UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.93

(03/98)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

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

Services numériques auxiliaires propres aux transmissions télévisuelles

Prescriptions d'accès conditionnel dans le réseau de distribution secondaire de la télévision numérique par câble

Recommandation UIT-T J.93

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE J

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

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

RECOMMANDATION UIT-T J.93

PRESCRIPTIONS D'ACCÈS CONDITIONNEL DANS LE RÉSEAU DE DISTRIBUTION SECONDAIRE DE LA TÉLÉVISION NUMÉRIQUE PAR CÂBLE

Résumé

La présente Recommandation traite des prescriptions, des interfaces matérielles et logicielles, des politiques et des procédures relatives à l'accès conditionnel pour l'acheminement secondaire de signaux numériques de télévision et de données par systèmes câblés.

Source

La Recommandation UIT-T J.93, élaborée par la Commission d'études 9 (1997-2000) de l'UIT-T, a été approuvée le 18 mars 1998 selon la procédure définie dans la Résolution n° 1 de la CMNT.

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.

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.

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 J.93

PRESCRIPTIONS D'ACCÈS CONDITIONNEL DANS LE RÉSEAU DE DISTRIBUTION SECONDAIRE DE LA TÉLÉVISION NUMÉRIQUE PAR CÂBLE

(Genève, 1998)

1 Domaine d'application

La présente Recommandation énumère les prescriptions applicables aux systèmes d'accès conditionnel pour la distribution secondaire de la télévision numérique et de données au moyen d'un réseau de câbles. Les caractéristiques d'accès conditionnel précisément choisies pour mise en œuvre dans un système spécifique devront être déduites des prescriptions applicables à ce système.

2 Références

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] Recommandation UIT-T J.83 (1997), *Systèmes numériques multiprogrammes pour la distribution par câble des services de télévision, son et données*.

[2] Recommandation UIT-T J.84 (1997), *Distribution par réseaux à tête de réception collective par satellite de signaux numériques multiprogrammes pour services de télévision, son et données*.

3 Définitions

La présente Recommandation définit les termes suivants.

3.1 **algorithme**: processus mathématique qui peut être utilisé pour l'embrouillage et pour le désembrouillage d'un flux de données.

3.2 **authentification**: processus destiné à permettre au système de vérifier avec certitude l'identité d'un tiers.

3.3 **codage d'autorisation**: mot numérique qui décrit la personnalité de l'abonné ou la capacité d'accès au service de son décodeur.

NOTE – Ce mot de code, qui est fondé sur l'accès au service autorisé par le système de facturation, détermine les clés qui seront distribuées à chaque client. Ce mot est nécessaire au niveau de chaque décodeur pour autoriser le décryptage de tout programme.

3.4 **système d'accès conditionnel (CA, *conditional access system*)**: système complet qui garantit que les services de distribution par câble ne sont accessibles qu'à ceux qui sont habilités à les recevoir et que la commande de tels services n'est pas sujette à modification ou à répudiation.

3.5 **analyse cryptographique**: science de la récupération du contenu d'un message sans accéder à la clé physique (ou à la clé électronique dans un système cryptographique électronique).

3.6 **facteur d'utilisation cryptographique**: capacité maximale de sécurisation d'un processus cryptographique, fondée sur le nombre total de bits qui peuvent être chiffrés en sécurité, avant qu'il devienne souhaitable de modifier la clé.

3.7 **déchiffrement**: processus inverse de la fonction de chiffrement (voir ce terme) afin d'obtenir des services d'images, de son et de données utilisables.

3.8 **clé électronique**: signaux de données utilisés pour commander le processus de déchiffrement dans les décodeurs d'abonnés.

NOTE – Il existe au moins trois types de clés électroniques: celles qui sont utilisées pour les flux de signaux de télévision; celles qui sont utilisées pour protéger les opérations des systèmes de contrôle d'accès; et celles qui sont utilisées pour la distribution de clés électroniques sur le système câblé. Voir également ci-dessus le terme "codage d'autorisation", qui est aussi une clé.

3.9 **cryptage**: processus de chiffrement des signaux afin d'éviter un accès non autorisé.

3.10 **service plein temps**: service par abonnement qui reste à la disposition des abonnés au cours des heures de fonctionnement du système d'acheminement.

NOTE – D'autres services, comme les films au paiement par séance, ne sont au contraire disponibles que pendant une période spécifique.

3.11 **serveur**: dispositif offrant une fonctionnalité généralisée, où l'on peut se connecter à des modules contenant des fonctions spécialisées.

3.12 **intégrité**: capacité d'une fonction à résister à une usurpation pour un usage non autorisé, ou à une modification en vue de donner des résultats non autorisés.

3.13 **résistance à l'intrusion**: capacité d'un objet matériel à refuser l'accès physique, électrique ou électromagnétique d'un tiers non habilité à une fonctionnalité interne.

3.14 **module**: petit dispositif non autonome qui est conçu pour exécuter des tâches spécialisées en association avec un serveur.

3.15 **non-répudiation**: processus par lequel l'expéditeur d'un message (par exemple une demande de paiement à la séance) ne peut pas nier avoir envoyé ce message.

3.16 **condensation unilatérale**: processus mathématique ou algorithme permettant de convertir un message de longueur variable en mot numérique de longueur fixe, de telle manière qu'il soit très difficile de calculer le message original d'après ce mot et très difficile de trouver un deuxième message contenant le même mot.

3.17 **paiement à la séance**: système de paiement dans lequel l'abonné peut payer pour un programme individuel ou pour une période spécifiée.

3.18 **piraterie**: acte consistant à accéder sans autorisation à des programmes, habituellement afin de revendre cet accès pour réception non autorisée.

3.19 **cryptographie à clé publique**: technique cryptographique fondée sur un algorithme à deux clés (publique et privée), dans laquelle un message est chiffré avec la clé publique mais ne peut être déchiffré qu'au moyen de la clé privée. Egalement appelé *système PPK* (clé privée-publique).

NOTE – Le fait de connaître la clé publique ne permet pas d'en déduire la clé privée.

Par exemple, le correspondant A construit une clé publique et une clé privée de ce type. Il envoie la clé publique sans restriction à tous ceux qui souhaitent communiquer avec lui, mais il garde la clé privée secrète. Tous ceux qui possèdent la clé publique peuvent alors crypter un message pour le correspondant A, mais seul celui-ci peut décrypter ces messages, à l'aide de sa clé privée.

3.20 **chiffrement**: processus consistant à utiliser une fonction de cryptage pour rendre des signaux de télévision et de données inutilisables par des tiers non autorisés.

3.21 **signature sécurisée**: processus mathématique permettant de garantir l'origine et l'intégrité d'un message transmis.

NOTE – Si on utilise un système à signature sécurisée, l'expéditeur ne peut pas nier avoir envoyé le message et le destinataire peut déterminer si le message a été modifié.

3.22 **flux de transport**: flux de transport de type MPEG-2.

4 Travaux antérieurs

Compte tenu de l'avènement de la distribution de la télévision numérique par câble et de données, de nouvelles normes sont requises pour le sous-système d'accès conditionnel (CA, *conditional access*) ou de sécurité qui remplit les diverses fonctions associées à cet élément de système. Il existe de nombreuses activités normalisées qui s'appliquent directement à l'accès conditionnel des signaux de télévision et de données par câble: ces normes sont actuellement en cours d'élaboration à l'échelle mondiale. Il existe d'autres organisations qui traitent parallèlement de la sécurité de ces signaux en visant un objectif plus large, englobant également la télévision et les données.

4.1 Télévision

Comme dans le cas des transmissions actuelles de télévision analogique par câble, il existe diverses exigences pour les différents types de données numériques de programmation télévisuelle qui seront acheminés jusque dans les locaux des utilisateurs par des systèmes de distribution par câble. Ces exigences sont les suivantes:

- services de télévision par abonnement à une période entière au niveau de base;
- services de télévision par abonnement à une période entière au niveau d'une chaîne réservée;
- services de télévision transactionnelle cohérente comme le paiement à la séance;
- services de télévision à court terme, faisant partie d'une émission multimédia à des fins statistiques, commerciales ou informatives.

L'acheminement par câble de programmes de télévision pose les mêmes problèmes fondamentaux de sécurité que les systèmes de radiodiffusion, à satellites, de réception collective de télévision par satellite (SMATV, *satellite master antenna television*) et de radiodistribution multipoint (MMDS, *multichannel multipoint distribution systems*). Ces problèmes proviennent surtout de la nécessité de placer dans les locaux de l'utilisateur un décodeur opérationnel contenant les données actuelles de protection par clés, un de ces éléments pouvant aussi être le pirate car il peut y être soumis à des attaques évoluées sans risque de détection physique. Dans un système gouvernemental ou militaire traditionnel à clés symétriques, cela revient à donner à l'ennemi la clé cryptographique actuelle. Des mesures physiques, telles que des microprocesseurs protégés, rendent l'opération plus difficile mais aucune de ces contre-mesures ne retardera longtemps un professionnel. L'acheminement par câble présente l'avantage que sa nature de système fermé permet de mettre en œuvre certaines politiques et procédures – présentées ci-dessous – afin de rendre vains les efforts du pirate.

Lors de la formulation des prescriptions d'accès conditionnel, il faut toujours prêter attention à l'évaluation des risques et des dangers, ainsi que des coûts financiers et opérationnels des contre-mesures recommandées. La notion de *risque* vise ce qui pourrait être perdu si le système d'accès conditionnel devait être forcé. Dans le cas des systèmes câblés, le risque est la perte de revenu-système par vol de signal ou par usurpation de la commande du système par une tierce partie. La notion de *danger* vise l'individu, l'organisation ou le mécanisme par lequel les contre-mesures d'accès conditionnel sont forcées et font courir un risque. Toutes les contre-mesures, même s'il ne s'agit que de procédures, représentent une certaine dépense pour le système câblé mis en exploitation. Si la dépense nécessaire pour supprimer le danger est trop grande par rapport au risque, ce n'est pas une option rentable.

4.2 Distribution secondaire de données par câble

(Ce point fera l'objet d'un complément d'étude.)

5 Prescriptions d'accès conditionnel dans les systèmes câblés

On peut subdiviser et définir comme indiqué dans le Tableau 1 ci-dessous le domaine général de l'accès conditionnel (CA, *conditional access*), appliqué à la distribution secondaire de signaux numériques de télévision et de données sur des systèmes câblés.

Tableau 1/J.93 – Prescriptions d'accès conditionnel et explications

Prescription d'accès conditionnel	Explication
sécurité du signal	processus qui assure le cryptage des signaux numériques de télévision ou des messages associés afin d'empêcher un accès non autorisé à leur contenu (voir 5.1)
distribution de clés	processus par lequel ce sous-système produit, distribue et mémorise les clés cryptographiques pour les codeurs de tête de ligne et pour les décodeurs de locaux d'abonné (voir 5.2)
signature sécurisée	processus qui réalise l'authentification de l'utilisateur et sa non-répudiation transactionnelle (voir 5.3)
intégrité du système de commande	processus qui empêche l'usurpation de la commande du système par une entité non autorisée (voir 5.4)
codage d'autorisation	processus protégeant la personnalité d'accès du bloc de décodage d'abonné contre une modification non autorisée (voir 5.5)

5.1 Prescriptions relatives à la sécurité des signaux

Il est prescrit que tout canal numérique de télévision ou de données acheminé par un système câblé soit soumis à un chiffrement par cryptage numérique, au choix de la gestion-systèmes. L'accès à tous les services différenciés doit être contrôlé par un processus de chiffrement. Les prescriptions générales ci-après s'appliquent à de tels processus cryptographiques:

- le processus cryptographique choisi doit fonctionner en mode clé privée-clé publique (PPK, *private-public key*), en mode de clés symétriques ou en mode d'utilisation de processus PPK afin de distribuer des clés secrètes pour des transactions spécifiques;
- l'algorithme cryptographique choisi pour le chiffrement et le déchiffrement d'un flux de signaux de télévision ou de données associé à une porteuse radioélectrique unique doit être applicable aux systèmes de distribution décrits dans les Recommandations J.83 [1] et J.84 [2];
- le facteur d'utilisation du processus cryptographique assurant le chiffrement doit être suffisant pour satisfaire à de bons critères de conception cryptographique;
- l'algorithme cryptographique choisi pour le chiffrement doit être suffisamment robuste pour qu'une attaque cryptographique directe par une tierce partie soit rendue, aussi bien initialement qu'ultérieurement, inefficace en termes de coût et de temps;
- les caractéristiques opérationnelles du processus cryptographique – telles que l'élasticité aux erreurs, le temps de latence, le débit et ses variations, ainsi que les paramètres d'interface – doivent être optimisées selon les caractéristiques de flux de transport MPEG-2 ou de la transmission de données, selon le cas;
- l'algorithme cryptographique choisi pour le chiffrement des signaux doit être agréé au niveau international;
- le surdébit nécessaire dans le système de contrôle pour assurer un fonctionnement continu de l'algorithme de chiffrement doit être minimisé;
- l'algorithme doit être conçu de façon à faciliter l'accès aux points de diagnostic pour le matériel, le logiciel et la micrologique, requis pour les audits intensifs par système de sécurité et pour les mesures anti-altération frauduleuses.

5.2 Prescriptions relatives à la distribution et à la mémorisation des clés

L'élément fondamental de tous les systèmes de contrôle d'accès est la clé cryptographique binaire qui est utilisée en conjonction avec les autres éléments matériels et logiciels du système de contrôle d'accès afin de restreindre aux seuls utilisateurs autorisés l'accès au contenu des programmes. Une clé peut être attribuée à un groupe ou à un niveau de services de télévision se composant de plusieurs canaux chiffrés par la même clé. Une clé peut également être attribuée à un canal de télévision particulier, comme dans le cas d'un programme réservé. Une clé peut également être attribuée à un canal de télévision particulier, mais seulement pendant une période prédéterminée, comme dans le cas de services de paiement à la séance. Il est donc nécessaire que le mécanisme d'accès conditionnel ait la capacité de mémoriser des clés multiples, le cas échéant.

En plus des clés opérationnelles ci-dessus mentionnées, chaque codeur ou décodeur doit avoir la capacité de mémoriser un unique nombre binaire d'identification permanent et non modifiable, qui peut servir à identifier l'unité ou à constituer une clé pour la diffusion restreinte de signaux vers cette unité. Pour la télévision, il est parfois nécessaire que les codeurs et décodeurs aient la capacité de mémoriser et d'utiliser des clés additionnelles selon les nécessités de subdivision d'un système en compartiments afin de diminuer le risque présenté par des abonnés/pirates, par exemple un système de clé à cohérence de jonction, dont un certain élément est modifié selon l'adresse interurbaine de l'abonné. Le nombre et la nature exacts de ces clés à cohérence de système relèvent des spécifications établies par les vendeurs de produits de contrôle d'accès.

Toutes les clés, qu'elles soient de type opérationnel, à identificateur unique ou à cohérence de système, doivent être mémorisées dans des circuits protégés contre les intrusions de façon qu'il soit trop coûteux d'y accéder par des moyens physiques, électriques ou électromagnétiques, ou par des moyens cryptographiques.

La longueur d'une clé quelconque dépend des caractéristiques et des points faibles propres à l'algorithme cryptographique choisi. Mais elle doit être suffisante pour répondre aux prescriptions de sécurité opérationnelle de chaque système.

Le débit effectivement requis pour la transmission de données cryptographiques dépend du cycle de reconstitution des clés prescrit, du volume de l'univers enclavé, du nombre de clés opérationnelles utilisées et de la longueur des clés individuelles. Ces cahiers de charges doivent être clairement indiqués dans toute description de système de contrôle d'accès destiné à servir dans un système câblé.

La distribution des clés peut être réalisée dans la bande au moyen de paquets de données insérés dans le flux de paquets MPEG-2 ou hors bande au moyen d'une porteuse de données autonome dans le système. Dans un cas comme dans l'autre, les émissions de distribution de clés représentent une cible de haute valeur pour les pirates de signaux: il faut donc les protéger à un degré allant nettement au-delà de ce qui est nécessaire pour la sécurité des signaux de télévision. Si l'algorithme choisi pour la sécurité des signaux n'assure pas ce degré de protection, il faut utiliser un autre algorithme pour la distribution des clés. En toutes circonstances, une clé distincte est utilisée pour la protection du système de distribution de clés. La protection des données d'enclavement doit être suffisante pour résister à un forçage pendant une durée compatible avec les règles de sécurité applicables à chaque système d'exploitation de câbles.

5.3 Signature sécurisée

La signature sécurisée garantit de façon unique que le message reçu provient de la source indiquée, qu'il n'a pas été modifié et que son expéditeur ne peut pas nier l'avoir envoyé. Ce processus doit protéger les messages de commande et de contrôle qui peuvent être émis dans un sens ou dans l'autre sur le réseau câblé.

Il existe plusieurs exemples bien connus de ce type de signature, dont en particulier les algorithmes RSA (*Rivest-Shamir-Adleman*) ou algorithme de signature numérique (DSA, *digital-signature-algorithm*). Ces systèmes comportent un algorithme sûr de condensation qui réduit la longueur arbitraire d'un message à une longueur fixe par un hachage qui est très particulier au message original et qui a les caractéristiques suivantes:

- dans le cas d'un message quelconque, il est facile et rapide de calculer sa condensation unique;
- dans le cas d'une condensation quelconque, il est virtuellement impossible de calculer le message original;
- dans le cas d'un message quelconque et de sa condensation unique, il est virtuellement impossible de trouver un autre message qui produise la même condensation.

Certaines attaques classiques sur les condensations calculées limitent effectivement à environ $2^{(1/2 \text{ longueur de condensation})}$ le nombre d'opérations analytiques nécessaires pour attaquer l'algorithme. En d'autres termes, une condensation de 64 bits peut être rompue avec 2^{32} opérations, ce qui peut représenter une heure de travail sur un ordinateur personnel moderne, à vitesse élevée. C'est pourquoi toute condensation utilisée pour la fonction de signature sécurisée dans un système câblé doit avoir une longueur suffisante pour répondre aux cahiers des charges de ce système.

5.4 Intégrité du système de contrôle

Cette fonctionnalité est mise en œuvre afin de garantir que le système de contrôle ne peut pas être ouvert par des tiers non autorisés en vue de voler des signaux ou d'interrompre des services. Les signaux de commande présentant un assez faible risque de vol ou d'interruption sont chiffrés sous leur forme normale avant d'être transmis à un décodeur individuel, à un groupe de décodeurs, ou globalement à tout décodeur présent dans le système. Les messages de commande qui présentent une valeur élevée peuvent être soumis à des contre-mesures additionnelles. Le système de contrôle nécessite une clé distincte et unique par rapport aux clés utilisées pour la sécurité des signaux ou pour la distribution des clés.

5.5 Codage d'autorisation

En plus du processus de protection cryptographique des données de programme, il faut un processus sûr pour mettre en œuvre l'habilitation ou l'autorisation de chaque abonné. En tête de câble, cette personnalité de service détermine les clés cryptographiques dont le téléchargement vers chaque abonné est autorisé. Cette entité sert également, dans l'unité de l'abonné, de protection contre l'insertion non autorisée, à partir d'une source externe, de clés cryptographiques piratées. Ce processus peut être mis en œuvre par une technique quelconque.

6 Sécurité de fabrication et de distribution

Les équipements matériels qui sont fabriqués pour le contrôle d'accès de signaux numériques de télévision et de données sur des systèmes câblés sont tenus de répondre à certaines normes afin d'assurer l'intégrité des systèmes qui les emploient. Il s'agit de ce qui suit:

- tous les documents relatifs à la conception des circuits intégrés et aux vecteurs d'essai doivent être numérotés et contrôlés à intervalles réguliers, toute pièce manquante étant répertoriée pour examen par d'éventuels clients;
- tous les circuits intégrés qui ont été fabriqués pour utilisation dans un matériel de contrôle d'accès seront examinés et chaque élément sera répertorié quant à sa finalité, y compris son intégration dans un serveur, le numéro de série de ce serveur, son itinéraire de distribution et l'identification du système d'exploitation de câble dans lequel il doit fonctionner. En outre, tous les circuits intégrés seront marqués d'un numéro d'identification unique et indélébile, lisible aussi bien optiquement et électriquement.

7 Reprise sur défaillance et forçage

Pour des raisons d'ordre financier, opérationnel et sécuritaire, il est prescrit que les circuits ou logiciels de contrôle d'accès soient facilement amovibles et remplaçables, sans qu'il soit nécessaire de remplacer également les serveurs avec lesquels ils interagissent. De tels remplacements peuvent être nécessaires en raison d'une défaillance des éléments mécaniques, électriques ou logiciels du dispositif de contrôle d'accès, parce qu'une modification de structures commerciales et architecturales appelle une fonctionnalité nouvelle ou différente, ou parce qu'une attaque élaborée et déployée a provoqué un forçage rentable de la sécurité et donc une perte inacceptable de revenus ou de commande du système.

L'aptitude au retrait implique que l'ensemble des circuits et des logiciels de contrôle d'accès soit contenu dans un module qui a une interface avec un serveur, comme un décodeur placé au-dessus ou à l'arrière du récepteur, avec un téléviseur ou un magnétoscope, avec un modem ou avec un ordinateur personnel. L'aptitude au remplacement implique qu'il n'y ait pas de facteurs d'ordre interfacial, opérationnel, juridique ou financier, qui rendraient impossible le remplacement de la fonctionnalité CA.

Pour répondre à ces prescriptions, l'interface entre le module CA amovible et le serveur doit être d'architecture non exclusive et ouverte. Il existe un certain nombre de telles interfaces et des facteurs de forme de module ont été couramment définis pour d'autres applications internationales pouvant être appropriées dans ce cas, par exemple la spécification d'interface commune DVB (diffusion vidéo-numérique) (voir [I.3] ci-dessous) ou la spécification définie par la norme nationale sur la sécurité renouvelable (voir [I.4]). (Ce point fera l'objet d'un complément d'étude.)

8 Disposition concernant la retenue pour garantie de clé

Si la loi nationale d'un pays quelconque nécessite l'inclusion d'une capacité de retenue pour garantie de clé dans le système de contrôle d'accès, une fonctionnalité doit permettre de mettre en œuvre cette capacité. Au moment de l'approbation de la présente Recommandation, aucune prescription de ce type n'existe dans un pays membre signataire de l'UIT.

9 Politiques et procédures

Aucun système cryptographique n'est vraiment sûr sans un ensemble de politiques et de procédures opérationnelles sous-jacentes pour prendre en charge ces fonctions. La manière dont ces politiques et procédures sont mises en œuvre dans un système d'exploitation de câble donné dépend de la situation. Les directives suivantes sont donc à prendre comme des pratiques recommandées et adaptées à chaque situation opérationnelle selon les besoins:

- les personnes qui ont accès au système de contrôle d'accès en tête de câble ou dans un concentrateur régional, ou qui manipulent couramment des modules de raccordement d'abonné, doivent faire l'objet d'un programme de fiabilité humaine;
- l'accès aux éléments clés du système de contrôle d'accès doit être limité et la surveillance de ces zones doit être assurée;
- les grands systèmes ou réseaux de câbles doivent être compartimentés par des procédures cryptographiques afin de réduire l'aire d'activité des abonnés/pirates;
- les systèmes de contrôle d'accès non homologués qui sont en cours d'examen en vue d'un achat, doivent être soumis aux essais d'un organisme de certification indépendant;
- un système d'audits de sécurité à intervalles réguliers doit être mis en place et suivi;
- des procédures doivent être mises en place de façon que, si une unité illégale de contrôle d'accès est saisie en activité, l'identification du pirate/abonné puisse être effectuée par examen de l'identificateur unique se trouvant dans cette unité, avec son code d'autorisation.

Appendice I

Bibliographie

Les normes régionales et internationales suivantes sont énumérées ci-dessous à titre d'information d'appui, si applicables:

[I.1] ISO/CEI 13818-1:1996, *Technologies de l'information – Codage générique des images animées et du son associé*.

[I.2] ISO 7816: *Cartes d'identification*, Parties 1 à 6.

[I.3] Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, (Spécification d'interface commune pour l'accès conditionnel et autres applications des décodeurs pour diffusion vidéo-numérique), *DVB A007*, juillet 1995.

[I.4] National Renewable Security Standard, (Norme nationale sur la sécurité renouvelable), *EIA/NCTA IS-679*, Parties A et B.

[I.5] Digital Video Broadcasting – Support for use of Scrambling and Conditional Access with Digital Broadcasting Systems, (Diffusion vidéo-numérique – Prise en charge de l'utilisation de l'embrouillage et de l'accès conditionnel dans les systèmes de diffusion numérique), *UER*.

[I.6] *Caractéristiques générales d'un système de radiodiffusion à accès conditionnel*, Rapport 1079-1 du CCIR (1990).

[I.7] Recommandation 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*.

[I.8] Recommandation UIT-T J.91 (1994), *Méthodes techniques pour garantir la confidentialité sur les transmissions internationales de télévision à grande distance*.

[I.9] Contribution tardive D19 de la Commission d'études 9 de l'UIT-T (période 1997-2000): *The conditional access system of digital cable television in Japan*, (Le système d'accès conditionnel du réseau câblé de télévision numérique au Japon).

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	**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, de télégraphie, de télécopie, circuits téléphoniques 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 pour données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information
Série Z	Langages de programmation