UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.96

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2001)

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

Services numériques auxiliaires propres aux transmissions télévisuelles

Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89

Recommandation UIT-T J.96

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE J

RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Recommandations générales	J.1–J.9
Spécifications générales des transmissions radiophoniques analogiques	J.10–J.19
Caractéristiques de fonctionnement des circuits radiophoniques analogiques	J.20–J.29
Equipements et lignes utilisés pour les circuits radiophoniques analogiques	J.30–J.39
Codeurs numériques pour les signaux radiophoniques analogiques	J.40–J.49
Transmission numérique de signaux radiophoniques	J.50–J.59
Circuits de transmission télévisuelle analogique	J.60–J.69
Transmission télévisuelle analogique sur lignes métalliques et interconnexion avec les faisceaux hertziens	J.70–J.79
Transmission numérique des signaux de télévision	J.80–J.89
Services numériques auxiliaires propres aux transmissions télévisuelles	**J.90–J.99**
Prescriptions et méthodes opérationnelles de transmission télévisuelle	J.100–J.109
Services interactifs pour la distribution de télévision numérique	J.110–J.129
Transport des signaux MPEG-2 sur les réseaux par paquets	J.130–J.139
Mesure de la qualité de service	J.140–J.149
Distribution de la télévision numérique sur les réseaux locaux d'abonnés	J.150–J.159
IPCablecom	J.160–J.179
Divers	J.180–J.199
Application à la télévision numérique interactive	J.200–J.209

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

Recommandation UIT-T J.96

Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89

Résumé

La présente Recommandation constitue une norme commune relative à un système à accès conditionnel pour la transmission internationale longue distance de télévision numérique conformément au profil professionnel MPEG (4:2:2).

Elle contient par ailleurs une Annexe A qui décrit des mises en œuvre pratiques.

Source

La Recommandation J.96 de l'UIT-T, élaborée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 9 mars 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T J.96

Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89

1 Domaine d'application

La présente Recommandation constitue une norme commune relative à un système à accès conditionnel pour la transmission internationale longue distance de télévision numérique conformément au profil professionnel MPEG (4:2:2).

Elle contient par ailleurs une Annexe A qui décrit des mises en œuvre pratiques.

2 Références

2.1 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

[1] UIT-T H.222.0 (2000) | ISO/CEI 13818-1:2000, *Technologies de l'information – Codage générique des images animées et du son associé: systèmes*.

[2] ETSI ETR 162 (1995), *Allocation of Service Information (SI) codes for DVB systems*.

[3] ETSI ETR 289 (1996), *Digital Video Broadcasting (DVB); Support for use of scrambling and conditional access (CA) within digital broadcasting systems*.

[4] ETSI EN 300 468, *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*.

[5] UIT-T J.81 (1993), *Transmission des signaux de télévision numériques codés en composantes pour les applications de qualité contribution au troisième niveau de la hiérarchie numérique de la Recommandation UIT-T G.702*.

[6] UIT-T J.89 (1999), *Mécanisme de transport des signaux de télévision numérique codés en composantes, utilisant le profil MPEG-2 4:2:2 P@ML avec tous les éléments de service pour les liaisons de contribution et la distribution primaire*.

[7] UER Tech3290 (2000), *Basic Interoperable Scrambling System (BISS)*.

2.2 Référence bibliographique

– OKAPI: BOUCQUEAU (J.M.), SERRET (J.), QUISQUATER (J.J.) et MACQ (B.): "*Security in Multimedia Teleservices*" *in Multimedia Telecommunications Services*; *Cost 237 – Final Report, Springer,* septembre 1999, pp. 348–373.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

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

3.2 désembrouillage: restauration des caractéristiques d'un signal image/son/données afin de 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

La présente Recommandation utilise les abréviations suivantes:

3DES	algorithme DES triple (*triple DES*)
ABC	clés DES A, B et C (*DES keys A, B, C*)
ACS	système de contrôle d'accès (*access control system*)
Bit	contraction, en anglais, des mots "binary digit", signifiant chiffre binaire
bslbf	chaîne binaire, bit de gauche en premier (*bit string, left bit first*)
CA	accès conditionnel (*conditional access*)
CAT	table d'accès conditionnels (*conditional access table*)
CD	dispositif de contrôle (*controller device*)
CK	clé commune (*common key*)
CSA	algorithme commun d'embrouillage (*common scrambling algorithm*)
CW	mot de contrôle (*control word*)
DES	algorithme normalisé de cryptage de données (*data encryption standard*)
ECB	répertoire de codes électroniques (*electronic codebook*)
ECM	message de contrôle des titres d'accès (*entitlement control message*)
EDE	codage, décodage, codage (*encode, decode, encode*)
EMM	message de gestion des titres d'accès (*entitlement management message*)
KE	clé sous seing privé (*key escrow*)
lsb	bit de plus faible poids (*least significant bit*)
LSB	octet de plus faible poids (*least significant byte*)
MD	dispositif de gestion (*manager device*)
MH	en-tête de message (*message header*)
mot	groupe ou séquence de bits traités ensemble
msb	bit de plus fort poids (*most significant bit*)
MSB	octet de plus fort poids (*most significant byte*)
NMC	centre de gestion de réseau (*network management centre*)
Octet	séquence de 8 bits traitée comme un groupe ou un mot de données

OKAPI noyau ouvert pour l'accès à des services interactifs interopérables protégés (*open kernel for access to protected interoperable interactive services*)

PCMCIA Personal Computer Memory Card International Association

PKI infrastructure de clés publiques (*public key infrastructure*)

PMT table de mappage de programmes (*program map table*)

PRG générateur (de séquence) pseudo-aléatoire [*pseudo-random (sequence) generator*]

PSI information propre à un programme (*program specific information*)

RAS reportage d'actualités par satellite

RASN RAS numérique

RPCP réseau public à commutation de paquets

RTPC réseau téléphonique public commuté

SAM module d'autorisation d'embrouillage (*scrambling authorization module*)

SK clé de session (*session key*)

SM module de sécurité (*security module*)

SW mot de session (*session word*)

TTP tiers de confiance (*trusted third party*)

uimsbf entier non signé, bit de plus fort poids en premier (*unsigned integer, most significant bit first*)

5 Aperçu général du système

L'UIT-T J.89, qui définit le mécanisme de transport des signaux de télévision numérique codés en composantes, utilisant le profil MPEG-2 4:2:2 P@ML avec tous les éléments de service, est maintenant largement utilisée pour la contribution et la distribution primaire ainsi que pour les applications RAS (par exemple UIT-R SNG.1421).

Un système à accès conditionnel, nécessaire pour garantir la confidentialité dans la transmission internationale longue distance de télévision, est utilisé pour permettre aux utilisateurs autorisés de désembrouiller les composantes d'un service. En outre, pour les applications RAS, un système simplifié fondé sur une clé fixe peut être nécessaire.

Les informations nécessaires au désembrouillage peuvent être introduites manuellement dans le décodeur – "mot de contrôle" local fixe (Partie A de la Figure 1) ou mots de contrôle locaux variables pré-enregistrés auxquels on accède via un mot de passe ou une clé de session (Partie B de la Figure 1) – ou fournies par le système à accès conditionnel décrit sommairement dans la Partie C de la Figure 1.

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

La présente Recommandation utilise l'algorithme commun d'embrouillage DVB, y compris la modification destinée aux applications RASN. Pour pouvoir utiliser l'algorithme, il faut signer un accord de non-divulgation auprès de l'ETI et acquitter une redevance unique (pour plus de détails, allez à www.etsi.org et cliquez sur **security algoritms and codes** sous le titre **Publication and Products**.

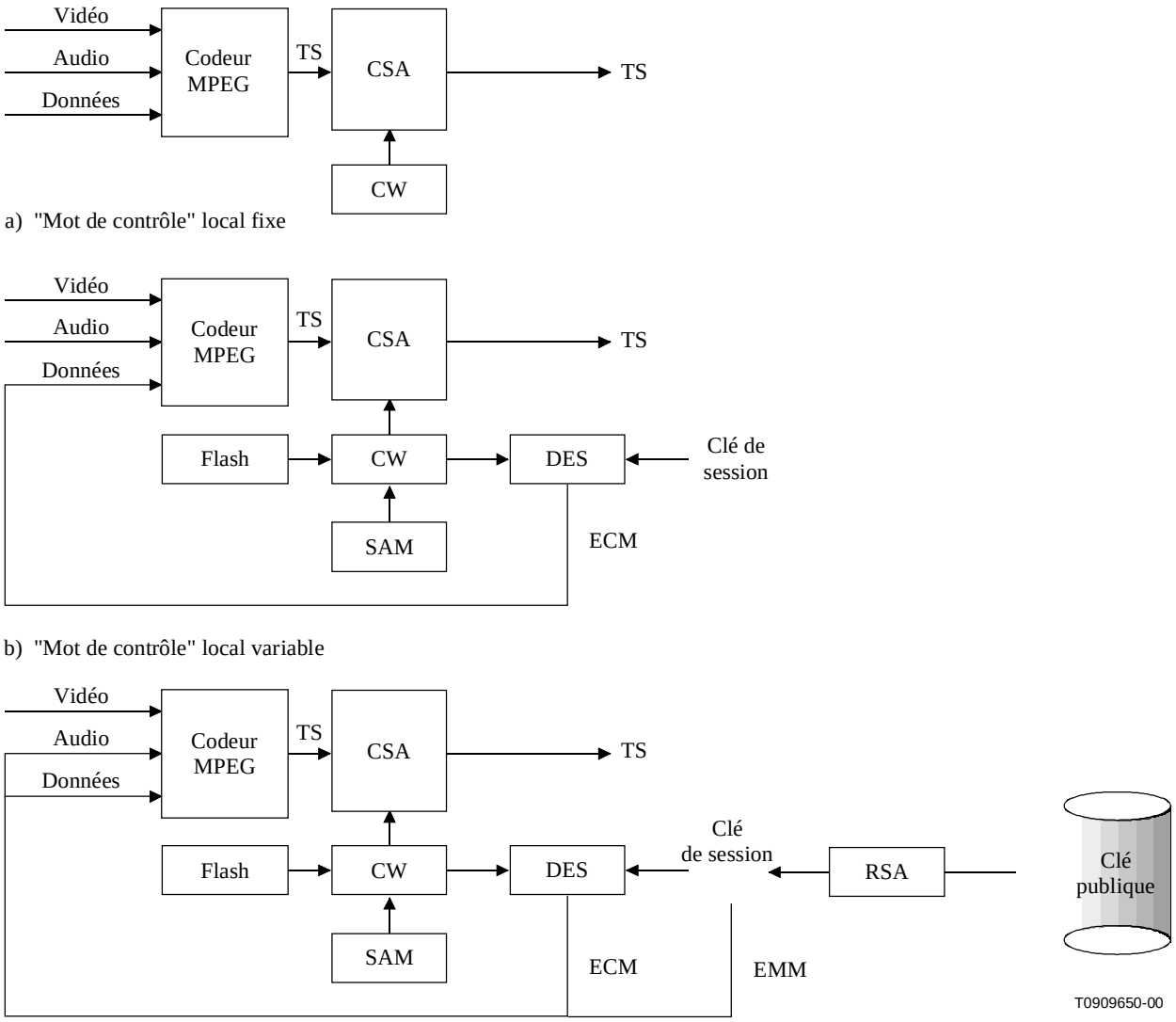


Figure 1/J.96 – Description générale des processus d'embrouillage/désembrouillage

Les trois mises en œuvre illustrées dans la Figure 1 sont décrites dans les Annexes A et B.

6 Application dans l'environnement MPEG/DVB

Embrouillage

L'embrouillage est un processus utilisé pour rendre une information incompréhensible aux récepteurs non autorisés pendant la transmission de cette information.

L'algorithme CSA utilise des clés communes pour initialiser le processus d'embrouillage/ désembrouillage à chaque paquet de transport. Ces clés communes sont émises à partir de mots de contrôle (CW) envoyés dans le flux.

L'embrouillage peut être effectué au niveau transport ou au niveau des paquets PES.

Les mots de contrôle peuvent changer dans le temps, avec une période appelée "période cryptographique". Afin de synchroniser les récepteurs, ils sont désignés par "CW impair" ou "CW pair". Chaque paquet embrouillé indique, par l'utilisation de bits "transport_scrambling_control" (contrôle d'embrouillage pour le transport), s'il est embrouillé ou non

et si le mot de contrôle courant est pair ou impair. La période cryptographique peut varier de quelques secondes (grand système CAS) à la durée d'une transmission complète ("mot de contrôle fixe" pour le reportage RASN).

Accès conditionnel

Un système à accès conditionnel (CAS, *conditional access system*) est composé d'outils permettant aux récepteurs autorisés d'obtenir des mots de contrôle afin de désembrouiller les informations.

Ces outils sont généralement des message de contrôle des titres d'accès (ECM) et des messages de gestion des titres d'accès (EMM) qui sont diffusés dans le flux de transport. La syntaxe de la partie privée des messages ECM et EMM dépend du système CAS.

Un message ECM contient généralement un cryptogramme de mots de contrôle et des critères d'accès. Son contenu varie avec une période égale à la période cryptographique.

Pour le reportage RASN, si le mot de contrôle est constant pour une transmission donnée, le message ECM peut être remplacé par n'importe quel moyen hors-bande pour préciser quel mot de contrôle sera utilisé pendant l'ensemble de la transmission.

6.1 Spécifications MPEG et ETR 289

6.1.1 Embrouillage

Le groupe MPEG a défini les bits Transport_Scrambling_Control des en-têtes de paquet de transport. Le Document ETR 289 [3] contient une spécification de ces bits, reproduite dans le Tableau 1:

Tableau 1/J.96 – Valeurs de transport_scrambling_control

Valeur	Description
00	Pas d'embrouillage de la charge utile du paquet TS
01	Réservée à une utilisation future par le groupe DVB
10	Paquet TS embrouillé avec une clé paire
11	Paquet TS embrouillé avec une clé impaire

NOTE – En Europe, tous les systèmes CAS doivent utiliser cet algorithme (disponible à l'ETSI qui en est le dépositaire sur la base d'un accord de non-divulgation).

6.1.2 PSI/SI

L'ISO a défini un identificateur PID = 0x01 réservé à la table d'accès conditionnels (CAT). Le contenu de cet identificateur est utilisé par le récepteur pour trouver des identificateur PID EMM.

La syntaxe de la table CAT est donnée dans le Tableau 2 (Tableau 2-27, référence [1]).

Tableau 2/J.96 – Tableau d'accès conditionnel

Syntaxe	Nombre de bits	Mnémonique
CA_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
reserved	**18**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
CRC_32	**32**	**rpchof**
}		

La syntaxe de CA_Descriptor (descripteur d'accès conditionnel) est donnée dans le Tableau 3 (Tableau 2-51, référence [1]).

Tableau 3/J.96 – Descripteur d'accès conditionnel

Syntaxe	Nombre de bits	Mnémonique
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
for (i = 0; i < N; i++) {		
private_data_byte	**8**	**uimsbf**
}		
}		

L'ISO a défini la table de mappage de programmes (PMT) dans laquelle les descripteurs CA_Descriptor peuvent être utilisés par les récepteurs pour trouver des identificateurs PID ECM. Voir Tableau 4 (Tableau 2-28, référence [1]).

Tableau 4/J.96 – Table de mappage de programmes

Syntaxe	Nombre de bits	Mnémonique
TS_program_map_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
'0'	**1**	**bslbf**
reserved	**2**	**bslbf**
section_length	**12**	**uimsbf**
program_number	**16**	**uimsbf**
reserved	**2**	**bslbf**
version_number	**5**	**uimsbf**
current_next_indicator	**1**	**bslbf**
section_number	**8**	**uimsbf**
last_section_number	**8**	**uimsbf**
reserved	**3**	**bslbf**
PCR_PID	**13**	**uimsbf**
reserved	**4**	**bslbf**
program_info_length	**12**	**uimsbf**
for (i = 0; i < N; i++) {		
descriptor()		
}		
for (i = 0; i < N1; i++) {		
stream_type	**8**	**uimsbf**
reserved	**3**	**bslbf**
elementary_PID	**13**	**uimsnf**
reserved	**4**	**bslbf**
ES_info_length	**12**	**uimsbf**
for (i = 0; i < N2; i++) {		
descriptor()		
}		
}		
CRC_32	**32**	**rpchof**
}		

Le document EN 300 468 [4] contient la spécification d'un bit free_CA_mode (mode d'accès conditionnel libre) dans la table de description de service (SDT, *service description table*) et dans la table d'information sur les événements (EIT, *event information table*). Ce bit doit être mis à 1 lorsque l'accès à au moins une composante est contrôlé par un système à accès conditionnel (voir § 5.2.4, référence [4]).

6.1.3 Messages relatifs à l'accès conditionnel

La syntaxe pour la table de messages CA et les valeurs de Table_Id (identificateur de table) sont données dans les Tableaux 5 et 6 (Tableaux 3 et 4 respectivement, référence [4]). La valeur de CA_section_length est limitée à 253 (longueur maximale de section = 256 octets).

Tableau 5/J.96 – Syntaxe de la table de messages CA (CMT)

Syntaxe	Nombre de bits	Identificateur
CA_message_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
DVB_reserved	**1**	**bslbf**
ISO_reserved	**2**	**bslbf**
CA_section_length	**12**	**uimsbf**
for(i=0; I<N; i++) {		
CA_data_byte	**8**	**bslbf**
}		
}		

Tableau 6/J.96 – Attribution des identificateurs de table

Valeur de table_id	Description
0x00 – 0x02	Spécifiées pour le groupe MPEG
0x03 – 0x3F	Réservées pour le groupe MPEG
0x40 – 0x72	Spécifiées pour le V2-SI
0x73 – 0x7F	Réservées pour le groupe DVB
0x80	CA_message_section, ECM
0x81	CA_message_section, ECM
0x82 – 0x8F	CA_message_section, valeurs privées du système CA
0x90 – 0xFE	Privées
0xFF	Réservées pour l'ISO

6.2 Spécifications relatives au reportage RASN

Dans ce qui suit, on se fonde sur les quatre modes définis dans UIT-T J.81:

– mode 0: pas d'embrouillage;

– mode 1: les composantes sont embrouillées avec un mot de contrôle fixe unique;

– mode 2: toutes les composantes du programme sont embrouillées avec un mot de contrôle unique;

– mode 3: les composantes sont embrouillées avec plusieurs mots de contrôle.

Un identificateur CA_System_Id (identificateur de système à accès conditionnel) doit être fourni par l'ETSI avec une valeur comprise entre 0x1 et 0xff (systèmes CA normalisés) conformément à la référence [2].

Dans les modes 1 à 3, l'embrouillage sera appliqué au niveau TS.

Dans tous les modes, les messages ECM ou EMM, s'ils sont présents, seront conformes à la référence [3], en ce qui concerne la longueur maximale de section de 256 octets, la syntaxe de la section et les valeurs d'identificateur table_id.

6.2.1 Mode 0

Il n'y a pas d'embrouillage. Les deux bits Transport_Scrambling_Control sont mis à zéro.

Une table CAT et un flux EMM peuvent être présents si nécessaire pour transmettre des droits pour des programmes prévus dans l'un des modes 1 à 3 (contenu à définir).

Il n'y a pas de descripteur CA_descriptor dans la table PMT et pas de message ECM dans le flux.

6.2.2 Mode 1

Le premier bit Transport_Scrambling_Control est mis à 1. Le second peut varier aux frontières d'événement pendant la transmission. Le mot de contrôle utilisé appartient à une liste de mots de contrôle présents dans l'équipement d'embrouillage et de désembrouillage.

Une table CAT et un flux EMM peuvent être présents si nécessaire.

Un descripteur CA_descriptor et un seul est présent dans la table PMT au niveau programme. Un exemple est donné ci-dessous:

Syntaxe	Nombre de bits	Mnémonique
CA_descriptor() {		
descriptor_tag = 0x09	**8**	**uimsbf**
descriptor_length = 0x07	**8**	**uimsbf**
CA_system_ID = 0x0001 to 0x00ff (t.b.d)	**16**	**uimsbf**
reserved	**3**	**bslbf**
CA_PID = dummy value	**13**	**uimsbf**
Mode_id = 0x01	**8**	**uimsbf**
Odd_CW_index	**8**	**uimsbf**
Even_CW_index	**8**	**uimsbf**
}		

Mode_id = 0x01 indique au récepteur qu'il n'a pas besoin de recevoir de message ECM (dans ce mode, aucun message ECM n'est présent, l'identificateur CA_PID a une valeur fictive) et que les octets suivants donnent l'indice CW_index (indice de mot de contrôle).

Les indices Odd_CW_index (indice de mot de contrôle impair) et Even_CW_index (indice de mot de contrôle pair) sont utilisés pour sélectionner un mot de contrôle dans la liste des mots de contrôle enregistrés dans le récepteur.

Toute modification de la valeur de l'indice CW_index sera signalée par un nouveau numéro de version dans la table PMT. Un traitement correct des mots de contrôle pairs et impairs peut autoriser la "modification" du mot de contrôle "fixe" aux frontières d'événement avec des transitions transparentes ou la modification d'une liste de mots de contrôle dans le récepteur et l'embrouilleur (liste courante, liste suivante).

6.2.3 Modes 2 et 3

Le premier bit Transport_Scrambling_Control est mis à 1. Le second varie pendant la transmission et indique au désembrouilleur quel type de mot de contrôle est utilisé (impair ou pair).

Une table CAT et un flux EMM peuvent être présents si nécessaire.

Un descripteur CA_descriptor peut être présent dans la table PMT au niveau programme, donnant un identificateur ECM_pid pour toutes les composantes du programme. D'autres descripteurs CA_descriptor peuvent être présents au niveau composante. Dans ce cas, la valeur d'un tel

descripteur annule et remplace la valeur qui a été spécifiée au niveau programme, uniquement pour la composante concernée.

Exemple 1: mode 2, toutes les composantes sont embrouillées avec le mot de contrôle CW1:

– soit un descripteur CA_Desc est présent au niveau programme avec l'identificateur ECM_Pid_1;

– soit un descripteur CA_Desc est présent au niveau composante avec l'identificateur ECM_Pid_1 pour chaque composante.

Exemple 2: mode 3, la composante vidéo et la composante son 1 sont embrouillées avec le mot de contrôle CW1, la composante son 2 est embrouillée avec le mot de contrôle CW2 et la composante son 3 avec le mot de contrôle CW3:

– un descripteur CA_Desc est présent au niveau programme avec l'identificateur ECM_Pid_1;

– et un descripteur CA_Desc est présent au niveau audio 2 avec l'identificateur ECM_Pid_2;

– et un descripteur CA_Desc est présent au niveau audio 3 avec l'identificateur ECM_Pid_3.

6.2.4 Résumé

Le tableau ci-dessous récapitule les éléments présents pendant une transmission:

Elément	Mode 0	Mode 1	Mode 2	Mode 3
Transport_Scrambling_Control	**00**	**Constant 10 ou 11**	**Variable 10/11**	**Variable 10/11**
CAT	**Optionnel**	**Optionnel**	**Optionnel**	**Optionnel**
EMM	**Optionnel**	**Optionnel**	**Optionnel**	**Optionnel**
CA_Descriptor(s) in PMT	**Non**	**Oui**	**Oui**	**Oui**
ECM	**Non**	**Non**	**Oui**	**Oui**

ANNEXE A

Mise en œuvre pratique permettant l'interopérabilité

A.1 Introduction

A.1.1 Aperçu

La présente annexe décrit les mécanismes additionnels nécessaires pour l'accès conditionnel afin de permettre une interopérabilité des équipements de reportage RASN.

Seul le mode 1 (embrouillage avec mot de contrôle fixe) est obligatoire.

A.1.2 Nomenclature

Dans toute la présente annexe, le terme "embrouilleur" désigne l'ensemble des mécanismes requis pour répondre à la spécification de l'algorithme CSA.

Dans toute la présente annexe, le terme "module d'embrouillage" désigne les mécanismes de super-embrouillage requis pour répondre à la spécification de l'algorithme CSA.

NOTE – Pour pouvoir obtenir la spécification de l'algorithme CSA, il faut signer un accord de non-divulgation auprès de l'ETSI et acquitter une redevance unique (pour plus de détails, allez à www.etsi.org et cliquez sur **security algorithms and codes** sous le titre **Publication and Products**.

Dans toute la présente annexe, le terme SAM (*scrambling authorization module*) désigne le module d'autorisation d'embrouillage requis pour répondre à la spécification de l'algorithme CSA.

Dans toute la présente annexe, le terme "clé de session" désigne la clé qui est unique et constante pendant la durée de la transmission. Il peut s'agir d'un mot de contrôle fixe utilisé pour embrouiller le flux de transport directement ou en ajoutant un niveau d'adressage indirect ou bien d'une clé utilisée pour embrouiller des mots de contrôle variables dans des messages de contrôle des titres d'accès.

Dans toute la présente annexe, le terme "mot de session" désigne le mot à partir duquel la clé de session est obtenue, autrement dit le mot de session n'est pas utilisé directement dans le processus d'embrouillage, mais il est transformé par un certain mécanisme en clé de session.

A.1.3 Prescriptions de sécurité

Le modèle du reportage RASN nécessite la saisie directe d'un mot de session au niveau de l'émetteur et au niveau du récepteur pour contrôler l'accès à la transmission. L'émetteur et les récepteurs de la transmission partagent le mot de session, ainsi seules les parties voulues recevront la transmission, selon le processus ci-dessous:

1) le mot de session est saisi au niveau de l'unité RASN dans le champ;
2) le mot de session est saisi au niveau des IRD de réception;
3) si les mots de session sont identiques, les IRD sont capables de décrypter les données diffusées;
4) si les mots de session sont différents, les données diffusées ne sont pas reçues.

Les prescriptions de sécurité pour les systèmes de contribution fixes sont quelque peu différentes de celles du modèle RASN. La sécurité de l'échange de clés de session est fondamentale pour ces systèmes et elle est atteignable. En ce qui concerne les systèmes fixes nécessitant une interopérabilité avec des unités RASN, on peut employer des systèmes de contrôle externe pour permettre la transmission de messages de gestion des titres d'accès (EMM) en vue d'échanger en toute sécurité des clés de session entre site émetteur et site récepteur. Ce modèle fonctionne pour les sites de transmission qui font partie du réseau fixe, mais lorsque des sites récepteurs acceptent une transmission en provenance d'une unité RASN, il faut revenir à la méthode de saisie directe décrite plus haut.

NOTE – Pour pouvoir obtenir la spécification de l'algorithme CSA, il faut signer un accord de non-divulgation auprès de l'ETSI et acquitter une redevance unique (pour plus de détails, allez à www.etsi.org et cliquer sur **security algorithms and codes** sous le titre **Publication and Products**).

A.2 Prescriptions fonctionnelles

A.2.1 Modes de fonctionnement

L'embrouilleur doit être capable de prendre en charge les quatre modes de fonctionnement suivants:

- mode 0: pas d'embrouillage;
- mode 1: toutes les composantes sont embrouillées avec un mot de contrôle fixe;
- mode 2: toutes les composantes sont embrouillées avec une séquence de mots de contrôle unique. Le module d'embrouillage fixe un mot de contrôle de la séquence pendant la durée de la période cryptographique;
- mode 3: chaque composante peut être embrouillée avec une séquence de mots de contrôle différente comme dans le mode 2.

L'embrouilleur mettra en œuvre les opérations de super-embrouillage telles que définies dans la spécification de l'algorithme CSA. Le mécanisme d'embrouillage ne sera appliqué qu'au niveau transport.

Pour prendre en charge les divers modes de fonctionnement, l'embrouilleur doit être capable d'insérer des flux ECM dans le multiplex et ces flux doivent être identifiés correctement dans la table PMT. L'utilisation de flux EMM n'a pas d'application dans les modes de fonctionnement décrits dans la présente Recommandation; toutefois, les équipements compatibles RASN peuvent utiliser de tels flux lorsqu'ils sont employés dans une architecture de réseau fixe.

Une table CAT doit être présente dans le multiplex pour les modes 1, 2 et 3, même si elle doit être vide, car aucun flux EMM ne sera présent. A nouveau, les équipements compatibles RASN employés dans une architecture de réseau fixe utilisant des flux EMM doivent les identifier correctement dans la table CAT.

Un embrouilleur qui ne prend en charge qu'un sous-ensemble des modes de fonctionnement définis doit procéder conformément à une hiérarchie imposée. Un embrouilleur prenant en charge le mode 2 doit aussi prendre en charge les modes 0 et 1. De même, un embrouilleur prenant en charge le mode 3 doit aussi prendre en charge les modes 0, 1 et 2.

A.2.2 Mode 0

L'embrouilleur doit être capable de désactiver l'opération d'embrouillage. Dans ce mode, il n'y aura pas de descripteur CA_descriptor dans la table PMT et il n'y aura pas de flux ECM. Les bits Transport_Scrambling_Control des paquets de transport seront mis à "00".

A.2.3 Mode 1

A.2.3.1 Aperçu général

Dans ce mode, l'embrouilleur utilise un mot de contrôle (CW) fixe pendant la durée de la transmission. L'opérateur doit saisir un mot de session, qui est transformé en clé de session (SK) pour être utilisé par le module d'embrouillage. Dans ce mode, les termes mot de session et clé de session sont respectivement synonymes des termes "mot de contrôle" et "clé commune" utilisés dans la spécification de l'algorithme CSA. La Figure A.1 donne un aperçu général.

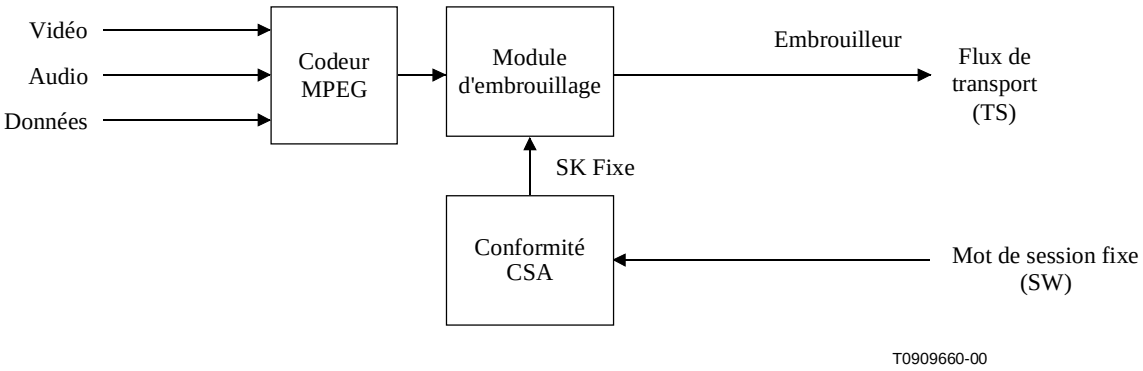


Figure A.1/J.96 – Aperçu général: Mode 1

Le mot de session est un mot de 48 bits qui est transformé par l'embrouilleur en une clé de session de 64 bits au moyen du mécanisme de conformité défini dans la spécification de l'algorithme CSA.

Le mot de session de 48 bits est d'abord mappé sur le mot de contrôle de 64 bits par l'embrouilleur avant que le mécanisme de conformité CSA ne soit appliqué. Le mappage d'octets entre le mot de session de 48 bits et le mot de contrôle de 64 bits est donné dans le Tableau A.1:

Tableau A.1/J.96 – Mappage entre mot de session et mot de contrôle fixe

Mot de contrôle de 64 bits	Mot de session de 48 bits
CW(1)	SW(1)
CW(2)	SW(2)
CW(3)	SW(3)
CW(4)	(Note 1)
CW(5)	SW(4)
CW(6)	SW(5)
CW(7)	SW(6)
CW(8)	(Note 2)
NOTE 1 – CW(4) est obtenu à partir de SW(1)..SW(6) par le mécanisme de conformité CSA. NOTE 2 – CW(8) est obtenu à partir de SW(1)..SW(6) par le mécanisme de conformité CSA.	

Dans ce mode, il y aura un descripteur CA_descriptor dans la table PMT, présent au niveau programme, mais il n'y aura pas de flux ECM. Un seul identificateur de système CA unique est assigné pour identifier le mode 1.

Les bits Transport_Scrambling_Control des paquets de transport sont mis à "10".

La saisie manuelle du mot de session doit se faire en hexadécimal, les chiffres de plus fort poids étant saisis en premier, c'est-à-dire de gauche à droite du point de vue de la notation hexadécimale.

Par exemple 0xA13DBC42908F serait saisi dans la séquence suivante: A,1,3,D,B,C,4,2,9,0,8,F.

La saisie à distance du mot de session doit aussi être possible, même si la spécification de cette interface n'entre pas dans le cadre de la présente Recommandation.

L'embrouilleur doit faire en sorte que la clé de session utilisée par le module d'embrouillage ne puisse pas être modifiée plus de 10 fois par période de 5 minutes et qu'il y ait au moins 10 secondes entre deux modifications consécutives.

A.2.3.2 Descripteur CA

Le descripteur CA_descriptor, qui doit être présent dans la table PMT pour prendre en charge le mode 1, est défini dans le Tableau A.2:

Tableau A.2/J.96 – Descripteur d'accès conditionnel: Mode 1

Syntaxe	Nombre de bits	Identificateur
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
Reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
}		

Sémantique

CA_system_ID: c'est un champ de 16 bits indiquant le type de système à accès conditionnel applicable pour les flux ECM associés. Pour le mode 1, ce champ vaut 0x2600 [2].

CA_PID: c'est un champ de 13 bits indiquant l'identificateur PID des paquets de flux de transport devant contenir l'information ECM. Pour le mode 1, aucune information ECM n'est nécessaire, ce champ doit donc contenir la valeur 0x1FFF.

A.2.4 Modes 2 et 3

A.2.4.1 Aperçu général

Dans ce mode, l'embrouilleur utilise un mot de contrôle variable pour une transmission donnée (mode 2) ou pour les composantes constituant une transmission (mode 3). Un aperçu général est donné sur la Figure A.2.

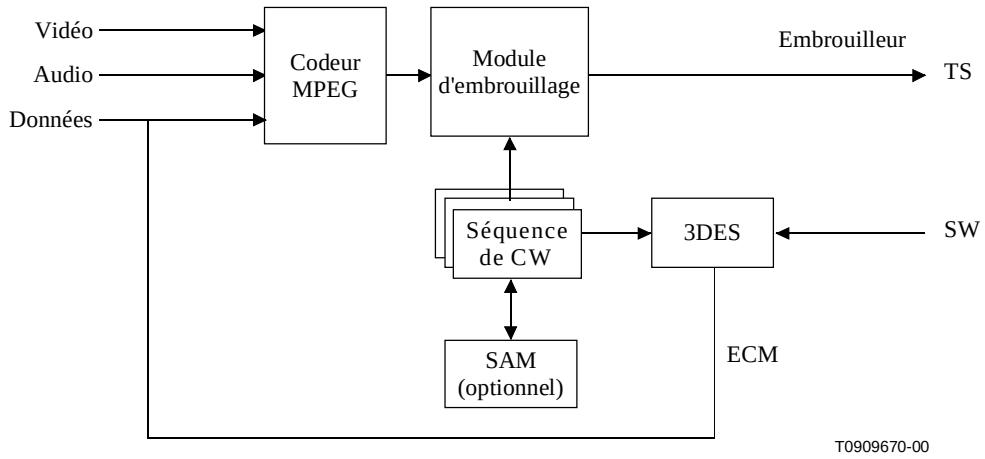


Figure A.2/J.96 – Aperçu général: Modes 2 et 3

Pour prendre en charge les modes 2 et 3, des séquences de mots de contrôle conformes aux spécifications DVB doivent être produites en avance et enregistrées localement au niveau de l'embrouilleur, par exemple dans un dispositif à mémoire FLASH. L'embrouilleur doit fixer le mot de contrôle suivant à partir de la séquence de mots de contrôle dans le module d'embrouillage pendant la durée appelée période cryptographique (généralement de quelques secondes). Les mots de contrôle doivent être cryptés et transmis dans un flux ECM, protégés par la clé de session. Le module SAM, s'il est présent, doit uniquement procéder à l'authentification des mots de contrôle mais pas à leur création.

Les mots de contrôle doivent être cryptés au moyen de l'algorithme DES en mode ABC EDE 3DES sans chaînage (répertoire ECB) et une taille de clé de 168 bits. Pour que cet algorithme puisse être exporté, seuls 56 bits de la clé doivent correspondre au mot de session dépendant de l'opérateur, tandis que les 112 autres bits doivent être constants.

En mode 2, il y aura un descripteur CA_descriptor dans la table PMT, présent au niveau programme, identifiant le flux ECM pour la séquence de mots de contrôle. En mode 3, il y aura un descripteur CA_descriptor dans la table PMT, présent pour chaque composante, identifiant le flux ECM pour la séquence de mots de contrôle de cette composante (voir la Note). Un seul identificateur de système à accès conditionnel unique est assigné pour identifier les deux modes 2 et 3. Les deux modes ne sont distingués que par la position des descripteurs CA_descriptor dans la table PMT comme décrit ci-dessus.

NOTE – En mode 3, il devrait être possible de saisir un mot de session distinct pour chaque composante qui nécessite un contrôle des titres d'accès spécifique.

Pour les deux modes, les bits Transport_Scrambling_Control des paquets de transport peuvent être mis à "10" ou "11" suivant si, respectivement, on utilise la clé paire ou la clé impaire.

A.2.4.2 Cryptage du mot de contrôle

La clé de session (SK) de 168 bits utilisée pour le cryptage 3DES du mot de contrôle est obtenue comme suit:

1) un mot de session (SW) de 56 bits fourni par l'opérateur;
2) une clé sous seing privé (KE) de 112 bits;
3) 1 et 2 sont concaténés et les 168 bits résultant sont utilisés comme clé de session pour le cryptage 3DES.

SK(167..0) = [KE & SW]

Autrement dit, la clé sous seing privé constitue les bits de plus fort poids de la clé de session et le mot de session en constitue les bits de plus faible poids.

- SK(167..56) = KE(111..0)
- SK(55..0) = SW(55..0)
- Si KE = 0x00000000000000000000000000000 et SW = 0x11223344556677, alors SK = 0x00000000000000000000000000011223344556677.

Le mappage entre la clé de session et la clé ABC 3DES est indiqué ci-dessous. Il est à noter que la clé de session utilise la notation ingénierie (à savoir msb = 55, lsb = 0) tandis que la clé 3DES utilise la notation FIPS (à savoir msb = 1, lsb = 56).

Tableau A.3/J.96 – Mappage clé de session – Clé 3DES

	A(1..56)	**B(1..56)**	**C(1..56)**
Mode DES	E	D	E
Clé de session	SK(167..112)	SK(111..56)	SK(55..0)

L'algorithme autorise jusqu'à 256 options de clé sous seing privé, de sorte que, pendant une transmission, une clé sous seing privé donnée peut être utilisée pour sécuriser la session. L'option de clé sous seing privé est identifiée dans le champ fixed_bits_option (option de bits fixes) du message ECM, de sorte qu'un désembrouilleur peut sélectionner la même clé sous seing privé que celle utilisée par l'embrouilleur de la transmission.

Pour l'interopérabilité, il est essentiel que l'embrouilleur et le désembrouilleur partagent la même clé sous seing privé pour toute session donnée. L'application spécifique des options de clé sous seing privé n'entre pas dans le cadre de la présente Recommandation. Toutefois, pour permettre une vraie interopérabilité, une valeur de clé sous seing privé de "00000000000000000000000000000" est assignée au champ fixed_bits_option = "0x00" (valeur par défaut).

Le mappage de bits entre le mot de contrôle et le bloc de cryptage 3DES est indiqué dans le Tableau A.4. Il est à noter que le mot de contrôle utilise la notation ingénierie (à savoir msb = 63, lsb = 0) tandis que le bloc de cryptage 3DES utilise la notation FIPS (à savoir msb = 1, lsb = 64).

Tableau A.4/J.96 – Mappage mot de contrôle – Bloc de cryptage 3DES

3DES(1) <= CW(63)	3DES(33) <= CW(31)
3DES(2) <= CW(62)	3DES(34) <= CW(30)
3DES(3) <= CW(61)	3DES(35) <= CW(29)
3DES(4) <= CW(60)	3DES(36) <= CW(28)
3DES(5) <= CW(59)	3DES(37) <= CW(27)
3DES(6) <= CW(58)	3DES(38) <= CW(26)
3DES(7) <= CW(57)	3DES(39) <= CW(25)
3DES(8) <= CW(56)	3DES(40) <= CW(24)
3DES(9) <= CW(55)	3DES(41) <= CW(23)
3DES(10) <= CW(54)	3DES(42) <= CW(22)
3DES(11) <= CW(53)	3DES(43) <= CW(21)
3DES(12) <= CW(52)	3DES(44) <= CW(20)
3DES(13) <= CW(51)	3DES(45) <= CW(19)
3DES(14) <= CW(50)	3DES(46) <= CW(18)
3DES(15) <= CW(49)	3DES(47) <= CW(17)
3DES(16) <= CW(48)	3DES(48) <= CW(16)
3DES(17) <= CW(47)	3DES(49) <= CW(15)
3DES(18) <= CW(46)	3DES(50) <= CW(14)
3DES(19) <= CW(45)	3DES(51) <= CW(13)
3DES(20) <= CW(44)	3DES(52) <= CW(12)
3DES(21) <= CW(43)	3DES(53) <= CW(11)
3DES(22) <= CW(42)	3DES(54) <= CW(10)
3DES(23) <= CW(41)	3DES(55) <= CW(9)
3DES(24) <= CW(40)	3DES(56) <= CW(8)
3DES(25) <= CW(39)	3DES(57) <= CW(7)
3DES(26) <= CW(38)	3DES(58) <= CW(6)
3DES(27) <= CW(37)	3DES(59) <= CW(5)
3DES(28) <= CW(36)	3DES(60) <= CW(4)
3DES(29) <= CW(35)	3DES(61) <= CW(3)
3DES(30) <= CW(34)	3DES(62) <= CW(2)
3DES(31) <= CW(33)	3DES(63) <= CW(1)
3DES(32) <= CW(32)	3DES(64) <= CW(0)

A.2.4.3 Message de contrôle des titres d'accès

Le message de contrôle des titres d'accès (ECM) se présente sous la forme d'une section comme défini par l'UIT-T H.222.01 | ISO/CEI 13818-1 [1]. Le format d'un message ECM, défini dans cette Recommandation, est donné dans le Tableau A.5.

Tableau A.5/J.96 – Section de message de contrôle des titres d'accès

Syntaxe	Nombre de bits	Identificateur
entitlement_control_message_section() {		
table_id	**8**	**uimsbf**
section_syntax_indicator	**1**	**bslbf**
DVB_reserved	**1**	**bslbf**
ISO_reserved	**2**	**bslbf**
CA_section_length	**12**	**uimsbf**
fixed_bits_option	**8**	**uimsbf**
even_cw_encrypted	**64**	**bslbf**
odd_cw_encrypted	**64**	**bslbf**
for (i = 0; i < N; i++) {		
CA_data_byte	**8**	**bslbf**
}		
}		

Sémantique

table_id: ce champ peut prendre la valeur 0x80 ou 0x81 pour identifier le fait qu'il s'agit d'une section ECM. Toute modification de la valeur du champ table_id indique une modification du contenu du message ECM.

fixed_bits_option: ce champ identifie l'option de clé sous seing privé à partir de l'ensemble de bits fixes, la valeur par défaut étant "0x00".

even_cw_encrypted: il s'agit du mot de contrôle pair crypté par 3DES.

odd_cw_encrypted: il s'agit du mot de contrôle impair crypté par 3DES.

La programmation de l'émission d'un nouveau message ECM est un équilibre entre fiabilité et sécurité. En émettant un message ECM bien avant la période cryptographique à laquelle il est associé, le système est plus fiable. Toutefois, si le message ECM apparaît trop en avance, l'attaque du flux ECM est beaucoup plus facile. Pour obtenir un bon équilibre, la fréquence de répétition des messages ECM doit être de 10/s et l'émission ne doit pas être rendue obligatoire mais soumise à des contraintes, la période cryptographique étant limitée à une durée minimale de 500 ms. Ainsi, la durée s'écoulant entre l'émission d'un message ECM se rapportant à une nouvelle période cryptographique et le début de cette période doit être au moins égale à la période cryptographique minimale.

L'émission d'un nouveau message ECM doit être telle qu'un récepteur puisse traiter le message à temps pour la période cryptographique suivante. Si la fiabilité est plus importante que la sécurité, le message ECM associé à une période cryptographique donnée peut être émis pendant la période cryptographique antérieure.

A.2.4.4 Descripteur CA

Le descripteur CA_descriptor, qui doit être présent dans la table PMT pour prendre en charge les modes 2 et 3, est défini dans le Tableau A.6.

Tableau A.6/J.96 – Descripteur d'accès conditionnel – Modes 2 et 3

Syntaxe	Nombre de bits	Identificateur
CA_descriptor() {		
descriptor_tag	**8**	**uimsbf**
descriptor_length	**8**	**uimsbf**
CA_system_ID	**16**	**uimsbf**
Reserved	**3**	**bslbf**
CA_PID	**13**	**uimsbf**
}		

Sémantique

CA_system_ID: il s'agit d'un champ de 16 bits indiquant le type de système à accès conditionnel applicable pour les flux ECM associés. Pour les modes 2 et 3, ce champ vaut 0x2601. Un seul identificateur CA-system-ID identifie les deux modes, qui sont alors distingués par la position du descripteur CA_descriptor dans la table PMT.

CA_PID: il s'agit d'un champ de 13 bits indiquant l'identificateur PID des paquets de flux de transport devant contenir l'information ECM.

APPENDICE I

Description générale d'un système ouvert à accès conditionnel fondé sur OKAPI

L'accès au contrôle de la séquence d'embrouillage est sécurisé grâce à l'infrastructure de clés publiques (PKI), qui est un système ouvert pour les applications cryptographiques.

I.1 Systèmes cryptographiques à clé publique

La notion de cryptographie à clé publique a été introduite par Diffie et Hellman. Les systèmes à clé publique diffèrent des systèmes classiques par le fait qu'il n'y a plus de secret unique partagé par une paire d'utilisateurs. En revanche, chaque utilisateur a ses propres données de clé. En outre, les données de clé de chaque utilisateur comprennent deux parties, une composante privée et une composante publique. La composante publique crée une transformation publique *E* et la composante privée crée une transformation privée *D*. Par analogie avec le cas classique, *E* et *D* pourraient respectivement être désignés par fonction de cryptage et fonction de décryptage. Toutefois, cela est imprécis: dans un système donné, on peut avoir *D(E(M))=M*, *E(D(M))=M*, ou les deux.

Il est nécessaire que *E* soit une fonction unidirectionnelle à trappe. Unidirectionnel renvoie au fait que *E* devrait être facile à calculer à partir des données de clé publique mais difficile à inverser sauf si on possède le *D* correspondant ou, de façon équivalente, les données de clé privée permettant de créer *D*. La composante privée crée ainsi une "trappe", rendant le problème de l'inversion de *E* difficile aux yeux du décrypteur mais facile pour le possesseur (seul légitime) de *D*. Par exemple, la trappe peut correspondre à la connaissance de la factorisation d'un entier.

On remarque que les fonctions à trappe employées comme transformation publique dans des systèmes à clé publique ne constituent qu'une sous-classe de la classe des fonctions unidirectionnelles.

On note par ailleurs que la dichotomie public/privé de *E* et *D* dans les systèmes publics n'a pas d'analogue dans un système cryptographique classique: dans le deuxième cas, E_k et D_k sont paramétrés par une seule clé *k*. Par conséquent, si E_k est connu, on peut supposer que *K* a été compromise, d'où on peut aussi supposer que D_k est également connu, ou vice versa. Par exemple, dans l'algorithme DES, *E* et *D* sont calculés essentiellement par le même algorithme public à partir d'une clé commune; ainsi *E* et *D* sont tous deux connus ou inconnus, suivant si la clé a été compromise ou pas.

Les systèmes cryptographiques à clé publique offrent au moins la même sécurité que ceux à clé secrète. Leur principal inconvénient est le temps de calcul, qui est environ 1000 fois plus élevé. Mais ces systèmes présentent le gros avantage de la simplicité du système de gestion de clé.

Qu'un système cryptographique classique ou un système cryptographique à clé publique soit utilisé, il est nécessaire que les utilisateurs obtiennent les clés d'autres utilisateurs. Dans un sens, cela crée un problème circulaire: pour communiquer en toute sécurité sur des canaux peu sûrs, les utilisateurs doivent d'abord échanger des informations de clé. S'il n'existe pas de solution au problème des canaux peu sûrs, l'échange en toute sécurité d'informations de clé présente essentiellement le même problème de sécurité que la communication en toute sécurité qui suit.

Dans les systèmes cryptographiques classiques, ce cercle peut être rompu de diverses façons. Par exemple, on pourrait supposer que deux utilisateurs communiquent sur un canal sûr supplémentaire, dans le cadre d'un service de messager. Dans ce cas, il est fréquent que le canal sûr soit coûteux, peu pratique, à faible largeur de bande et lent; en outre, l'utilisation d'un messager ne peut pas être considérée comme vraiment sûre. Une autre solution consisterait, pour les deux utilisateurs, à échanger des informations de clé via une autorité centrale. Le recours à une autorité centrale présente plusieurs inconvénients.

Dans les systèmes à clé publique, le problème de gestion de clé est plus simple en raison de la nature publique des données de clé échangées entre les utilisateurs ou entre un utilisateur et une autorité centrale. En outre, les solutions au problème du canal peu sûr peuvent être plus simples; par exemple, un système de messagerie physique pourrait suffire, notamment si des informations redondantes sont envoyées via le canal (électronique) peu sûr. Néanmoins, les clés d'un système cryptographique asymétrique sont gérées de la manière la plus efficace via un système de certification.

I.2 Technique relative aux certificats

L'un des premiers problèmes qui se posent lorsqu'on établit un protocole à clé publique est le problème de l'architecture des certificats.

Une nouvelle technique relative aux certificats, SPKI, a été développée récemment au sein de l'IETF.

Les certificats SPKI sont des certificats d'autorisation centrés sur une *clé*. Ils n'expriment pas de lien entre un nom et une clé mais, en revanche, ils expriment directement une délégation d'autorisation sur une clé publique. Dans la terminologie SPKI, les clés publiques sont appelées "principaux". Un principal est une entité qui peut exprimer une certaine autorité en signant ou en déchiffrant certaines informations. Un principal agit aussi en tant que nom unique universel pour lui mais, pour simplifier et réduire la quantité des données traitées, le hachage en toute sécurité d'un principal est également admis être son identificateur unique.

La technique SPKI prend aussi en charge les certificats d'identité, mais OKAPI n'utilise que les certificats d'autorité. Les certificats d'autorité SPKI sont émis au départ par l'entité vérificatrice. L'autorité exacte qui est déléguée peut être réglée facilement avec des étiquettes explicites en texte libre définies par le vérificateur.

Pour donner une certaine souplesse au système, l'autorité qui est déléguée à un principal peut être redéléguée par ce principal à un autre principal. Pour permettre ce mécanisme, il faut ajouter le

champ "propagate" au certificat d'origine. Les certificats SPKI ne sont pas censés être uniques (dans le sens où ils exprimeront toutes les informations requises par toutes les entités) et, idéalement, un certificat différent doit être émis pour couvrir chacune des autorités qui sont déléguées.

Lorsqu'une entité (le démonstrateur) souhaite démontrer une certaine autorité à un vérificateur, il lui appartient de fournir tous les certificats dont le vérificateur a besoin. Il faut aussi que le démonstrateur les ordonne de sorte que, si un certificat nécessite qu'un autre certificat soit validé, celui-ci a déjà été traité. A la fin, le vérificateur réduira la chaîne de certificats à un seul certificat de la forme:

(émetteur = auto, objet = démonstrateur, autorité = X, une certaine contrainte temporelle).

Dans la technique SPKI, on introduit deux nouvelles techniques relatives à la révocation de certificat: la vérification en ligne[1] et le certificat de revalidation de certificat (CRC). Dans la première, le vérificateur est contraint de contacter l'émetteur (ou un tiers) chaque fois que le certificat doit être vérifié. Dans la deuxième, le démonstrateur est contraint de contacter l'émetteur (ou un tiers) pour obtenir un certificat CRC, puis transmettre le certificat CRC et le certificat d'origine au vérificateur. Bien entendu, le certificat CRC a aussi une période de validité.

OKAPI a décidé d'utiliser la méthode de revalidation car elle présente les avantages suivants:

- pas besoin de publier de longs CRL;
- il n'est pas nécessaire de contacter l'émetteur pour chaque vérification. Une fois qu'un certificat CRC est obtenu, il peut être utilisé jusqu'à ce que la temporisation qui lui est associée ait expiré;
- la durée de vie d'un certificat de revalidation est facile à ajuster;
- l'émission du certificat de revalidation de certificat peut être contrôlée strictement. Un tel certificat ne doit être fourni qu'au propriétaire principal du certificat d'origine.

En ce qui concerne la technique SPKI, on a formulé une approche philosophique Internet au problème avec une représentation des données. Les certificats SPKI sont représentés par des expressions-S canoniques [4]. Les expressions-S sont simples, faciles à analyser et clairement lisibles (jusqu'à un certain point). Les expressions-S présentent par ailleurs un préfixe très court aux données réelles qu'elles contiennent. On donne ci-après une traduction libre d'un extrait du projet SPKI de l'IETF: *"Nous définissons une expression-S canonique comme contenant des chaînes d'octets binaires ayant chacune une longueur et une ponctuation données "()[]" en vue de la constitution de listes. La longueur d'une chaîne d'octets est exprimée par un nombre décimal ASCII non négatif, sans chiffres "0" d'en-tête inutiles, et terminée par":". En outre, il ne doit pas y avoir de liste vide et le premier élément d'une liste doit être une chaîne d'octets (comme défini ci-dessous). Cette forme est une représentation unique d'une expression-S et elle est utilisée comme entrée pour toutes les fonctions de hachage et de signature."* Bien entendu, les expressions-S peuvent aussi être utilisées pour l'enregistrement et la transmission. Pour faciliter la compréhension du lecteur et illustrer la simplicité des expressions-S, on donne ci-après quelques exemples d'expressions-S canoniques valides (entre guillemets):

- "(10:not-before19:1998-01-19_17:00:00)"
- "(11:hello world)"
- "(4:this(2:is(1:a(5:valid)(12:s-expression))))"

---

[1] Revalidation en un temps dans la nomenclature SPKI.

I.3 Fonctionnement pratique avec OKAPI

I.3.1 Introduction

Il existe deux types de sites:

– le centre de gestion de réseau comprend un dispositif de contrôle et un dispositif de gestion;

– chaque site de communication comprend un ou plusieurs dispositifs d'accès conditionnel.

Le centre de gestion de réseau (NMC) est unique pour un réseau donné. Il est responsable de la gestion des ressources du réseau, de l'attribution des canaux disponibles (un lien direct entre la planification (TPP) et la gestion du système CAS est proposé) et de la synchronisation entre émetteurs et récepteurs. Le centre NMC pourrait facilement étendre ses responsabilités pour prendre en charge de nouveaux services tels que la caractérisation par filigranage.

Il existe plusieurs sites de communication. Chacun peut émettre ou recevoir simultanément un ou plusieurs programmes de télévision embrouillés. Dans chaque site de communication, il y a au moins un dispositif d'accès conditionnel qui gère plusieurs émetteurs et plusieurs récepteurs.

Un troisième type de site pourrait être envisagé. Le système nécessite une autorité de certification pour la personnalisation des cartes à mémoire. Pour des raisons de sécurité, ce système spécialisé hors ligne pourrait être situé en dehors du centre NMC.

Les principales caractéristiques du système sont les suivantes:

– une gestion centralisée des échanges de programmes de télévision;

– la possibilité de sélectionner et d'autoriser des récepteurs très rapidement, presque en temps réel;

– une interface homme-machine simple au niveau du centre de gestion de réseau et au niveau des sites de communication;

– aucune nécessité de connexion permanente entre le centre de gestion de réseau et les sites de communication;

– une très haute protection contre le piratage des programmes de télévision transmis via des réseaux ouverts, tels que les réseaux à satellite;

– de nombreuses possibilités de nouveaux services reposant sur les caractéristiques de sécurité du système CAS;

– une série de modes permettant un haut niveau de protection, même avec des moyens limités sur le site.

Par ailleurs, les sites de communication qui ne sont pas directement connectés au centre de gestion de réseau sont néanmoins capables d'émettre ou de recevoir des programmes de télévision embrouillés.

Sur la Figure I.1 et dans le texte qui suit, le centre de gestion de réseau est désigné par NMC et les dispositifs d'accès conditionnel par CAD.

Il n'est pas obligatoire d'avoir une carte à mémoire dans le centre de gestion de réseau.

On utilise une ou plusieurs cartes à mémoire pour l'émission et la réception au niveau de chaque site de communication.

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

Une transmission est caractérisée par:

– un canal par satellite ou un autre canal de communication;

– un site de communication servant d'émetteur;

– un ou plusieurs sites de communication servant de récepteurs;

– une date et une heure de début et une date et une heure de fin;
– un ensemble de composantes de télévision: son ou sons, image et données.

Un programme est caractérisé par:
– un nom de programme;
– une ou plusieurs transmissions;
– une clé d'autorisation;
– un ou plusieurs critères d'accès.

Par conséquent, une transmission peut être utilisée pour diffuser un ou plusieurs programmes et un programme peut être transmis via une ou plusieurs transmissions.

Trois comportements différents sont examinés:
– le comportement du centre de gestion de réseau;
– le comportement de l'émetteur d'un site de communication lors de l'utilisation de l'un de ses codeurs;
– le comportement du récepteur d'un site de communication lors de l'utilisation de l'un de ses décodeurs.

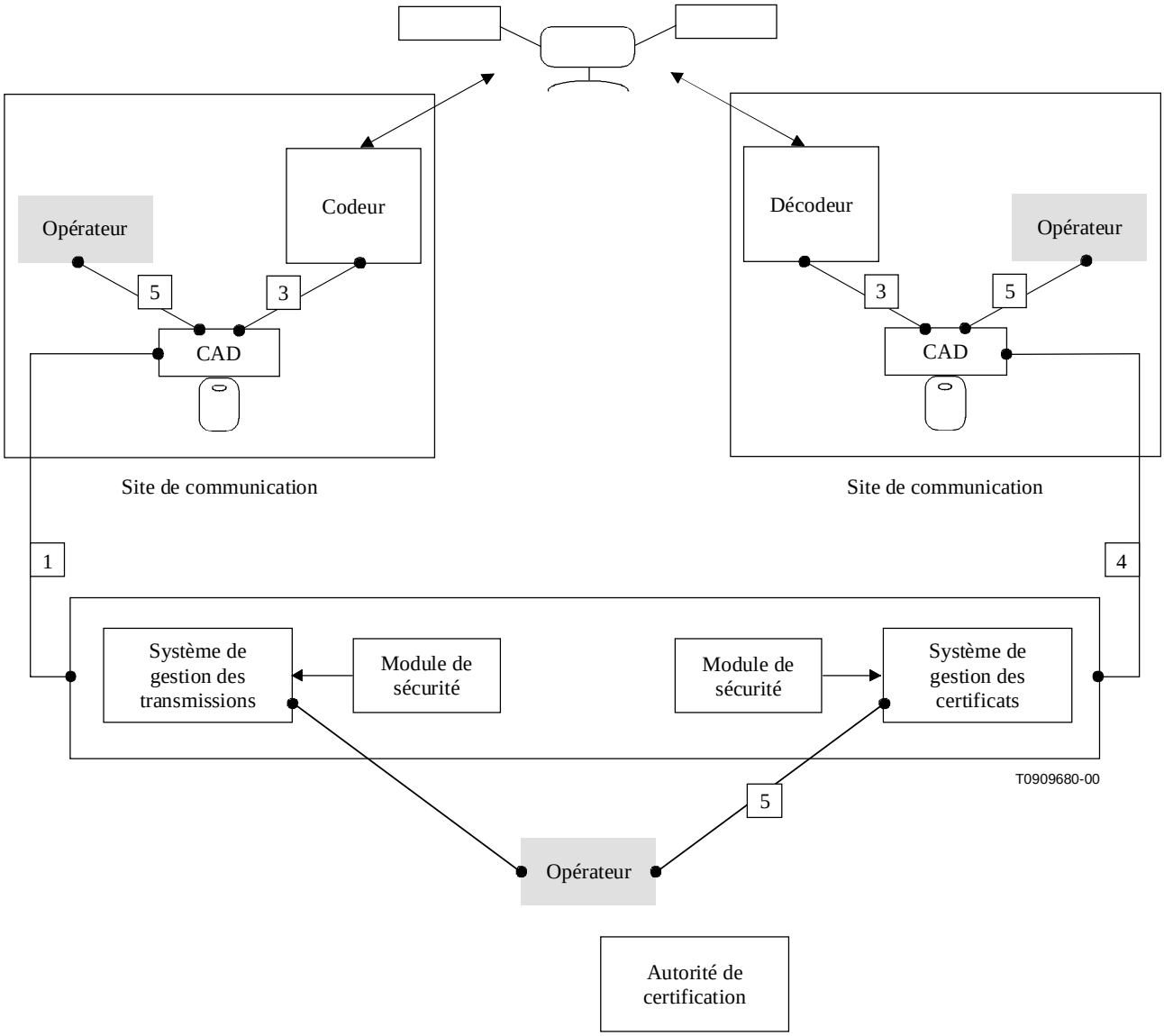


Figure I.1/J.96 – Architecture du réseau

I.3.2 Fonctionnalité du centre de gestion de réseau

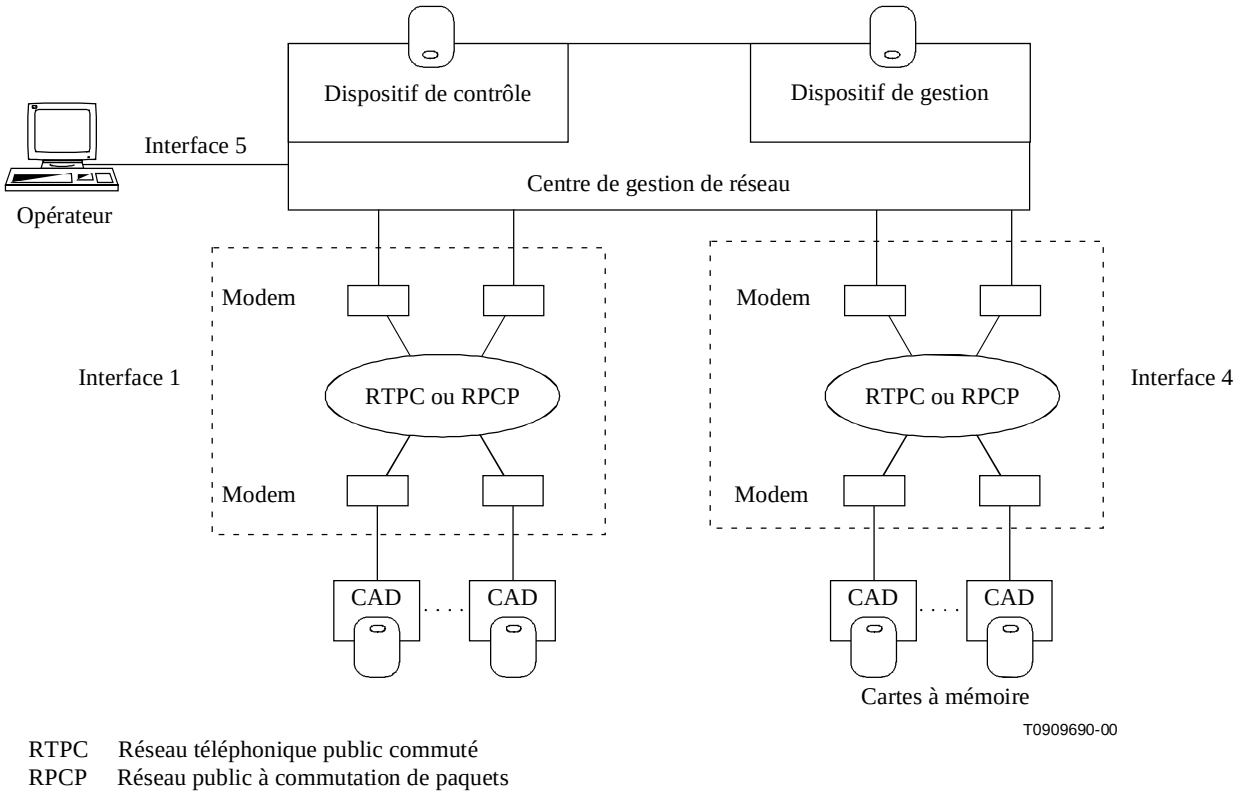
Il appartient au centre de gestion de réseau (NMC) de faire en sorte que l'émetteur et tous les récepteurs autorisés obtiennent la clé d'autorisation et les titres d'accès corrects avant la transmission du programme. Il incombe aussi au centre NMC de mettre à jour régulièrement les clés d'autorisation pour des raisons de sécurité. Pour cela, le centre NMC établit et envoie des messages ECM et EMM.

Le centre NMC assure en outre la surveillance de toutes les cartes à mémoire, dans le cadre de son rôle de tiers de confiance.

Le centre NMC gère un répertoire de clés publiques; des solutions telles que UIT-T X.500 | ISO/CEI 9594-1 pourraient être envisagées dans l'avenir.

Il appartient au centre NMC de prendre une décision en ce qui concerne le scénario appliqué (procédure bidirectionnelle, procédure unidirectionnelle, jetons et mot de contrôle local).

Le centre NMC est représenté schématiquement sur la Figure I.2.



RTPC Réseau téléphonique public commuté
RPCP Réseau public à commutation de paquets

Figure I.2/J.96 – Centre de gestion de réseau (NMC)

I.3.2.1 Création de message ECM

Le centre NMC doit créer les messages ECM. Pour cela, il crée des mots de contrôle, chiffre ces mots de contrôle éventuellement au moyen d'une carte à mémoire et crée les messages ECM correspondants. Chaque message ECM est protégé par une somme de contrôle cryptographique calculée par des moyens cryptographiques. Pendant la transmission, un nouveau message ECM est envoyé régulièrement. Les messages ECM sont envoyés au dispositif CAD de l'émetteur via l'interface 1.

Une mise en œuvre immédiate du schéma consiste à créer régulièrement des messages ECM et à les envoyer "en ligne" au dispositif CAD de l'émetteur. Une telle mise en œuvre suppose que, pendant toute la transmission, le centre NMC reste raccordé au dispositif CAD de l'émetteur. En outre, le centre NMC, qui pilote tous les émetteurs, aurait à créer plusieurs ensembles de messages ECM (autant qu'il y a de canaux en fonctionnement à l'instant considéré) et à les envoyer en même temps.

Le recours à des fichiers cycliques de messages ECM permet de supprimer cette contrainte. Ces fichiers contiennent autant de messages ECM qu'il en faut pour la durée estimée de la transmission. Si la transmission devait déborder, le dernier message ECM est établi de telle sorte qu'il puisse être suivi par le premier message ECM du même fichier, afin de pouvoir parcourir en boucle le même ensemble de messages ECM.

Le centre NMC peut créer un ensemble de fichiers cycliques de messages ECM avant qu'on y fasse appel et les envoyer au dispositif CAD en avance ou au dernier moment avant une transmission.

L'envoi de plusieurs fichiers cycliques de messages ECM en avance au dispositif CAD le rendra prêt à fonctionner presque immédiatement, même dans le cas de transmissions de télévision inattendues (décidées à la dernière minute) ou dans le cas d'un émetteur transportable isolé.

L'aspect le plus novateur en ce qui concerne le système CAS OKAPI réside dans les messages EMM pour lesquels les fonctionnalités PKI sont entièrement exploitées. Conformément au document DSNG219, la protection de la transmission via un message EMM unique et aucun message ECM doit être envisagée.

Il convient de souligner que le système proposé gagnerait en efficacité si on associait étroitement la planification et la protection de la transmission.

I.3.2.2 Création de message EMM

Le centre NMC doit aussi créer les messages EMM pour la distribution de clés et de titres d'accès à des cartes à mémoire spécifiées.

Un message EMM et un seul est destiné à l'émetteur: il permettra au dispositif CAD de l'émetteur (avec l'aide de sa carte à mémoire) de déchiffrer le mot de contrôle de tous les messages ECM ci-dessus.

Les autres messages EMM sont destinés aux récepteurs. Ils permettront aux cartes à mémoire autorisées des dispositifs CAD des récepteurs de déchiffrer le mot de contrôle des messages ECM ci-dessus. Les messages EMM peuvent être transmis de deux façons différentes:

– ils peuvent être transmis directement par l'interface 4 (via une connexion téléphonique, X.25, Vsat ou directe) au dispositif CAD concerné de chaque récepteur;
– ils peuvent être diffusés à tous les récepteurs via le codeur de l'émetteur et le canal par satellite.

Les messages EMM peuvent être créés en avance et enregistrés soit localement soit à distance dans les cartes à mémoire. Cela correspond au scénario des jetons.

I.3.2.3 Surveillance des cartes à mémoire et des certificats associés

Le centre NMC gère le contenu de chaque carte à mémoire, éventuellement avec le soutien d'une autorité externe si l'accès conditionnel est délocalisé.

En cas d'utilisation du paiement à la séance par impulsions, le centre NMC examine les achats des cartes à mémoire.

Le centre NMC possède une base de données dans laquelle figurent le contenu de toutes les cartes à mémoire et des informations détaillées sur tous les dispositifs CAD (emplacements, clé publique de carte à mémoire, etc.). La clé privée associée à chaque carte à mémoire POURRAIT être connue à ce niveau.

Si une carte à mémoire n'a plus de mémoire disponible, le centre NMC doit nettoyer la mémoire en supprimant les clés et les titres d'accès obsolètes.

I.3.2.4 Production de carte à mémoire

Le centre 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 opérateur. Ces scénarios sont envoyés à un outil de production, qui initialise les cartes. Cet outil renvoie au centre NMC un ensemble de cartes et un fichier de rapport. Ce fichier de rapport est utilisé pour mettre à jour la base de données du centre NMC. Une autorité de certification garantit la production de la carte à mémoire. Elle correspond à un ordinateur personnel spécialisé qui est sécurisé physiquement. Cette autorité de certification POURRAIT être située dans le centre NMC.

I.3.2.5 Interface homme-machine

L'interface homme-machine (MMI) 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 configurées pour le paiement à la séance par impulsions;
– un relevé des alarmes (une carte à mémoire est pleine ou hors d'usage, il existe des problèmes de connexion avec un dispositif CAD).

Au niveau du centre NMC, l'interface MMI doit être développée avec les personnes concernées. Plusieurs journaux permettant d'identifier rapidement un problème quelconque doivent être accessibles.

I.3.3 Mise en œuvre des dispositifs CAD

Le comportement du dispositif CAD de l'émetteur comprend les opérations suivantes:
– maintien de la liaison avec le centre NMC (par exemple bruits métalliques réguliers destinés au serveur du centre NMC);
– authentification (premier niveau) de l'émetteur de messages EMM;
– transmission des messages EMM appropriés à sa ou ses cartes à mémoire afin d'enregistrer une ou plusieurs nouvelles clés et un ou plusieurs nouveaux titres d'accès;
– transmission régulière d'un message ECM à sa carte à mémoire pour obtenir en retour le mot de contrôle correspondant qui doit être donné au codeur pour embrouiller le programme de télévision;
– transmission régulière au codeur d'un message ECM à diffuser aux décodeurs;
– si nécessaire, transmission également au codeur des messages EMM à envoyer aux décodeurs.

Le comportement du dispositif CAD du récepteur comprend les opérations suivantes:
– maintien de la liaison avec le centre NMC (par exemple bruits métalliques réguliers destinés au serveur du centre NMC);
– authentification (premier niveau) de l'émetteur des messages EMM;
– obtention des messages EMM appropriés en provenance du décodeur ou de la liaison directe avec le centre NMC et transmission à sa ou ses cartes à mémoire afin d'enregistrer une ou plusieurs nouvelles clés et un ou plusieurs nouveaux titres d'accès;
– obtention régulière des messages ECM en provenance du décodeur et envoi de ces messages à sa carte à mémoire pour obtenir en retour les mots de contrôle correspondants et pour redonner au décodeur ces mots de contrôle.

I.3.3.1 Cas d'une station émettrice isolée

"Isolée" signifie qu'il n'y a pas de connexion entre le dispositif CAD de l'émetteur et le centre NMC au moment de la transmission. Cela peut se produire, par exemple, pour une unité spéciale de reportage d'actualités pour laquelle la station émettrice est très mobile. Tout émetteur doit être capable de fonctionner dans ce mode en cas d'urgence.

Dans ce contexte, il est tout de même possible de sécuriser la transmission de programmes de télévision. Pour que cette sécurisation soit possible, le dispositif CAD de l'émetteur doit être chargé à l'avance avec un fichier cyclique de messages ECM (au moyen d'une diskette, d'une carte à puce PCMCIA ou de la carte à mémoire proprement dite). Il ne reste alors à l'opérateur de l'émetteur plus qu'à sélectionner le fichier cyclique de messages ECM approprié.

En cas de transmission faisant intervenir à la fois des stations connectées et des stations isolées, il convient d'appliquer le scénario des jetons. Ce scénario fait actuellement l'objet d'une procédure de demande de brevet.

Ce mode convient parfaitement en cas de paiement à la séance par impulsions. Les cartes à mémoire des récepteurs enregistreront automatiquement le numéro du programme (avec l'accord de l'opérateur du récepteur). Le centre NMC examinera ultérieurement le contenu des cartes.

I.3.4 Mise en œuvre de l'interface 1

L'interface 1 relie le centre NMC au dispositif CAD de l'émetteur. L'initialisation se fait par le centre NMC.

Les messages et commandes qui suivent sont échangés:

– messages ECM: dans la mise en œuvre recommandée, un fichier cyclique de messages ECM est calculé par le centre NMC et transmis à l'avance au dispositif CAD de l'émetteur avec la référence du programme de télévision qui utilisera ces messages ECM. Une autre mise en œuvre consisterait à envoyer un message ECM "en ligne" toutes les 8,2 secondes;

– messages EMM: dans la mise en œuvre recommandée, un fichier de messages EMM est calculé par le centre NMC et transmis à l'avance au dispositif CAD de l'émetteur. Une autre mise en œuvre est possible au moyen de l'interface 4 pour l'adressage de chaque récepteur.

L'interface 2 peut être mise en œuvre sur le réseau téléphonique public commuté ou sur le réseau public à commutation de paquets, voire sur une disquette ou sur une carte à puce PCMCIA.

I.3.5 Mise en œuvre de l'interface 4

L'interface 4 relie le centre NMC à une carte à mémoire, via un dispositif CAD. L'initialisation se fait par le dispositif CAD.

Elle est principalement utilisée pour la surveillance des cartes à mémoire raccordées au dispositif CAD. La surveillance des cartes comprend les opérations suivantes:

– examen des paiements à la séance par impulsions enregistrés sur la carte;

– nettoyage de la mémoire EEPROM de la carte. Si une carte n'a plus de mémoire disponible, le centre NMC supprime les anciennes autorisations.

En outre, comme indiqué ci-dessus, on peut utiliser l'interface 4 pour envoyer des messages EMM.

L'interface 4 peut être mise en œuvre sur le réseau téléphonique public commuté ou sur le réseau public à commutation de paquets.

Les informations d'ouverture de session sont enregistrées sur la carte à mémoire dans un bloc de fonctionnalité ad hoc. L'appel est lancé par le dispositif CAD après réception d'un message EMM de démarrage du modem.

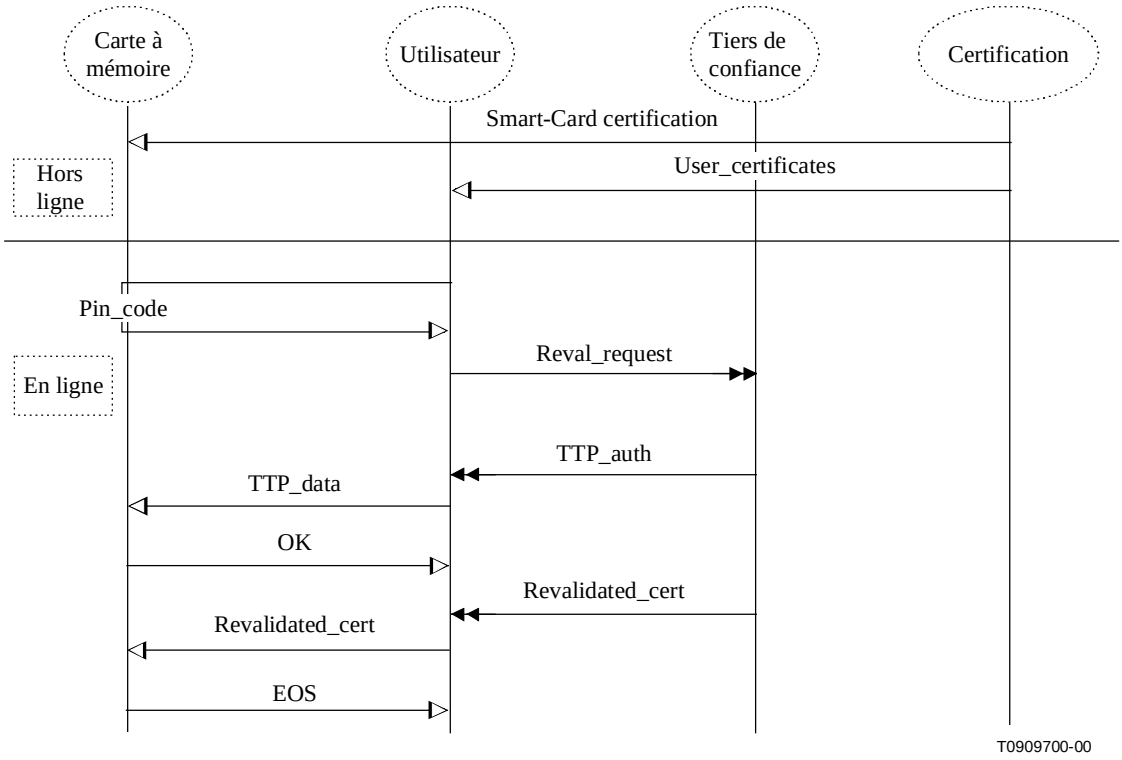
I.3.6 Principaux protocoles bidirectionnels

Les protocoles correspondant à chaque mode peuvent être présentés. On donne ici un diagramme de séquence pour les plus importants, compte tenu de la disponibilité d'un canal de données bidirectionnel à faible débit entre le dispositif de gestion et les sites de communication. Ces protocoles facilitent la gestion, permettent d'offrir une large diversité de nouveaux services et facilitent la récupération.

I.3.6.1 Revalidation des certificats

Afin de faciliter entre autres la mise sur liste rouge d'un utilisateur, le contrôleur doit revalider périodiquement les certificats figurant dans les cartes à mémoire des sites de communication. Lorsque la gestion relèvera exclusivement du centre NMC, cette phase sera beaucoup moins importante. La base de données des clés publiques du tiers de confiance (contrôleur) est la même que pour la gestion.

Sur la Figure I.3 qui suit, le tiers de confiance représente UN rôle du contrôleur. L'utilisateur est le responsable de la carte à mémoire (celui qui connaît le code pin) au niveau du site de communication.



Les flèches noires doubles représentent les messages; les flèches blanches simples représentent les flux de données.

Figure I.3/J.96 – Diagramme de séquence pour la revalidation de certificat

En ce qui concerne les autres services partageant la sécurité du système CAS, d'autres tiers de confiance pourraient être introduits. Des serveurs de certificats SPKI apparaissent sur l'Internet et peuvent être utilisés pour le commerce électronique, les réseaux privés virtuels, etc. Cela suppose une certification croisée entre tiers de confiance et donc l'accord du centre NMC, évitant ainsi toute compromission de la sécurité.

I.3.6.2 Demande de titres d'accès

Dans la Figure I.4, on présente les messages dans le cas d'un canal bidirectionnel entre le centre NMC et les sites de communication. Les notations sont les mêmes que pour le paragraphe précédent.

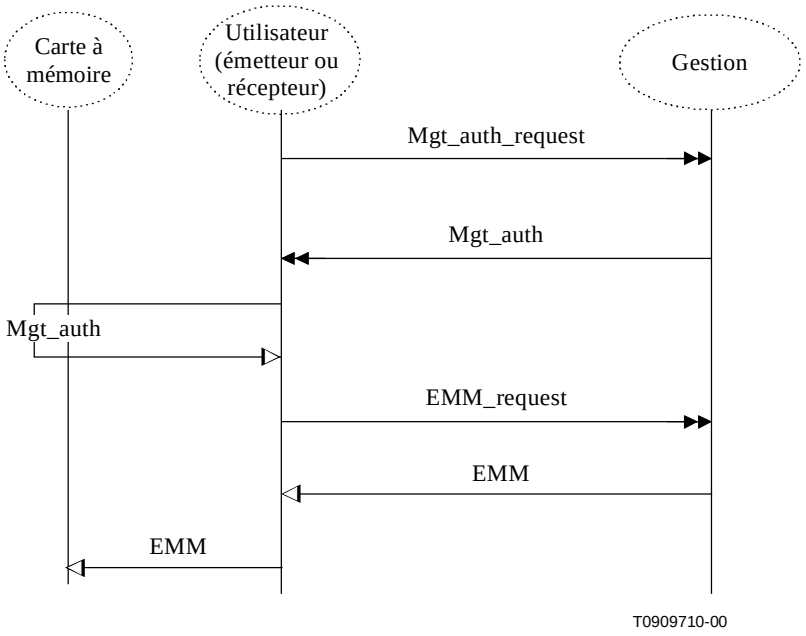


Figure I.4/J.96 – Demande de titres d'accès

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Genève, 2001