UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.91

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(08/94)

TRANSMISSIONS TÉLÉVISUELLES ET SONORES

MÉTHODES TECHNIQUES POUR GARANTIR LA CONFIDENTIALITÉ SUR LES TRANSMISSIONS INTERNATIONALES DE TÉLÉVISION À GRANDE DISTANCE

Recommandation UIT-T J.91

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'Union internationale des télécommunications (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.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études 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 n° 1 de la CMNT (Helsinki, 1er-12 mars 1993).

La Recommandation UIT-T J.91, que l'on doit à la Commission d'études 9 (1993-1996) de l'UIT-T, a été approuvée le 22 août 1994 selon la procédure définie dans la Résolution n° 1 de la CMNT.

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 de télécommunications.

TABLE DES MATIÈRES

RÉSUMÉ

La présente Recommandation constitue une norme commune pour un système à accès conditionnel de transmissions internationales de télévision numérique à grande distance, conformément à la Recommandation J.81[1)]. Elle donne d'abord une vue d'ensemble du système à accès conditionnel en spécifiant les catégories des messages à accès conditionnel qui doivent être transmis. La Recommandation spécifie un protocole de transport fondé sur les trames HDLC pour les messages à accès conditionnel transmis sur le canal CA1 conformément à la Recommandation J.81.

Par ailleurs, la Recommandation décrit l'architecture de l'ensemble du système de transmission, y compris les caractéristiques de l'accès conditionnel. Cette architecture diffère de celle des systèmes classiques de télévision payante dans la mesure où elle requiert expressément la mise en place d'un dispositif de contrôle qui n'est pas situé au même endroit que les émetteurs.

En outre, la Recommandation présente une modélisation des principales installations et interfaces nécessaires à l'exploitation d'un système à accès conditionnel, avec indication de leurs fonctions et d'un certain nombre de configurations proposées selon les applications. Enfin, les modalités de mise en oeuvre pratique sont abordées compte tenu du niveau de sécurité et des fonctions nécessaires des applications.

1) La Recommandation J.81 était anciennement la Recommandation UIT-R CMTT.723.

Recommandation J.91

MÉTHODES TECHNIQUES POUR GARANTIR LA CONFIDENTIALITÉ SUR LES TRANSMISSIONS INTERNATIONALES DE TÉLÉVISION À GRANDE DISTANCE

(Genève, 1994)

L'UIT-T,

considérant

(a) que, de par leur nature, les signaux radioélectriques sont susceptibles d'être captés par un grand nombre de récepteurs non identifiés et que, dans le cas de transmissions internationales par satellites de télécommunication, des stations auxquelles cette information n'est pas destinée risquent de recevoir et d'interpréter les signaux;

(b) que le nombre de stations capables de recevoir ces signaux augmente constamment;

(c) que ces accès indésirables au signal transmis sont facilités quand les caractéristiques techniques de la radiodiffusion et des transmissions sont semblables;

(d) que la Recommandation J.81 qui définit le codec de réduction du débit binaire à utiliser dans les applications de qualité contribution au troisième niveau hiérarchique de la Recommandation G.702 tient compte de la nécessité d'avoir un système à accès conditionnel,

recommande

que les méthodes techniques de radiocommunication qu'il convient d'utiliser pour garantir la confidentialité sur les transmissions internationales de télévision à grande distance, conformément à la Recommandation J.81, soient définies comme suit.

1 Objet

La présente Recommandation UIT-T constitue une norme commune pour un système à accès conditionnel de transmissions internationales de télévision numérique à grande distance, conformément à la Recommandation J.81.

Elle définit les interfaces et les équipements nécessaires pour exploiter le système à accès conditionnel et spécifie un protocole de transport des messages à accès conditionnel sur le canal CA1 de la Recommandation J.81.

Les annexes indiquent aussi les moyens pratiques de mise en œuvre.

2 Références

– Recommandation J.81, *Transmission de signaux vidéo numériques à codage en composantes pour les applications de qualité contribution au troisième niveau de la hiérarchie numérique de la Recommandation G.702*.

– EN 50094, 1992, *Access control system for the MAC/Packet family: EUROCRYPT*.

– ISO 7816-1:1987, *Cartes d'identification – Cartes à circuit(s) intégré(s) à contacts – Partie 1: Caractéristiques physiques*.

ISO 7816-2:1988, *Cartes d'identification – Cartes à circuit(s) intégré(s) à contacts – Partie 2: Dimensions et emplacements des contacts*.

– ISO/CEI 7816-3:1989, *Cartes d'identification – Cartes à circuit(s) intégré(s) à contacts – Partie 3: Signaux électroniques et protocoles de transmission*.

3 Termes et définitions

Pour les besoins de la présente Recommandation, les définitions suivantes s'appliquent:

embrouillage: 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: 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).

4 Abréviations

Pour les besoins de la présente Recommandation, les abréviations suivantes sont utilisées:

ACS	Système de contrôle d'accès (*access control system*)
Bit	Contraction des mots nombre binaire (*binary digit*)
CA	Adresse de l'usager (*customer address*)
CA1	Canal 1 à accès conditionnel (partie du multiplex de service du codec) (*conditional access channel 1*)
CA2	Canal 2 à accès conditionnel (partie du multiplex de service du codec) (*conditional access channel 2*)
CAD	Dispositif d'accès conditionnel (*conditional access device*)
CD	Dispositif de contrôle (*controller device*)
CI	Identificateur de commande (*command identifier*)
CIW	Mot d'identification du conteneur (*container identification word*)
CMSM	Module de contrôle à haute sécurité (*control major security module*)
CW	Mot de contrôle (*control word*)
ECM	Message de contrôle des titres d'accès (*entitlement control message*)
ECW	Mot de contrôle pair (*even control word*)
EEPROM	Mémoire morte programmable effaçable électriquement (circuit intégré) [*electrically erasable programmable read only memory (integrated circuit*)]
EMM	Message de gestion des titres d'accès (*entitlement management message*)
HDLC	Commande de liaison de données à haut niveau (*high level data link control*)
IW	Mot d'initialisation chargé dans les générateurs de séquence pseudo-aléatoire en vue du désembrouillage (*initialization word*)
LI	Indicateur de longueur (*length indicator*)
MD	Dispositif de gestion (*manager device*)
MH	En-tête du message (*message header*)
MMSM	Module de gestion à haute sécurité (*management major security module*)
NMC	Centre de gestion du réseau (*network management centre*)
Octet	Séquence de 8 bits traitée comme un groupe ou un mot de données
OCW	Mot de contrôle impair (*odd control word*)
PCMCIA	Personal Computer Memory Card International Association

PPI	Identificateur de parité de phase indiquant le CW à utiliser pour le désembrouillage (*phase parity identifier*)
PRG	Générateur (de séquence) pseudo-aléatoire [*pseudo-random (sequence) generator*]
RPCP	Réseau public à commutation par paquets
RTPC	Réseau téléphonique public commuté
SA	Adresse partagée (*shared address*)
UA	Adresse unique (*unique address*)
USM	Module de sécurité de l'usager (*user security module*)
Mot	Groupe ou séquence de bits traités en bloc

5 Vue d'ensemble du système

Un système à accès conditionnel sert à permettre aux usagers autorisés de désembrouiller les éléments d'un service.

Les processus d'embrouillage et de désembrouillage sont spécifiés dans la Recommandation J.81 et résumés au 5.1. Ces processus se déroulent, respectivement, dans les codeurs et les décodeurs.

L'information nécessaire pour le désembrouillage peut soit être introduite manuellement dans le décodeur (mot de contrôle local, par exemple), soit être fournie par le système à accès conditionnel dont la description est résumée au 5.2.

De l'émetteur au(x) récepteur(s), cette information est intégrée à des messages de sécurité multiplexés avec le signal lui-même sur les canaux CA1 et CA2 (voir l'article 12/J.81). Ces messages sont tirés du signal par les décodeurs et interprétés par le système à accès conditionnel du ou des récepteurs autorisés afin de contrôler le désembrouillage des éléments du service.

5.1 Description générale des processus d'embrouillage et de désembrouillage

La Figure 1 illustre les processus d'embrouillage/désembrouillage.

Pour l'accès conditionnel, il faut que les signaux de télévision soient embrouillés par le codeur avant d'être transmis. Ce processus est commandé par une séquence d'embrouillage fournie par un générateur pseudo-aléatoire.

Le processus de désembrouillage dans les décodeurs suppose que la séquence correspondante (dans le cas présent, la séquence de désembrouillage) reconstitue le signal original.

Pour fournir cette séquence et assurer le synchronisme entre l'émetteur et le ou les récepteurs, l'état du générateur pseudo-aléatoire au départ est contrôlé par un mot d'initialisation.

En fait, l'accès conditionnel à un service correspond à l'accès conditionnel au mot d'initialisation qui résulte d'une combinaison du complément d'initialisation et du mot de contrôle.

Le complément d'initialisation sert à fournir un nouveau mot d'initialisation pour chaque conteneur TV comme le définit la Recommandation J.81. Le complément d'initialisation, qui a été appelé CIW dans la Recommandation J.81, est transmis en clair sur le canal CA2.

En marge des processus d'embrouillage/désembrouillage, le système à accès conditionnel crée des paires de mots de contrôle actifs. Chaque paire comprend un mot de contrôle pair (ECW) valable pour les blocs pairs et un mot de contrôle impair (OCW) valable pour les blocs impairs. La parité des blocs transmis est donnée par l'indicateur de parité de phase PPI sur le canal CA2 (voir l'article 12/J.81).

C'est du mot de contrôle que dépend la sécurité. Sa valeur arbitraire reste la même tout au long de n'importe quel bloc de conteneurs TV (65 534 conteneurs TV, ce qui correspond à 8,2 secondes). Le codeur reçoit des cryptogrammes des mots de contrôle et les transmet au(x) décodeur(s) via le canal CA1.

5.2 Description générale du système à accès conditionnel

Le système à accès conditionnel a pour rôle de créer, lors de chaque nouvelle transmission, une nouvelle séquence de mots de contrôle et de distribuer exclusivement chaque séquence aux usagers concernés (un émetteur et un ou plusieurs récepteurs, selon la configuration de la transmission). A cette fin, le système à accès conditionnel crée, transmet et utilise des messages à accès conditionnel.

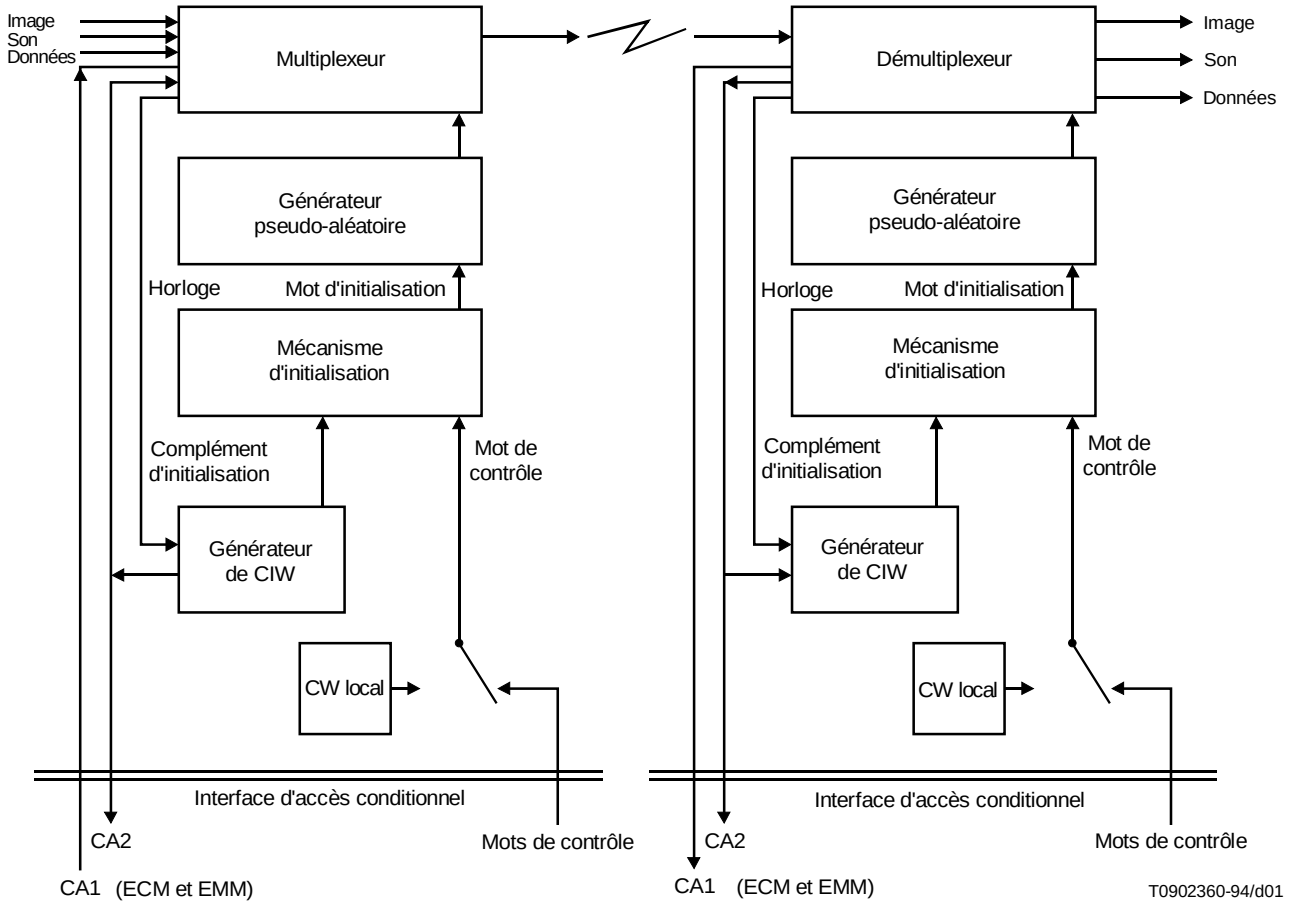

FIGURE 1/J.91

Processus d'embrouillage/désembrouillage

Pour garantir la sécurité de ces messages à accès conditionnel, on utilise deux sortes de mécanismes cryptographiques:

- le chiffrement et le déchiffrement des blocs servent à garantir la confidentialité (par exemple, pour acheminer les mots de contrôle et les clés dans les cryptogrammes);

- le calcul et la vérification du total de contrôle cryptographique servent à assurer que le message est complet (par exemple, pour les messages d'authentification).

Les modules à haute sécurité effectuent le chiffrement de bloc et le calcul du total de contrôle cryptographique.

Les modules de sécurité de l'usager effectuent le déchiffrement de bloc et la vérification du total de contrôle cryptographique.

Un total de contrôle cryptographique doit protéger chaque message à accès conditionnel où il y a un ou plusieurs cryptogrammes. A la réception d'un tel message, chaque module de sécurité doit constater que le total cryptographique est valable avant de continuer l'opération. Le déchiffrement de tout cryptogramme n'est donc possible que si la vérification a montré que le message à accès conditionnel était complet.

Dans tout système à accès conditionnel, il faut une instance de direction qui produise les mots de contrôle mais aussi qui calcule et transmette leurs cryptogrammes. Cette instance est la seule à détenir et à utiliser les modules à haute sécurité.

Dans maints systèmes de TV payante traditionnelle, l'instance de direction joue aussi le rôle d'émetteur. Dans la présente Recommandation, on a délibérément séparé les fonctions de direction et d'émission pour les deux raisons suivantes:

– il est préférable que les modules à haute sécurité ne soient pas dispersés;

– la gestion des échanges internationaux de télévision peut être centralisée (à l'EBU, par exemple).

L'émetteur et le ou les récepteurs ne détiennent et n'utilisent donc que des modules de sécurité de l'usager.

Le système à accès conditionnel met en œuvre deux types de messages à accès conditionnel: les messages de contrôle des titres d'accès (ECM) et les messages de gestion des titres d'accès (EMM).

Le canal CA1 est consacré à la transmission de messages de l'émetteur au(x) récepteur(s). Les messages à accès conditionnel ont une longueur moyenne d'environ 300 bits. La protection contre les erreurs (par code de Golay, par exemple) peut en doubler la longueur. Un nouvel ECM est émis au moins toutes les 8,2 secondes. S'il est répété à chaque seconde, on dispose d'environ 7 kbit/s pour émettre 10 EMM par seconde.

Chaque message à accès conditionnel est une série de paramètres en option. Un paramètre vise à acheminer un ou plusieurs cryptogrammes; un autre à acheminer un total de contrôle cryptographique.

5.2.1 Messages de contrôle des titres d'accès (ECM)

Les ECM ont pour rôle de fournir des mots de contrôle à tous les utilisateurs autorisés et à eux seulement. Le paramètre essentiel de chaque mot de contrôle est donc un ou plusieurs cryptogrammes du mot de contrôle.

Les ECM peuvent commencer par un ou plusieurs critères d'accès. Dans ce cas, il faut que le module de sécurité de l'usager trouve qu'au moins un des critères d'accès est satisfait avant de continuer à traiter le message.

Le dernier paramètre de chaque ECM doit être un total de contrôle cryptographique qui protège tout le message.

5.2.2 Messages de gestion des titres d'accès (EMM)

Les EMM ont pour rôle de fournir aux modules de sécurité de l'usager voulus les titres d'accès et les clés appropriés. Ces titres d'accès et ces clés servent à déchiffrer les cryptogrammes du mot de contrôle émis dans les ECM.

Les paramètres principaux des EMM sont les adresses du module de sécurité de l'usager, les titres d'accès, les cryptogrammes des clés et enfin, un total de contrôle cryptographique qui protège tout le message.

6 Modèles d'interface et équipement

La Figure 2 présente un modèle d'interface qui répond à la description générale ci-dessus.

La partie supérieure de la figure représente l'instance de direction. Le dispositif de gestion et le dispositif de contrôle peuvent se trouver en un autre emplacement.

La partie inférieure de la Figure 2 représente les utilisateurs qui, en principe, sont tous capables d'émettre et de recevoir.

6.1 Liste des interfaces

– *Interface 1* – Cette interface assure la transmission des EMM du dispositif de gestion au dispositif de contrôle. Ces EMM serviront à configurer les modules de sécurité de l'usager que met en jeu le futur échange de programmes de télévision.

– *Interface 2* – Cette interface assure la transmission de messages (EMM suivis d'ECM) de l'instance de direction (dispositif de contrôle) à l'émetteur (dispositif d'accès conditionnel). La transmission (8 kbit/s au plus) peut avoir lieu en temps réel sur un canal réservé ou sur une ligne téléphonique. Elle peut aussi se faire moyennant l'envoi à l'avance d'une disquette par la poste. Les messages (EMM et ECM) sont traités par le dispositif d'accès conditionnel en vue de leur insertion sur le canal CA1.

– *Interface 3* – Cette interface relie les modules de sécurité à divers dispositifs comme les dispositifs d'accès conditionnel pour les usagers et les dispositifs de contrôle et de gestion pour les instances de direction. Le module de sécurité peut se présenter sous la forme d'une carte à mémoire. Dans ce cas, l'interface est spécifiée dans la série des normes internationales ISO/CEI 7816.

– *Interface 4* – Cette interface relie les dispositifs d'accès conditionnel des usagers aux codeurs et aux décodeurs. Elle est spécifiée par la Recommandation J.81.

– *Interface 5* – Cette interface relie les modules de sécurité de l'usager des utilisateurs au dispositif de gestion via le dispositif d'accès conditionnel. L'information relevée dans les modules de sécurité de l'usager peut servir à des fins statistiques ou financières. L'interface 5 peut être mise en œuvre au moyen du réseau téléphonique public commuté ou du réseau public à commutation par paquets.

– *Interface 6* – Cette interface permet le dialogue avec l'exploitant local et introduit une interface homme-machine dans les dispositifs de contrôle et de gestion ainsi que dans chaque dispositif d'accès conditionnel.

La mise en œuvre détaillée (protocole, mise en œuvre concrète) des interfaces 1, 2, 5 et 6 dépend de l'application et sort du cadre de la présente Recommandation.

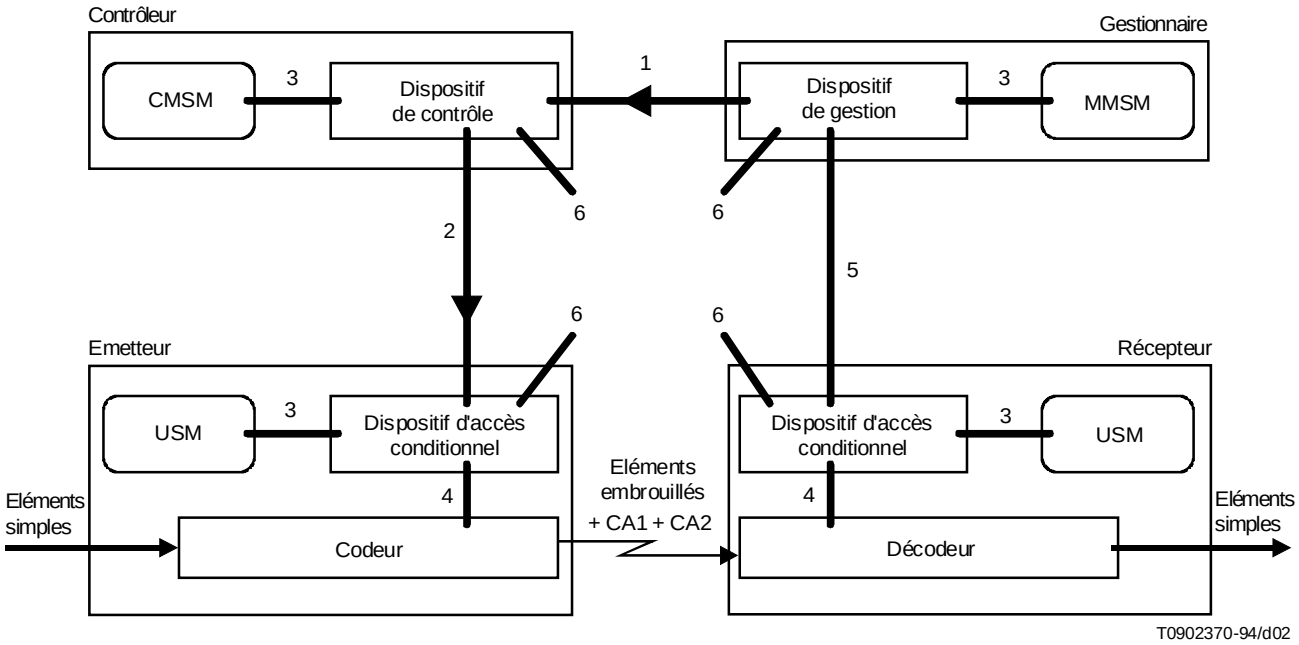

FIGURE 2/J.91

Modèle d'interface

6.2 Liste des équipements

La Recommandation J.81 décrit les codeurs et décodeurs.

Les modules à haute sécurité pour le contrôle et les modules correspondants pour la gestion (capables d'effectuer le chiffrement des blocs et le calcul du total de contrôle cryptographique) servent respectivement à calculer les ECM et les EMM.

Le module de sécurité de l'usager (capable d'effectuer le déchiffrement de blocs et uniquement la vérification du total de contrôle cryptographique) sert à interpréter les ECM et les EMM. Il garde en mémoire les titres d'accès et les clés de son utilisateur afin de déchiffrer les cryptogrammes des mots de contrôle. Il peut aussi garder en mémoire les accès effectifs de l'usager au système en cas de paiement à la durée par impulsions.

Tout module de sécurité peut être mis en œuvre sous la forme d'une carte à mémoire. Dans ce cas, les modules à haute sécurité sont parfois appelés «cartes-mères» et les modules de sécurité de l'usager «cartes-filles».

Le dispositif de gestion est relié à un ou plusieurs modules de gestion à haute sécurité qui calculent les EMM. Le dispositif de contrôle envoie ces EMM à l'usager. Si le nombre d'usagers est de quelques milliers, le dispositif de gestion peut être mis en œuvre sous forme d'un ordinateur personnel.

Le dispositif de contrôle produit de façon aléatoire les mots de contrôle et élabore les ECM avec le concours de ses modules de contrôle à haute sécurité. Ces ECM, ainsi que les EMM communiqués par le dispositif de gestion, sont envoyés à l'émetteur. Si le nombre d'usagers est de quelques milliers, le dispositif de contrôle peut être mis en œuvre sous forme d'un ordinateur personnel.

Le dispositif d'accès conditionnel est relié à un ou plusieurs codeurs ou décodeurs et à un ou plusieurs modules de sécurité de l'usager. Côté codeur, ce dispositif produit le canal CA1 qui achemine les EMM et les ECM vers le(s) récepteur(s). Le dispositif d'accès conditionnel reçoit les EMM et choisit ceux qui s'adressent à son ou à ses modules de sécurité. Il reçoit aussi les ECM que traitent les modules de sécurité de l'usager.

Le «système de contrôle d'accès» (ACS) que décrit la Recommandation J.81 correspond à la combinaison d'un dispositif d'accès conditionnel et d'un ou plusieurs modules de sécurité de l'usager.

7 Protocole de transport des messages à accès conditionnel sur le canal CA1

Les messages à accès conditionnel sont diffusés sur le canal CA1 au débit nominal de 8 kbit/s (voir la Recommandation J.81).

Deux sortes de messages à accès conditionnel ont été décrits jusqu'ici: les ECM et les EMM.

Selon le mode de chiffrement (voir 12.7.3/J.81), il peut y avoir:

- aucun ECM (modes 0 et 1);
- un nouvel ECM à chaque bloc (mode 2);
- plusieurs nouveaux ECM à chaque bloc (mode 3).

En mode 3, chaque ECM doit être associé aux éléments auxquels il s'applique.

Les EMM peuvent être envoyés à:

- *tous les usagers* – Dans ce cas, ils sont appelés EMM-G et sont envoyés sans adresse;
- *un groupe d'usagers* – Dans ce cas, ils sont appelés EMM-S et sont envoyés avec une adresse partagée (SA, 24 bits);
- *un seul usager* – Dans ce cas, ils sont appelés EMM-U et sont envoyés avec une adresse unique (UA, 36 bits).

Les ECM et les EMM sont protégés par des algorithmes cryptographiques. La référence de l'algorithme de chiffrement utilisé doit être envoyée avec le message.

Il faut émettre plusieurs fois les mêmes ECM et EMM [par exemple, l'ECM change pour chaque bloc (8,2 secondes) mais le même ECM peut être répété toutes les secondes afin de réduire le délai d'acquisition]. Il faut aménager un mécanisme qui permette aux récepteurs de distinguer les nouveaux messages à accès conditionnel de ceux qui sont répétés.

7.1 Trame de transmission

La structure de trame que décrit 9.2.4/J.81 sert à transmettre les messages à accès conditionnel. Elle est basée sur une structure de trame HDLC (commande de liaison de données à haut niveau).

La trame de transmission se compose des informations suivantes (voir la Figure 3):

- un drapeau de début (START): «01111110»;
- un en-tête de message (MH): 2 octets;
- un message à accès conditionnel: n octets;
- un CRC détecteur d'erreurs à 16 bits (FCS: séquence de contrôle de trame) (CRC): 2 octets;
- un drapeau de fin, identique à celui du début (END): 1 octet.

Pour éviter la confusion entre les drapeaux et les données, la commande HDLC définit une méthode permettant de supprimer les longues séries de «1» dans les zones de données et de CRC.

Dans chaque octet transmis, le bit 0 est celui de plus faible poids et conformément à la spécification de la HDLC, il est émis le premier. Toutefois, à l'émission, l'octet de plus fort poids est le premier.

Après le drapeau de fin, la ligne HDLC revient au mode «repos».

START	MH	Messages à accès conditionnel	CRC	END
1 octet	2 octets	n octets	2 octets	1 octet

FIGURE 3/J.91

Structure de trame

Les 2 octets MH sont codés comme l'indiquent les Tableaux 1 et 2.

Il ne sera pas tenu compte des messages que le récepteur ne reconnaît pas.

En mode 3 de chiffrement (voir 12.7.3/J.81), plusieurs ECM précédés de leur en-tête de message associé peuvent être émis en une seule trame HDLC.

TABLEAU 1/J.91

Codage de l'en-tête de message dans le cas de messages à accès conditionnel

b_{16}	b_{15}	b_{14}	b_{13}	b_{12} b_7	b_6 b_1	Signification
0	0	0	0	RFU	Voir le Tableau 2	ECM
0	0	Autre valeur		RFU	Voir le Tableau 2	Réservé à 3 types spéciaux d'ECM au maximum
0	1	0	0	RFU	1 1 1 1 1 1	EMM-U
0	1	0	1	RFU	1 1 1 1 1 1	EMM-S
0	1	1	0	RFU	1 1 1 1 1 1	EMM-G
Toute autre valeur				RFU	1 1 1 1 1 1	Réservé à 9 autres types d'EMM au maximum
NOTE – Les bits b_{12} à b_7 sont réservés pour une utilisation future (RFU) et mis à 0.						

TABLEAU 2/J.91

Signification des bits b_6 à b_1 dans l'en-tête du message pour les ECM

b_6	b_5	b_4	b_3	b_2	b_1	Signification
0	0	0	0	0	0	RFU
0	X	X	X	X	1	L'élément T est concerné par l'ECM
0	X	X	X	1	X	L'élément A est concerné par l'ECM
0	X	X	1	X	X	L'élément T′ est concerné par l'ECM
0	X	1	X	X	X	L'élément A′ est concerné par l'ECM
0	1	X	X	X	X	L'élément V est concerné par l'ECM
Toute autre valeur						RFU

7.2 Contenu du message à accès conditionnel

7.2.1 Identificateur de commande (CI)

Tous les ECM et EMM contiennent un champ d'identification de commande à 8 bits (CI) qui décrit le format utilisé dans le champ de message et le type d'algorithme cryptographique mis en œuvre. Son codage est décrit dans la Figure 4.

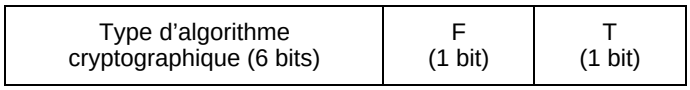

FIGURE 4/J.91

Codage de l'identificateur de commande (CI)

NOTES

1 Type d'algorithme cryptographique (6 bits) – Ce paramètre sert à identifier simultanément jusqu'à 64 types d'algorithmes cryptographiques. Seuls les messages d'un type qui coïncide avec celui du module de sécurité de l'usager peuvent être interprétés et traités par le module de sécurité de l'usager du récepteur.

2 F est un bit qui décrit le format du champ de données du message.

a) F = 1 – Le champ de données est structuré selon le format variable défini par EUROCRYPT.

b) F = 0 – Réservé pour une utilisation future.

3 T est le bit basculant – Il reste dans le même état tant que le contenu du message ne change pas. Il est utilisé dans les EMM-G et les ECM pour signaler que le contenu d'information de leur message a changé. Il n'a aucune signification pour les EMM-U et les EMM-S.

7.2.2 Contenu de l'ECM

L'ECM se présente comme indiqué à la Figure 5, avant son insertion dans une trame.

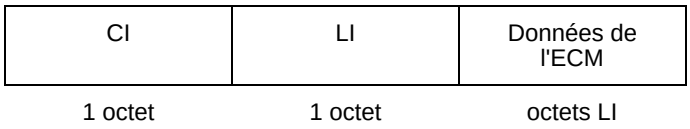

FIGURE 5/J.91

Message ECM

7.2.3 Contenu de l'EMM

L'EMM se présente comme indiqué à la Figure 6, avant son insertion dans la trame.

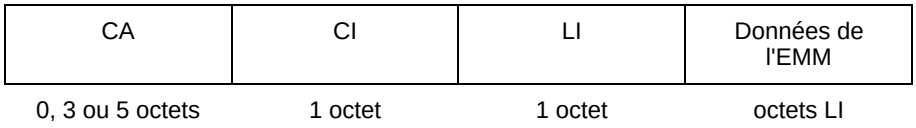

FIGURE 6/J.91

Message de l'EMM

Tous les EMM, sauf l'EMM-G, commencent par une adresse d'usager (CA). La longueur du champ CA est de:

- 40 bits pour l'EMM-U – Dans ce cas, les 4 premiers bits sont mis à 0 et les 36 derniers transportent l'UA (adresse unique);
- 24 bits pour l'EMM-S – Dans ce cas, la CA transporte les 24 bits de l'adresse partagée (SA).

8 Mise en œuvre pratique

Dans la pratique, les fonctions décrites ci-dessus peuvent être mises en œuvre de diverses façons, depuis l'établissement de mots de contrôle locaux par le seul biais de systèmes réservés à accès conditionnel pour de petits réseaux ou à configuration simple jusqu'à l'utilisation de systèmes à accès conditionnel bien définis, disponibles sur le marché et susceptibles d'être exploités dans un environnement de réseau ouvert ou encore lorsqu'il y a un nombre important d'abonnés du réseau et que la diversité des fonctions de contrôle d'accès nécessaires est grande.

L'Annexe A décrit l'exploitation avec mot de contrôle local. L'Annexe B décrit le système à accès conditionnel EUROCRYPT[2)] qui assure toutes les fonctions décrites dans le paragraphe ci-dessus; les annexes suivantes porteront sur d'autres systèmes qui pourraient être ajoutés par la suite.

Annexe A

Exploitation avec mot de contrôle local

(Cette annexe fait partie intégrante de la présente Recommandation)

A.1 Exploitation pratique avec mot de contrôle local

On peut utiliser des mots de contrôle locaux. Cela signifie qu'au point de télécommunication d'où part la transmission, le codeur n'utilise qu'un seul mot de contrôle pour toute la transmission. Ce mot de contrôle sera introduit dans le codeur par l'exploitant de l'émetteur. Afin de désembrouiller le signal au point de télécommunication où le signal est reçu, il faut que le décodeur reçoive le même mot de contrôle de la part de l'exploitant du récepteur.

Cette mise en œuvre suppose une nouvelle action spécifique de l'exploitant. Bien qu'elle soit bien moins sûre du point de vue du contrôle d'accès, elle serait en fait totalement indépendante des dispositifs de gestion et de contrôle et du CAD et pourrait facilement coexister avec un système de contrôle d'accès.

Annexe B

Exploitation avec EUROCRYPT[3)]

(Cette annexe fait partie intégrante de la présente Recommandation)

B.1 Introduction

La présente annexe décrit une mise en œuvre pratique qui recourt au système d'accès conditionnel normalisé EUROCRYPT bien défini où les fonctions des divers modules de sécurité sont assumées par la famille des cartes à mémoire PC2.

EUROCRYPT est un système à accès conditionnel normalisé par l'UTE (EN 50094, 1992) qui sert actuellement à contrôler l'accès aux signaux D2MAC/paquets. Il spécifie les ECM et les EMM.

La famille PC2 de cartes à mémoire consiste en modules de sécurité qui ont été mis au point en vue d'assurer les fonctions de sécurité d'EUROCRYPT. Il existe plusieurs catégories de cartes PC2 (voir la Figure B.2).

- Les cartes-mères PC2 de gestion assurent les fonctions des modules de gestion à haute sécurité.
- Les cartes-mères PC2 de contrôle assurent les fonctions des modules de contrôle à haute sécurité.
- Les cartes-filles PC2 assurent les fonctions des modules de sécurité de l'usager.

---

2) EUROCRYPT est normalisé par l'UTE (EN 50094, 1992).

3) EUROCRYPT est normalisé par l'UTE (EN 50094, 1992).

On distingue deux sortes d'implantations:

- le centre de gestion du réseau qui comprend un dispositif de contrôle et un dispositif de gestion;
- chaque point de télécommunication qui comprend un ou plusieurs dispositifs d'accès conditionnel.

Il n'y a qu'un seul centre de gestion du réseau par réseau. Il est responsable de la gestion des ressources du réseau, de l'attribution des canaux disponibles et de la synchronisation entre émetteurs et récepteurs.

Il y a plusieurs points de télécommunication. Chacun peut émettre ou recevoir simultanément un ou plusieurs programmes de TV embrouillés. En chacun de ces points, il se trouve au moins un dispositif d'accès conditionnel qui gère plusieurs émetteurs et récepteurs.

Les principales caractéristiques du système sont les suivantes:

- une gestion centralisée des échanges de programmes de TV;
- la possiblité de sélectionner et d'autoriser très rapidement les récepteurs, presque en temps réel;
- une interface homme-machine simple au centre de gestion du réseau et aux points de télécommunication;
- aucun besoin de liaison permanente entre le centre de gestion du réseau et les points de télécommunication;
- une très haute protection contre le piratage des programmes de TV transmis par des réseaux ouverts, comme les satellites.

En outre, les points de télécommunication qui ne sont pas directement reliés au centre de gestion du réseau sont néanmoins capables d'émettre ou de recevoir des programmes de TV embrouillés.

La Figure B.1 représente le réseau du point de vue du contrôle d'accès. Sur la Figure B.1 et dans le texte qui suit, on a abrégé l'expression centre de gestion du réseau en NMC et celle de dispositifs d'accès conditionnel en CAD.

Les cartes-mères PC2 ne sont nécessaires que dans le centre de gestion du réseau.

Une ou plusieurs cartes-filles servent à l'émission ou à la réception dans chaque point de télécommunication.

B.1.1 Programmes et transmissions

Il est important de préciser ce qui distingue une transmission d'un programme.

Une transmission se caractérise par:

- un satellite ou tout autre canal de télécommunication;
- un point de télécommunication qui sert d'émetteur;
- un ou plusieurs points de télécommunication qui sert (servent) de récepteur(s);
- une date et une heure de début et de fin;
- un ensemble de composantes de TV, y compris son(s), image et données.

Un programme se caractérise par:

- un nom de programme;
- une ou plusieurs transmissions;
- une clé d'autorisation;
- un ou plusieurs critères d'accès.

Une transmission peut donc servir à diffuser un ou plusieurs programmes et un programme peut être transmis au moyen d'une ou plusieurs transmissions.

Il faut considérer trois sortes d'activités:

- l'activité du centre de gestion du réseau;
- l'activité de l'émetteur d'un point de télécommunication quand on utilise un de ses codeurs;
- l'activité du récepteur d'un point de télécommunication quand on utilise un de ses décodeurs.

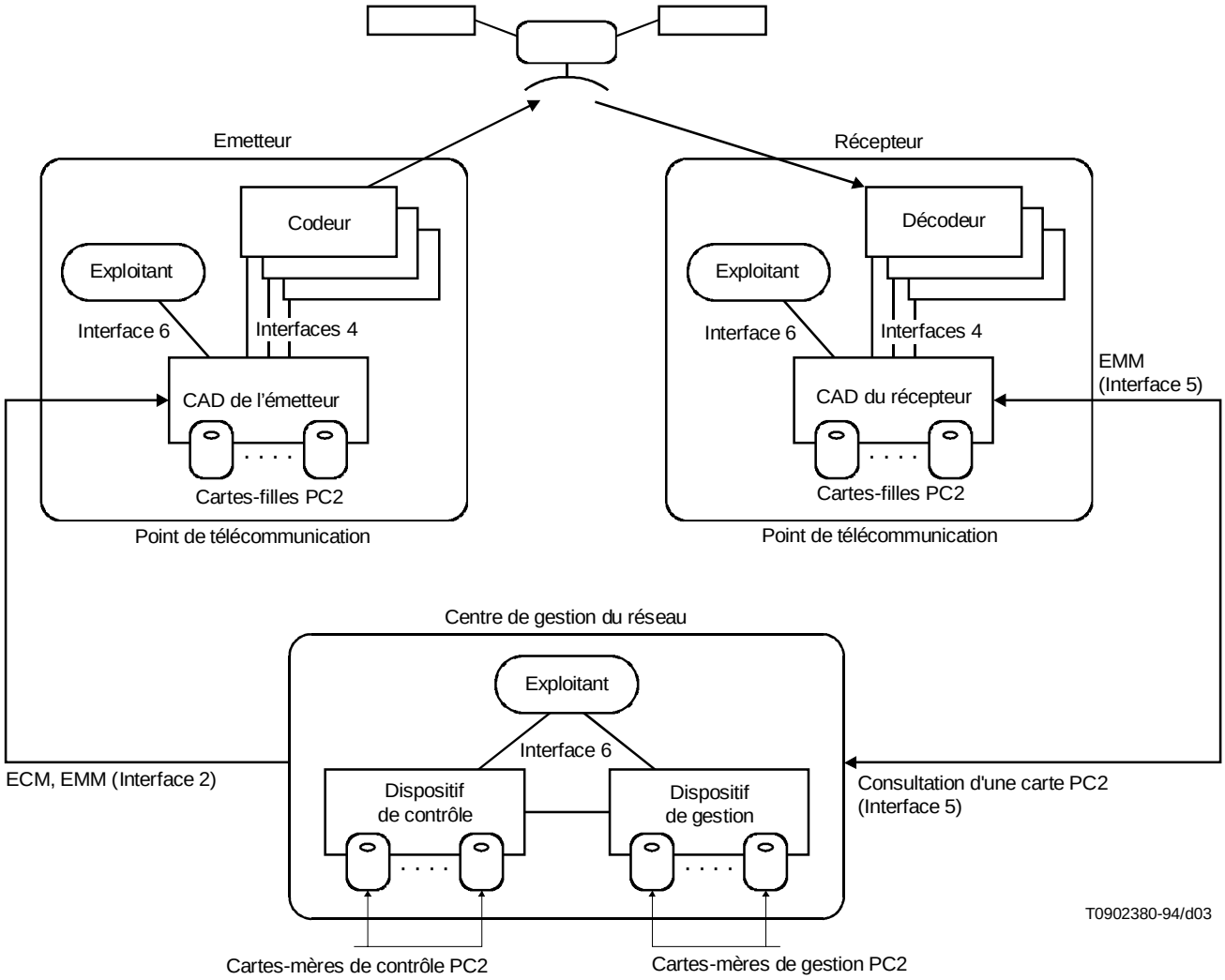

FIGURE B.1/J.91

Architecture du réseau

B.2 Fonctions du centre de gestion du réseau (NMC)

Il incombe au NMC d'assurer que l'émetteur et tous les récepteurs autorisés reçoivent la clé d'autorisation et les titres d'accès appropriés avant la transmission du programme. Le NMC est aussi responsable de la mise à jour régulière, pour raison de sécurité, des clés d'autorisation. A cet effet, il produit et envoie les ECM et les EMM.

Le NMC contrôle aussi l'envoi de toutes les cartes à mémoire du système et supervise toutes les cartes-filles.

Le schéma du NMC est représenté sur la Figure B.2.

B.2.1 Production des ECM

Le NMC doit produire les ECM. A cette fin, il produit des mots de contrôle, les chiffre au moyen d'une carte-mère et crée l'ECM correspondant. Chaque ECM est protégé par un total de contrôle cryptographique calculé par la carte-mère. Au cours de la transmission, on utilise un nouvel ECM toutes les 8,2 secondes. Les ECM sont envoyés au CAD de l'émetteur via l'interface 2.

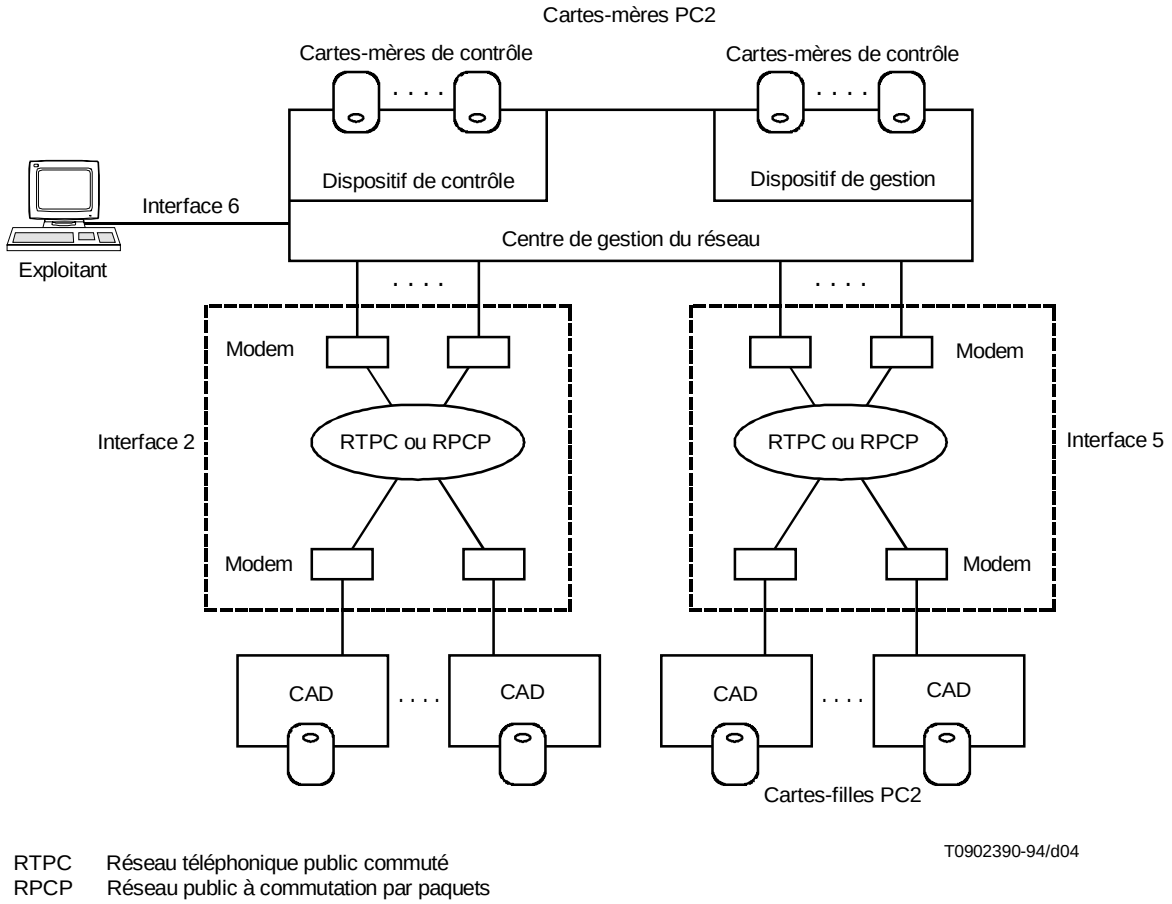

FIGURE B.2/J.91

Centre de gestion du réseau (NMC)

Pour permettre une mise en œuvre simple de ce principe, on crée régulièrement des ECM qu'on envoie «en ligne» au CAD de l'émetteur. Cela signifie que le NMC doit rester relié au CAD de l'émetteur pendant toute la durée de la transmission. En outre, le NMC qui pilote tous les émetteurs devra produire plusieurs jeux d'ECM (autant que de canaux en fonctionnement à ce moment-là) et les envoyer en même temps.

Cette contrainte est abolie par le recours à des fichiers cycliques d'ECM. Ces fichiers contiennent autant d'ECM qu'il en faudra pour la durée prévue de la transmission. Si la transmission déborde, le dernier ECM est composé de telle sorte qu'il puisse être suivi du premier ECM du même fichier afin de pouvoir parcourir en boucle le même ensemble d'ECM. Avec les ECM d'EUROCRYPT, un fichier de 16 k octets procure des ECM pour un programme d'environ une heure.

Le NMC peut produire un jeu de fichiers cycliques d'ECM avant qu'on y fasse appel et les envoyer au CAD en avance, ou au dernier moment avant une transmission.

En envoyant à l'avance plusieurs fichiers cycliques d'ECM au CAD, on le rend capable de fonctionner presque immédiatement, même dans le cas d'une transmission TV inattendue (décidée à la dernière minute) ou d'un émetteur transportable isolé.

B.2.2 Production des EMM

Le NMC doit aussi produire des EMM pour distribuer les clés et les titres d'accès à des cartes-filles spécifiées.

Il y a un EMM pour l'émetteur: il doit permettre au CAD de l'émetteur (avec l'aide de la carte-fille) de déchiffrer le mot de contrôle de tous les ECM ci-dessus.

Les autres EMM sont destinés aux récepteurs. Les cartes-filles autorisées des CAD des récepteurs peuvent ainsi déchiffrer le mot de contrôle des ECM ci-dessus. Il y a deux façons distinctes de transmettre les EMM.

- Ils peuvent être transmis directement au moyen de l'interface 5 (par téléphone, X.25, liaison directe) vers le CAD intéressé de chaque récepteur.
- Ils peuvent être diffusés à tous les récepteurs via le codeur de l'émetteur et le canal du satellite.

Deux catégories d'EMM sont définies: les EMM-U et les EMM-S.

Un EMM-U contient l'adresse propre à une seule carte-fille. Pour distribuer un titre d'accès donné à *n* cartes-filles, il faudra donc calculer et transmettre *n* EMM-U.

Un EMM-S contient l'adresse partagée par un groupe de cartes-filles. Un EMM-S peut s'adresser jusqu'à 256 cartes-filles, qui partagent la même clé de gestion. Grâce à l'EMM-S, on diminue le nombre d'EMM qu'il faut produire et transmettre pour une transmission de TV.

B.2.3 Contrôle des cartes-filles

Le NMC gère le contenu de chaque carte-fille.

En cas de paiement par impulsions à la durée, le NMC examine les achats de cartes-filles.

Il y a une base de données qui contient la teneur de toutes les cartes à mémoire et les informations sur tous les CAD (emplacement, cartes à mémoire, etc.).

Si une carte-fille n'a plus de mémoire disponible, le NMC doit nettoyer la mémoire en retirant les clés et les titres d'accès périmés. Si cette opération n'est pas possible (carte PC2-1), le NMC demande à son exploitant et à celui du CAD de changer la carte-fille.

B.2.4 Production de cartes à mémoire

Le NMC crée des scénarios de production (description de toutes les clés et de tous les paramètres à inscrire sur chaque carte) à la demande de son exploitant. Ces scénarios sont envoyés à un appareil de production qui émet les cartes. Cet appareil renvoie au NMC un ensemble de cartes et un rapport. Ce rapport sert à mettre à jour la base de données du NMC.

B.2.5 Interface homme-machine

L'interface homme-machine doit comprendre:

- une demande de transmission;
- une description de toutes les références de transmission décrites ci-dessus;
- une consultation et une mise à jour de la base de données;
- un examen périodique des cartes conçues pour paiement à la durée par impulsions;
- un relevé des alarmes (une carte à mémoire est pleine ou hors d'usage, il y a un problème de liaison avec un CAD).

B.3 Mise en œuvre des CAD

L'activité du CAD de l'émetteur comprend:

- la transmission du ou des EMM appropriés à leur(s) carte(s)-mère(s) afin de stocker une (de) nouvelle(s) clé(s) et une (de) nouveaux titre(s) d'accès;
- la transmission régulière (toutes les 8,2 secondes) d'un ECM à sa carte-fille afin de recevoir en retour le CW correspondant qu'il faut donner au codeur pour embrouiller le programme de TV;
- la transmission régulière (toutes les secondes) au décodeur d'un ECM à diffuser aux décodeurs (via le canal CA1 dans le multiplex à 34 Mbit/s);
- si besoin est, la transmission également des EMM au codeur pour envoi aux décodeurs (via le canal CA1 dans le multiplex à 34 Mbit/s).

L'activité du CAD du récepteur comprend:

- l'obtention des EMM appropriés à partir du décodeur ou de la liaison directe avec le NMC et la transmission de cet EMM à sa ou ses carte(s)-fille(s) afin de stocker une (de) nouvelle(s) clé(s) et un (de) nouveau(x) titre(s) d'accès;
- l'obtention régulière d'ECM à partir du décodeur et leur envoi à leur carte-fille afin d'avoir en retour les mots de contrôle correspondants qui seront renvoyés au décodeur.

L'architecture du CAD est représentée sur la Figure B.3.

Les ECM et les EMM transmis sur le canal CA1 peuvent être protégés par un code de Golay. Dans ce cas, l'émetteur doit, avant l'émission, protéger ces messages par un code de Golay et, à la réception, chaque récepteur doit corriger les messages avant de continuer à les traiter.

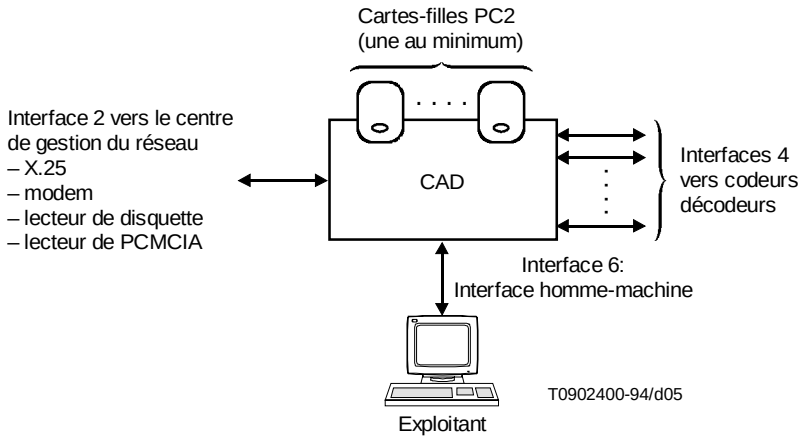

FIGURE B.3/J.91

Architecture du CAD

B.3.1 Cas d'une station d'émission isolée

«Isolée» veut dire qu'il n'y a pas de liaison entre le CAD de l'émetteur et le NMC au moment de la transmission. Cela peut se produire, par exemple, pour un groupe de reportage où la station d'émission est très mobile. Tout émetteur doit être capable de fonctionner dans ces conditions en cas d'urgence.

Dans ce contexte, il est tout de même possible de protéger la transmission de programmes TV. A cette fin, le CAD de l'émetteur doit à l'avance être chargé avec un fichier cyclique d'ECM (au moyen d'une disquette ou d'une carte à mémoire PCMCIA). L'exploitant de l'émetteur n'a plus alors qu'à choisir le fichier ECM cyclique approprié.

Ce mode convient parfaitement en cas de paiement à la durée par impulsions. Les cartes-filles des récepteurs garderont automatiquement le nombre de programmes (avec l'accord de l'exploitant du récepteur). Le NMC examinera ultérieurement le contenu des cartes.

B.4 Mise en œuvre de l'interface 2

L'interface 2 relie le NMC au CAD de l'émetteur. L'initialisation se fait par le NMC.

Les messages et ordres suivants sont échangés:

- ECM – Pour la mise en œuvre, on recommande un fichier cyclique d'ECM que calcule le NMC et qui est transmis à l'avance au CAD de l'émetteur en même temps que la référence du programme TV qui utilisera ces ECM. On peut aussi envoyer «en ligne» un ECM toutes les 8,2 secondes.
- EMM – Pour la mise en œuvre, on recommande un fichier d'EMM que calcule le NMC et qui est transmis à l'avance au CAD de l'émetteur. On peut aussi se servir de l'interface 5 pour s'adresser à chaque récepteur.

L'interface 2 peut être mise en œuvre sur le réseau téléphonique public commuté ou sur le réseau public à commutation par paquets ou même sur une disquette ou une carte à mémoire PCMCIA.

B.5 Mise en œuvre de l'interface 5

L'interface 5 relie le NMC à une carte-fille, via un CAD. L'initialisation se fait par le CAD.

Elle sert surtout à contrôler les cartes-filles reliées au CAD. Ce contrôle des cartes consiste en:

- un examen des paiements à la durée par impulsions stockées sur la carte;
- un nettoyage de l'EEPROM de la carte (cartes PC2-2 seulement). Si une carte n'a plus de mémoire disponible, le NMC supprime les anciennes autorisations. Si le nettoyage n'est pas possible (cartes PC2 1), le NMC conseille à son exploitant et à l'exploitant du CAD de changer la carte-fille.

En outre, comme cela a déjà été indiqué, l'interface 5 peut servir à envoyer des EMM.

L'interface 5 peut être mise en œuvre avec le réseau téléphonique public commuté ou le réseau public à commutation par paquets.

L'information d'ouverture de la session est stockée sur la carte-fille dans un bloc de service ad hoc. L'appel se déclenche sous l'action du CAD à la réception d'un EMM de démarrage du modem (voir les spécifications d'EUROCRYPT, § 11 de l'Appendice 2).

B.6 Illustration du système qui emploie les caractéristiques d'EUROCRYPT

Pour calculer les mots de contrôle à partir d'un fichier cyclique d'ECM associés à une transmission donnée, la carte-fille PC2 du récepteur doit contenir la clé d'autorisation correcte et au moins un titre d'accès valable. Les clés et les titres d'accès sont définis par le NMCr qui émet des EMM pour autoriser les cartes appropriées. A cette fin, le NMC a le choix entre les divers modes d'exploitation décrits ci-dessous.

Les abréviations qui figurent dans le texte suivant et qui représentent le contenu des ECM et des EMM sont définies par EUROCRYPT (EN 50094, 1992) avec des détails supplémentaires sur l'utilisation des EMM-U et des EMM-S.

B.6.1 Possibilité de contrôle d'accès par mise à jour de la clé d'autorisation

Les clés d'autorisation de toutes les cartes concernées peuvent être mises à jour avant chaque nouveau programme. L'EMM-U ci-après est destiné à mettre à jour une clé d'autorisation dans une carte adressée par une UA:

EMM-U (37 octets): UA, CI LI, PI LI PPID, PI LI IDUP, PI LI clé chiffrée, PI LI HASH

B.6.2 Possibilité de contrôle d'accès par abonnement

Le NMC peut envoyer des abonnements à des cartes sélectionnées. Une carte d'abonnement permet l'accès à une catégorie de programmes pour un certain temps. L'EMM-U ci-après est destiné à munir d'un abonnement une carte adressée par une UA:

EMM-U (30 octets): UA, CI LI, PI LI PPID, PI LI DATES+TH/LE, PI LI HASH

B.6.3 Possibilité de contrôle d'accès par numéro de programme

Le NMC peut associer un numéro à chaque programme (PNUMB). L'EMM-U ci-après est destiné à munir la carte adressée par UA d'un titre d'accès pour un ou plusieurs numéros de programme à venir:

EMM-U (30 octets): UA, CI LI, PI LI PPID, PI LI INUMB+FNUMB, PI LI HASH

On peut aussi utiliser un ou plusieurs EMM-S précédés d'un EMM-G. Une SA peut s'adresser à un groupe pouvant atteindre 256 cartes. Dans chaque groupe chaque carte a un rang, de 1 à 256. Dans un groupe, une carte donnée accepte ou refuse l'action selon que le ième bit de l'ADF vaut 1 ou 0:

EMM-G (15 octets): CI LI, PI LI PPID, PI LI INUMB+FNUMB

EMM-S (79 octets): SA, CI LI, ADF, PI LI HASH

Avec seulement un EMM-G + EMM-S, il est possible d'envoyer un titre d'accès sélectif à un groupe de 256 cartes. Ce mode est très intéressant pour les programmes qui sont annoncés longtemps avant leur émission.

B.6.4 Possibilité de contrôle d'accès par paiement à la durée par impulsions pour un numéro de programme

Dans ce cas, les récepteurs n'ont pas besoin d'EMM. Tous les récepteurs envisageables qui ont la clé d'autorisation voulue peuvent désembrouiller le programme en mode paiement à la durée (avec l'accord de l'exploitant du récepteur). La carte garde en mémoire la manœuvre de l'exploitant. Ce mode est très intéressant pour des transmissions urgentes.

B.6.5 ECM avec les trois derniers critères d'accès

On peut utiliser à la fois plusieurs modes d'accès pour le même programme. Plusieurs types de récepteurs ont alors accès au même programme:

- les abonnés ont un accès par abonnement;
- les usagers qui ont réservé ont un accès selon le numéro du programme;
- les abonnés de dernière minute peuvent avoir accès à un numéro de programme par paiement à la durée par impulsions.

L'ECM suivant propose un accès par abonnement, réservation ou paiement à la durée par impulsions. La carte examine dans l'ordre les critères d'accès jusqu'à ce qu'elle trouve un titre d'accès valable:

ECM (53 octets): CI LI, PI LI PPID, PI LI DATE+TH/LE, PI LI PNUMB, PI LI PNUMB+PPV-P, PI LI ECW/OCW, PI LI HASH

Annexe C

Exploitation avec d'autres systèmes

Cette annexe appelle un complément d'étude.