture de protection de service*) ci-dessus. Ces fonctions et blocs fonctionnels sont uniquement décrits de façon générale et sont regroupés en trois parties correspondant à chacun de ces trois paragraphes.

7.4.1 Fonctions et blocs fonctionnels de l'architecture générale

Fonctions de réseau d'accès: assurent la collecte et le regroupement du trafic de commande et de données ayant pour origine les réseaux; permettent d'assurer la QoS/QoE y compris la gestion de tampon, la mise en file d'attente et la programmation, le filtrage des paquets, la classification du trafic, le marquage, la régulation et le modelage du trafic.

NOTE 1 – Ces fonctions sont indépendantes des fonctions de protection de service et de contenu du point de vue de la protection de service et de contenu de TVIP.

Fonctions d'application: réparties entre le côté serveur (fournisseur de service) et le côté client (locaux de l'utilisateur final), elles sont constituées de composants fonctionnels qui préparent, envoient, reçoivent et traitent les applications de TVIP au niveau service telles que la télévision linéaire, la vidéo à la demande, et le contenu connexe, par exemple les informations d'accessibilité, les applications interactives, etc.

Bloc fonctionnel d'authentification et d'attribution IP: assure l'authentification du bloc fonctionnel de passerelle de réseau de fourniture se raccordant aux fonctions de réseau ainsi que l'attribution d'adresse IP aux fonctions de terminal de TVIP.

Fonctions de protection de contenu: offrent des mécanismes permettant d'appliquer les politiques d'utilisation du contenu, y compris le regroupement, la distribution et la gestion des droits et des clés, la production et l'insertion optionnelles d'informations de traçage de contenu (par exemple filigranes) et le chiffrement de contenu (sous la commande des fonctions de protection de service).

NOTE 2 – Les blocs fonctionnels spécifiques constituant les fonctions de protection de contenu sont examinés plus en détail aux § 7.2 et 7.4.2.

Fonctions de client de protection de contenu: interagissent avec les fonctions de protection de contenu côté serveur pour appliquer les politiques d'utilisation du contenu.

Fonctions de fournisseur de contenu: fournissent aux fournisseurs de service le contenu ainsi que les métadonnées relatives aux droits et aux clés concernant le contenu.

Fonctions de passerelle de réseau de fourniture: assurent la connectivité entre le dispositif terminal et le réseau de fourniture; gèrent la connectivité IP locale (locaux de l'utilisateur final), obtiennent la ou les adresses IP et la configuration IP pour le dispositif terminal.

NOTE 3 – Ces fonctions sont indépendantes des fonctions de protection de service et de contenu du point de vue de la protection de service et de contenu de TVIP.

Fonctions de protection de service: offrent des mécanismes d'authentification et d'autorisation ainsi que de contrôle d'accès aux services de TVIP et au contenu associé, y compris la commande et la mise en œuvre directe du chiffrement des signaux de commande et des échanges de contenu, soit de façon indépendante soit conjointement avec les fonctions de protection de contenu.

NOTE 4 – Ces fonctions sont indépendantes des fonctions de protection de service et de contenu du point de vue de la protection de service et de contenu de TVIP.

NOTE 5 – Les blocs fonctionnels spécifiques constituant les fonctions de protection de service sont examinés plus en détail aux § 7.3 et 7.4.3.

Fonctions de client de protection de service: interagissent avec les fonctions de protection de service côté serveur pour réaliser le contrôle d'accès aux services et d'autres fonctions de protection.

Fonctions de terminal: contiennent des clients de protection de service et de protection de contenu pour le déchiffrement et l'application des politiques d'utilisation de service et de contenu conformément aux métadonnées relatives aux droits d'utilisation; exécutent le chiffrement de couche liaison et la conversion SCP (échange) nécessaires pour la transmission du contenu en aval ou la redistribution et le stockage de contenu interne (ou externe), y compris la prise en charge de conduits de traitement des médias sécurisés (résistants aux altérations), le stockage local des secrets (par exemple des clés), le remplacement des logiciels de sécurité, l'authentification et la vérification des actifs logiciels téléchargés et la protection des données d'utilisateur stockées localement et échangées faisant l'objet de considérations de respect de la vie privée de l'utilisateur final.

7.4.2 Fonctions et blocs fonctionnels de l'architecture de protection de contenu

Fonctions de client d'application: principal point de coordination et de commande d'interaction entre l'utilisateur final et les services offerts par les fonctions d'application de TVIP; pour des applications classiques comme le visionnage de télévision linéaire, font office de principale interface avec l'utilisateur et permettent à l'utilisateur final d'obtenir un service.

- **Bloc fonctionnel de client de découverte et de choix d'application:** permet à l'utilisateur final et/ou au dispositif terminal de découvrir l'existence et de choisir des applications et des services applicatifs offerts par les fournisseurs de service.

Fonctions d'application de TVIP: entités logiques d'où proviennent certains services de TVIP comme la télévision linéaire, la vidéo à la demande, etc.; chargées d'organiser l'ensemble des fonctionnalités des fournisseurs de service pour permettre l'existence opérationnelle de certains services.

- **Bloc fonctionnel de découverte et de choix d'application:** interagit avec le bloc fonctionnel de client de découverte et de choix d'application ci-dessus pour permettre à l'utilisateur final et/ou au dispositif terminal de découvrir l'existence et de choisir des applications et des services applicatifs.

Bloc fonctionnel de profil d'application: stocke et gère les informations de configuration des applications et des services, qu'elles soient globales ou qu'elles concernent un utilisateur final (abonné) particulier; généralement utilisé pour permettre aux serveurs d'application de personnaliser les services et le contenu pour l'utilisateur final, il interagit fréquemment avec divers systèmes de comptabilité ou les met en œuvre (en interne).

Fonctions de préparation de contenu: réalisent différents types de prétraitement de contenu avant sa fourniture, comme l'analyse du traçage de contenu (par exemple filigranes) et la production de métadonnées, le multiplexage du contenu et des métadonnées de contenu, et le chiffrement du contenu.

- **Bloc fonctionnel de traitement du contenu et des filigranes:** une ou plusieurs étapes de traitement optionnelles consistant à analyser le contenu pour produire des métadonnées de

traçage du contenu (par exemple filigranes) à utiliser dans le traitement aval ultérieur, en particulier un processus de singularisation de ces métadonnées (identification avec des informations fournies par la source d'association).

- **Bloc fonctionnel de traitement des métadonnées:** gère et traite les métadonnées liées aux programmes et les informations relatives aux droits d'utilisation fournies par le fournisseur de contenu.
- **Bloc fonctionnel de chiffrement de contenu:** réalise le chiffrement du contenu protégé (l'embrouille) pour faciliter le contrôle d'accès et la confidentialité pendant le processus de fourniture du contenu; le contenu peut être chiffré en temps réel ou être préalablement chiffré (le chiffrement du contenu peut, à titre d'option, prendre en charge le transcodage sécurisé sans déchiffrement).

NOTE 1 – Le chiffrement du contenu peut être mis en œuvre dans les fonctions de préparation de contenu au sein de la couche application. Dans certains cas, il peut aussi, à titre d'option, être mis en œuvre dans les fonctions de fourniture de contenu.

Bloc fonctionnel de gestion des droits et des clés: corrèle les droits et les clés avec le contenu et gère leur distribution au bloc fonctionnel de client de protection de contenu dans le dispositif terminal.

Bloc fonctionnel de client de protection de contenu: obtient ou reçoit les droits et clés et utilise ces informations pour commander le déchiffrement du contenu et appliquer les règles d'utilisation; ce bloc fonctionnel doit être résistant aux altérations.

Fonctions de fourniture de contenu: assurent des fonctionnalités de mise en mémoire cache et de stockage et fournissent le contenu demandé par les fonctions d'utilisateur final; elles peuvent, à titre d'option, traiter (par exemple coder, chiffrer) le contenu.

Fonctions de client de fourniture de contenu: chargées de la réception du contenu dans les fonctions de terminal de TVIP; assurent le déchiffrement des médias du contenu, leur démultiplexage, leur décodage et leur présentation ultérieure ainsi que le traitement pour le stockage du contenu (ces fonctions doivent aussi être résistantes aux altérations).

- **Bloc fonctionnel de détection de filigranes:** s'il est présent, il détecte l'utilisation de filigranes dans le contenu reçu des fournisseurs de service pour vérifier ou appliquer les règles d'utilisation de contenu souhaitées dans le dispositif terminal ou les interfaces en aval du dispositif terminal.
- **Bloc fonctionnel d'insertion de filigranes:** s'il est présent, il assure la singularisation de l'instance de contenu en vue de sa présentation et de son stockage ultérieur ou de sa redistribution.

Sources de droits: sont à l'origine des métadonnées de contenu concernant les droits d'utilisation du contenu.

Sources de contenu: sont à l'origine du contenu à regrouper, à traiter, puis à fournir aux utilisateurs finals au moyen d'applications de service comme la télévision linéaire, la vidéo à la demande, etc.

Bloc fonctionnel de stockage en dehors du dispositif: mécanismes de stockage du contenu après réception qui sont physiquement situés à l'extérieur du dispositif terminal et dont le stockage et l'utilisation du contenu ne sont pas gérés par le dispositif terminal.

NOTE 2 – Si un stockage externe existe et que son utilisation est commandée en permanence par le dispositif terminal, il peut alors être considéré comme un stockage interne au dispositif via une interface protégée et autorisée, qui dépend des règles applicables de robustesse et de conformité du dispositif terminal.

7.4.3 Fonctions et blocs fonctionnels de l'architecture de protection de service

Bloc fonctionnel de contrôle d'accès au service: principalement chargé du contrôle d'accès aux services; utilise des mécanismes de sécurité comme l'embrouillage et le chiffrement pour éviter que des utilisateurs accèdent à des services ou acquièrent des services sans permission.

Bloc fonctionnel de client de contrôle d'accès au service: réalise des tâches liées à la protection de service côté client comme défini par le bloc fonctionnel de contrôle d'accès au service côté serveur.

Bloc fonctionnel d'authentification de service: réalise l'authentification pour vérifier l'authenticité de l'utilisateur et/ou du dispositif terminal; il prend également en charge les demandes d'authentification qui proviennent du dispositif terminal afin de vérifier le serveur.

Bloc fonctionnel de client d'authentification de service: outre la réalisation de tâches liées à l'authentification de l'abonné côté client, il inclut également la fonction de vérification de l'authenticité du côté serveur de la protection de service pour l'authentification mutuelle.

8 Mécanismes de sécurité

La présente Recommandation ne définit pas de mécanisme ou de solution de sécurité spécifique; en revanche, il décrit de façon générale certains mécanismes de sécurité qui peuvent être envisagés pour définir ou mettre en œuvre des mécanismes qui tiennent compte des spécifications de sécurité, des entités fonctionnelles de l'architecture de sécurité et des menaces de sécurité.

L'ensemble des mécanismes de sécurité décrits ci-dessous ne répond pas de façon exhaustive à toutes les spécifications de sécurité décrites ci-dessus.

8.1 Mécanismes de sécurité pour la protection de contenu

Les mécanismes de sécurité du contenu comprennent un ensemble de fonctions mises en œuvre entre les sources de contenu et les dispositifs terminaux pour faire en sorte que le contenu puisse être distribué (ou transmis) de façon sécurisée par un réseau et puisse être acquis, consommé, exporté, stocké et redistribué (ou retransmis) de façon sécurisée par un utilisateur final.

Les mécanismes de sécurité du contenu peuvent être appliqués à la distribution, à l'acquisition, à la consommation, au stockage, à l'exportation et à la redistribution du contenu. Les mécanismes suivants peuvent être utilisés pour répondre aux spécifications de la protection de contenu et de service de TVIP (tous sont optionnels):

8.1.1 Chiffrement du contenu

Dans de nombreux cas, le contenu peut être chiffré afin d'éviter son utilisation illégale pendant la fourniture.

8.1.2 Traçage et identification du contenu

Le traçage du contenu sert à identifier l'origine (la source) du contenu et/ou l'entité responsable (par exemple l'utilisateur final) et à en garder la trace afin de faciliter les investigations ultérieures en cas d'accès non autorisé au contenu ou d'utilisation non autorisée du contenu.

Les informations de traçage du contenu peuvent être jointes au contenu sous forme de métadonnées ou de filigranes numériques. Les filigranes de traçage du contenu sont généralement conçus pour être robustes et imperceptibles afin d'éviter leur suppression délibérée ou involontaire.

Pour faciliter l'identification du contenu, une technologie de signature vidéo est recommandée.

8.1.3 Filigranage

Le filigranage consiste à ajouter des informations au contenu en modifiant certaines de ses caractéristiques. Il s'agit d'un domaine d'étude appelé *stéganographie*.

Le filigranage est recommandé pour de nombreuses applications en raison de la difficulté à supprimer ces informations du contenu. Dans un service de TVIP, le filigranage peut désigner l'inclusion directe d'informations cachées dans un flux de contenu multiplexé vidéo ou audio. Idéalement, les filigranes sont invisibles et/ou inaudibles pour les êtres humains mais survivent aux conversions entre différents formats de média.

8.1.4 Etiquetage du contenu

L'étiquetage du contenu consiste à insérer dans le contenu ou à associer au contenu des métadonnées décrivant la nature du contenu ainsi que des aspects et des caractéristiques du contenu. Le contenu étiqueté avec ces métadonnées peut être trié, filtré ou catégorisé plus facilement par les dispositifs intermédiaires appartenant à la chaîne de fourniture du contenu.

Certaines régions ou administrations ou certains déploiements spécifiques de la TVIP pourront nécessiter la présence de certains types d'étiquettes de contenu, par exemple des informations de classement pour permettre à l'utilisateur final (abonné) d'exercer un certain contrôle sur l'accès à un contenu jugé inapproprié ou préjudiciable.

8.1.5 Mécanisme transcodable sécurisé

Un mécanisme transcodable sécurisé (STS) est un type de mécanisme de sécurité permettant à un nœud de réseau intermédiaire d'effectuer un transcodage sans déchiffrement tout en préservant la sécurité de bout en bout. Pour exécuter ce mécanisme, on peut combiner un codage modulable, un chiffrement progressif et une mise en paquets.

Ce mécanisme fait intervenir trois entités: un émetteur, un nœud de réseau intermédiaire et un utilisateur avec un terminal de TVIP. L'émetteur exécute une fonction transcodable sécurisée pour produire des paquets chiffrés modulables à partir d'une vidéo et ajoute un en-tête non chiffré pour envoyer des informations; le nœud de réseau intermédiaire lit l'en-tête non chiffré et utilise les informations pour tronquer ou éliminer les paquets appropriés en fonction de l'opération de transcodage souhaitée, tandis que le terminal de TVIP déchiffre les paquets chiffrés et décode les paquets de texte en clair pour produire la vidéo. L'Appendice V contient une description détaillée.

NOTE – Le présent paragraphe n'est pas destiné à définir ou décrire plus en détail le mécanisme transcodable sécurisé. Ce sujet nécessite un complément d'étude dans d'autres Recommandations.

8.2 Mécanismes de sécurité pour la protection de service

Les mécanismes de sécurité de service comprennent l'authentification et l'autorisation et peuvent aussi comprendre des mises en œuvre de certains mécanismes de contrôle d'accès comme des systèmes de chiffrement et de déchiffrement.

8.2.1 Authentification de service

Dans le cas de services gérés pour lesquels un utilisateur final (abonné) a une relation directe avec un certain fournisseur de service, ce dernier exigera généralement que le dispositif terminal et/ou l'utilisateur final (abonné) soit authentifié de manière sécurisée avant d'offrir le service; dans ce cas, pour l'authentification, il faut produire et présenter de manière sécurisée des justificatifs d'identité/informations qui puissent être corrélés avec la base de données des abonnés du fournisseur de service afin de vérifier l'authenticité du dispositif terminal et/ou de l'utilisateur final en vue de la fourniture de service.

8.2.2 Autorisation de service

Après authentification de l'utilisateur final (abonné) et/ou du dispositif terminal en vue de la fourniture de service, un mécanisme d'autorisation de service est utilisé pour autoriser et accorder l'accès à des services spécifiques et au contenu associé conformément à la configuration des services et de l'abonné.

8.2.3 Contrôle d'accès aux services

Dans la plupart (si ce n'est la totalité) des cas, un système de protection de service contiendra des mécanismes de chiffrement (embrouillage) et déchiffrement (désembrouillage) du trafic de signalisation pour la commande de service et du trafic de contenu. Généralement, le trafic de commande de service bidirectionnel sera chiffré dans les deux sens – du serveur au client et du client au serveur. En revanche, les flux de contenu seront généralement chiffrés uniquement du serveur (fournisseur de service) au client (dispositif terminal). Néanmoins, dans certains scénarios d'utilisation, un flux de contenu peut être téléchargé d'un client vers un serveur, auquel cas ce contenu peut être chiffré par le dispositif terminal en vue de son téléchargement (par exemple pour faire en sorte que seul un fournisseur de service authentifié et autorisé puisse accéder au contenu téléchargé).

8.3 Mécanismes de sécurité pour la protection de réseau

La présente Recommandation ne définit et ne décrit aucun mécanisme de sécurité de réseau. D'une manière générale, les mises en œuvre de réseaux centraux, d'accès, support et de fourniture sont censées permettre de mettre en œuvre les mécanismes jugés nécessaires pour protéger l'intégrité opérationnelle du réseau, en particulier, par exemple, pour détecter et empêcher les dénis de service (DoS). Les mécanismes de sécurité employés par les fournisseurs de service de TVIP et les dispositifs terminaux seront généralement transparents pour ces réseaux, sous réserve que ces mécanismes fonctionnent au niveau ou au-dessus des éléments de données de charge utile fournis par les couches de réseau.

8.4 Mécanismes de sécurité pour la protection de dispositif terminal

Les mécanismes de sécurité de dispositif terminal comprennent des fonctionnalités très diverses: stockage des données secrètes sécurisé et résistant aux altérations, authentification des services, autorisation des services, chiffrement et déchiffrement des signaux de commande, déchiffrement du contenu, décodage des métadonnées relatives aux droits concernant le contenu, application des règles d'utilisation du contenu, détection et insertion de filigranes, authentification et vérification du contenu des programmes, pontage et échange pour la protection de service et de contenu, chiffrement au port (à l'interface) de sortie numérique, résistance aux altérations des trajets de média, processeurs et composants de sécurité enfichables et remplaçables, basés à la fois sur des matériels et sur des logiciels, etc.

8.5 Mécanismes de sécurité pour les abonnés ou les utilisateurs finals

Les mécanismes de sécurité des abonnés ou des utilisateurs finals se rapportent essentiellement à la collecte, au stockage et à la transmission d'informations pouvant faire l'objet de considérations de respect de la vie privée ou de confidentialité. En tant que tels, ces mécanismes peuvent être répartis entre le point de collecte, le dispositif terminal et le fournisseur de service, susceptibles de collecter, de conserver et de réutiliser ces informations. Par conséquent, les descriptions et définitions de ces mécanismes devraient figurer dans les paragraphes décrivant la sécurité de service et la sécurité de dispositif terminal.

Dans sa version actuelle, la présente Recommandation ne définit pas de mécanismes de sécurité des abonnés ou des utilisateurs finals. Ce sujet devrait être traité de façon plus approfondie dans de futures versions de la présente Recommandation.

L'Annexe A contient des informations complémentaires sur la sécurité des abonnés.

Annexe A

Protection de la sécurité des abonnés

(Cette annexe fait partie intégrante de la présente Recommandation)

A.1 Protection des données des utilisateurs

Lors de la mise en place de services de TVIP, il est essentiel de bien prendre en compte la protection de la sécurité des données d'abonné.

Les données d'abonné peuvent aussi inclure des données qui sont suivies comme le numéro de chaîne avant et après un changement de chaîne, l'heure du changement et des informations d'utilisateur pour le service EPG, l'identification du paquetage, l'heure de lecture, etc. Ces données sont personnelles et confidentielles. Pour que l'ensemble de ces données d'abonné soient protégées contre les abus, il faut que le fournisseur de service de TVIP prenne en compte les questions de protection de la vie privée des utilisateurs.

- Le service de TVIP peut, à titre d'option, utiliser les données personnelles d'abonné minimales nécessaires pour fournir les services de TVIP.
- Le service de TVIP peut, à titre d'option, expliquer l'utilisation prévue des données personnelles d'abonné et obtenir l'accord de l'abonné avant de collecter les informations nécessaires pour fournir les services de TVIP.
- Le service de TVIP peut, à titre d'option, détruire les données personnelles d'abonné qui deviennent inutiles pour la continuité des services de TVIP.
- Lorsque le fournisseur de service gère les données personnelles d'abonné, le service de TVIP peut, à titre d'option, stocker les données collectées en garantissant une sécurité stricte.

Il existe de nombreuses possibilités de fuite des données personnelles d'un abonné. Des fuites peuvent se produire au niveau du fournisseur de service, du réseau ou du domicile de l'abonné, par exemple par l'intermédiaire des dispositifs terminaux. Nous présentons ici des méthodes de protection des données personnelles d'abonné pour chacun de ces types de fuite.

Pour éviter toute fuite des données d'abonné, il est recommandé que le fournisseur de service de TVIP accorde une attention particulière à ce qui suit.

- Classer les données personnelles d'abonné en deux catégories: celles qui nécessitent un contrôle et celles qui n'en nécessitent pas.
- Gérer de façon sécurisée les données personnelles d'abonné nécessitant un contrôle.
- Faire en sorte que les données personnelles d'abonné nécessitant un contrôle ne soient pas utilisées à des fins autres que celle qui est prévue.

Il est recommandé que les fournisseurs de service de TVIP accordent une attention particulière aux points ci-dessous par rapport aux services et transactions utilisant des données personnelles d'abonné.

- Classer les données personnelles d'abonné en deux catégories: celles qui nécessitent un contrôle et celles qui n'en nécessitent pas.
- Utiliser des voies de communication chiffrées pour la transmission des données personnelles d'abonné nécessitant un contrôle.

Les fournisseurs de service de TVIP stockent parfois les données personnelles d'abonné dans les dispositifs terminaux pour améliorer l'efficacité des services. Dans ce cas, il leur est recommandé d'accorder une attention particulière aux points ci-dessous. En outre, il est recommandé de prendre en compte les questions de sécurité lors de l'échange de dispositifs terminaux.

- Faire en sorte qu'aucun tiers ne puisse lire facilement les données personnelles d'abonné stockées à l'intérieur du dispositif terminal.
- Le fournisseur de service de TVIP peut, à titre d'option, contrôler l'accès aux données personnelles d'abonné stockées dans le dispositif terminal.
- Faire en sorte que les données personnelles d'abonné stockées dans les dispositifs terminaux puissent être complètement supprimées par un abonné ou un fournisseur de service.
- Idéalement, nécessité pour les dispositifs terminaux d'être protégés contre toute attaque par des maliciels informatiques (par exemple virus et espionciels) dans un avenir proche.

A.2 Contrôle parental, protection des mineurs légaux, contrôle d'accès

Dans la plate-forme de TVIP, on peut utiliser un mécanisme de protection des mineurs légaux pour restreindre le contenu de TVIP auquel ces mineurs peuvent accéder. Dans un foyer, un dispositif terminal de TVIP est généralement utilisé en partage par plusieurs personnes, y compris des mineurs légaux. Pour les dispositifs terminaux, il est recommandé au fournisseur de service de TVIP de faire en sorte:

- qu'un classement parental du contenu puisse être établi en fonction des besoins;
- que les dispositifs terminaux puissent fonctionner conformément au classement parental;
- que les dispositifs terminaux puissent modifier le classement parental établi;
- que les dispositifs terminaux puissent mettre en œuvre des contrôles basés sur des mots de passe de sorte que seuls les responsables des mineurs légaux puissent modifier le classement parental;
- que le classement du contenu puisse être établi pour différents groupes d'âge;
- que des privilèges d'abonné puissent être attribués à différents groupes d'âge;
- que l'autorisation pour des mineurs légaux de visionner une chaîne ou un contenu particulier puisse être accordée dans les dispositifs terminaux, par exemple sur la base d'une demande de PIN;
- que les responsables des mineurs légaux qui ne se trouvent pas à leur proximité puissent surveiller à distance et recevoir le contenu destiné à ces mineurs, à partir d'une copie sur le réseau.

Il est à noter qu'il peut être nécessaire de prendre en considération les conditions de chaque administration ou région relatives aux organisations tierces pour l'élimination du contenu préjudiciable, étant donné qu'il existe un lien avec le contrôle du flux de contenu et de l'accès au contenu. On peut supposer que le créateur du contenu d'origine prend dûment en considération la retransmission simultanée des programmes de radiodiffusion au moment où il produit le contenu; d'où la nécessité d'accorder une attention suffisante aux retards de transmission et aux augmentations des coûts de distribution.

Appendice I

Menaces de sécurité

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

Le présent appendice décrit un ensemble de menaces de sécurité identifiées, prises en compte par certaines spécifications ou certains mécanismes décrits dans la présente Recommandation.

Le modèle des menaces de sécurité et d'autres éléments fondamentaux reposent sur les Recommandations UIT-T suivantes:

- [b-UIT-T X.800] définit les éléments d'architecture généraux liés à la sécurité qui peuvent être appliqués de façon appropriée dans les cas où il est nécessaire de protéger les communications entre systèmes ouverts.
- [b-UIT-T X.805] définit l'architecture de sécurité de réseau pour assurer la sécurité de réseau de bout en bout.

Ceux qui s'intéressent aux considérations de sécurité liées à la TVIP sont invités à lire ces Recommandations de base sur la sécurité; les lecteurs de la présente Recommandation sont supposés avoir connaissance des informations présentées dans ces Recommandations.

[b-UIT-T X.800] et [b-UIT-T X.805] identifient les menaces suivantes contre la sécurité des réseaux (qui constituent aussi des menaces contre la sécurité de service et de contenu de TVIP):

- Destruction d'informations et/ou d'autres ressources
- Corruption ou modification d'informations
- Vol, suppression ou perte d'informations et/ou d'autres ressources
- Divulgence d'informations
- Interruption de services.

I.1 Modèle des menaces de sécurité

Les menaces de sécurité pour la TVIP peuvent être classées dans les différentes catégories suivantes: menaces contre la sécurité de contenu, menaces contre la sécurité de service, menaces contre la sécurité de réseau, menaces contre la sécurité du dispositif terminal, et menaces contre la sécurité de l'abonné.

La Figure I.1 illustre le modèle des menaces de sécurité, qui montre les relations entre ces différentes menaces.

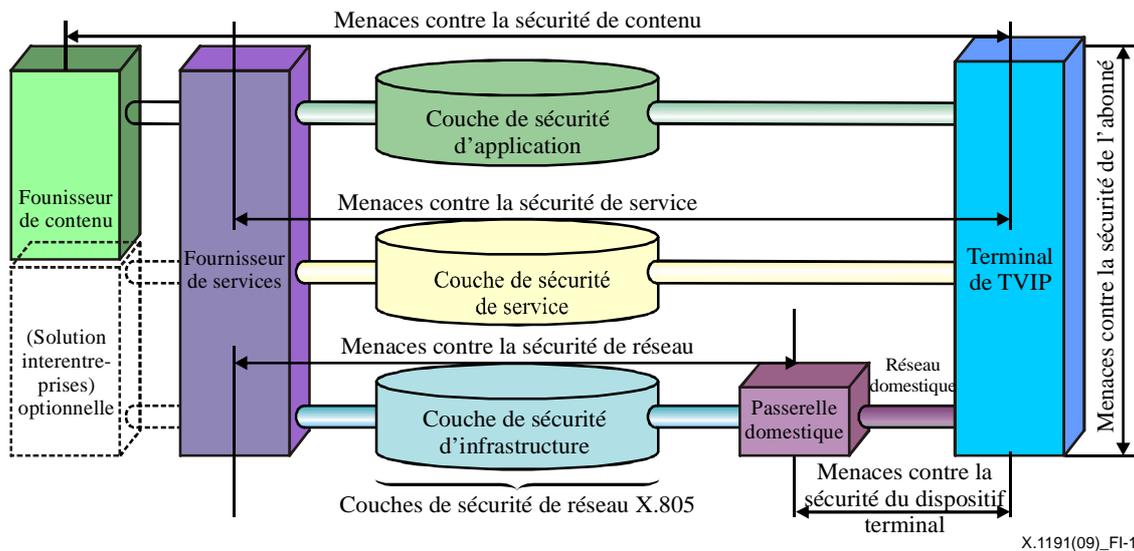


Figure I.1 – Modèle des menaces de sécurité

I.1.1 Menace contre la sécurité de contenu

Actifs de contenu: actifs appartenant à un fournisseur de contenu et/ou à un fournisseur de service, qui peuvent être consommés par l'utilisateur final via un dispositif terminal.

Les actifs de contenu à protéger sont les suivants: contenu de télévision linéaire, contenu de vidéo à la demande, contenu de vidéo à la demande avec distribution sélective, contenu d'enregistreur PVR, applications téléchargées, etc.

Les menaces visant le contenu sont les suivantes:

- Interception: atteinte à la confidentialité du contenu numérique découlant d'une surveillance illégale des réseaux de service.
- Visionnage non autorisé.
- Reproduction ou redistribution non autorisée.

I.1.2 Menace contre la sécurité de service

Actifs de service: actifs appartenant à un fournisseur de service: serveurs de média, serveurs SCP et informations opérationnelles telles que journaux de service et informations de facturation au minimum.

Les menaces visant les services sont les suivantes:

- Violation des droits d'auteur afférents aux programmes fournis aux abonnés par la plateforme de service de TVIP.
- Usurpation de l'identité du fournisseur de service de TVIP.
- Menaces malveillantes contre les serveurs de TVIP (serveurs SCP, serveurs de média, etc.): par exemple piratage afin de conduire à des failles de sécurité dans le logiciel applicatif ou dans le protocole de communication, attaque par déni de service, etc.
- Vol d'informations d'abonné (par exemple informations d'identification, informations de facturation, informations d'abonnement), souvent en utilisant des programmes malveillants tels que les chevaux de Troie.

I.1.3 Menace contre la sécurité de réseau

Actifs de réseau: actifs qui appartiennent au fournisseur de réseau: équipements physiques (par exemple routeurs, commutateurs), ressources de réseau (par exemple largeur de bande, services de multidiffusion), etc.

Les menaces visant le réseau sont les suivantes:

- Menaces intentionnelles contre des équipements ou des ressources de réseau (largeur de bande): attaques malveillantes contre le réseau support (par exemple déni de service).
- Menaces contre la sécurité de la technique de multidiffusion utilisée dans le réseau support de TVIP, par exemple usurpation de l'identité de sources de multidiffusion de télévision ou membres de groupes de multidiffusion illégitimes.
- Attaques malveillantes (par exemple DoS, piratage) contre des nœuds du réseau de distribution de contenu.

I.1.4 Menace contre la sécurité du dispositif terminal

Actifs du terminal: actifs appartenant à un dispositif terminal qui peuvent être utilisés par l'utilisateur final pour traiter et stocker un contenu et d'autres informations pertinentes pour le service de TVIP.

Les menaces visant le terminal sont les suivantes:

- Accès illégal à un contenu en clair par altération d'éléments matériels ou logiciels du dispositif; par exemple, un contenu en clair peut être copié par interception d'un bus de données ou par craquage d'un logiciel SCP.
- Accès illégal à des clés ou à d'autres informations secrètes dans des dispositifs par craquage de logiciel ou altération de matériel; les attaquants peuvent altérer la mémoire du dispositif ou analyser le flux de données pour obtenir les clés et autres secrets (l'exposition de clés de contenu entraîne une fuite de contenu, et la fuite de clés de dispositif entraîne l'usurpation d'identité du dispositif).
- Dysfonctionnement du dispositif créé par une méthode matérielle (par exemple commande du système d'horloge du dispositif afin de désactiver les fonctions des systèmes SCP) ou par une méthode logicielle (par exemple installation de virus afin d'épuiser les ressources du dispositif).
- Téléchargement, exécution et stockage d'applications non autorisées (par exemple des programmes logiciels) dans des dispositifs terminaux.
- Panne de l'équipement terminal (matériel et logiciel) causée par des codes/virus malveillants provenant du réseau.
- Raccordement au réseau domestique de dispositifs terminaux non authentifiés.
- Utilisation non autorisée par des abonnés.

I.1.5 Menace contre la sécurité de l'abonné

Actifs de l'abonné: actifs qui appartiennent à un abonné; ils peuvent être constitués d'informations sur l'abonné, le foyer de l'abonné, leurs transactions de TVIP, etc.

Pour assurer la sécurité de l'abonné, il faut qu'un mécanisme de sécurité de contenu et un mécanisme de sécurité de service fonctionnent conjointement car dans les services de TVIP, la sécurité de contenu et la sécurité de service sont liées.

Le Tableau I.1 donne des exemples de menaces pour l'abonné.

Tableau I.1 – Catégories de sécurité pour l'abonné

	Sécurité de l'abonné		
	Exemple de service	Exemple de menace	Exemple de mécanisme de protection
Sécurité de contenu	service de télévision linéaire, de vidéo à la demande	copie illégale	identification du dispositif terminal (protection de service, protection de contenu)
Sécurité de service	service bidirectionnel	hameçonnage	identification de la personne (protection des données personnelles, PIN/mot de passe)
	parental	usurpation d'identité	identification de la personne (PIN/mot de passe, authentification)
Sécurité de réseau	non spécifié	écoute clandestine	identification de la ligne d'abonné données de chiffrement, contrôle de raccordement multidestinataire
Sécurité de dispositif terminal	service P2P	copie illégale	protection de contenu (P2P)

Appendice II

Interopérabilité SCP

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

II.1 Aperçu de l'interopérabilité SCP

Il existe plusieurs scénarios d'interopérabilité SCP: SCP-EE, SCP-B et SCP-IX, qui peuvent être appliqués au domaine du fournisseur de service ou au domaine de l'utilisateur final. Le présent appendice porte uniquement sur le côté terminal.

II.2 Scénarios d'interopérabilité SCP

Pour les scénarios d'interopérabilité SCP, on distingue au moins trois modes: SCP de bout en bout (SCP-EE), SCP avec pontage (SCP-B) et SCP avec échange (SCP-IX).

1) SCP-EE

Utilisant une seule SCP, deux dispositifs ou plus s'échangent un contenu et y accèdent en fonction des droits accordés. C'est le mode le plus simple à mettre en œuvre, étant donné qu'une seule SCP est utilisée.

2) SCP-B

Sur un même dispositif terminal, deux SCP ou plus sont déployées. Le contenu acquis via une SCP (par exemple en provenance d'un réseau) peut être consulté via une autre SCP résidant sur le même dispositif en fonction des droits accordés.

3) SCP-IX

Ce cas est caractérisé par deux dispositifs ou plus, une ou plusieurs SCP étant déployées dans chaque dispositif. Le contenu acquis par un dispositif via l'une de ses SCP peut être transféré en toute sécurité à un autre dispositif et consulté par ce dispositif via une SCP différente en fonction des droits accordés.

La Figure II.1 modélise les cas décrits ci-dessus.

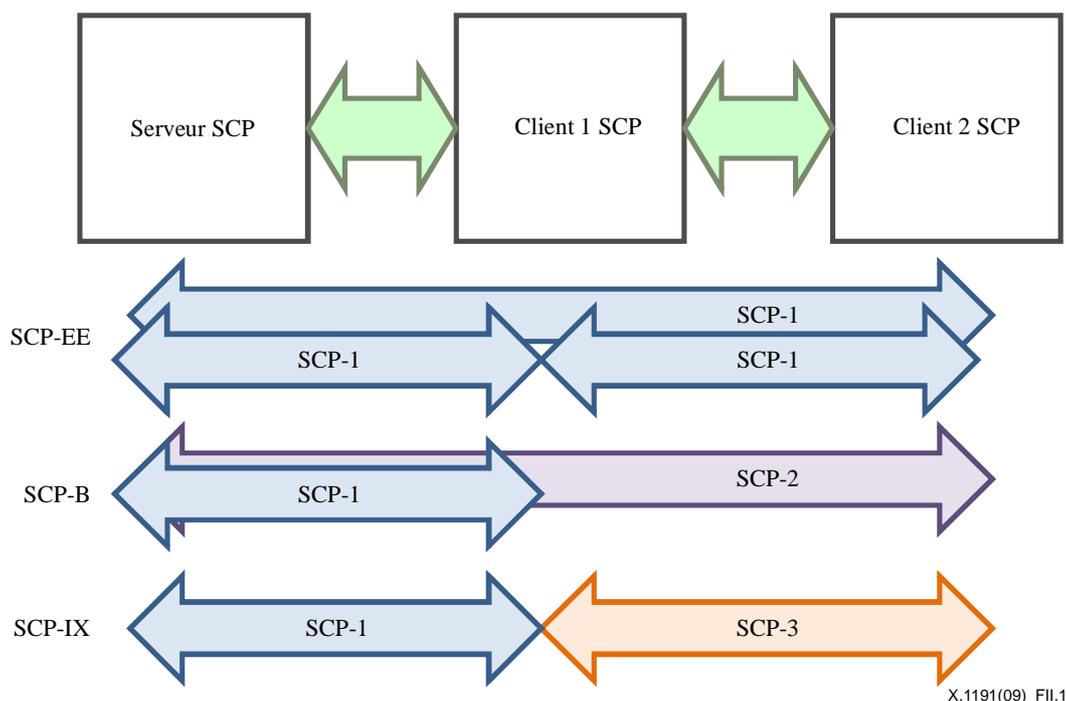


Figure II.1 – Modes d'interopérabilité SCP

II.3 Domaines techniques d'interopérabilité SCP

Les domaines suivants représentent les principaux éléments d'interopérabilité nécessaires dans les modes SCP-EE, SCP-B et SCP-IX:

1) Authentification des dispositifs, des utilisateurs et des SCP

Avant qu'un contenu puisse être échangé entre deux entités, l'identifiant du dispositif terminal et éventuellement celui de ses utilisateurs doivent être établis de façon sécurisée. De plus, étant donné que les fournisseurs de contenu ne font pas nécessairement confiance à certaines SCP, il devrait être possible d'authentifier les SCP de réception ou les niveaux de mise en œuvre avant l'échange de contenu. Cette authentification devrait être fondée sur une base cryptographique solide et pourra employer diverses techniques de signature numérique bien connues. En particulier, la cryptographie à clé publique constitue un bon mécanisme pour les signatures numériques dans les protocoles d'authentification.

2) Echange d'expression des droits

Les langages d'expression de droits ou les formats de licence utilisés varient suivant les SCP. Pour que les modes SCP-B et SCP-IX puissent fonctionner, il faut un moyen commun d'expression des droits, qui peut prendre la forme d'un langage commun d'expression des droits ou d'un convertisseur d'expression des droits. La négociation de licence est un autre mécanisme possible pour l'échange d'expression des droits.

3) Algorithmes de chiffrement communs pour l'échange de contenu

Pour que le contenu puisse passer de façon sécurisée du contrôle d'une SCP à une autre ou d'un dispositif physique à un autre mais dans le cadre de la même SCP, un chiffrement du contenu est nécessaire. Ainsi, le contenu est rendu inutilisable sauf pour les entités qui possèdent les clés appropriées nécessaires pour le déchiffrement. Il existe un grand nombre de types différents d'algorithmes de chiffrement (par exemple chiffrement par bloc, chiffrement par flux, chiffrement basé sur une clé publique, etc.), mais ceux qui utilisent des clés symétriques ont généralement tendance à être les mieux adaptés pour l'échange de contenu à haut débit. Dans un souci

d'interopérabilité, il faut choisir un petit nombre d'algorithmes largement adoptés. Idéalement, il faudrait aussi spécifier un seul algorithme par défaut.

4) Gestion et/ou échange de clés pour les algorithmes de chiffrement communs

Avant qu'un contenu puisse être échangé en toute sécurité, les clés à utiliser dans des instances particulières doivent être échangées ou générées en commun par les entités authentifiées. La gestion de clés est généralement la partie la plus difficile à mettre en œuvre dans un système de sécurité. Des techniques comme la cryptographie à clé publique ont simplifié la distribution des clés entre les dispositifs mais nécessitent une infrastructure de clé publique (PKI) pour établir et maintenir la validité de ces clés. Cette infrastructure pourrait être autorisée et maintenue par une autorité sous licence chargée de la protection de contenu (par opposition à la sécurité de réseau générale).

5) Téléchargement sécurité du client SCP

L'idéal serait que n'importe quel dispositif terminal puisse échanger un contenu obtenu (légitimement) par le biais d'autres dispositifs et/ou en utilisant n'importe quelle SCP en fonction des droits accordés (à savoir mode SCP-IX). Il est toutefois à noter qu'il n'est guère possible de précharger dans chaque dispositif terminal au moment de sa fabrication toutes les SCP requises par les forces du marché; d'où la nécessité d'un mécanisme sécurisé permettant de télécharger et de mettre en œuvre une SCP choisie dans un dispositif terminal. Des éléments comme les amorceurs sécurisés et les protocoles de téléchargement sécurisés jouent un rôle dans ce domaine d'interopérabilité.

NOTE – Lorsque l'interopérabilité SCP est déployée dans les dispositifs et dans les systèmes d'extrémité, les dispositifs de TVIP devraient avoir une architecture fiable pour prendre en charge l'interopérabilité de la sécurité de contenu.

6) Exportation sécurisée des droits

Pour exporter des droits numériques en toute sécurité, le client SCP de TVIP devrait vérifier si l'exportation de droits d'utilisation est permise en ce qui concerne le système SCP cible. Certaines expressions de droits numériques permettent au système SCP cible d'exporter des droits. Dans ce cas, le client SCP de TVIP devrait vérifier ces expressions et autoriser les systèmes SCP cibles appropriés à exporter des droits numériques.

II.4 Architectures d'interopérabilité SCP

Deux sortes d'architectures possibles d'interopérabilité SCP peuvent être envisagées. L'une est une architecture d'interopérabilité basée sur un médiateur, qui utilise un système médiateur situé entre deux systèmes SCP pour assurer une transmission interopérable. L'autre est une architecture basée sur un protocole normalisé, qui utilise des interfaces et des protocoles normalisés pour transformer le contenu numérique protégé et associer des informations entre deux systèmes SCP différents.

Les deux architectures possibles sont illustrées sur les Figures II.2 et II.3.

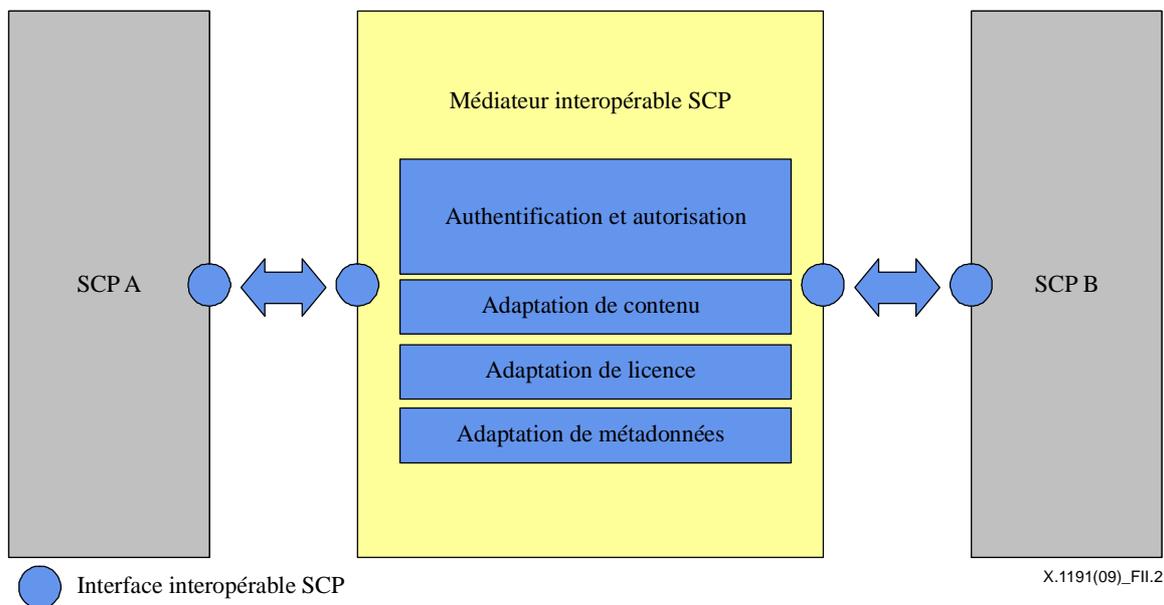


Figure II.2 – Architecture d'interopérabilité SCP basée sur un médiateur

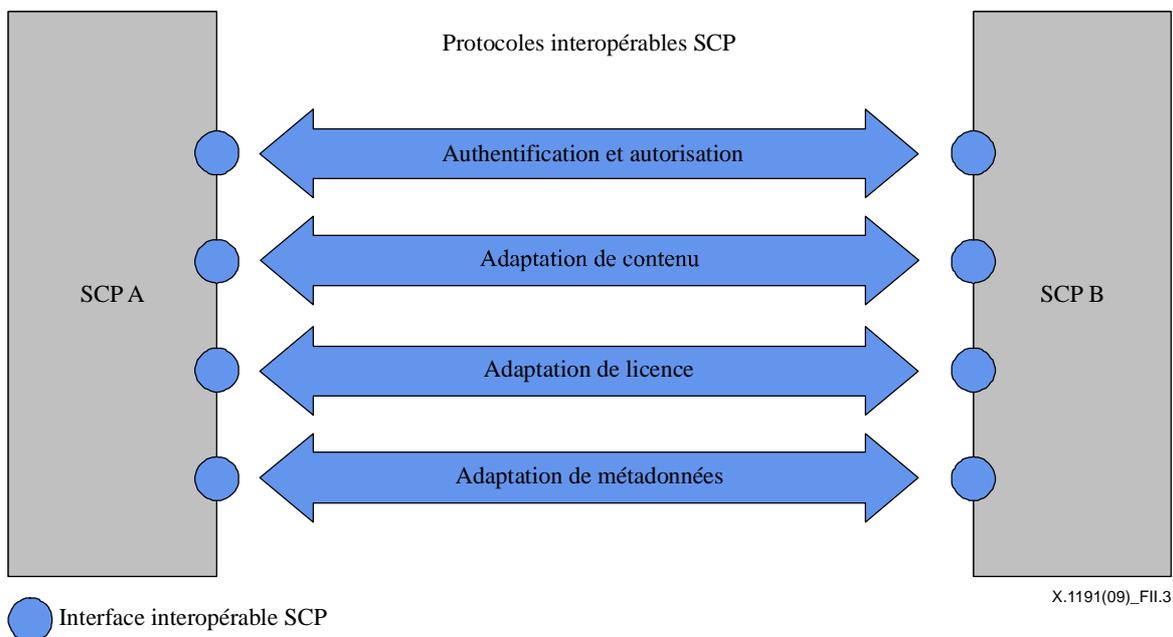


Figure II.3 – Architecture d'interopérabilité SCP basée sur un protocole normalisé

Description des blocs fonctionnels

- **Adaptation de contenu:** l'adaptation de contenu est chargée de la conversion de l'algorithme de chiffrement, qui sera facilitée par les quelques algorithmes de chiffrement normalisés prédéfinis qui sont donnés.
- **Adaptation de licence:** l'adaptation de licence est chargée de la conversion d'une licence. Toute licence temporelle ou classique dont les deux entités ont connaissance devrait conserver quasiment les mêmes comportements de permission (paire d'actifs de média et de permissions de consommation) que ceux qui sont définis dans la licence d'origine. Un ensemble de conversion des droits (conversion d'expression des droits et conversion sémantique) peut être inclus dans l'adaptation de licence. De plus, l'adaptation de licence peut être chargée de rempaqueter les informations relatives aux droits et de les fournir de façon sécurisée aux clients SCP natifs.

- **Adaptation de métadonnées:** l'adaptation de métadonnées est chargée de la conversion des métadonnées. Les métadonnées temporelles ou classiques dont les deux entités ont connaissance devraient être identiques aux métadonnées d'origine. Un ensemble de conversion des métadonnées (conversion syntaxique et sémantique) peut être inclus dans l'adaptation de métadonnées. De plus, l'adaptation de métadonnées peut être chargée de rempaqueter les métadonnées et de les fournir de façon sécurisée à l'autre entité SCP.
- **Authentification et autorisation:** chaque entité SCP devrait déterminer si l'autre entité est une cible appropriée pour parvenir à l'interopérabilité SCP. Cette opération est généralement accompagnée d'une étape préliminaire d'authentification mutuelle entre les deux entités SCP.

Cas particulier: Si la SCP A et la SCP B sont situées dans le même dispositif ou s'il existe un canal de communication sécurisé dédié entre les deux SCP, l'adaptation de contenu ne nécessitera peut-être pas de traitement interopérable.

II.5 Scénarios de déploiement des modes SCP-B et SCP-IX dans des dispositifs terminaux

Le présent paragraphe décrit trois scénarios possibles nécessitant un SCP avec échange entre la sécurité de service et la sécurité de contenu.

II.5.1 Définitions de termes utilisés dans les diagrammes

- SCP_IN: port d'entrée du contenu de TVIP protégé par la SCP.
- SCP_OUT: port de sortie du contenu de TVIP protégé par la SCP.

II.5.2 Scénario 1: SCP avec SCP-IX

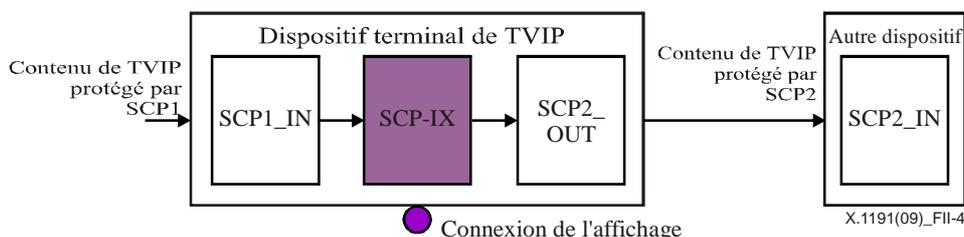


Figure II.4 – SCP avec SCP-IX

Dans ce cas, le dispositif terminal de TVIP utilise une SCP avec SCP-IX pour prendre en charge l'interopérabilité entre le dispositif terminal de TVIP sans stockage ayant uniquement une sécurité de service et le dispositif externe avec stockage ayant uniquement une protection de contenu.

Pour prendre en charge une connectivité souple et sécurisée avec n'importe quel type de dispositif externe mettant en œuvre divers mécanismes de protection de contenu, le dispositif terminal de TVIP devrait être basé sur le mode SCP-IX plutôt que sur une mise en œuvre au cas par cas pour la connexion de sécurité entre deux dispositifs.

II.5.3 Scénario 2: SCP avec SCP-B facultatif et stockage

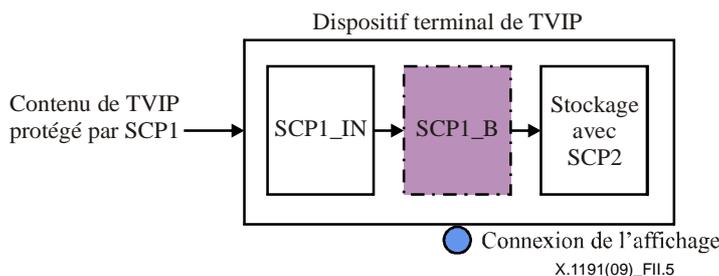


Figure II.5 – SCP avec SCP-B facultatif et stockage

Dans ce cas, le dispositif terminal de TVIP utilise une SCP avec SCP-B pour prendre en charge l'interopérabilité entre la protection de service et la protection de contenu sur le même dispositif.

Le fabricant du dispositif terminal de TVIP peut utiliser un mécanisme propriétaire de protection de contenu pour le stockage interne. Dans ce cas, le mode SCP_B n'est pas nécessaire et la SCP1 peut être utilisée pour le stockage.

Pour prendre en charge une connectivité souple avec n'importe quel type de stockage interne mettant en œuvre divers mécanismes de protection de contenu, il est recommandé que le dispositif terminal de TVIP soit basé sur le mode SCP_B plutôt que sur une mise en œuvre au cas par cas pour la connexion de sécurité entre la protection de service et la protection de contenu.

II.5.4 Scénario 3: SCP avec stockage et SCP-IX

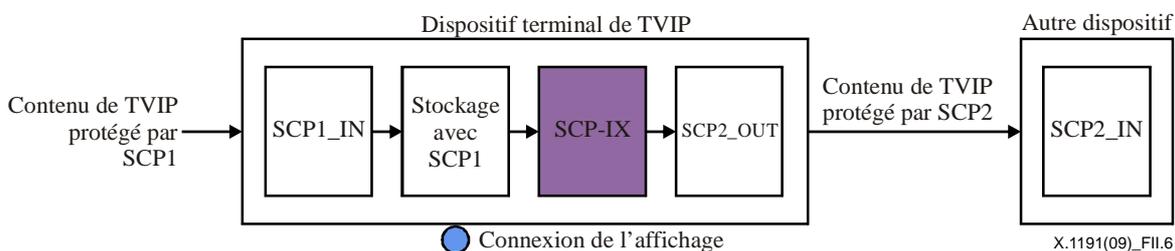


Figure II.6 – SCP avec stockage et SCP-IX

Dans ce cas, le dispositif terminal de TVIP utilise une SCP avec stockage et le mode SCP-IX pour prendre en charge l'interopérabilité entre les mécanismes interne et externe de protection de contenu.

Pour prendre en charge une connectivité souple avec n'importe quel type de stockage externe mettant en œuvre divers mécanismes de protection de contenu, il est recommandé que le dispositif terminal de TVIP soit basé sur le mode SCP-IX plutôt que sur une mise en œuvre au cas par cas pour la connexion de sécurité entre les mécanismes interne et externe de protection de contenu.

Appendice III

Exemple de processus de protection de contenu de TVIP

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

On décrit ci-après un exemple de processus de protection de contenu dans le cas d'une application de vidéo à la demande:

- *Phase d'authentification de l'abonné*
 - Un abonné choisit une application de vidéo à la demande (VoD) par le biais du "bloc fonctionnel de client de découverte et de choix de service et d'application".
 - Dès qu'elles ont reçu la demande, les "fonctions d'application de TVIP" l'envoient au "bloc fonctionnel de profil d'application" pour vérifier cet abonné. Si la vérification aboutit, les informations d'autorisation de cet abonné sont mises en mémoire cache dans le "bloc fonctionnel de profil d'application" pour consultation.
- *Phase de choix du contenu*
 - L'abonné peut choisir un contenu média en utilisant les informations de la passerelle ECG, et le "bloc fonctionnel d'application de VoD" fournit les informations d'emplacement du contenu choisi (URL) au dispositif terminal.
 - Le "bloc fonctionnel de client de VoD" du dispositif terminal reçoit l'emplacement du contenu à transmettre aux "fonctions de client de fourniture de contenu".
- *Phase de fourniture du contenu chiffré*
 - Les "fonctions de client de fourniture de contenu" demandent le contenu média (chiffré) en utilisant les informations d'emplacement du contenu; elles demandent aussi les droits et clés associés à ce contenu au "bloc fonctionnel de client de protection de contenu".
- *Phase de distribution des droits et des clés*
 - S'il ne possède pas les droits et les clés, le "bloc fonctionnel de client de protection de contenu" demande ces informations au "bloc fonctionnel de gestion des droits et des clés" du fournisseur de service de TVIP.
 - Le "bloc fonctionnel de gestion des droits et des clés" demande les informations d'autorisation de cet abonné au "bloc fonctionnel de profil d'application" pour vérifier si l'abonné a le droit de consommer ce contenu en utilisant ces informations.
 - Si cette opération aboutit, le droit et la clé pour le contenu choisi sont fournis au "bloc fonctionnel de client de protection de contenu".
 - Dès qu'il a reçu la clé et le droit, le "bloc fonctionnel de client de protection de contenu" les transfère aux "fonctions de client de fourniture de contenu" afin de déchiffrer le contenu et de commander son utilisation.

Appendice IV

Protection du contenu et gestion des copies de DVB

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

Le présent appendice décrit l'ensemble des spécifications de protection du contenu et de gestion des copies de DVB (DVB-CPCM, DVB content protection and copy management), qui ont été élaborées par l'ETSI.

Le système DVB-CPCM est un exemple de système entièrement normalisé pour la protection de contenu télévisuel ou autre aussi bien à l'intérieur qu'à l'extérieur d'un réseau domestique. Il acquiert un contenu auprès d'un mécanisme de protection de service de TVIP défini par l'UIT (ou autre) et maintient la protection du contenu de TVIP tout au long du cycle de vie du contenu depuis l'acquisition jusqu'à la consommation, en passant par le stockage, le traitement et l'exportation de contenu protégé à d'autres mécanismes de sécurité de TVIP, tout en maintenant l'utilisation autorisée correcte.

IV.1 Introduction

Le système DVB-CPCM est un système destiné à protéger le contenu numérique commercial ou en clair fourni aux produits grand public et aux réseaux domestiques et à en gérer les copies. La norme CPCM permet de gérer l'utilisation du contenu depuis l'acquisition dans le système CPCM jusqu'à sa consommation finale ou à son exportation du système CPCM conformément aux règles d'utilisation particulières de ce contenu. Elle est destinée à être utilisée pour protéger tous les types de contenu, par exemple audio, vidéo, et les applications et données associées. Elle contient des spécifications visant à faciliter l'interopérabilité de ce contenu après son acquisition dans le système CPCM avec les dispositifs de consommateur en réseau, à la fois pour les réseaux domestiques et pour l'accès à distance. Certaines parties des spécifications définissent la signalisation et les actions nécessaires pour la conformité technique tandis que d'autres parties contiennent des explications, y compris des lignes directrices relatives à la mise en œuvre. Un modèle de référence définit le cadre du système CPCM et sert de fondement pour les autres éléments des spécifications.

IV.2 Définitions

Le présent appendice définit les termes suivants en plus de ceux qui sont définis dans le texte principal:

IV.2.1 acquérir: recevoir et ingérer dans le système CPCM un contenu provenant de l'extérieur de ce système

IV.2.2 point d'acquisition (AP, *acquisition point*): entité fonctionnelle CPCM abstraite au niveau de laquelle l'acquisition de contenu a lieu

IV.2.3 acquisition: réception et ingestion dans le système CPCM d'un contenu provenant de l'extérieur de ce système

IV.2.4 domaine autorisé (AD, *authorized domain*): ensemble distinguable de dispositifs compatibles DVB-CPCM qui sont possédés, loués ou contrôlés par les membres d'un même foyer; le foyer désigne l'unité sociale constituée de tous les individus qui vivent ensemble en tant qu'occupants du même domicile (aucune hypothèse n'est faite quant aux emplacements physiques des dispositifs possédés, loués ou contrôlés par les membres du foyer)

IV.2.5 utilisation autorisée: utilisation permise du contenu CPCM; constituée d'un ensemble d'assertions de règles d'utilisation appliquées à ce contenu

IV.2.6 consommer: restituer concrètement un contenu, à l'exclusion de toute autre utilisation

IV.2.7 point de consommation (CP, *consumption point*): entité fonctionnelle CPCM abstraite au niveau de laquelle la consommation est exécutée

IV.2.8 consommation: restitution concrète d'un contenu ou d'une sortie de dispositif contenant une transformation ou un signal destiné à empêcher une utilisation autre que la conversion immédiate du contenu en sons et en images

IV.2.9 élément de contenu: instance discrète de contenu de durée déterminée, par exemple programme/événement ou segment incomplet de programme/événement

IV.2.10 licence de contenu: structure de données maintenue et communiquée de façon sécurisée contenant les informations nécessaires pour gérer la sécurité d'un élément de contenu CPCM

IV.2.11 contenu: données devant être protégées par le système CPCM; il s'agit généralement d'un contenu audiovisuel incluant des données d'accompagnement facultatives comme des sous-titres, des images/graphiques, des animations, des pages web, du texte, des jeux, des logiciels (en code source ou en code objet), des scripts, ou toute autre information destinée à être fournie à un utilisateur et à être consommée par cet utilisateur

IV.2.12 copie: processus géré par le système CPCM consistant à créer un nouvel élément de contenu stocké à partir du contenu acquis ou d'un élément de contenu stocké existant

IV.2.13 dispositif CPCM: dispositif qui héberge une ou plusieurs instances CPCM

IV.2.14 système CPCM: ensemble de tous les dispositifs CPCM conformes

IV.2.15 application de dispositif: toute fonctionnalité non CPCM d'un dispositif CPCM

IV.2.16 point d'exportation (EP, *export point*): entité fonctionnelle CPCM abstraite au niveau de laquelle le contenu CPCM quitte le système CPCM

IV.2.17 exportation: abandon par le système CPCM de la protection et de la gestion explicites d'un contenu CPCM au profit d'un système CPS contrôlé, d'un système CPS de confiance ou d'un espace non fiable

IV.2.18 transfert: exécution d'une copie, l'original étant ensuite supprimé, effacé ou rendu inaccessible

IV.2.19 sortie: interface de dispositif ou système CPS utilisé pour transmettre un contenu CPCM, un contenu consommé ou un contenu exporté

IV.2.20 entité de traitement (PE, *processing entity*): entité fonctionnelle CPCM abstraite au niveau de laquelle le contenu CPCM est traité

IV.2.21 traitement: opération compatible CPCM sur un contenu chiffré ou non chiffré autre que la consommation ou l'exportation, Par exemple, un contenu CPCM subit une transformation permise par rapport de sa forme d'origine pour créer un nouveau contenu CPCM transformé, ou des informations comme des niveaux de volume audio ou des images fixes sont extraites du contenu

IV.2.22 informations d'état d'utilisation (USI, *usage state information*): métadonnées relatives au contenu CPCM qui signalent l'utilisation autorisée pour chaque élément de contenu CPCM

IV.2.23 visionner: consommer.

NOTE – Comprend aussi l'action d'écouter pour un contenu uniquement audio.

IV.2.24 visionnage: consommation.

NOTE – Comprend aussi l'écoute pour un contenu uniquement audio.

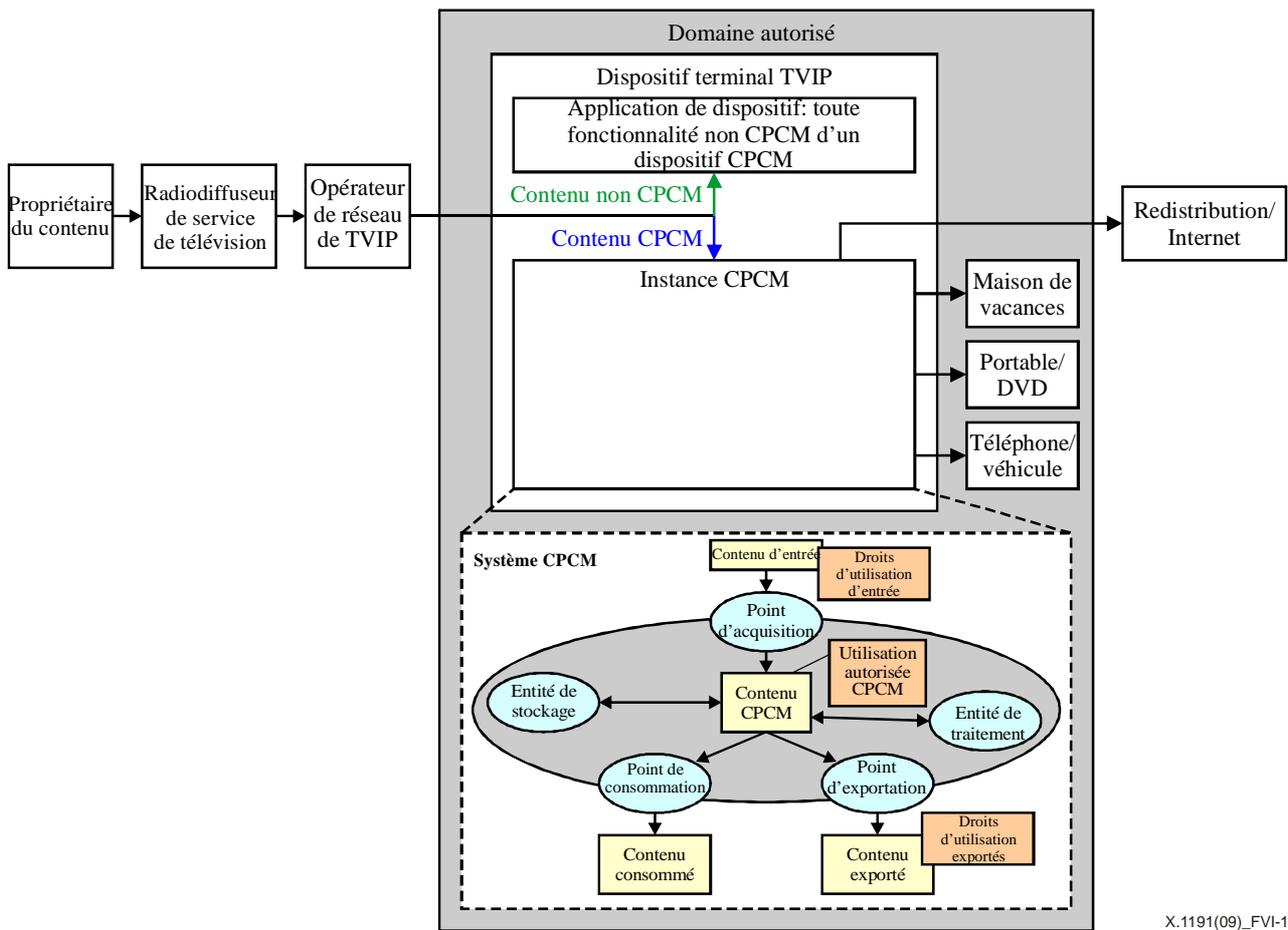
IV.3 Abréviations et acronymes

Le présent appendice utilise les abréviations suivantes en plus de celles qui sont utilisées dans le texte principal:

AP	point d'acquisition (<i>acquisition point</i>)
APECS	acquisition, traitement, exportation, consommation, stockage (<i>acquisition, processing, export, consumption, storage</i>)
CL	licence de contenu (<i>content license</i>)
CP	point de consommation (<i>consumption point</i>)
CPCM	protection de contenu et gestion de copie (<i>content protection and copy management</i>)
CPE	équipement local de client (<i>customer premises equipment</i>)
CPS	système de protection de contenu (<i>content protection system</i>)
DVB	radiodiffusion vidéonumérique (<i>digital video broadcasting</i>)
EP	point d'exportation (<i>export point</i>)
PE	entité de traitement (<i>processing entity</i>)
SE	entité de stockage (<i>storage entity</i>)
USI	informations d'état d'utilisation (<i>usage state information</i>)

IV.4 Architecture CPCM

Le système CPCM est articulé autour du "domaine autorisé", ensemble de dispositifs appartenant à un foyer, même lorsqu'ils sont à l'extérieur du domicile. Le concept de domaine autorisé reconnaît qu'à l'époque des loisirs en réseau, il est insuffisant de relier un contenu à un seul boîtier-adaptateur (dispositif terminal) et à un téléviseur rattaché. Le système CPCM prend le contenu auprès d'une source de confiance telle qu'un système SCP de TVIP, matérialisant tout ou partie d'un dispositif terminal, et protège le flux ou le fichier de contenu reçu, gérant la façon dont il peut être visionné, transféré et copié. Dans le modèle de base de gestion de contenu CPCM, le contenu d'entrée pénètre dans le système CPCM et devient le contenu CPCM. Ce contenu CPCM est géré et protégé à l'intérieur du système CPCM; il quitte le système CPCM lorsqu'il est consommé par l'utilisateur ou exporté vers un autre système.



X.1191(09)_FVI-1

Figure IV.1 – Flux de contenu dans un environnement CPCM

Le système CPCM prend en charge diverses utilisations du contenu dans un réseau domestique; il peut aussi gérer l'accès au contenu depuis des emplacements distants, par exemple depuis un ordinateur portable raccordé à l'Internet via une liaison large bande. Le système CPCM permet aux fournisseurs de service de signaler aux fabricants de dispositifs les scénarios admissibles pour chaque type de contenu. De nombreuses méthodes de protection actuelles peuvent ainsi être étendues, par exemple celles qui sont utilisées dans les technologies SCP de TVIP dans lesquelles le contenu est généralement restreint à un seul câble d'interconnexion point à point entre le dispositif source du contenu (par exemple un boîtier-adaptateur) et le dispositif d'affichage numérique.

Le système CPCM ne se limite pas à une protection localisée, donnant aux radiodiffuseurs, aux opérateurs de réseau et aux propriétaires de contenu la possibilité d'offrir un accès à un membre du foyer depuis un emplacement distant, par exemple depuis un hôtel pendant un voyage d'affaires ou pendant des vacances.

Le système CPCM peut aussi permettre aux utilisateurs de copier un contenu dans des dispositifs portables et sur des supports de stockage amovibles comme les DVD. Tant que le dispositif de lecture appartient au même domaine autorisé, il pourra lire le contenu même s'il est déconnecté du domicile et du fournisseur de service d'origine. Le contenu CPCM ne nécessite aucune autorisation en ligne de la part d'un fournisseur de service pour ce qui est de l'ajout ou de la suppression de dispositifs dans le domaine autorisé.

Le système de protection de contenu CPCM n'est pas une entité autonome; il est incorporé/superposé dans le système global de distribution SCP de TVIP de bout en bout. En tant que tel, il ne remplace pas un système SCP de TVIP mais coexiste avec un tel système. Dans tout dispositif terminal, l'instance CPCM est facultative; toutefois, si elle est absente, l'accès au contenu

protégé par le système CPCM ne sera pas accordé au dispositif terminal. Néanmoins, le dispositif terminal n'a pas besoin de mettre en œuvre la totalité des éléments CPCM, mais seulement ceux qui lui sont utiles pour réaliser la fonctionnalité dont il a besoin. Par exemple, un simple dispositif peut ne mettre en œuvre que les fonctionnalités d'acquisition et de consommation CPCM s'il n'a pas besoin d'effectuer de stockage ou d'exportation CPCM.

IV.5 Modèle de référence et entités fonctionnelles CPCM

Le modèle de référence CPCM définit l'ensemble des cinq fonctions abstraites de gestion de contenu couvrant tous les scénarios applicables d'utilisation de contenu dans l'environnement du consommateur: acquisition, stockage, traitement, consommation et exportation. Ces fonctions correspondent aux cinq entités fonctionnelles CPCM suivantes: point d'acquisition, entité de stockage, entité de traitement, point de consommation et point d'exportation. La Figure IV-1 représente le système CPCM avec l'ensemble des entités fonctionnelles abstraites.

Ainsi, pour pénétrer dans le système CPCM, le contenu d'entrée est acquis à un point d'acquisition par un dispositif CPCM mettant en œuvre ce point d'acquisition et devient un contenu CPCM. Ce contenu CPCM peut être stocké ou traité par les entités fonctionnelles correspondantes (entité de stockage, entité de traitement) mises en œuvre dans un dispositif CPCM. Le contenu CPCM quitte le système CPCM lorsqu'il est consommé à un point de consommation ou exporté à un point d'exportation. Ces entités fonctionnelles peuvent également être mises en œuvre à l'intérieur de n'importe quel dispositif CPCM.

IV.6 Domaine autorisé CPCM

Les dispositifs CPCM peuvent être regroupés de façon logique en domaines autorisés. Si tous ces dispositifs appartiennent à un même foyer, ils constituent le domaine autorisé de ce foyer. Le domaine autorisé constitue donc une destination pour le contenu qui correspond au cadre d'un seul foyer. D'une manière générale, le domaine autorisé peut être considéré comme le regroupement logique de tous les dispositifs CPCM appartenant à un même foyer: dispositifs situés dans le domicile principal, dispositifs situés dans un autre domicile (par exemple maison de vacances), dispositifs de poche portables qui ne sont connectés que de façon intermittente avec les dispositifs fixes susmentionnés, ou dispositifs équipant les véhicules qui appartiennent à ce foyer. Le domaine autorisé est conçu pour être un groupe logique autonome de dispositifs; il ne nécessite pas d'administration externe. Il est toutefois à noter que, dans certains cas, le domaine autorisé peut être lié à un fournisseur de service particulier qui peut proposer d'administrer le domaine autorisé dans le cadre de sa fourniture de service au consommateur.

IV.7 Règles d'utilisation du contenu CPCM

L'utilisation autorisée de n'importe quel élément de contenu CPCM est l'ensemble des assertions d'utilisation exprimées dans les règles d'utilisation CPCM liées au contenu. Les règles d'utilisation CPCM peuvent être fixées par le fournisseur de contenu ou de service ou déterminées à partir de la forme de fourniture (par exemple radiodiffusion en clair). La mesure dans laquelle les opérations de stockage, de consommation et d'exportation peuvent être réalisées peut dépendre de l'utilisation autorisée du contenu. Le système CPCM définit un ensemble commun de règles d'utilisation parmi lesquelles tout fournisseur de contenu peut faire son choix et déterminer en conséquence l'utilisation autorisée souhaitée pour le contenu à l'intérieur du système CPCM. L'ensemble des règles d'utilisation CPCM est conçu pour être suffisamment souple pour couvrir tous les modèles applicables de protection et de gestion du contenu et suffisamment concis pour que les modèles d'utilisation du contenu restent clairs et relativement simples pour le consommateur.

IV.8 Informations d'état d'utilisation

L'utilisation autorisée d'un élément de contenu est codée sous la forme de métadonnées relatives au contenu CPCM appelées informations d'état d'utilisation (USI). Le contenu CPCM est géré et

protégé conformément aux informations USI appliquées à chaque élément de contenu. Mises à part les transitions d'état USI conformes réalisées implicitement par le système CPCM, les entités bénéficiant d'une autorisation légitime sur le contenu à l'intérieur du système CPCM peuvent exécuter d'autres changements de l'état USI d'un élément de contenu après son acquisition dans le système CPCM.

IV.9 Contenu CPCM

Le "contenu" désigne généralement un contenu audiovisuel plus des données d'accompagnement facultatives comme des sous-titres, des images/graphiques, des animations, des pages web, du texte, des jeux, des logiciels (en code source ou en code objet), des scripts, ou toute autre information destinée à être fournie à un utilisateur et consommée par cet utilisateur. Le contenu CPCM est un contenu protégé et géré par le système CPCM et en conformité avec ce système. Un élément de contenu est une instance discrète de contenu de durée déterminée. Chaque élément de contenu CPCM est accompagné d'une licence de contenu acheminant les informations USI associées ainsi que d'autres métadonnées CPCM. Le système CPCM peut manipuler la licence de contenu et l'élément de contenu proprement dit de différentes manières suivant la fonctionnalité cible et/ou l'application des règles d'utilisation requise par les informations USI.

IV.10 Dispositif CPCM

Un dispositif CPCM est un dispositif qui met en œuvre n'importe quelle fonctionnalité CPCM de manière conforme. La mise en œuvre d'une fonctionnalité CPCM est appelée instance CPCM. Un dispositif CPCM est un dispositif qui héberge une ou plusieurs instances CPCM. Il peut aussi contenir d'autres fonctions non CPCM en plus de sa fonctionnalité CPCM. Le contenu CPCM n'est manipulé que par l'instance CPCM à l'intérieur du dispositif. La partie non CPCM du dispositif n'a pas accès au contenu CPCM. Le dispositif CPCM peut aussi héberger une fonctionnalité sécurisée non CPCM pour l'acquisition sécurisée de contenu auprès d'autres systèmes de protection ou l'exportation sécurisée (ou éventuellement la consommation) de contenu CPCM.

IV.11 Règle d'utilisation et informations d'état d'utilisation

Dans le système CPCM, une règle d'utilisation est une opération ou un comportement particulier concernant le contenu qui doit être contrôlé dans le cadre du système CPCM. L'ensemble complet d'assertions de règles d'utilisation pour un élément de contenu CPCM particulier est appelé utilisation autorisée de cet élément de contenu CPCM. L'utilisation autorisée d'un élément de contenu est exprimée par son codage dans les informations d'état d'utilisation (USI), à savoir les métadonnées relatives au contenu CPCM qui signalent l'utilisation autorisée pour ce contenu particulier.

Appendice V

Mécanisme transcodable sécurisé

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

V.1 Aperçu du mécanisme transcodable sécurisé

Une grande attention a été accordée au transcodage de contenu en raison de la popularité croissante de divers types de dispositifs comme les PDA, les dispositifs non PC, les téléphones cellulaires et les terminaux mobiles intelligents. Le transcodage désigne la transformation du format d'origine d'un contenu multimédia (par exemple images, texte, signaux audio et signaux vidéo) en un format différent ou en une qualité différente.

Le transcodage vise à réduire le temps de téléchargement d'un contenu multimédia sur les liaisons d'accès à faible largeur de bande (par exemple les liaisons par modem et les liaisons d'accès sans fil) et à résoudre les incompatibilités entre le format de codage pris en charge par un dispositif client et celui employé par un fournisseur de contenu multimédia. Il permet aussi aux terminaux qui ont des capacités de calcul limitées d'afficher le contenu codé sur la base de la capacité de transcodage.

Le mécanisme transcodable sécurisé fait intervenir trois entités: un émetteur, un nœud de réseau intermédiaire et un utilisateur avec un terminal de TVIP. La fonction de transcodage réside dans un nœud de réseau intermédiaire placé entre le fournisseur de contenu et le dispositif client. Il existe deux types d'architectures de transcodage: architecture de transcodage traditionnelle et architecture de transcodage sécurisée.

Dans l'architecture de transcodage traditionnelle, un proxy de transcodage est utilisé comme nœud de réseau intermédiaire entre le serveur de contenu et le dispositif client. L'émetteur chiffre le contenu avec une compression adéquate et envoie le contenu chiffré au nœud de réseau intermédiaire appelé proxy de transcodage. Le proxy de transcodage déchiffre le contenu chiffré et le décompresse. Puis il modifie la taille du contenu ou son format avec une nouvelle compression et, enfin, il rechiffre les données de transcodage pour transmission au dispositif client. Le dispositif client déchiffre le contenu chiffré et décompresse le contenu en utilisant un nouvel algorithme de compression. Il est toutefois à noter qu'un problème de sécurité se pose dans le proxy de transcodage: en effet, une fois que le contenu a été déchiffré dans le proxy de transcodage et avant qu'il ne soit rechiffré, le contenu non chiffré réside dans le proxy de transcodage. En d'autres termes, un observateur peut accéder au contenu non chiffré par écoute clandestine. Ce contenu non chiffré affaiblit la garantie de sécurité de bout en bout en termes de respect de la vie privée, dans laquelle seuls l'émetteur et le client légitime sont supposés accéder au contenu dans l'état non chiffré.

Pour résoudre le problème de la sécurité, une architecture de transcodage sécurisée a été proposée. Un mécanisme transcodable sécurisé est une sorte de mécanisme de sécurité qui permet au nœud de réseau intermédiaire d'effectuer le transcodage sans déchiffrement tout en préservant la sécurité de bout en bout. Pour exécuter ce mécanisme, on peut combiner un codage modulable, un chiffrement progressif et une mise en paquets. L'émetteur exécute une fonction transcodable sécurisée pour produire des paquets chiffrés modulables à partir d'une vidéo et ajoute un en-tête non chiffré pour envoyer des informations; le nœud de réseau intermédiaire lit l'en-tête non chiffré et utilise les informations pour tronquer ou éliminer les paquets appropriés en fonction de l'opération de transcodage souhaitée, tandis que le terminal de TVIP déchiffre les paquets chiffrés et décode les paquets de texte en clair pour produire la vidéo.

Bibliographie

- [b-UIT-T H.222.0] Recommandation UIT-T H.222.0 (2006) | ISO/CEI13818-1:2007, *Technologies de l'information – Codage générique des images animées et du son associé: Systèmes.*
- [b-UIT-T H.622.1] Recommandation UIT-T H.622.1 (2008), *Architecture et spécifications fonctionnelles pour la prise en charge des services de TVIP dans le réseau domestique.*
- [b-UIT-T M.1400] Recommandation UIT-T M.1400 (2006), *Désignations des interconnexions entre opérateurs de réseau.*
- [b-UIT-T Q.1290] Recommandation UIT-T Q.1290 (1998), *Glossaire utilisé dans la définition des réseaux intelligents.*
- [b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*
- [b-UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout.*
- [b-UIT-T Y.101] Recommandation UIT-T Y.101 (2000), *Infrastructure mondiale de l'information: termes et définitions.*
- [b-UIT-T Y.1901] Projet de Recommandation UIT-T Y.1901 (2009), *Prescriptions applicables à la prise en charge des services de TVIP.*
- [b-UIT-T Y.2012] Projet de Recommandation UIT-T Y.2012 (2006), *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1.*
- [b-ETSI TS 102 825] ETSI TS 102 825 (all parts), *Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM).*
<<http://pda.etsi.org/pda/AQuery.asp>>
- [b-ATIS 0800001] ATIS 08000001, *IPTV DRM Interoperability Requirements, ATIS-IIF*, avril 2007. <<https://www.atis.org/docstore/product.aspx?id=21212>>
- [b-ATIS 0800006] ATIS 0800006, *IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification*, février 2007.
<<https://www.atis.org/docstore/product.aspx?id=22663>>

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	Terminaux et méthodes d'évaluation subjectives et objectives
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