Union internationale des télécommunications

UIT-R

Secteur des Radiocommunications de l'UIT

Recommandation UIT-R BT.1852

(09/2009)

Systèmes à accès conditionnel pour la radiodiffusion numérique

Série BT

Service de radiodiffusion télévisuelle

ITU Union internationale des télécommunications

Avant-propos

Le rôle du Secteur des radiocommunications est d'assurer l'utilisation rationnelle, équitable, efficace et économique du spectre radioélectrique par tous les services de radiocommunication, y compris les services par satellite, et de procéder à des études pour toutes les gammes de fréquences, à partir desquelles les Recommandations seront élaborées et adoptées.

Les fonctions réglementaires et politiques du Secteur des radiocommunications sont remplies par les Conférences mondiales et régionales des radiocommunications et par les Assemblées des radiocommunications assistées par les Commissions d'études.

Politique en matière de droits de propriété intellectuelle (IPR)

La politique de l'UIT-R en matière de droits de propriété intellectuelle est décrite dans la «Politique commune de l'UIT-T, l'UIT-R, l'ISO et la CEI en matière de brevets», dont il est question dans l'Annexe 1 de la Résolution UIT-R 1. Les formulaires que les titulaires de brevets doivent utiliser pour soumettre les déclarations de brevet et d'octroi de licence sont accessibles à l'adresse http://www.itu.int/ITU-R/go/patents/fr, où l'on trouvera également les Lignes directrices pour la mise en œuvre de la politique commune en matière de brevets de l'UIT-T, l'UIT-R, l'ISO et la CEI et la base de données en matière de brevets de l'UIT-R.

Séries des Recommandations UIT-R

(Egalement disponible en ligne: http://www.itu.int/publ/R-REC/fr)

Séries	Titre
BO	Diffusion par satellite
BR	Enregistrement pour la production, l'archivage et la diffusion; films pour la télévision
BS	Service de radiodiffusion sonore
BT	**Service de radiodiffusion télévisuelle**
F	Service fixe
M	Services mobile, de radiorepérage et d'amateur y compris les services par satellite associés
P	Propagation des ondes radioélectriques
RA	Radio astronomie
RS	Systèmes de télédétection
S	Service fixe par satellite
SA	Applications spatiales et météorologie
SF	Partage des fréquences et coordination entre les systèmes du service fixe par satellite et du service fixe
SM	Gestion du spectre
SNG	Reportage d'actualités par satellite
TF	Emissions de fréquences étalon et de signaux horaires
V	Vocabulaire et sujets associés

***Note**: Cette Recommandation UIT-R a été approuvée en anglais aux termes de la procédure détaillée dans la Résolution UIT-R 1.*

Publication électronique
Genève, 2010

RECOMMANDATION UIT-R BT.1852

Systèmes à accès conditionnel pour la radiodiffusion numérique

(Question UIT-R 49/6)

(2009)

Domaine d'application

La présente Recommandation fixe des principes destinés à faciliter l'élaboration de méthodes d'accès conditionnel efficaces pour la radiodiffusion numérique utilisant des flux de transport MPEG-2; elle fournit des informations sur la protection des services de radiodiffusion contre tout accès non autorisé.

L'Assemblée des radiocommunications de l'UIT,

considérant

a) que dans de nombreux pays il existe une demande croissante de protection des programmes de radiodiffusion contre toute réception non autorisée;

b) qu'une façon efficace d'assurer la protection des paquets de flux de transport MPEG-2, multiplexés conformément aux dispositions de la Recommandation UIT-T H.222.0, est de mettre en œuvre des systèmes de radiodiffusion à accès conditionnel;

c) que des exemples de systèmes à accès conditionnel ont été conçus et sont exploités pour les services numériques de Terre, numériques par câble, numériques par satellite et la télévision IP (protocole Internet) ainsi que pour les services sonores, multimédias et de données;

d) qu'il existe de nombreux cas de mise en œuvre de systèmes de radiodiffusion numérique conformes aux dispositions pertinentes de Recommandations des séries BT et BO, telles que la Recommandation UIT-R BO.1516 pour les systèmes de radiodiffusion numérique par satellite;

e) qu'il est souhaitable de limiter le nombre des systèmes à accès conditionnel différents, tout en tenant compte des impératifs différents des divers services de radiodiffusion et des divers systèmes d'émission;

f) que l'installation d'un nombre aussi élevé que possible d'éléments communs d'accès conditionnel dans les récepteurs dès le début serait la meilleure solution pour permettre aux usagers d'accéder à des services protégés moyennant un coût d'équipement réduit;

g) que les systèmes à accès conditionnel assurent une protection et que les titulaires de droits d'auteur, les fournisseurs de programmes et les prestataires de services souhaitent disposer de réseaux de radiodiffusion/distribution hautement sécurisés pour permettre la protection de leurs programmes par le contrôle d'accès,

recommande

1 que les systèmes à accès conditionnel pour les services de radiodiffusion numérique protégeant les paquets de flux de transport MPEG-2 devraient:

– fournir les services disponibles uniquement aux récepteurs autorisés;

– partager le plus grand nombre d'éléments communs possibles dans le récepteur; et

– être conçus suivant les principes fondamentaux visés à l'Annexe 1.

NOTE 1 – Des exemples de mise en œuvre de systèmes à accès conditionnel pour la radiodiffusion numérique sont donnés à l'Appendice 1.

Annexe 1

Principes fondamentaux de conception de systèmes à accès conditionnel pour la radiodiffusion numérique

1 Introduction

Les principes énoncés ci-après devraient faciliter le développement de systèmes à accès conditionnel efficaces pour la radiodiffusion numérique, fondés sur des flux de transport conformes aux dispositions de la Recommandation UIT-T H.222.0 (flux de transport MPEG-2) qui conviennent tant aux abonnés qu'aux prestataires de services, assurant une protection fiable des informations contre tout accès non autorisé.

Les principes s'appliquent en général à la fourniture de services de télévision numérique, aux services sonores ainsi qu'aux services de radiodiffusion multimédia et de données. Ils s'appliquent à la fourniture de paquets de flux de transport conformes à la Recommandation UIT-T H.220.0 aux utilisateurs par différents supports, tels que les supports de Terre numérique, par câble numérique, par satellite numérique et la radiodiffusion IP (protocole Internet).

2 Références

2.1 Références normatives

La Recommandation UIT-T H.222.0: Technologies de l'information – Codage générique des images animées et du son associés: Systèmes.

2.2 Références informatives

Recommandation UIT-R BT.810: Systèmes de radiodiffusion à accès conditionnel

ARIB STD-B25: Spécifications des systèmes à accès conditionnel pour la radiodiffusion numérique

CEI 62455: Internet Protocol (IP) and transport stream (TS) based services access.

3 Termes, définitions et abréviations

3.1 Termes et définitions

Embrouillage en radiodiffusion numérique

Codage cryptographique du contenu de radiodiffusion, notamment visuel/sonore/de données, pour empêcher la réception non autorisée des informations dans un format non crypté. Ce codage cryptographique est un processus spécifié géré par le système à accès conditionnel (extrémité émettrice).

Désembrouillage en radiodiffusion numérique

Décodage cryptographique du contenu de radiodiffusion, notamment visuel/sonore/de données, pour permettre la réception des informations dans un format non crypté. Ce décodage cryptographique est un processus spécifié géré par le système à accès conditionnel (extrémité réceptrice).

Accès conditionnel

Un utilisateur accède à un service protégé en interagissant via la fonctionnalité à accès conditionnel du récepteur. Si, pendant l'opération, toutes les conditions d'accès sont réunies, l'autorisation est donnée, la clé de décodage cryptographique est libérée et le contenu est récupéré.

L'authentification de l'abonné, la confirmation de son compte et la validation d'un paramètre de disponibilité du service ou bien d'autres paramètres de gestion du programme activent la clé de chiffrement/déchiffrement de la session pour permettre à cette dernière de conclure le processus d'autorisation.

Contrôle d'accès conditionnel

La fonction de contrôle d'accès conditionnel à l'extrémité émettrice consiste à générer l'information de contrôle d'embrouillage et les clés "de chiffrement" associées au service.

La fonction de contrôle d'accès conditionnel à l'extrémité réceptrice consiste à produire l'information de contrôle de désembrouillage parallèlement aux "clés" associées au service.

Chiffrement et déchiffrement

Ces termes désignent les méthodes qui servent à protéger (et interpréter) certaines des informations à l'intérieur des "messages concernant l'accès" qui doivent être transmis entre l'extrémité émettrice et l'extrémité réceptrice des fonctions de contrôle d'accès conditionnel.

Point d'origine

Il s'agit du point dans un système de distribution où le programme, ou tout autre contenu, devient pour la première fois un signal dans son format final de radiodiffusion/distribution; il marque le début de la protection de bout en bout. Le contenu d'entrée peut avoir n'importe quelle forme, et non pas nécessairement une forme humainement perceptible. Les données d'entrée du contenu n'ont pas besoin en soi d'être intelligibles.

NOTE 1 – Les titulaires de droits d'auteur, prestataires de services et distributeurs forment une importante hiérarchie de nombreux points d'origine possibles dans un flux d'informations destiné à un usager et donc dans le flux du contenu embrouillé et des clés cryptées qui lui sont destinés. Le point d'origine devrait commencer avec un titulaire de droits d'auteur ou un producteur. Dans la pratique, la plupart des points d'origine seront simplement les points d'entrée, où qu'ils soient dans le système pour des raisons commerciales et opérationnelles. Bien qu'ils puissent être nombreux, chaque point d'entrée est un point unique et indépendant à partir duquel l'information peut être constamment maintenue indépendamment du format dans lequel elle peut être acheminée jusqu'à la destination finale d'un usager.

Point de présentation

Il s'agit du point où un programme, ou tout autre contenu, se produit pour la dernière fois sous forme d'un signal dans un système de distribution avant d'exister sous une forme humainement perceptible au niveau de l'écran et des haut-parleurs du récepteur; il marque le produit final de la protection.

Contenu

Il s'agit d'une forme quelconque de données numériques susceptibles d'être acquises et présentées par un dispositif.

Service

Il s'agit d'un ou de plusieurs flux de données destinées à être présentées ensemble.

Protection du service

Il s'agit de la protection d'un service permettant aux seuls dispositifs autorisés de pouvoir le recevoir et le décoder.

3.2 Abréviations

Ks Clé d'embrouillage (*scrambling key*)

Kw Clé de travail (*work key*)

Km Clé principale (*master key*)

EMM Message de gestion d'habilitation (*entitlement management message*)

ECM Message de commande d'habilitation (*entitlement control message*)

CRC Contrôle de redondance cyclique (*cyclic redundancy check*)

DES Norme de chiffrement de données (*data encryption standard*)

4 Description générale d'un système à accès conditionnel

Il y a deux fonctions fondamentales que comprennent les systèmes à accès conditionnel pour la radiodiffusion numérique, à savoir l'embrouillage et le contrôle d'accès. Dans un système à accès conditionnel, il existe des éléments distincts, et souvent indépendants, dont chacun constitue un processus d'information séparé.

4.1 Modèle de référence

L'accès conditionnel exige que l'information soit embrouillée avant d'être diffusée; pour ce faire on emploie un codage cryptographique pour diffuser des flux binaires.

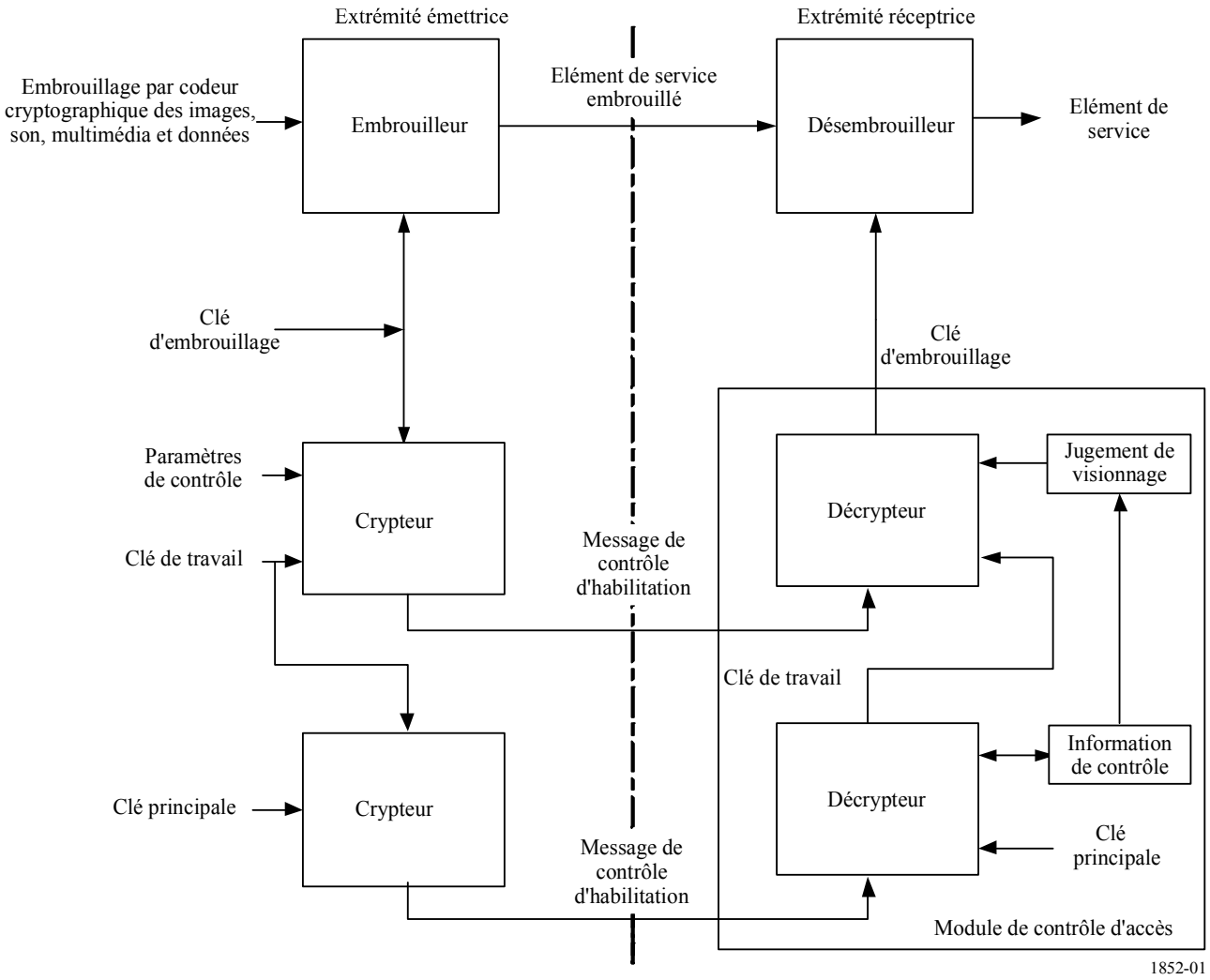
Le processus de désembrouillage à l'extrémité réceptrice exige l'utilisation du même décodage cryptographique (dans le cas présent, il s'agit de la procédure de désembrouillage) pour récupérer le flux binaire originel.

Pour obtenir cette séquence et garantir la synchronisation entre les processus d'émission et de réception, les conditions de décodage cryptographique sont contrôlées par une donnée émise depuis le codeur cryptographique à destination du décodeur suivant un protocole particulier.

La structure détaillée de ce processus est illustrée à la Fig. 1.

FIGURE 1

Exemple de schéma fonctionnel d'un système à accès conditionnel pour la radiodiffusion numérique



4.2 Embrouillage

L'embrouillage est le processus de protection d'une partie ou de la totalité des éléments d'un service pour résoudre le problème des accès non autorisés en utilisant un codage cryptographique géré par le système d'accès conditionnel à l'extrémité émettrice.

4.3 Contrôle d'accès

Consiste en la fourniture d'informations pour permettre aux utilisateurs autorisés de désembrouiller le service protégé. La disponibilité de ces informations est gérée par le système à accès conditionnel.

Entre l'émetteur et le ou les récepteurs, ces informations sont structurées dans des messages spéciaux, qui peuvent soit être multiplexés au sein du flux binaire de radiodiffusion soi-même, soit être acheminés par d'autres moyens, par exemple via une ligne de télécommunication.

A l'extrémité ou aux extrémités réceptrices, ces messages sont interprétés par le système à contrôle d'accès dans le but de piloter le désembrouillage des parties autorisées dans le flux binaire reçu au niveau du ou des récepteurs autorisés.

5 Spécifications utilisateur

5.1 Pouvoir anti-intrusion d'un chiffrement pour un embrouilleur et un désembrouilleur

Un chiffrement utilisé dans des blocs d'embrouilleurs et de désembrouilleurs devrait être bien éprouvé pour une utilisation anti-intrusion. Il est recommandé d'utiliser un chiffrement sélectionné parmi les normes internationales.

5.2 Sûreté

La sûreté d'un système se mesure par le degré de difficulté rencontrée par un utilisateur non autorisé quand il cherche à accéder à un service protégé.

– *Désembrouiller le signal sans référence au processus de contrôle d'accès*. Est fonction de la nature des services et de la méthode d'embrouillage. La télévision future, les services de radiodiffusion sonore et de transmission de données sont appelés à être pour la plupart numériques par nature et permettront donc des procédures d'embrouillage hautement sécurisées.

– *Obtention de la clé de contrôle d'accès de manière non autorisée*. Est fonction de la sûreté des algorithmes de chiffrement par clé.

5.3 Sélection d'un algorithme d'embrouillage commun ou privé

L'accès est accordé, à tout utilisateur autorisé remplissant les conditions d'accès, via un algorithme d'embrouillage commun (universel) ou privé.

L'utilisation d'un algorithme d'embrouillage commun suppose que le désembrouillage soit commun à tous les récepteurs, basés sur un algorithme d'embrouillage normalisé, indépendamment des supports d'émission utilisés; cet algorithme permet une réduction des coûts et une plus grande flexibilité de l'équipement tout en préservant le jeu de la concurrence par la mise en œuvre de solutions spécifiques aux prestataires de services.

L'utilisation d'un algorithme d'embrouillage privé suppose que la procédure de désembrouillage soit mise en œuvre sur les récepteurs uniquement mettant en œuvre un algorithme spécifique.

5.4 Modes d'accès

Un système à accès conditionnel peut permettre le recours à plusieurs modes d'accès, par exemple:

– disponibilité d'une période (souscription du service) – l'autorisation courant d'un temps début jusqu'à un temps fin;

– élément de programme ou de service (achat d'un événement) – la disponibilité correspondant à un élément de service spécifique, qui soit ou non complètement utilisé;

– taxe de service (basée sur l'utilisation de jetons) – la taxe ou l'utilisation d'un crédit étant proportionnelle à la durée d'utilisation et/ou à la valeur du service en question;

– gratuité d'émission – le service étant protégé, mais l'accès étant fourni à titre gracieux.

Les modes d'accès doivent être variables par rapport à plusieurs paramètres, par exemple:

– la durée;

– divers segments du service;

– les groupes d'utilisateurs visés.

5.5 Normalisation de l'équipement

Pour favoriser au maximum les économies d'échelle au niveau de la fabrication des équipements de réception et pour simplifier les opérations de gestion et de maintenance:

– il faudrait normaliser des équipements communs, pour qu'ils puissent prendre en charge autant d'options de service que possible;

– il faut disposer d'une architecture récepteur grand public pour prendre en charge les spécifications de fonctionnalité d'accès conditionnel du système à accès conditionnel retenu; selon le système qui sera choisi, la fonctionnalité peut en effet être appelée à prendre en charge une fonctionnalité de sûreté soit intégrée, soit amovible (par exemple, carte intelligente).

5.6 Gestion de l'accès

La définition de l'accès conditionnel est basée sur la notion formelle d'*habilitation*, ce qui peut prendre plusieurs formes. Une habilitation donne à son titulaire l'*autorisation* d'accéder au service correspondant. Il conviendrait d'éviter d'utiliser de manière non économique les ressources du fait des frais généraux de gestion ou de transmission.

5.7 Eviter les interruptions du service

Il conviendrait d'éviter que le service soit interrompu à cause d'une acquisition erronée ou peu fiable des données de contrôle d'accès.

6 Messages de contrôle d'habilitation (ECM)

Un message ECM fournit la clé d'embrouillage nécessaire pour désembrouiller le service protégé.

L'accès par la clé d'embrouillage d'un message ECM est géré par des habilitations, ou droits, fournis dans un message EMM.

En général, un message ECM est transmis dans le flux de radiodiffusion, en même temps que le service protégé.

Les clés d'embrouillage sont en règle générale changées fréquemment pour réduire au minimum les dommages pouvant découler de fuites concernant les clés d'embrouillage.

Le contenu d'un message ECM est spécifique au système.

7 Messages de gestion d'habilitation (EMM)

Le traitement d'un message de gestion d'habilitation valide ou fournit l'habilitation nécessaire pour désembrouiller le service protégé. Un message EMM peut contenir une clé de travail pour assurer le chiffrement ou le déchiffrement de la clé d'embrouillage. Les messages et/ou clés de travail adressés à des récepteurs individuels sont chiffrés. Le chiffrement peut utiliser la clé principale, laquelle peut être stockée dans le dispositif de réception.

Dans les systèmes à accès conditionnel destinés à la radiodiffusion numérique, les messages de gestion d'habilitation (EMM) sont acheminés par l'équipement de radiodiffusion ou d'autres supports.

– L'acheminement par les services de radiodiffusion est connu en anglais sous l'appellation "over-the-air addressing", adressage par voie hertzienne. La durée du cycle associée à l'acheminement des clés par voie hertzienne peut être réduite par l'application des principes

de chiffrement partagé des clés. Les messages de gestion d'habilitation peuvent être distribués également par d'autres supports.

– L'acheminement par d'autres supports se réalise en général via une connexion point à point, fournissant ainsi une mesure de sûreté additionnelle garantissant que seuls les dispositifs visés puissent avoir accès aux messages.

Voici un exemple de fonctionnement:

Dans le cas d'un paiement, par unité de temps ou par programme, les messages de gestion peuvent contenir un code du coût chiffré, transmis dans le cadre du service. Le crédit peut être positionné dans le récepteur et peut prendre la forme de jetons d'argent chiffrés qui sont transmis dans le cadre du service d'adressage par voie hertzienne. Autrement, le crédit peut prendre la forme de jetons d'argent stockés qui sont distribués par d'autres moyens. Le paiement consiste à réduire proportionnellement le crédit stocké en fonction du code du coût reçu.

Le contenu d'un message EMM est spécifique au système.

8 Fonctionnalité de contrôle d'accès du récepteur

A l'extrémité réceptrice, l'accès conditionnel peut prendre plusieurs formes, dont les suivantes:

Type 1: La fonctionnalité de sûreté (qui peut comporter un algorithme de chiffrement par clé et des clés principales) et la fonctionnalité de désembrouillage sont mises en œuvre dans le récepteur.

Type 2: La fonctionnalité de sûreté est amovible (par exemple, carte intelligente) alors que la fonctionnalité de désembrouillage est mise en œuvre dans le récepteur.

Type 3: Les fonctionnalités de sûreté et de désembrouillage sont amovibles; toutes les fonctions assurant le rétablissement du flux de données d'entrée sont mises en œuvre dans un module amovible, communiquant avec le récepteur via une interface normalisée (par exemple, une interface commune); dans ce cas, on peut utiliser n'importe quel récepteur pourvu d'une interface de ce type.

Lorsqu'il le lui est demandé, la fonctionnalité de sûreté vérifie l'état des conditions et, si ces dernières sont satisfaites, elle fournit la clé d'embrouillage au descripteur. Ces conditions peuvent comprendre notamment:

– un délai à observer, la date du paramètre de contrôle tombant entre la date de début et la date d'expiration du paramètre d'autorisation;

– un niveau de prix auquel une autorisation peut être fournie uniquement si une taxe est acceptée par le module de sûreté.

Un système à accès conditionnel peut procéder à une transaction mettant à contribution la fonctionnalité de sûreté qui comprend différentes étapes, par exemple:

– des instructions préliminaires, le cas échéant (par exemple, mot de passe, acceptation de l'utilisateur, etc.);

– des instructions de fonctionnement utilisant le module de sûreté;

– le traitement du résultat (par exemple fourniture d'un mot d'embrouillage).

Appendice I
à l'Annexe 1

TABLEAU 1

Exemples de la mise en œuvre d'un système à accès conditionnel pour la radiodiffusion numérique

Référence dans l'Annexe 1	Système «Roscrypt»	Système «CAS-R»	«CEI 62455 avec systèmes DVB»
§ 4 Type de chiffrement pour embrouilleur et désembrouilleur	Basé sur la norme 28147-89 de la Fédération de Russie	MULTI2 (ISO/CEI 9979)	DVB-CSA ou AES-128 (obligatoire pour les dispositifs); sont aussi possibles les DES, 3DES et MULTI2 (facultatif pour les dispositifs).
§ 4 Processus d'embrouillage	Transition multi-étape cyclique basée sur des enregistreurs à décalage utilisant des polynômes du 64ème ordre. Basé sur des algorithmes non linéaires et est pratiquement une séquence aléatoire (n'a pas de forme analytique).	a) Pour des séquences codées à 64 bits, le codage originel est remplacé par une autre chaîne de codage binaire utilisant des variables à 64 et 256 bits. b) Pour des chaînes de caractères codés de moins de 64 bits, la méthode décrite au a) ci-dessus est utilisée pour générer une série de séquences codées pseudo-aléatoire, qui sont combinées pour créer le signal embrouillé.	DVB-CSA: Suivant la norme ETR-289 de l'ETSI; AES-128: suivant la norme FIPS PUB 197:2001 utilisant un mode ECB ou CBC; DES ou 3DES: selon les normes FIPS PUB 46-3:1999 et FIPS PUB 81:1980; MULTI2 suivant la norme ISO/CEI 9979.
§ 4 Synchronisation du processus d'embrouillage	Synchronisation mutuelle de séquences aléatoires et de circuits de formage de flux DVB.	Utilisation pour synchroniser le processus d'embrouillage d'informations pertinentes dans des messages ECM (pour le programme et le contrôle), des messages EMM (informations individuelles), des messages communs EMM et des messages individuels EMM.	Odd_even_flag et initial_vector sont inclus dans le message de flux de clés fournissant la Clé de chiffrement traffic pour faciliter la synchronisation. Les valeurs correspondantes des bits transport_scrambling_control et pes_scrambling_control déterminent la clé qui doit être utilisée à un moment donné.

TABLEAU 1 (*suite*)

Référence dans l'Annexe 1	Système «Roscrypt»	Système «CAS-R»	«CEI 62455 avec systèmes DVB»
§ 6 Messages de contrôle d'habilitation (ECM)	Contenu ECM: – Identificateur de la clé de travail – Clé d'embrouillage (impaire/paire) – Compteur chiffré et total de contrôle cryptographique Sont utilisées la redondance structurelle de flux DVD ou des réserves attribuées en plus.	Section ECM et son architecture de base de la charge utile ECM: – Toute la section ECM est assujettie à un CRC de section. – La charge utile ECM comprend une partie fixe, qui est toujours transmise, et une partie variable dont le contenu varie suivant l'objectif de l'émission. – Seuls les renseignements nécessaires concernant la fonction ECM sont insérés dans la partie variable du message ECM.	L'ECM achemine un message de flux de clés, qui comprend des champs pour transporter les informations suivantes: – content_key_index – odd_even_flag – cipher mode – next_initial_vector – encrypted_traffic_key_material – traffic_key_lifetime – timestamp – access_criteria_descriptors – permissions_category – encrypted_programme encryption key – programme_CID_extension – programme_MAC – service_CID_extension – service_MAC La question de savoir lesquels de ces champs sont inclus dans un message de flux de clés particulier dépend de plusieurs facteurs, par exemple de la décision du prestataire de services de permettre l'accès sur la base de programmes individuels.
Clé principale	256 bits	256 bits	Il n'y a pas de «clé principale» en tant que telle. La protection des clés de chiffrement de service (SEK) ou des clés de chiffrement de programme (PEK) est basée sur des clés RSA, qui comptent 1 024, 2 048 ou 4 096 bits, selon l'autorité de tutelle. En mode radiodiffusion, la clé de chiffrement déduite (IEK) à 128 bits joue un rôle analogue; elle est obtenue à partir d'un jeu de clés qui sont transmises au récepteur pendant l'enregistrement. La protection du jeu de clés est basée sur des clés RSA à 1 024, 2 048 ou 4 096 bits.

TABLEAU 1 (*suite*)

Référence dans l'Annexe 1	Système «Roscrypt»	Système «CAS-R»	«CEI 62455 avec systèmes DVB»
§ 6 Changement de clé et de drapeau d'embrouillage	La clé d'embrouillage est changée selon les besoins. On utilise les quatre états du drapeau d'embrouillage	Les clés d'embrouillage (impaire/paire) sont changées normalement toutes les deux secondes.	La clé de chiffrement de trafic change fréquemment, de l'ordre d'une fois par minute à une fois par seconde.
§ 7 Message de gestion d'habilitation (EMM)	Contenu EMM: – Numéro du protocole – Identificateur du groupe radiodiffuseur – Clé de travail – Identificateur de programme – Identificateur du module de sûreté – Droits d'accès – Compteur chiffré et total de contrôle cryptographique – On utilise la redondance structurelle du flux DVB ou des réserves attribuées en plus.	La section EMM peut comporter plusieurs charges utiles. La section EMM dans sa totalité est assujettie à la détection d'erreurs CRC. La charge utile EMM comprend une partie fixe, qui est toujours transmise, et une partie variable dont le contenu varie en fonction de l'objectif d'émission. Seules les informations fonctionnelles EMM nécessaires sont insérées dans la partie variable du message EMM. L'ID de la carte (6 octets) et la longueur en octets des informations associées (1 octet) sont expédiées au début de la partie fixe du message EMM (partie non cryptée). Le récepteur filtre cette zone pour déterminer les charges utiles EMM qui lui sont adressées.	En mode interactif, des Objets Droits OMA DRM 2.0 sont utilisés en lieu et place de messages de gestion d'habilitation pour transmettre aux récepteurs les droits et clés de chiffrement de service (SEK) ou clés de chiffrement de programme (PEK); la transmission se fait sur un canal d'interactivité. En mode radiodiffusion, c'est une version binaire spéciale (appelée BCRO) de ces Objets Droits qui est utilisée.
§ 8 Fonctionnalité de contrôle d'accès	Se trouve à l'intérieur du module d'accès conditionnel (CAM) ou est intégrée au STB	Type 2: Le module de sûreté est amovible et le module de désembrouillage est intégré au récepteur.	C'est le type 1 qui est envisagé, mais d'autres mises en œuvre ne sont pas exclues, non plus.

TABLEAU 1 (*fin*)

Référence dans l'Annexe 1	Système «Roscrypt»	Système «CAS-R»	«CEI 62455 avec systèmes DVB»
Compteur chiffré et total de contrôle cryptographique	ECM, EMM	Un code d'authentification de message (MAC) est inclus dans les paquets tant ECM que EMM.	Un code d'authentification de message (MAC) est inclus dans les messages de flux de clés et dans les Objets Droits en mode de radiodiffusion. Les Objets Droits en mode interactif sont protégés par une signature.
§ 8 Fonctionnalité de sûreté	Se trouve à l'intérieur du module d'accès conditionnel (CAM) ou est intégrée au STB	Authentifié mutuellement entre la carte intelligente et le récepteur.	La mise en œuvre n'est pas dictée par la norme. L'autorité de tutelle fixe des règles de conformité et de robustesse.

1 Description d'un système «Roscrypt»

Un système à accès conditionnel (CAS) «Roscrypt» est actuellement mis en service en Fédération de Russie dans le cadre du passage à la télédiffusion numérique. Ce système «Roscrypt» est conçu pour protéger les flux de données DVB contre toute réception non autorisée; il offre toute une gamme d'utilisations avec les différentes chaînes DVB de radiodiffusion soit par satellite, soit de Terre, et offre une grande flexibilité pour la gestion des abonnés.

Un système «Roscrypt» se compose de:

- l'*embrouilleur*, qui procède à un chiffrement des éléments du flux de transport DVB présélectionnés; il peut fonctionner en mode autonome ou être géré par PC;
- un *module CAM*, inséré dans l'intervalle de l'interface commune (CI) du récepteur pour désembrouiller les éléments sélectionnés;
- un *module de sûreté*, qui intègre un boîtier convertisseur décodeur.

L'équipement nécessaire au fonctionnement du système de commande et de contrôle commun est installé du côté de l'extrémité émettrice.

Un système «Roscrypt» résout les problèmes suivants:

- limitation de la radiodiffusion à l'intérieur de la zone du pays pour protéger les droits des auteurs des programmes à une radiodiffusion limitée;
- protection d'une radiodiffusion collective et départementale contre tout accès non autorisé;
- organisation d'une radiodiffusion commerciale.

Ce système tient compte des caractéristiques des chaînes protégées contre tout accès non autorisé.

1.1 Caractéristiques fonctionnelles et techniques du système «Roscrypt»:

- Le modèle de fonctionnement commun du système «Roscrypt» CAS correspond à la Fig. 1 de l'Annexe 1.
- *Algorithme d'embrouillage*: il existe deux algorithmes d'embrouillage privés, qui ont été réalisés pour l'embrouillage et le désembrouillage du système «Roscrypt» CAS. L'opérateur peut changer d'algorithme à n'importe quel moment.
- *Clés de sûreté*: Les clés suivantes sont utilisées dans le système «Roscrypt» CAS:
  - La clé d'embrouillage et la clé de travail permettent l'embrouillage/le désembrouillage du contenu.
  - La base de clés générales originelles permet le déchiffrage (clés de travail) des messages ECM et le contrôle d'accès au niveau de l'abonné.
  - Le groupe des clés de programme permet de séparer les abonnés des différents opérateurs les uns des autres et de répartir tous les abonnés selon divers critères.
  - Les opérateurs peuvent procéder à un changement rapide de clé sans distribution physique ni électronique.
- *Mode d'accès*: il existe deux modes d'accès pour gérer efficacement les abonnés soit par disponibilité périodique, soit par éléments de programme ou de service.
  - Paramètres du mode d'accès: le temps de gestion des abonnés est de 1 000 abonnés par seconde; le nombre d'abonnés n'est pas limité; le nombre d'éléments d'embrouillage est de 150; groupes d'utilisateurs visés – 64 000.

– *EMM et ECM*: la structure des signaux EMM et ECM correspond aux dispositions des § 6 et 7 de l'Annexe 1.
  – Il y a un compteur chiffré et un total de contrôle cryptographique à la fin de chaque paquet EMM et ECM.
  – Pour les commandes de gestion (EMM et ECM), il est possible d'utiliser la fourniture soit de ressources additionnelles de largeur de bande de flux DVB, soit de réserves de vitesse structurelles (redondance structurelle) de flux de transport DVB.
– *L'équipement de réception*: à l'extrémité réceptrice, il est possible d'avoir deux types de système à accès conditionnel «Roscrypt», à savoir:
  – Un module de sûreté, qui comprend un algorithme de chiffrement par clé des clés de sûreté et un module de désembrouillage, est intégré dans le boîtier convertisseur décodeur.
  – Un module à accès conditionnel (CAM) qui comprend des modules de sûreté et de désembrouillage, communiquant avec le récepteur via une interface commune normalisée (CI), est amovible. Ce module CAM à lui seul peut restaurer les éléments embrouillés du flux de transport d'entrée simultanément.

1.2 Divers:

– Un seul ensemble d'équipements émetteur «Roscrypt» peut chiffrer le contenu de plusieurs fournisseurs indépendants. Cette propriété est utilisée pour de grands opérateurs de radiodiffusion par satellite ou de Terre.
– Le système de commande et de contrôle commun permet de gérer l'accès des abonnés au contenu.
– Le système de commande et de contrôle commun permet une opération centralisée à distance et le contrôle de l'ensemble des équipements d'émission «Roscrypt» sur tout le réseau. Cette propriété est utilisée pour de grands opérateurs de radiodiffusion par satellite ou de Terre.

2 Description d'un système «CAS-R»

2.1 Objet du système

La norme STD-B25 ARIB concerne un système de contrôle à accès conditionnel destiné à être utilisé en radiodiffusion numérique, fixant les spécifications d'embrouillage et d'information associées ainsi que les spécifications de réception correspondant à un système qui assure une gestion pendant la réception du signal (appelé ci-après «CAS-R»).

Cette norme spécifie les systèmes CAS pour les systèmes de radiodiffusion numérique de Terre ou par satellite actuellement utilisés au Japon.

2.2 Spécification du système CAS-R et de ses systèmes délibératifs

La norme STD-B25 ARIB stipule que les systèmes CAS devront satisfaire aux impératifs suivants:

1 Nombre maximum d'abonnés:

Le système peut être étendu pour assurer des fonctions de gestion des usagers pour tous les ménages se trouvant dans la zone de couverture.

2 Durée de vie du système:

Le système peut être géré par la prise en charge de supports de radiodiffusion applicables.

3 Antipiraterie:

Le système est pourvu d'une fonctionnalité de sûreté évoluée et peut prendre des mesures en cas d'attaque.

4 Les systèmes sont applicables à tous les systèmes de radiodiffusion numérique dans une zone spécifique.

5 Types de réception:

a) Réception en temps réel, en particulier émission en continu A/V et radiodiffusion de données utilisant un format de fichier (CAS-R).

b) Réception avec mise en mémoire (la réception n'est pas en temps réel).

c) Réception enregistrée (y compris réception réservée).

6 Au système on peut appliquer les structures de règlement financier suivantes: forfait simple/forfait par palier, paiement à la séance «pay per view» (impulsion PPV (IPPV)) et gratuité.

2.3 Spécifications pour le module de sûreté

1 Chiffrement des informations associées:

Le système de chiffrement utilise une architecture à trois couches avec des clés équivalentes DES et privées. Pour une mise en œuvre sur une carte intelligente, il devrait avoir la taille d'un programme compact et permettre le traitement à grande vitesse au moyen d'un microcontrôleur d'au moins 8 bits.

2 Fonctionnalité administrative:

Pour faire face aux attaques de pirates, le système peut changer de protocole de chiffrement.

3 Une procédure d'authentification mutuelle devrait être mise en œuvre entre la carte intelligente et le récepteur:

Lors de l'utilisation de la carte intelligente CAS pour éliminer les récepteurs ne satisfaisant pas aux droits de protection de l'information dans des applications utilisant ce système à accès conditionnel au titre d'une technologie de protection de droits pour la radiodiffusion numérique, le système doit permettre une authentification mutuelle entre cette carte intelligente et le récepteur.

2.4 Une description détaillée du système est donnée dans le document suivant

Les spécifications du système à accès conditionnel ARIB STD B-25 peuvent être consultées à: http://www.arib.co.jp/english/html/overview/doc/6-STD-B25v5_0-E1.pdf.

3 Description de la norme «CEI 62455 pour systèmes DVB»

La norme CEI 62455 spécifie un système normalisé pour contrôler l'accès aux services de radiodiffusion basé sur un flux de transport MPEG2. Elle spécifie également l'utilisation qui peut être faite de ce même système pour contrôler l'accès aux services de radiodiffusion basé sur le protocole Internet (IP). C'est dire que ces spécifications sont largement applicables à différents systèmes de radiodiffusion, notamment des systèmes pour lesquels la protection ne peut pas être assurée sur des paquets de flux de transport MPEG2 (par exemple, services basés IP assurés sur des réseaux utilisant un protocole autre que le MPEG2).

En ce qui concerne les systèmes de radiodiffusion à accès conditionnel, la norme CEI 62455 spécifie une interface complète entre l'extrémité émettrice et l'extrémité réceptrice. Grâce à cette interface totalement spécifiée, le fabricant du serveur et le fabricant du récepteur peuvent indépendamment mettre en œuvre le support nécessaire au système de protection, sans être obligés de s'en remettre à un seul organisme de sûreté pour en faciliter la mise en œuvre et sur le serveur et sur le récepteur. Cette intégration dans le système permet de ne pas être lié à un seul organisme de sûreté et, donc, de pouvoir changer de fabricant de telle ou telle composante du système à accès conditionnel sans avoir à changer les autres éléments ou leurs fabricants.

La norme CEI 62455 couvre toutes les couches du système suivantes, mais fait référence à des spécifications existantes dans toute la mesure du possible:

– Couche enregistrement
– Couche gestion des droits
– Couche flux des clés
– Couche trafic.

La couche gestion des droits se fonde sur une norme de gestion des droits numérique bien établie et commercialement bien implantée de Open Mobile Alliance, OMA DRM 2.0; cette couche est responsable de l'attribution des droits et gère les contraintes correspondantes imposées aux récepteurs, ainsi que les clés sur le long terme, c'est-à-dire la clé de chiffrement du service (SEK) ou la clé de chiffrement de programme (PEK), selon que l'accès est accordé au titre d'un abonnement ou par programme.

Dans le mode interactif, c'est-à-dire lorsqu'un canal de communication bidirectionnel existe entre le récepteur et le prestataire de services, c'est aussi cette norme OMA DRM 2.0 qui est utilisée. Pour un fonctionnement en radiodiffusion unidirectionnel en l'absence de canal d'interaction, le système a été renforcé par des versions binaires d'économie de largeur de bande des Objets Droits OMA DRM 2.0 (appelés Objets Droits binaires codés, ou BCRO suivant son abréviation en anglais), et doté d'une méthode pour protéger ces Objets BCRO lors d'une émission sur le canal de radiodiffusion. Avec ces Objets BCRO, divers modes d'adressage sont utilisés, qui réduisent encore plus la largeur de bande nécessaire à la distribution des Objets Droits. La méthode de protection est fondée sur un chiffrement de la radiodiffusion du message 0, empêchant qu'une violation des règles de sûreté au niveau d'un seul récepteur permette d'obtenir l'accès à des clés ou à des droits attribués à d'autres récepteurs; l'utilisation de la largeur de bande de radiodiffusion est très optimisée.

Le jeu de clés requis pour un fonctionnement en mode radiodiffusion est fourni au récepteur pendant l'opération d'enregistrement qui doit être réalisée pour que le service puisse être transmis sur le canal de radiodiffusion. A cette fin, l'utilisateur doit uniquement communiquer le numéro de dispositif originel, «unique device number» (UDN), du récepteur à son prestataire du service, qui vérifiera alors le certificat du récepteur dans une base de données adaptée; ce certificat contient la clé publique du récepteur, qui est utilisée pour protéger le jeu de clés pendant l'opération de transfert.

Pour protéger un flux de transport MPEG2, le chiffrement (embrouillage) du contenu du service se fait au moyen de chiffres courants tels que le DVB-CSA ou l'AES-128 conformément à la norme CEI 62455. Cette dernière autorise l'utilisation par ailleurs d'autres normes de chiffrement, telles qu'IPsec, SRTP et ISAMcryp, pour faciliter la protection des paquets de flux de transport autres que MPEG2.

Pour faciliter le changement fréquent des clés de chiffrement trafic (TEK) utilisées pour protéger le contenu du service, la norme CEI 62455 spécifie une couche de flux de clés qui intervient entre la couche gestion des droits et la couche trafic. Le système permet d'accorder l'accès au même flux via les Objets Droits du service ou du programme. Si le prestataire de service souhaite autoriser un

accès programme par programme, dans le cas où les programmes sont également souscrits par abonnement, le message de flux de clés comportera une clé PEK chiffrée avec la clé SEK, en plus d'une clé TEK chiffrée par une clé PEK. La couche de flux de clés peut véhiculer également d'autres informations, telles que des critères d'accès ou une valeur permissions_category, ou peut être utilisée pour choisir entre différents droits dans l'Objet Droits de service, se rapportant au fragment particulier du flux auquel s'applique le message de flux de clés, ce qui permet d'avoir différents droits pour différents programmes, même si l'accès est basé sur un abonnement à un service comprenant plusieurs programmes consécutifs.