RECOMMANDATION UIT-R BT.810*

Systèmes de radiodiffusion à accès conditionnel

(1992)

L'Assemblée des radiocommunications de la UIT,

considérant

a) que, dans plusieurs pays, on cherche de plus en plus à protéger les programmes de radiodiffusion contre une réception non autorisée;

b) qu'un moyen efficace de garantir cette protection consiste à mettre en œuvre des systèmes de radiodiffusion à accès conditionnel;

c) qu'on a conçu et qu'on exploite des exemples de systèmes de radiodiffusion à accès conditionnel pour la télévision de Terre, par câble et par satellite, ainsi que pour les services de télétexte et de données;

d) qu'il est souhaitable de limiter le nombre de systèmes à accès conditionnel différents, tout en tenant compte des exigences propres aux divers services de radiodiffusion et systèmes de transmission;

e) que, si les organes d'accès conditionnel dans les récepteurs disposent d'un maximum d'éléments en commun, cela permettra au public de profiter de ces services à accès protégé à un prix réduit;

f) que les titulaires de droits d'auteur, les fournisseurs de programmes et de services désirent que les réseaux de radiodiffusion et de distribution jouissent d'une protection sûre grâce au contrôle d'accès,

recommande

que les systèmes d'accès conditionnel de la radiodiffusion:

– soient bien protégés,

– partagent, dans le récepteur, un maximum d'éléments communs,

– soient conçus selon les principes fondamentaux qu'énumère l'Annexe 1.

---

* La Commission d'études 6 des radiocommunications a apporté des modifications rédactionnelles à cette Recommandation en 2002 conformément aux dispositions de la Résolution UIT-R 44.

ANNEXE 1

Principes fondamentaux de l'accès conditionnel dans les systèmes de radiodiffusion

1 Introduction

D'une façon générale, les principes qui suivent s'appliquent à la fourniture des services de télévision actuels et futurs, des programmes radiophoniques ainsi que des services de radiodiffusion de télétexte et de données. Ces principes s'appliquent à la diffusion et à la distribution aux usagers par divers supports de Terre, câble, satellites, enregistrement, etc.*

2 Eléments d'un système à accès conditionnel

Dans un système à accès conditionnel, il y a deux éléments distincts, souvent indépendants. Chacun d'eux se caractérise par un traitement distinct de l'information. Ces deux éléments sont présentés ci-après et définis dans l'Appendice 1.

2.1 Embrouillage

Ce traitement rend le contenu du service inutilisable pour les utilisateurs non autorisés en modifiant, côté émission et sous le contrôle du système d'accès conditionnel, certaines de ses caractéristiques. Le service peut contenir un programme ou autre chose, des données par exemple.

2.2 Contrôle d'accès

Ce sont les dispositions prises pour fournir une information qui permettra aux utilisateurs de désembrouiller le service. Cette information est rendue disponible par le système d'accès conditionnel.

De l'émetteur au(x) récepteur(s), cette information est structurée sous forme de messages protégés multiplexés avec le signal lui-même.

A la réception, les messages sont interprétés par le système d'accès conditionnel pour provoquer le désembrouillage du signal dans le (ou les) récepteur(s) autorisé(s).

3 Exigences auxquelles doit satisfaire le système de commande de l'accès conditionnel

3.1 Qualité

L'embrouillage et le désembrouillage ne doivent pas altérer de façon perceptible la qualité des images, sons et données reçus.

---

* L'Appendice 2 donne des exemples de mise en œuvre de systèmes d'accès conditionnel orientés vers la radiodiffusion télévisuelle par satellite en France, au Royaume-Uni et au Japon.

3.2 Sécurité

La sécurité d'un système est le degré de difficulté que rencontre un usager non autorisé lorsqu'il tente d'accéder à un service. Il y a deux façons de battre cette sécurité en brèche qui présentent deux types de difficultés:

– *désembrouiller le signal sans référence au processus de contrôle d'accès*. Cette fonction dépend de la nature des services et de la méthode d'embrouillage. Les futurs services de radiodiffusion télévisuelle, sonore et de données seront essentiellement de nature numérique et se prêteront donc à des systèmes d'embrouillage très sûrs;

– *obtenir de façon illicite la clé de contrôle d'accès**. Cette fonction dépend de la sécurité des algorithmes utilisés et de la méthode de distribution des clés.

3.3 Accès conditionnel universel

L'accès est autorisé à tout utilisateur répondant aux conditions d'accès au moyen d'un algorithme d'embrouillage commun ou universel. Accès conditionnel universel signifie simplement l'accès pour tous à l'aide de processus et d'équipements communs, selon des règles et des processus communs et faciles à appliquer afin de remplir les conditions d'accès définies par le producteur, le fournisseur ou le distributeur. Cela encouragera la généralisation des services à accès conditionnel grâce à un matériel simple, peu coûteux et souple. L'accès conditionnel universel suppose que le désembrouillage sera commun à tous les récepteurs, fondé sur un algorithme normalisé, indépendant du support de distribution utilisé sans pour autant entraver la concurrence entre organismes qui le mettent en œuvre à leur façon.

3.4 Protection du contenu de bout en bout

Protéger de bout en bout les services de distribution de télévision, sons et données, signifie protéger le contenu (programme ou autre) et l'information relative à l'accès (commande ou données) de l'origine à l'extrémité, pendant toute la durée de la distribution. La protection commence au point d'origine et elle est garantie jusqu'à la livraison au consommateur*. Cela empêche d'avoir facilement accès par des moyens frauduleux à une transmission bien protégée en enregistrant le contenu du programme chez soi.

Ainsi, à partir de n'importe quelle origine, la protection de bout en bout assure que l'information, une fois masquée, le reste, tout au long des stades intermédiaires du système de distribution, jusqu'à ce qu'elle atteigne le récepteur où l'accès dépendra de la question de savoir si l'utilisateur satisfait ou non aux conditions qu'impose le service d'origine ou distributeur. Qu'il soit transmis ou stocké, le contenu protégé ou toute autre information n'apparaît jamais nulle part en clair tant qu'un utilisateur autorisé n'y a pas accès. Ainsi, toute transmission ou tout stockage du contenu se fera «tel quel». Cela n'impose aucune contrainte aux intermédiaires, qui mettent en œuvre leur propre «enveloppe de protection» autour de l'information protégée pourvu qu'ils garantissent son intégrité, c'est-à-dire qu'ils la maintiennent intacte «telle quelle». Comme le contenu qui passe par une origine ne peut être embrouillé qu'une fois, le contenu embrouillé est envoyé tel quel. Toutefois, la clé d'embrouillage est envoyée sous le contrôle d'une stratégie de distribution de clés, en principe chiffrée par une clé de distribution et envoyée au récepteur de l'usager pour être stockée chiffrée avec des clés d'embrouillage venues de diverses origines.

---

* Voir l'Appendice 1 pour les définitions.

3.5 Modes d'accès

Un système à accès conditionnel est plus efficace s'il comporte plusieurs modes d'accès.

Les modes d'accès peuvent être, par exemple:

– l'abonnement à la période – l'autorisation est accordée entre une date initiale et une date d'expiration;

– la taxation à la séance – l'accès au service est autorisé pour une session donnée, que cette session soit complètement utilisée ou non;

– la taxation à la consommation – la taxe, ou l'imputation, est proportionnelle à la durée d'utilisation et/ou à la valeur du service concerné.

Les modes d'accès doivent varier en fonction de plusieurs paramètres, par exemple:

– le temps;

– différents segments du service;

– des groupes d'usagers particuliers.

3.6 Normalisation des équipements

La normalisation permet de fabriquer le plus économiquement possible des équipements de réception et d'en simplifier la gestion et la maintenance:

– les équipements communs devraient être normalisés pour que ceux-ci puissent s'adapter à une quantité d'options de service aussi importante que possible;

– le schéma d'un récepteur grand public doit être assez souple pour mettre en œuvre le chiffrage-déchiffrage par clés de session et de distribution ainsi que les fonctionnalités de clé de désembrouillage sous une forme qui peut aller d'organes de traitement incorporés au récepteur et amovibles à un module de sécurité personnel portatif intelligent (carte à mémoire) qui comprend les clés de session secrètes et une logique de reconnaissance du code personnel.

3.7 Gestion de l'accès

La définition de l'accès conditionnel est fondée sur la notion de *titre* d'accès, et celui-ci peut se présenter sous différentes formes. En vertu de son titre d'accès, un usager dispose d'une *autorisation* d'accès au service correspondant. L'utilisation non économique des ressources due à la gestion et à un surplus de transmission est à éviter.

3.8 Moyens d'éviter les dégradations du service

Il existe deux catégories de dégradations importantes:

– les dégradations affectant le service offert qui sont dues aux processus d'embrouillage/de désembrouillage;

– les dégradations dues à une acquisition défectueuse ou non fiable des données de contrôle d'accès.

3.9 Interaction avec le traitement numérique

Il convient de noter que les processus d'embrouillage peuvent limiter sérieusement les possibilités de traitement supplémentaire comme la réduction du débit binaire.

3.10 Contrôle de l'effet

Le système pourrait offrir plusieurs niveaux d'intelligibilité du signal au choix du fournisseur du programme en fonction de sa stratégie commerciale.

4 Description générale d'un système à accès conditionnel

4.1 Généralités

Dans un système à accès conditionnel, l'information doit être *embrouillée* avant sa diffusion. Le processus d'embrouillage est placé sous le contrôle de la séquence d'embrouillage obtenue à partir d'un *générateur pseudo-aléatoire*.

Pour le processus de désembrouillage à la réception, il faut utiliser la même séquence (séquence de désembrouillage dans ce cas) afin de régénérer le signal d'origine.

En vue de fournir cette séquence et d'assurer la synchronisation entre les processus qui interviennent à l'émission et à la réception, on utilise un *mot d'initialisation* pour contrôler les conditions initiales du générateur pseudo-aléatoire du train de bits.

Le processus est présenté en détail sur la Fig. 1.

4.2 Mot d'initialisation

L'accès conditionnel à une composante d'un service est en fait, équivalent à l'accès conditionnel au mot d'initialisation qui est composé des deux éléments suivants: le *mot de contrôle* et le *complément d'initialisation*.

4.3 Mot de contrôle

Le mot de contrôle est l'élément de base de la sécurité. Sa valeur est choisie arbitrairement et peut être modifiée pendant l'exploitation du service pour améliorer la sécurité.

Le mot de contrôle est communiqué au récepteur comme suit:

– à l'émission, suivant le mode d'accès utilisé, un algorithme de chiffrement donne des versions chiffrées du mot de contrôle, qui est multiplexé avec le signal lui-même. Ce sont les messages de contrôle des titres d'accès;

– à la réception, l'équipement de contrôle d'accès utilise l'algorithme inverse pour restituer le mot de contrôle si toutes les conditions d'accès sont réunies. Le ou les modules de sécurité du ou des récepteurs peuvent aussi effectuer les calculs cryptographiques et les vérifications pour garantir l'intégrité.

4.4 Complément d'initialisation

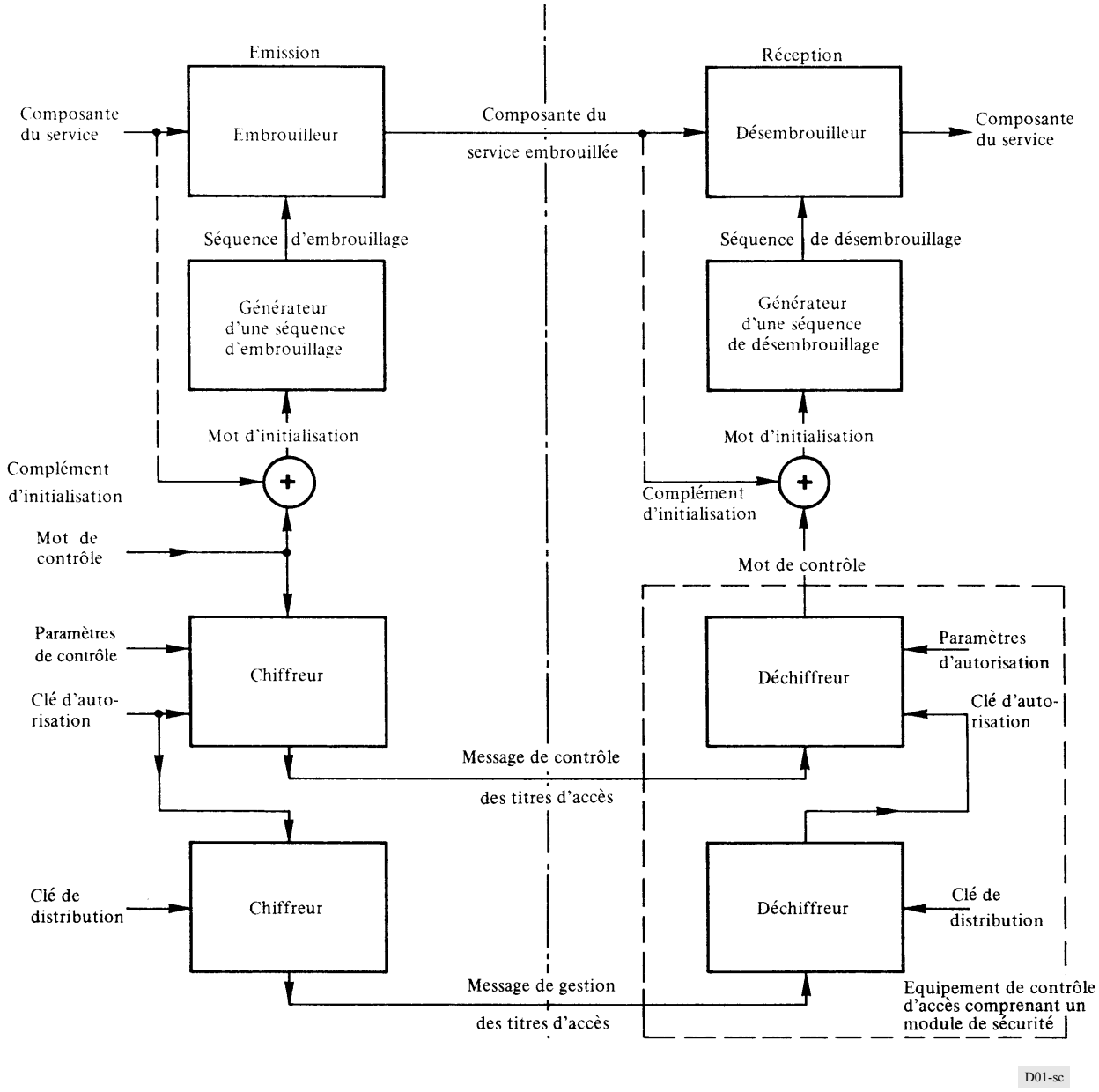
Le complément d'initialisation est utilisé pour imposer des séquences d'embrouillage suffisamment brèves permettant d'assurer la sécurité tout en évitant de procéder à des calculs trop fréquents du mot de contrôle. Ainsi, l'utilisation de différents compléments d'initialisation pour chaque unité structurelle de l'information embrouillée permet de modifier de façon suffisamment fréquente le mot d'initialisation. Le complément d'initialisation est également diffusé comme partie du signal.

4.5 Indice de mot de contrôle

Pour réaliser la segmentation d'un service, il est nécessaire de gérer plusieurs mots de contrôle associés aux différents segments du service. On identifie ces mots au moyen d'*indices*. L'indice du mot de contrôle utilisé pour accéder à une unité d'information embrouillée doit pouvoir être obtenu à partir du signal transmis.

FIGURE 1

Description fonctionnelle d'un système de radiodiffusion à accès conditionnel



Note 1 – Deux chiffreurs et déchiffreurs sont représentés sur cette figure dans un souci de clarté. En pratique, un chiffreur et un déchiffreur peuvent suffire si l'algorithme de chiffrement qui est commandé par la clé d'autorisation et celui qui est commandé par la clé de distribution sont identiques.

Note 2 – A la réception, les mécanismes de sécurité sont mis en œuvre dans le (ou les) module(s) de sécurité.

5 Messages de contrôle des titres d'accès

Chacun de ces messages comprend les éléments suivants:

– l'indice du mot de contrôle;

– un drapeau de modification du mot de contrôle: un changement d'état indique un changement de valeur du mot de contrôle;

– un *pointeur d'autorisation* qui identifie la clé d'autorisation située dans le module de sécurité du récepteur auquel le message est adressé;

– un *paramètre de contrôle* qui fournit des valeurs (par exemple, date, prix, etc.) destinées à être comparées aux limites qui leur sont fixées dans le module de sécurité du récepteur et que l'on appelle *paramètres d'autorisation*;
– le mot de contrôle chiffré.

Pour désembrouiller une unité d'information, le récepteur doit d'abord avoir extrait le mot de contrôle d'un message de contrôle des titres d'accès portant l'indice approprié.

Afin d'obtenir une efficacité optimale, il convient de regrouper sous le même indice les messages de contrôle des titres d'accès relatifs au même mot de contrôle mais correspondant soit à différents identificateurs d'audiences soit à différents types d'équipement de contrôle d'accès. Bien que ce ne soit pas sa seule application, le système d'indiçage décrit ci-dessus permet de réaliser la transmission anticipée des messages de contrôle des titres d'accès.

L'équipement d'accès conditionnel crée une table des mots de contrôle actifs, mise à jour par les messages de contrôle des titres d'accès indépendamment des données embrouillées. Pour identifier le mot de contrôle des titres correct, le dispositif de désembrouillage fournit à l'équipement de contrôle d'accès l'indice correspondant. La gestion de cette table fait partie intégrante des fonctions assurées à l'interface entre le désembrouilleur et l'équipement de contrôle d'accès.

6 Messages de gestion des titres d'accès

Le traitement d'un message de gestion des titres d'accès permet de valider ou d'acquérir le titre d'accès. Ce processus intervient dans le module de sécurité associé à un calcul cryptographique faisant intervenir une *clé de distribution*. La clé de distribution est utilisée pour chiffrer et déchiffrer des messages et/ou des clés d'autorisation adressées à des récepteurs individuels. Les cryptogrammes correspondants constituent le signal de validation et sont acheminés à l'intérieur des messages de gestion des titres d'accès.

Dans les systèmes de radiodiffusion à accès conditionnel, les messages de gestion des titres d'accès peuvent être radiodiffusés. C'est ce que l'on appelle l'adressage sur antenne. On peut réduire sensiblement la durée du cycle associé à la distribution des clés sur antenne en appliquant les principes des systèmes de chiffrement à clé partagée. Les messages de gestion des titres d'accès peuvent également être distribués par d'autres supports.

Voici la description d'un mode de fonctionnement. En cas de paiement par unité de temps ou par programme, les messages de gestion communiquent un code de coûts chiffré, qui est transmis dans le cadre du service offert. Le crédit stocké dans le récepteur peut revêtir la forme de jetons de sommes d'argent chiffrés qui sont transmis dans le cadre d'un service d'adressage sur antenne. Le crédit peut également prendre la forme de jetons de sommes d'argent stockés, qui sont distribués par d'autres moyens. Le paiement consiste à diminuer le crédit enregistré en fonction du code de coût reçu.

7 Equipement de contrôle d'accès

Cet équipement comprend notamment un module de sécurité qui reçoit les messages de contrôle des titres d'accès. Le module peut être fixe ou amovible (les deux cas autorisent des algorithmes de déchiffrement chargeables en aval). Dans le premier cas, l'accès est autorisé récepteur par récepteur, tandis que dans le cas du module amovible (carte à mémoire par exemple) l'accès n'est pas limité à un récepteur de télévision particulier. L'équipement de contrôle d'accès communique avec le désembrouilleur par l'intermédiaire d'une interface physique et de circuits logiques. La normalisation de cette interface est importante, car elle permet de préserver:

– l'indépendance du module de sécurité et de la fonction de désembrouillage intégrée au récepteur;

– le développement ultérieur de l'équipement de contrôle d'accès.

Si le module de sécurité contient une autorisation avec le même identificateur que le pointeur d'autorisation figurant dans le message de contrôle des titres d'accès, il fournit un mot de contrôle si, en outre, les paramètres de contrôle remplissent les conditions du paramètre d'autorisation. Parmi ces conditions, on peut trouver notamment:

– une condition de date, la date figurant dans le paramètre de contrôle devant être comprise entre les dates de départ et d'expiration du paramètre d'autorisation;

– une condition de coût qui permet à une autorisation d'être délivrée seulement si un débit de taxes est accepté par le module de sécurité.

Une transaction faisant intervenir le module de sécurité peut se diviser en trois étapes:

– instructions préliminaires, le cas échéant (par exemple, mot de passe, consentement de l'usager, etc.);

– instructions d'exploitation utilisant le module de sécurité;

– traitement (par exemple, délivrance du mot de contrôle).

Comme divers modules de sécurité peuvent être utilisés, il serait souhaitable que l'équipement de contrôle d'accès soit indépendant des transactions spécifiques. Cette indépendance peut être obtenue si l'équipement de contrôle d'accès sait interpréter une séquence d'instructions traduites dans un langage spécifique et transmise dans des messages particuliers.

APPENDICE 1

Termes et définitions liés aux systèmes de radiodiffusion à accès conditionnel

Embrouillage [en radiodiffusion] (scrambling, aleatorización)

Altération des caractéristiques d'un signal image/son/données radiodiffusé pour empêcher la réception non autorisée de l'information en clair. Cette altération est un processus bien défini, commandé par le système à accès conditionnel (côté émission).

Désembrouillage [en radiodiffusion] (descrambling, desaleatorización)

Restauration des caractéristiques d'un signal image/son/données radiodiffusé pour permettre la réception de l'information en clair. Cette restauration est un processus bien défini, commandé par le système à accès conditionnel (côté réception).

NOTE 1 – Les termes «embrouillage» et «désembrouillage» s'appliquent aussi bien aux signaux analogiques qu'aux signaux numériques.

NOTE 2 – Ces termes ne doivent pas être utilisés pour désigner des processus tels que la dispersion d'énergie dans un système à satellites.

Accès conditionnel

Un usager a accès à un service protégé en agissant sur le module de sécurité du récepteur, sur un module de sécurité ou sur un décodeur. Si au cours d'une session toutes les conditions d'accès sont réunies, l'autorisation est accordée, la clé de désembrouillage délivrée et le contenu désembrouillé.

L'authentification de l'abonné, la confirmation de la facturation et la validation de la disponibilité du service ou d'autres paramètres de contrôle du programme activent la clé de chiffrement-déchiffrement de la session afin que cette dernière mette fin au processus d'autorisation.

Commande de l'accès conditionnel

La fonction de la commande d'accès conditionnel à l'émission est de produire les signaux de commande d'embrouillage et les «clés» correspondant au service.

La fonction de la commande d'accès conditionnel à la réception est de produire les signaux de commande de désembrouillage en même temps que les clés correspondant au service.

Les termes *chiffrement* et *déchiffrement* s'appliquent à des méthodes utilisées pour protéger et interpréter certaines des informations contenues dans les messages relatifs à l'accès qui doivent être diffusés de l'extrémité émettrice à l'extrémité réceptrice des fonctions de commande d'accès conditionnel.

Point d'origine

Il s'agit, dans un système de distribution, du point où le programme ou tout autre contenu prend la forme du signal dans son format définitif de diffusion ou de distribution. C'est là que commence la protection de bout en bout. La forme du contenu à l'entrée est quelconque; il n'a pas forcément un sens pour l'observateur. L'entrée du contenu non plus n'est pas forcément intelligible.

Point de présentation

Il s'agit du point où le programme ou tout autre contenu apparaît finalement dans un système de distribution avant de devenir intelligible sur l'écran ou dans le haut-parleur de l'usager. C'est la sortie de la protection de bout en bout.

NOTE 1 – Les titulaires de droits d'auteur, les fournisseurs de service et les distributeurs forment une longue hiérarchie de points d'origine possibles du flux d'information destiné à l'usager ainsi que du flux de matériel embrouillé et de clés de chiffrement. L'origine doit se situer d'abord chez le titulaire de droits d'auteur ou le producteur. En pratique, la plupart des points d'origine sont simplement les points d'entrée à un niveau quelconque du système, dictés par des motifs financiers ou d'exploitation. Bien que ces points d'entrée puissent être nombreux, chacun d'eux est unique et indépendant et l'information y demeure tout le temps au format qu'elle peut avoir lorsqu'elle est envoyée sur tout le trajet qui aboutit à un usager.

APPENDICE 2

Exemples de mise en œuvre d'un système à accès conditionnel

Référence à l'Annexe 1	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (C-MAC/paquets et D2-MAC/paquets)	Sous-porteuse numérique/NTSC
	Télétexte système A	Télétexte système B	Lignes avec données indépendantes du télétexte système B	Couches 1 à 4 du télétexte système C adopté en France		
Processus d'embrouillage § 4.1	Combinaison par un OU-exclusif d'octets de données avec les octets d'un générateur pseudo-aléatoire. Un octet d'interprétation dans l'en-tête indique si l'article est embrouillé ou non	Combinaison par un OU-exclusif des octets de données avec les octets d'un générateur pseudo-aléatoire. Les liaisons du paquet 27 indiquent que la page est embrouillée	Combinaison par un OU-exclusif d'octets de données avec les octets d'un générateur de trains de données d'embrouillage. L'apparition régulière de blocs de clés de données d'utilisateur indique que le service est embrouillé	Combinaison par un OU-exclusif d'octets de données avec les octets d'un générateur pseudo-aléatoire. Dans le complément d'initialisation, un octet indique si le groupe de données est ou non embrouillé. Les groupes de données où GT = 0 ou 1 ne sont pas embrouillés	*Image:* rotation de composante à double coupure ou rotation de ligne à simple coupure, sous le contrôle d'un générateur pseudo-aléatoire *Son:* combinaison par un OU-exclusif bit par bit des bits de données avec les bits d'un générateur pseudo-aléatoire fonctionnant en continu	*Image:* rotation ou permutation des lignes ou combinaison des deux méthodes sous le contrôle d'un générateur pseudo-aléatoire *Son:* combinaison par un OU-exclusif bit par bit des bits de données avec les bits d'un générateur pseudo-aléatoire fonctionnant en continu
Générateur pseudo-aléatoire § 4.1	Combinaison de trois registres à décalage multi-étages à rétroaction linéaire	Utilisation d'une fonction unidirectionnelle employant un algorithme à rétroaction de chiffrement	Le générateur de trains d'embrouillage utilise un algorithme de chiffrement connecté en mode de sortie à rétroaction (ISO DIS 8372)	Combinaison de trois registres à décalage multi-étages à rétroaction linéaire	*Image:* deux registres à décalage multi-étages à rétroaction linéaire *Son:* deux registre à décalage multi-étage à rétroaction linéaire initialisant un autre registre à décalage multi-étage à rétroaction linéaire	Combinaison non linéaire de la sortie de trois registres à décalage multi-étages à rétro-action linéaire (13, 11, 8 étages chaque)

APPENDICE 2 (*suite*)

Référence à l'Annexe 1	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (C-MAC/paquets et D2-MAC/paquets)	Sous-porteuse numérique/NTSC
	Télétexte système A	Télétexte système B	Lignes avec données indépendantes du télétexte système B	Couches 1 à 4 du télétexte système C adopté en France		
Synchronisation du générateur pseudo-aléatoire. § 4.1	Premier octet suivant la première séquence US-X-Y de l'article	Premier octet de données du paquet 0 d'une page désignée	Le premier octet des données d'utilisateur se trouve dans le bloc de données d'utilisateur	Premier octet suivant le complément d'initialisation	Au départ de chaque trame	Un signal de synchronisation est transmis parmi les codes de contrôle de la trame son. L'embrouillage de l'image commence dès l'image qui suit immédiatement le signal de synchronisation et celui du son dès la trame d'embrouillage du son immédiatement après le signal de synchronisation
Mot d'initialisation § 4.2	12 octets	Clé de page de 56 bits	La variable initiale du train d'embrouillage est un octet unique au départ du bloc de données d'utilisateur; répété 8 fois	12 octets	60 bits	32 bits
Mot de contrôle § 4.3	8 octets aléatoires	Clé (56 bits) du système en vigueur	Clé d'utilisateur de 64 bits	8 octets aléatoires	60 bits, soit choisis de manière aléatoire soit sous forme de cryptogramme du compteur de 256 trames	32 bits choisis de façon aléatoire (comme pour le mot d'initialisation)
Complément d'initialisation § 4.4	4 octets suivant l'en-tête du message	Ne s'applique pas	Ne s'applique pas	4 octets suivant l'en-tête du groupe de données	La valeur du compteur de trames à 8 bits	Ne s'applique pas
Contrôle de l'effet § 3.10	Ne s'applique pas	Ne s'applique pas	Ne s'applique pas	Ne s'applique pas	Ne s'applique pas	*Image:* applicable *Son:* ne s'applique pas

APPENDICE 2 (*suite*)

Référence à l'Annexe 1	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (C-MAC/paquets et D2-MAC/paquets)	Sous-porteuse numérique/NTSC
	Télétexte système A	Télétexte système B	Lignes avec données indépendantes du télétexte système B	Couches 1 à 4 du télétexte système C adopté en France		
Message de contrôle des titres d'accès § 5	Articles désignés avec pour numéro de classification FFF et $Y_{11} = 1$; l'octet Y_{12} donne l'indice du mot de contrôle. Chaque message est introduit par la séquence US-3/F-3/F et comprend: – 3 octets pour le pointeur d'autorisation – 3 octets pour le paramètre de contrôle – 16 octets pour le mot de contrôle chiffré	Les paquets désignés comprennent des paramètres d'autorisation et de contrôle à 22 bits et un mot de contrôle chiffré de 112 bits	Un type de bloc de contrôle transmet une clé de données d'utilisateur à tous les utilisateurs disposant d'une clé de système valable leur permettant de la déchiffrer	Groupes de données pour lesquels GT (type du groupe de données, voir la Recommandation UIT-R BT.653, Tableau 1a, point 4.1) est égal à 14. Les groupes de données sont constitués d'ordres, chaque ordre étant identifié par un identificateur d'ordre et un identificateur de longueur d'ordre, et composé de paramètres identifiés par un identifi- cateur de paramètre et un identificateur de longueur de paramètre; on définit deux types d'ordre: CI = 0 référence du module de sécurité à utiliser; CI ≠ 0 ordre de contrôle des titres d'accès, où chaque paramètre transporte un ECH et comprend: – 3 octets pour l'impression de l'autorisation, – 3 octets pour le paramètre de contrôle, – 16 octets pour le mot du contrôle chiffré	Paquets désignés dans la voie d'identification du service. Pour le système d'accès conditionnel pour les services diffusés en D2-MAC/paquets, qu'utilise notamment le système français de radiodiffusion directe par satellite TDF1-TDF2, le codage de ces paquets est conforme aux dispositions de la spécification «Système d'accès conditionnel pour la famille MAC/paquets EUROCRYPT» (mars 1989). Au Royaume-Uni, où le système D-MAC/paquets a été adopté, le service de radiodiffusion par satellite britannique commencera l'exploitation du SRS en utilisant le système d'accès conditionnel Eurocypher (système d'accès conditionnel pour utilisation avec la famille de formats de trans- mission MAC/paquets)	Paquets transmis par la voie de données dans la trame sonore numérique. La signification de chaque bit est définie mais c'est le fournisseur de service qui donne les précision détaillées
Indice de mot de contrôle § 4.5	Octet Y_{16} de l'article embrouillé pour le désembrouillage et octet Y_{12} du message de contrôle de titre d'accès pour mise à jour	Ne s'applique pas	Ne s'applique pas		Ne s'applique pas	Ne s'applique pas

APPENDICE 2 (*suite*)

Référence à l'Annexe 1	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (C-MAC/paquets et D2-MAC/paquets)	Sous-porteuse numérique/NTSC
	Télétexte système A	Télétexte système B	Lignes avec données indépendantes du télétexte système B	Couches 1 à 4 du télétexte système C adopté en France		
Changement de mot de contrôle et de drapeau § 5	Bit b_8 de l'octet Y_{12} du message de contrôle de titre d'accès	Mots clés en vigueur et nouveaux inclus dans un paquet désigné de la page d'adressage à l'utilisateur	On identifie les versions correctes des clés en mettant en correspondance les clés d'étiquette transmises avec les clés et avec les blocs de données pour lesquels ces clés sont nécessaires	Bit b_8 de l'identificateur de paramètre de l'ordre de contrôle des titres d'accès	Un nouveau mot de contrôle est transmis toutes les 256 trames et devient le mot de contrôle en vigueur lorsque le comptage de trames atteint zéro	Mot de contrôle renouvelé par le signal de synchronisation. Les renouvellements ont lieu au plus toutes les secondes
Message de gestion des titres d'accès § 6	Le titre d'accès est actuellement géré par un système vidéotex sur un réseau de télé-communication	Le titre d'accès est géré par adressage sur antenne de l'équipement d'utilisateur au moyen de paquets d'adressage d'utilisateur en partage et d'utilisateur unique	Le titre d'accès est géré par adressage sur antenne du module de contrôle d'accès au moyen de blocs de données d'adressage d'utilisateur en partage et d'utilisateur unique. Les blocs de données pour adressage sur antenne sont multiplexés dans la même voie sous forme de données de message	Pas encore normalisé. Les titres d'accès peuvent être gérés par un système de vidéotex sur un réseau de télécommunications	Paquets désignés dans la voie d'identification du service. Pour le système d'accès conditionnel pour les services diffusés en D2-MAC/paquets, qu'utilise notamment le système français de radiodiffusion directe par satellite TDF1-TDF2, le codage de ces paquets est conforme aux dispositions de la spécification «Système d'accès conditionnel pour la famille MAC/paquets EUROCRYPT» (mars 1989).	Paquets transmis par la voie de données. On peut aussi les distribuer au moyen de cartes à circuits intégrés. La signification de chaque bit est définie mais c'est le fournisseur de service qui donne les précisions détaillées

APPENDICE 2 (*suite*)

Référence à l'Annexe 1	Systèmes de télétexte organisés par page		Systèmes de radiodiffusion de données		Famille MAC/paquets (C-MAC/paquets et D2-MAC/paquets)	Sous-porteuse numérique/NTSC
	Télétexte système A	Télétexte système B	Lignes avec données indépendantes du télétexte système B	Couches 1 à 4 du télétexte système C adopté en France		
Message de gestion des titres d'accès (*suite*)					Au Royaume-Uni, où le système D-MAC/paquets a été adopté, le service de radiodiffusion par satellite britannique commencera l'exploitation du SRS en utilisant le système d'accès conditionnel Eurocypher (système d'accès conditionnel pour utilisation avec la famille de formats de trans-mission MAC/paquets)	
Equipement de contrôle d'accès § 7	Incorporé dans le récepteur et comportant un lecteur de cartes à mémoire	Intégré dans le récepteur ou fonctionnellement séparé, au choix du fournisseur du service	Entièrement contenu dans le module de sécurité. Accepte des données série en provenance du décodeur de paquets et fournit à l'utilisateur des données série désembrouillées	Incorporé au récepteur et comportant un lecteur de cartes à mémoire	Fonctionnellement séparé des autres parties du récepteur au moyen d'une interface qui reste à normaliser	Fonctionnellement séparé des autres parties du récepteur moyennant son implantation dans un circuit intégré à usage exclusif
Module de sécurité § 7	Carte à mémoire avec interface proposée pour normalisation à l'ISO	Module intégré ou amovible ou carte à mémoire	Unité à microprocesseur contenant un logiciel d'application pour exécuter tous les algorithmes de déchiffrement et le traitement des protocoles de données	Carte à mémoire avec interface proposée pour normalisation à l'ISO	Deux solutions proposées: – la carte à mémoire ou – un module incorporé	Module incorporé