UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.95

(09/99)

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

Protection antipiratage de la propriété intellectuelle des émissions diffusées sur les systèmes de télévision par câble

Recommandation UIT-T J.95

(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.95

PROTECTION ANTIPIRATAGE DE LA PROPRIÉTÉ INTELLECTUELLE DES ÉMISSIONS DIFFUSÉES SUR LES SYSTÈMES DE TÉLÉVISION PAR CÂBLE

Résumé

La présente Recommandation décrit les prescriptions nécessaires à un système pour qu'il protège les droits de propriété intellectuelle (IPR, *intellectual property rights*) des entités de programmation télévisuelle contre la copie, la duplication et la distribution illégales de leur propriété de création. Le système décrit ici présente des aspects qui interdisent aux personnes individuelles non autorisées d'accéder à des flux de données cryptées du groupe d'experts pour les images animées (MPEG, *moving picture experts group*). La présente Recommandation présente également les techniques de filigranage des signaux télévisuels pour les identifications et les autorisations de copie.

Le matériel décrit dans la présente Recommandation contient à la fois des descriptions et des analyses des procédés techniques spécifiques de protection antipiratage.

Source

La Recommandation UIT-T J.95, élaborée par la Commission d'études 9 (1997-2000) de l'UIT-T, a été approuvée le 16 septembre 1999 selon la procédure définie dans la Résolution n° 1 de la CMNT.

Mots clés

Accès conditionnel, enregistrement vidéo, MPEG, sécurité, télévision, télévision numérique.

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.95

PROTECTION ANTIPIRATAGE DE LA PROPRIÉTÉ INTELLECTUELLE DES ÉMISSIONS DIFFUSÉES SUR LES SYSTÈMES DE TÉLÉVISION PAR CÂBLE

(Genève, 1999)

1 Introduction et travaux antérieurs

L'enregistrement et la duplication sans autorisation de la propriété intellectuelle en télévision ont entraîné un vaste trafic international illégal, et ont coûté aux détenteurs de la propriété intellectuelle des sommes importantes en manque à gagner. Avec le passage à la télévision MPEG numérique, le problème est plus grave encore dans la mesure où les enregistrements numériques peuvent être dupliqués dans leur qualité originale sur de nombreuses générations, alors que la fidélité des enregistrements analogiques se réduit avec chaque génération successive, ce qui rend lesdits enregistrements finalement inutilisables. Dans les systèmes où le signal numérique MPEG est reçu et transformé en un signal analogique équivalent pour la visualisation des images sur un récepteur de télévision uniquement analogique, la qualité de ce signal analogique fait qu'il constitue également une cible pour le piratage, et qu'il doit donc être protégé.

Compte tenu de ces objectifs, des procédés ont été développés afin de masquer les marquages numériques de propriété intellectuelle en télévision numérique, d'une manière qui soit à la fois non détectable et inviolable. Ce procédé, appelé *filigranage*, est fondé sur la cryptographie mais n'est pas de nature cryptographique. Il contient l'identité du détenteur du droit de propriété intellectuelle ainsi que les règles de propriété relatives aux copies, à savoir: pas de copie, copie unique pour usage personnel ou nombre de copies illimité.

Outre le filigranage, la protection antipiratage nécessite que les signaux télévisuels numériques MPEG avec texte en clair, ou leurs équivalents analogiques, ne puissent jamais passer par des lignes de signaux extérieures aux limites physiques du matériel électronique grand public. Pour répondre à cette prescription, un système de chiffrement secondaire doit prendre en charge temporairement ces signaux lors de leur distribution à l'intérieur, en format numérique ou analogique. Un système cryptographique est proposé pour couvrir les signaux numériques MPEG et un système commercialisé existant, qui modifie rapidement la base de temps, est proposé pour couvrir les signaux analogiques.

Afin de faciliter les poursuites à l'encontre de toute personne susceptible de contourner ces parades, il est souhaitable que les procédés soient déposés et protégés par des procédures d'attribution de licences. Il convient toutefois que l'attribution de licences soit effectuée avec soin de manière à n'entraîner aucune discrimination inutile ou tout autre inconvénient pour les entreprises qui doivent produire ces systèmes de protection antipiratage.

2 Domaine d'application

La présente Recommandation décrit à la fois les techniques cryptographiques de protection de l'accès aux signaux de télévision numérique MPEG avec texte en clair, et un procédé, dit de *filigranage*, qui marque de manière indélébile la propriété intellectuelle quant à son détenteur et quant aux exigences du détenteur concernant la copie. Un système de protection antipiratage satisfaisant protège le privilège juridique du détenteur des droits de propriété intellectuelle afin de contrôler la distribution du produit protégé.

Il convient d'envisager l'utilisation des procédés de protection antipiratage des contenus décrits dans la présente Recommandation dans d'autres applications qui nécessitent une protection similaire, telles que la diffusion par la voie des ondes (hertziennes), la distribution de programmes enregistrés par exemple par vidéodisque numérique (DVD, *digital video disk*), etc.

3 Références (informatives)

– 1394 Association commerciale, *Specification for AV/C Digital Interface Command Set*.

– Digital Transmission Protection License Agreement, *Development and Evaluation License*, Digital Transmission Licensing Authority.

– Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 1, Version 0.91.

- Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 2, Version 0.90.
- Publication de la CEI 61883-1 (1998), *Interface numérique pour matériel audio/vidéo grand public – Partie 1: Généralités*.
- IEEE Std 1394-1995, *Norme en matière de bus en série à hautes performances*.
- IEEE P1363, *Editorial Contribution to Standard for Public Key Cryptography*, Preliminary Draft, P1363/D3 (11 mai 1998).
- National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS Publication 180-1, 17 avril 1995.
- Toshiba Corporation, *Efficient Implementation of an Elliptic Curve Cryptosystem* (disponible sur http://www.dtcp.com).

4 Définitions

La présente Recommandation définit les termes suivants:

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

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

4.3 **codage d'autorisation**: mot numérique qui décrit l'identité ou la capacité d'accès au service du décodeur de l'abonné.

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 du décodeur d'abonné afin d'autoriser le déchiffrement de tout programme.

4.4 **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.

4.5 **analyse cryptographique**: science de l'extraction du contenu d'un message en l'absence de la clé de chiffrement (ou de la clé électronique dans un système cryptographique électronique).

4.6 **cycle 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.

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

4.8 **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 commande; et celles qui sont utilisées pour la distribution de clés électroniques sur le réseau câblé. Voir également ci-dessus le terme "codage d'autorisation", qui est aussi une clé.

4.9 **cryptage**: processus de chiffrement des signaux destiné à éviter un accès non autorisé.

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

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

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

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

4.13 **intensité 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.

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

4.15 **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.

4.16 **hachage irréversible**: algorithme ou processus mathématique 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 produisant le même mot.

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

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

4.19 **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 (PPK, *private-public key*).

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.

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

4.21 **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.

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

5 Filigranage de la propriété intellectuelle en télévision numérique

5.1 Rappel et prescriptions fonctionnelles

Une des conditions fondamentales de la définition de la propriété intellectuelle est que celle-ci doit être marquée d'une manière qui l'identifie en tant que telle et qui stipule l'identité du détenteur de ladite propriété. Pour les documents imprimés, cette propriété s'exprime communément par le symbole de marque commerciale universellement reconnu, un renvoi indiquant le détenteur de la propriété. Ce symbole peut souvent être suivi d'une déclaration qui détermine les instructions du propriétaire par rapport à son utilisation, par exemple: "copie possible uniquement pour usage non commercial". Toutes les monnaies utilisent différentes méthodes pour distinguer le cours légal de toute contrefaçon.

Les producteurs de la propriété télévisuelle souhaitent pouvoir marquer leur droit de propriété intellectuelle d'une manière qui délimite ce droit ainsi que les restrictions d'utilisation imposées en la matière. Les prescriptions relatives au système de filigranage sont les suivantes:

1) indiquer clairement le détenteur du droit de propriété ainsi que les autorisations de copie associées;

2) le marquage du produit télévisuel doit être présent dans toutes ou presque toutes les trames;

3) le marquage doit être non détectable dans la présentation du produit artistique, même de manière subliminale;

4) la modification non autorisée du marquage doit être pratiquement impossible sans dégrader le produit original au-dessous de sa fidélité commerciale;

5) le marquage du produit doit pouvoir être lu par une machine;

6) le taux d'erreurs par fausse détection doit être négligeable à long terme (par exemple 1 s sur 30 ans);

7) les données incorporées doivent être décelables par le truchement d'adaptations qui modifient le format d'écran ou lors des fonctions de zoom;

8) les nombreux filigranes doivent pouvoir coexister sans aucun brouillage.

La façon dont ces fonctions sont assurées dans un système de filigranage constitue l'objet d'un travail considérable, dont deux procédés sont indiqués dans les Appendices I et II.

5.2 Incidences pour le procédé de conception

Ces prescriptions fonctionnelles laissent entendre que la meilleure façon de procéder au marquage de la propriété intellectuelle télévisuelle consiste à utiliser certains aspects de la cryptologie. En utilisant différents procédés, le détenteur de la propriété intellectuelle peut être assuré que le marquage est difficile à détecter, pratiquement impossible à modifier, facilement intégrable à chaque trame, si nécessaire, et déchiffrable par un matériel dûment autorisé d'identification et d'électronique grand public. L'incidence de l'utilisation d'un procédé cryptographique sur la vidéo originale est la très faible augmentation du bruit de fond du signal. La sélection d'un ensemble de procédés cryptographiques communs ainsi que le choix du mode d'application de ces algorithmes dans le matériel ne font pas partie de la présente Recommandation.

6 Mesures de protection antipiratage du contrôle d'accès

6.1 Contexte et prescriptions fonctionnelles – Signaux analogiques

Les signaux analogiques protégés contre la copie qui sont transmis par l'intermédiaire d'un câblage d'interconnexion au téléspectateur après avoir été reçus d'un système câblé secondaire et émis à l'origine en format analogique ou convertis en format analogique à partir du format numérique dans le boîtier décodeur, doivent être protégés contre toute copie imprévue au moyen d'un ou de plusieurs systèmes actuellement disponibles afin de prévenir la copie des signaux analogiques sur un magnétoscope traditionnel. Les signaux qui n'impliquent aucune protection antipiratage, ou ceux qui sont convertis pour être utilisés dans le dispositif d'affichage et qui ne sont pas disponibles en format de texte clair à l'extérieur de ce dispositif, n'ont pas besoin d'être ainsi protégés.

6.2 Contexte et prescriptions fonctionnelles – Signaux numériques MPEG

Le principal objectif de la présente Recommandation est de s'assurer que l'on ne peut accéder facilement aux signaux de télévision numérique MPEG en texte clair afin d'en faire des enregistrements non autorisés. Cela signifie que tous les signaux MPEG, lorsqu'ils sont acheminés vers les locaux client par un système câblé ou lorsqu'ils sont transférés d'un appareil électronique à l'autre dans ces locaux, doivent être protégés contre tout accès non autorisé. La science relative à l'accès conditionnel, décrite dans la Recommandation J.93, s'applique aux signaux MPEG qui sont acheminés par le système de distribution secondaire. La protection antipiratage s'applique aux signaux transférés entre appareils électroniques dans les locaux client.

Un système qui assure le cryptage et le décryptage des signaux MPEG afin de les transmettre par l'intermédiaire du câblage d'interconnexion dans les locaux client est déclaré satisfaire cette prescription. Le système de cryptage sélectionné doit comprendre les attributs suivants:

1) mise en application simple et économique dans le matériel de grand public;

2) régénération automatique en cas de perte du synchronisme cryptographique;

3) mise en œuvre aussi bien en format de module interne qu'en format de module de point de déploiement (POD, *point of deployment*);

4) possibilité d'autorisation et de retrait d'autorisation depuis un point distant et indication d'état à ce point;

5) impossibilité de défaillance unilatérale intentionnelle ou inintentionnelle empêchant le système de chiffrer le signal MPEG sur le câblage d'interconnexion.

6.3 Fonctionnalité du centre d'autorisation

Avec le système cryptographique décrit ci-dessus, qui est utilisé pour protéger les signaux sur le câblage d'interconnexion, un élément de système externe est requis afin d'exécuter les fonctions suivantes:

1) autoriser et fournir une clé pour le matériel électronique grand public nouvellement installé;

2) retirer le droit d'utiliser des matériels électroniques grand public illégaux ou volés;

3) faciliter les modes de rétablissement sur défaut;

4) fournir un système de contrôle de sécurité et d'exploitation;

5) fournir des rapports aux propriétaires de matériels dont la protection antipiratage a été affectée;

6) coordonner les actions prévues avec les têtes de réseaux de systèmes câblés.

L'efficacité d'exploitation requiert que les domaines d'activité de ces centres d'autorisation soient au moins multiples. Ces centres peuvent être répartis à l'échelle géographique d'une région ou peuvent englober des populations moins importantes. Ils nécessitent une liaison de communications bidirectionnelles avec chaque foyer client concerné et avec chaque dispositif doté de la fonctionnalité de protection antipiratage. Les fonctions d'autorisation et de résolution de mode défaut requièrent un accès en temps quasi réel au matériel électronique grand public. Les impératifs de coût et de commodité feront que ces communications s'effectueront par le biais de réseaux titulaires sans surcharger indûment les opérations existantes.

De plus, des voies de communication sont nécessaires entre les divers centres d'autorisation, avec des voies de retour vers les fournisseurs d'émissions télévisées qui paient pour la protection antipiratage de leurs matériels. La nature de ces voies de retour étant inconnue, leur définition appelle un complément d'étude.

7 Facteurs relatifs à l'inclusion d'une fonctionnalité de protection antipiratage dans la télévision par câble et dans le matériel électronique grand public

7.1 Filigranage

Dans la mesure où le filigrane est incrusté dans la vidéo d'origine au moment de la production et ne peut être déchiffré que par un certain matériel grand public au point d'utilisation, le réseau d'acheminement, *en soi*, n'a aucune responsabilité par rapport à cette fonctionnalité.

7.2 Protection antipiratage du contrôle d'accès

L'impact le plus important sur les systèmes de distribution par câble se produit avec la protection des signaux sur le câblage d'interconnexion dans les locaux client. Chaque élément de l'équipement de traitement des signaux vidéo dans l'installation de l'utilisateur final doit pouvoir être authentifié par le système d'autorisation avec tous les autres dispositifs conjoints de l'utilisateur permettant le traitement des signaux de télévision MPEG. Il doit être également capable de crypter et de décrypter les signaux de télévision MPEG. Tous les dispositifs de source ou d'enregistrement qui constituent le matériel grand public, tels que les lecteurs de vidéodisques, les magnétoscopes ou les boîtiers décodeurs, doivent également pouvoir lire le signal de filigrane de manière à déterminer la position du propriétaire quant à l'enregistrement du programme. Ces fonctions doivent être normalisées car elles doivent s'exercer quel que soit le constructeur ou le secteur industriel et quel que soit le support.

7.3 Autres impacts

Le système décrit requiert la présence de canaux de commande bidirectionnels en temps réel entre les centres de commande régionaux et tous les équipements concernés dans cette région. Le support à utiliser et les protocoles requis ne sont pas encore connus. La définition de ces éléments appelle un complément d'étude.

Appendice I

Approche de l'UER en matière de protection antipiratage de la propriété intellectuelle télévisuelle sur les systèmes de distribution de télévision par câble

Afin de garantir le respect des droits de propriété intellectuelle associés aux programmes TV, la proposition faite ici par l'UER est qu'il doit être possible d'identifier tout objet numérique et de relier cette identification à une base de données contenant toutes les données nécessaires sur les droits de propriété intellectuelle appropriés. En faisant correspondre cette exigence à l'état de l'art dans le domaine de la protection des moyens numériques, l'UER définit les remarques suivantes et propose le modèle de référence ci-après (voir Figure I.1):

1) il convient qu'aucun objet numérique, par exemple une séquence TV, ne soit mis à la disposition du public sans une protection appropriée intégrée à l'objet lui-même, c'est-à-dire que, de manière idéale et à long terme, aucun objet non identifié ne pourra être vendu sur le marché numérique;

2) dans la mesure où les détenteurs des droits de propriété ont besoin de différents types d'informations, il paraît impossible de satisfaire toutes les exigences par le marquage direct des données associées: il convient par conséquent de n'utiliser l'identificateur que comme élément de liaison à une base de données protégée contenant toutes les informations nécessaires;

3) toute partie de séquence pouvant être isolée et réutilisée, aussi petite soit-elle, doit acheminer l'identificateur qui est un élément de liaison à la base de données relative aux droits de propriété intellectuelle;

4) l'identificateur unique le plus court a été établi à 64 bits, permettant ainsi un grand nombre de combinaisons allant de 16 chiffres décimaux à une combinaison d'un nombre moins important de lettres et de chiffres. Un exemple de procédé d'identification à 64 bits est donné dans l'ISO 10918-4 (identification des images fixes); un procédé ISBN, ISSN, ISRC, ISMN, ISWC ou ISAN peut également être utilisé dans le même espace de 64 bits;

5) il convient que le marquage de l'identificateur à 64 bits se situe à l'intérieur de l'objet lui-même de sorte qu'il soit à la fois invisible et qu'il ne puisse être effacé ou modifié sans produire des effets visibles;

6) le contenu de l'identificateur à 64 bits, qui doit être fourni par une autorité d'enregistrement, peut être appelé "plaque d'immatriculation" ou (LP, *license plate*);

7) l'identificateur peut être utilisé pour la liaison avec une base de données contenant les informations relatives aux droits de propriété intellectuelle (filigrane de création) ou les informations relatives à la distribution (filigrane de distribution);

8) par conséquent, deux filigranes peuvent être intégrés au flux de données, avec référence aux remarques 5) à 8). En vue du marquage de toutes les trames, chaque trame I doit être marquée si l'on utilise le format MPEG-2;

9) dans la mesure où un identificateur ne peut être totalement significatif du fait de sa petite taille, il ne peut être utilisé que comme élément de liaison. Le type de liaison peut être une liaison hypertexte entre l'objet et la base de données contenant les informations appropriées;

10) afin de protéger le filigrane, il a été proposé de reproduire le contenu (64 bits) sur une étiquette figurant dans le fichier du flux binaire. Un espace de 64 bits est réservé à cet effet dans le format MPEG-2;

11) il convient également de recommander l'utilisation de l'espace de 64 bits réparti en deux moitiés, les 32 premiers bits définissant l'autorité d'enregistrement originale (REGAUT, *registration authority*) qui a fourni l'identificateur, tandis que les 32 derniers bits seraient utilisés pour numéroter l'objet, avec une capacité de 4 milliards d'identificateurs;

12) un identificateur de ce type actuellement utilisé, est la plaque d'immatriculation ISO multimédia pour l'identification des images fixes (IMLP, *ISO multimedia license plate for still picture identification*) dont la structure est la suivante:

    /code de pays ISO (16 bits)/identité REGAUT (16 bits)/numéro d'enregistrement (32 bits)/

13) les tableaux permettant d'obtenir l'adresse URL de l'autorité d'enregistrement à partir de l'identité de celle-ci seront disponibles sur un site Web permettant d'établir une liaison automatique entre l'objet et ses données relatives aux droits de propriété intellectuelle;

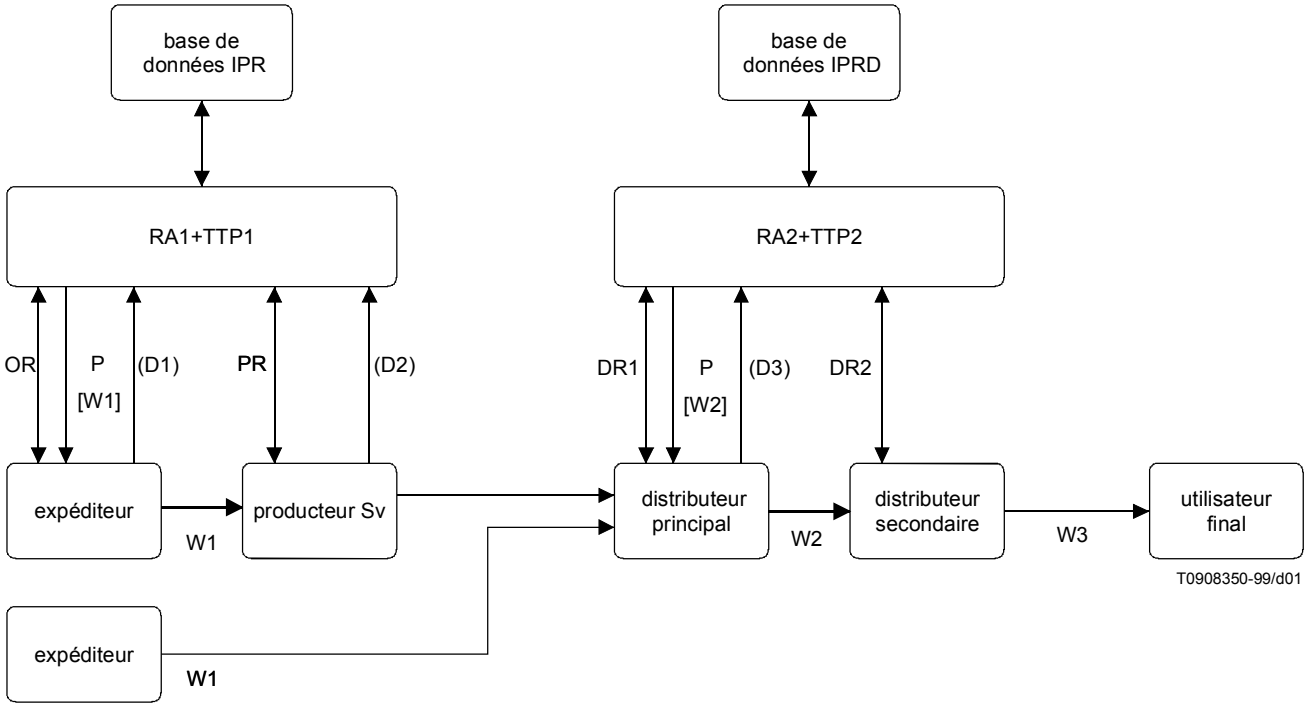
14) le contrôle du flux binaire permettra de déchiffrer les deux filigranes, avec possibilité de liaison automatique aux bases de données où les informations requises sont conservées;

15) le contenu du filigrane peut être utilisé à des fins juridiques, en particulier s'il est fourni par une autorité d'enregistrement;

16) le contenu du filigrane est fourni en échange d'informations supposées fiables et conservées définitivement dans un endroit sûr par l'autorité d'enregistrement;

17) chaque autorité d'enregistrement peut définir son procédé d'enregistrement et doit garantir l'authenticité des données enregistrées;

18) le contrôle d'accès aux données appropriées dépend de la direction de l'autorité d'enregistrement.



OR	immatriculation expéditeur	D2	déclaration de la tâche réalisée (mise en forme ou montage)
P	protection (contenu du filigrane)	DR1	immatriculation distributeur (principal)
D1	déclaration (de la tâche relative à W1)	D3	déclaration (de la distribution effective)
PR	immatriculation producteur Sv	DR2	immatriculation distributeur (secondaire)

Figure I.1/J.95 – Modèle de référence IPR

Appendice II

Proposition de filigrane Galaxy

Résumé

La technique de filigranage Galaxy proposée intègre 8 bits de données comme filigrane numérique transparent dans un flux vidéonumérique non comprimé. Ce filigrane peut être décelé à la fois dans les domaines de la bande de base et du signal MPEG-2. Nous l'appelons *Marque primaire*. Les deux premiers bits de la Marque primaire représentent les informations relatives au contrôle de copie (CCI, *copy control information*) telles que "pas de copie", "copie de première génération" et "plus de copies". Le détecteur utilise l'algorithme adaptatif de période de détection pour déceler la Marque primaire avec un taux de fausse détection prédéterminé. Même à partir d'un contenu fortement endommagé, une détection fiable peut être réalisée sans dépasser le taux maximal prédéterminé de fausse détection, fixé à moins de 10^{-12}, qui dépend de la durée de détection.

Galaxy propose d'intégrer un autre filigrane transparent dans le flux vidéo des dispositifs d'enregistrement numériques, comme moyen d'identification du matériel copié. On appelle cela l'*incorporation de la marque de copie*. La technique employée intègre un autre filigrane transparent sans aucune altération de la Marque primaire préincorporée. L'insertion de cette marque de copie peut s'effectuer à la fois dans les domaines de la bande de base et du signal MPEG-2. La détection de cette marque de copie peut également s'effectuer dans les deux domaines. On ajoute la marque de copie au contenu protégé par un CCI "copie de première génération" afin de le faire passer à l'état "plus de copies", dans le cadre du contrôle de copies par génération. Il est à noter que les marques de copie incorporées dans les deux domaines concernés sont identiques.

La technique de filigranage Galaxy est compatible et interchangeable entre le domaine MPEG et le domaine de la bande de base; elle laisse par conséquent un grand degré de liberté aux constructeurs de dispositifs quant à l'emplacement d'activation du détecteur de filigrane et de l'appareil d'incorporation de la marque de copie. Il convient que la décision finale de l'emplacement du détecteur de l'appareil d'incorporation soit prise compte tenu de l'aspect de sécurité et du coût d'implémentation.

Galaxy a réalisé la conception et le prototype logiciel d'une technique unique de filigranage unifié et a effectué des essais intensifs de bonne tenue et de transparence afin de rendre l'algorithme stable. Les essais de bonne tenue qui ont été réalisés sont consignés ci-dessous. La technique est suffisamment éprouvée pour que le CPAC procède à un essai de vérification immédiat. Le présent appendice décrit également la façon dont la valeur seuil peut faire varier le taux de fausse détection.

Enfin, une technique d'insertion automatique ainsi qu'un système d'insertion facile à exploiter et sûr sont décrits. Le système d'incorporation en temps réel est un système DSP fonctionnant sur ordinateur.

II.1 Architecture du système

II.1.1 Aperçu général de l'usage du filigrane

Dans le système de filigranage Galaxy, la Marque primaire comporte 8 bits d'informations dont les deux premiers sont utilisés pour les informations relatives au contrôle de copie (CCI). L'utilisation des autres bits ne relève pas du domaine d'application du présent appendice mais il convient qu'elle fasse l'objet d'un accord entre les parties concernées de l'ICPAC, y compris les bits de déclenchement de l'APS. La technique Galaxy peut également intégrer et déceler un autre filigrane indépendant appelé *Marque de copie*, qui coexiste avec le filigrane primaire et qui est utilisé pour modifier l'interprétation des informations CCI de la Marque primaire pour le contrôle des copies par génération.

Dans l'utilisation des informations CCI, les termes suivants sont communément assimilés par le DHSG:

1) le contenu transmis par des moyens électroniques tels que la télévision numérique peut être marqué (1,1), (1,0), (0,0) ou ne pas l'être;
2) tous les contenus transmis par DVD-ROM sont soit marqués (1,1), (0,0), soit non marqués;
3) tous les contenus transmis par DVD-ROM marqués (1,1) sont chiffrés par CSS;
4) les lecteurs de DVD sont capables de différencier les supports inscriptibles des supports à lecture seulement;
5) l'état "plus de copies" est autorisé uniquement avec des supports inscriptibles.

Des exemples de commande d'enregistrement et de commande de lecture sont décrits ci-dessous. La technique de filigranage Galaxy possède la capacité et la flexibilité nécessaires pour traiter tous les scénarios d'implémentation possibles. Il convient de traiter l'implémentation réelle en liaison avec la conception du système intégral de protection antipiratage.

Commande d'enregistrement et de copie par génération

Les informations CCI énumérées dans le Tableau II.1 peuvent être utilisées pour déclencher le fonctionnement d'enregistreurs numériques tels que les enregistreurs DVD. L'abréviation CFP représente ici l'appel de proposition émis par le DHSG en mai 1997.

Tableau II.1/J.95 – Définition des informations CCI et réponse requise pour la commande de copie dans les enregistreurs

Informations CCI détectées	Définition dans l'appel de proposition	Réponse de l'appareil enregistreur
1,1	Pas de copie	Eviter toute copie
1,0	Copie de première génération	Autoriser la copie et ajouter une marque de copie
1,0 avec marque de copie	Plus de copies	Eviter toute copie
0,0 ou aucune marque	Copie autorisée	Copie autorisée

Commande de lecture

Les informations CCI détectées et les informations des supports de lecture peuvent être utilisées pour déclencher le fonctionnement des lecteurs DVD conformes. Un exemple de définition est indiqué dans le Tableau II.2. En supposant que le filigrane ne peut être détecté avec le chiffrement CSS, nous avons l'état "lecture interdite" à une copie non autorisée lorsque les informations CCI = (1,1) sont détectées à partir de supports DVD-ROM sans chiffrement CSS.

Tableau II.2/J.95 – Définition des informations CCI et réponse de la commande de lecture des lecteurs DVD

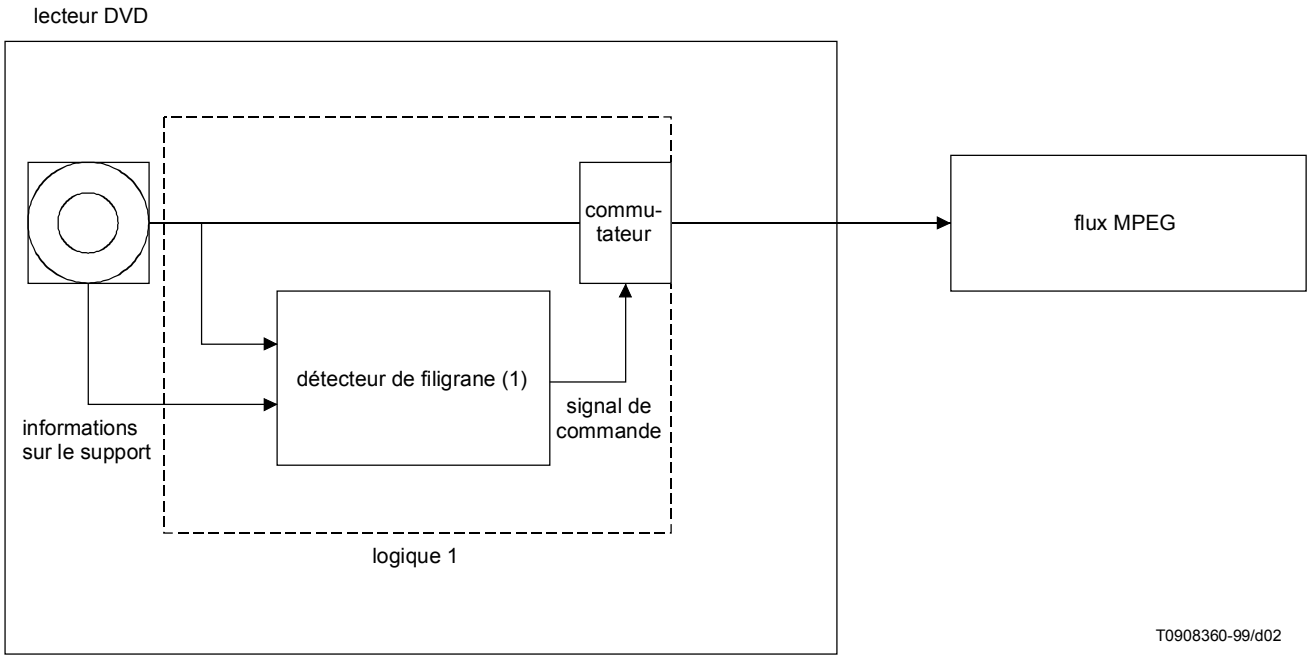
Type de support détecté	Informations CCI détectées	Réponse du dispositif
Lecture seule	1,1	Lecture interdite*
	1,0	Lecture interdite
	1,0 avec marque de copie	Lecture interdite
	0,0 ou aucune marque	Lecture autorisée
Inscriptible et réinscriptible	1,1	Lecture interdite
	1,0	Lecture interdite
	1,0 avec marque de copie	Lecture autorisée
	0,0 ou aucune marque	Lecture autorisée

II.1.2 Configuration du système

La configuration système des commandes de lecture et d'enregistrement du système DVD est expliquée dans le présent sous-paragraphe à l'aide de trois types de logique de détection de filigrane/d'insertion de marque de copie. Ces trois types sont les modules essentiels de la conception du système intégral de commande de copie. La Marque primaire peut être décelée à la fois au niveau du MPEG-2 et de la bande de base et la marque de copie peut être insérée et décelée aux deux niveaux concernés. Cette caractéristique laisse une grande liberté de choix aux fabricants des dispositifs quant à l'emplacement d'activation du détecteur de filigrane et de l'appareil d'insertion de la marque de copie.

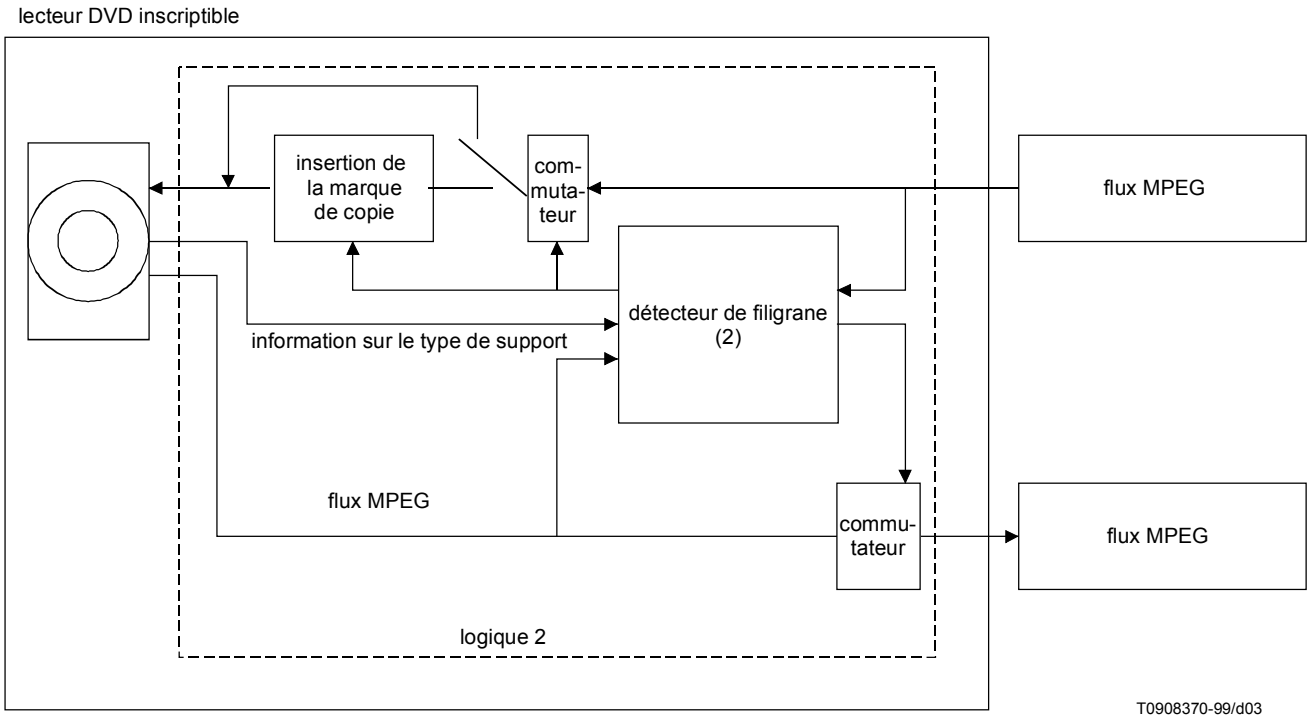
Logique 1: commande de lecture DVD

Cette logique détecte la Marque primaire et la marque de copie directement à partir des données MPEG. Les informations CCI et la marque de copie obtenues seront utilisées avec les informations relatives au type de support par le contrôleur du lecteur DVD pour la commande de lecture, selon l'action définie au II.1.1. Le cadre délimité par la ligne pointillée représente le schéma de principe de cette logique.



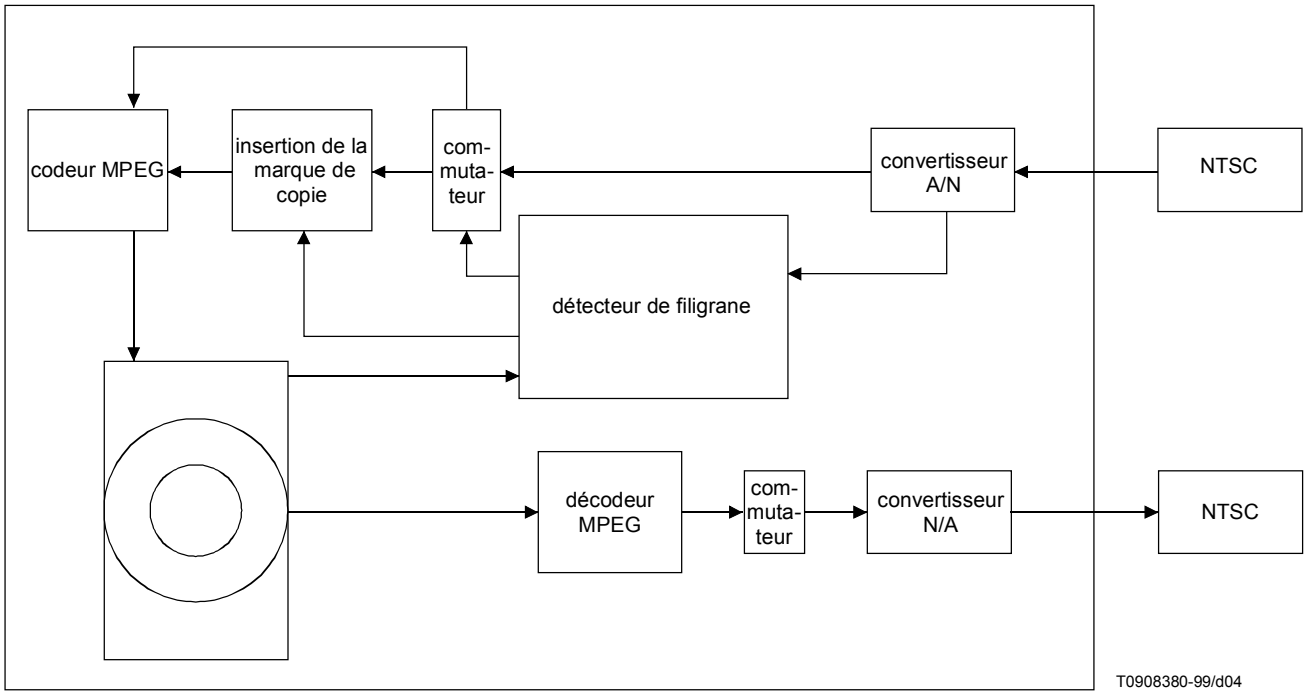
Logique 2: commande de lecture, de copie et de copie par génération de DVD

Outre la commande de lecture, cette logique exécute la commande d'enregistrement et de copie par génération à l'aide de la fonction d'insertion de la marque de copie et au moyen du même détecteur de filigrane que dans la logique 1. Les informations relatives au type de support sont également requises pour la fonction de lecture. Avec cette logique, toutes les fonctions sont exécutées directement sur le flux vidéo MPEG, qui peut ainsi être inséré dans le lecteur DVD si nécessaire. Le cadre délimité par la ligne pointillée représente le schéma de principe de la logique 2.



Logique 3: commande de copie et commande de copie par génération en bande de base

Cette logique s'applique à la commande d'enregistrement et à la commande d'enregistrement par génération des enregistreurs avec entrée vidéo en bande de base ou des magnétoscopes DVD. Cette fonctionnalité est équivalente à la partie entrée de la logique 2; la différence résidant dans le fait que les données vidéo non comprimées constituent le flux vidéo cible. La figure ci-dessous représente un exemple d'implémentation avec commande de lecture de DVD.



II.2 Commande de copie par génération

La technique Galaxy peut insérer un autre filigrane transparent appelé *marque de copie* sans aucune destruction de la Marque primaire au niveau des domaines de la bande de base et du MPEG-2. Elle détecte également ce filigrane dans ces deux domaines. L'insertion de la marque de copie au niveau du domaine MPEG-2 est conçue pour conserver strictement la taille de paquet du flux MPEG-2 afin de satisfaire la contrainte d'implémentation matérielle. La présence de la marque de copie modifiera l'interprétation des informations CCI (1,0) de l'état "copie de première génération" à l'état "plus de copies" pour la commande de copie par génération comme indiqué dans les Tableaux II.1 et II.2.

En utilisant le procédé de marque de copie, le système peut prendre en charge entièrement la transmission numérique et la transmission analogique à partir du boîtier adaptateur de base d'installation, sans recourir à aucune action coopérative des dispositifs existants sur les voies de transmission.

II.3 Maturité technique

Les compagnies membres de Galaxy développent de manière indépendante et conjointe une technique de filigranage pour la vidéonumérique depuis le début de 1996, qui vise à assurer la protection antipiratage du contenu des vidéodisques numériques. Elles ont déjà implémenté la logique de détection par FPGA (réseau logique programmable) et l'algorithme d'insertion par DSP, et ont démontré la faisabilité de l'incorporation et la détection en temps réel au DHSG en 1997 et 1998. La bonne tenue du filigrane a été prouvée et la faisabilité du refiligranage a été démontrée pour le contrôle de copie par génération lors des essais opérationnels réalisés au DHSG en février 1998. Galaxy a reconnu l'expertise technique de chaque membre et a annoncé la fusion des différentes propositions en février 1999.

La technique de filigranage de Galaxy est suffisamment mûre pour pouvoir procéder à un essai de vérification immédiat, réalisé par le CPAC. Toutes les fonctions décrites dans le Tableau II.3 ont été soumises à l'essai de transparence, de fiabilité et de bonne tenue de la Marque primaire (PM, *primary mark*) et de la marque de copie (CM, *copy mark*), qui couvrent à la fois le domaine du MPEG et celui de la bande de base. Un prototype de système d'incorporation en temps réel sera bientôt disponible pour un essai en studio. Un calendrier de présentation de produits détaillé dépend toutefois du calendrier de sélection final du CPAC.

Tableau II.3/J.95 – Disponibilité de la fonction requise telle que définie en mars 1999

		Description de fonctionnement	Disponibilité
Incorporation du filigrane dans la vidéo de bande de base	Système studio	Système d'incorporation automatique du filigrane avec information complète 8 bits par champ Pseudo-incorporation en temps réel avec E/S de type UIT-R-656	Oui
Détection de la Marque primaire dans le domaine MPEG	Logiques 1, 2	Détection directe à partir du flux MPEG en temps réel	Oui
Détection de la Marque primaire dans le domaine de la bande de base	Logique 3	Détection après conversion A/N	Oui
Insertion de la marque de copie dans le domaine MPEG	Logique 2	Insertion de la marque de copie directement dans le flux MPEG avec maintien de la taille du paquet MPEG	Oui
Insertion de la marque de copie dans le domaine de la bande de base	Logique 3	Insertion de la marque de copie sur la bande vidéo après conversion A/N	Oui
Détection de la marque de copie dans le domaine MPEG	Logiques 1, 2	Détection directe à partir du flux MPEG en temps réel	Oui
Détection de la marque de copie dans le domaine de la bande de base	Logique 3	Détection après conversion A/N	Oui

II.4 Analyse du nombre de portes

L'estimation du nombre de portes des logiques 1, 2 et 3 décrites au II.2 est reprise dans le Tableau II.4.

Tableau II.4/J.95 – Fonction et résumé du nombre de portes des puces de détection du filigranage Galaxy

Type de logique	Objet	Description de fonctionnement	Nombre de portes	Dispositifs récepteurs
1	Commande de lecture	Détection du filigrane de la Marque primaire et de la marque de copie à partir du flux MPEG	Portes 30 k RAM 5 kO	Lecteur DVD
2	Commande de lecture Commande d'enregistrement Commande de copie par génération	Détection du filigrane de la Marque primaire et de la marque de copie et insertion de la marque de copie dans le flux MPEG	Portes 35 k RAM 5 kO	Lecteur DVD inscriptible
3	Commande de lecture Commande d'enregistrement Commande de copie par génération	Détection du filigrane de la Marque primaire et de la marque de copie et insertion de la marque de copie dans le domaine de la bande de base après conversion A/N	Portes 30 k RAM 42 kO	Lecteurs DVD inscriptibles avec entrée vidéo analogique

L'estimation du nombre de portes peut varier en fonction de l'architecture et de la disponibilité des ressources des systèmes à semi-conducteurs du dispositif d'enregistrement et de lecture. Le nombre de portes de la logique 3 ne comprend pas de conversion analogique-numérique avant l'intervention du processus de détection.

Ce nombre de portes ne représente pas nécessairement la spécification future du produit. Il est soumis à des variations dans la mesure où le détail de la spécification de fonctionnement peut varier selon les nouvelles prescriptions du CPAC.

II.5 Tests de robustesse

Le test de bonne tenue a été effectué dans les conditions suivantes:

- charge utile des données: 8 bits (256 états arbitraires peuvent être représentés);
- taux de fausse détection inférieur à 10^{-12} sur une période de détection de 10 s.

Ces conditions doivent être spécifiées avant de procéder à une quelconque comparaison des différentes techniques dans la mesure où il existe une relation de compromis entre la transparence, la charge utile des données, le taux de fausse détection et la bonne tenue du filigrane.

Huit bits de données ont été détectés à partir des vidéo-clips d'essai par algorithme adaptatif de période de détection de Galaxy avec une fenêtre de détection d'une durée maximale de 20 s dans les domaines du MPEG-2 et de la bande de base. Vingt clips échantillons fournis par le DHSG en 1997 ont été utilisés. Les procédés successifs de traitement des signaux vidéo en studio → compression MPEG-2 → enregistrement VHS → recompression MPEG-2 ont été appliqués afin de simuler la dégradation prévue en situation opérationnelle. Le traitement des signaux vidéo en studio et les paramètres de chaque procédé sont énumérés dans le Tableau II.5. Huit bits ont été correctement détectés généralement en 1 s ou en un temps inférieur à l'issue de la première compression de MPEG-2 et dans un délai de 10 s dans la plupart des cas, même après la recompression du signal MPEG-2.

Tableau II.5/J.95 – Liste des éléments du test de bonne tenue

Traitement des signaux vidéo en studio (DVNR-1000)	Note
Filtre en mur de briques	
Facilitation d'ouverture	
Réduction du bruit	
Réduction de la vitesse de 98%	Sauter 1 trame sur 50
Mélange du filigrane à 50%	(test de référence)
Conversion au format extra-large	
Conversion au format extra-large par décalage	
Décalage spatial aléatoire	Plus de 10 décalages par 20 secondes
Décalage des teintes	Décalage des teintes de 30 degrés

Compression MPEG	4 Mbit/s-10 Mbit/s, différents groupes d'images (GOP), sous-trame/tame
Enregistrement VHS	3 DNR, marche/arrêt du correcteur d'erreurs de temps, etc.
Recompression MPEG	Codeur temps réel CBR, modification de l'intervalle de groupes d'images

Outre le test de simulation, les trois tests suivants de bonne tenue en environnement réel ont été effectués:

1) compression MPEG → transmission satellite → transmission analogique par câble → enregistrement VHS;

2) compression MPEG → transmission satellite → transmission TV directe → enregistrement VHS;

3) incorporation format HD → transposition de fréquence vers format SD → conversion analogique → compression MPEG → analyse de fausse détection.

II.6 Analyse des fausses détections

Une fausse détection se produit lorsque le détecteur interprète de manière incorrecte un segment vidéo non marqué comme étant un segment marqué. Le taux de fausse détection doit être extrêmement faible, par exemple 10^{-12}, car il empêche le dispositif de produire une copie légitime. La technique Galaxy peut contrôler le taux prévu de fausse détection par un seuil prédéterminé de détection du filigrane.

Brève description de l'algorithme

L'algorithme proposé détecte 8 bits d'informations CCI dans chaque sous-trame du flux MPEG-2 ou de la vidéo de la bande de base de la manière suivante. Tout d'abord, l'intensité du filigrane de chaque bit est calculée en additionnant les sorties observées à partir des blocs secondaires attribués dans la sous-trame concernée. Les bits sont ensuite interprétés lorsque l'intensité de chaque bit excède un seuil prédéterminé. Soit ε_B la probabilité que l'intensité détectée d'un seul bit dépasse le seuil. Les valeurs de détection des 8 bits étant indépendantes l'une de l'autre, la probabilité pour que les 8 bits dépassent le seuil dans une trame non marquée est donnée par:

$$\varepsilon = \varepsilon_B^{\,8}$$

Conformément au théorème de la limite centrale, la distribution de l'intensité du signal observée dans les trames non marquées (c'est-à-dire l'intensité du bruit) peut être traitée comme une distribution normale dont la variance peut être calculée sur la base des variances de chacune des données de sortie. Cela est dû au fait que l'intensité est la somme linéaire d'un nombre important de données de sortie aléatoires. Par conséquent, la probabilité que l'intensité normalisée du bruit R dépasse la valeur seuil T peut être estimée en utilisant la densité de probabilité normale:

$$\varepsilon_B = \mathrm{P}(|R| > T) = 2\int_T^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}}\, dt$$

où "P(x)" indique la probabilité d'occurrence d'un événement "x".

Si l'intensité normalisée du signal est inférieure au seuil, le signal sera cumulé de manière continue avec les trames (sous-trames) suivantes. Le cumul du signal se poursuit jusqu'à ce que l'intensité du signal cumulé atteigne le seuil (détection du filigrane), ou jusqu'à ce que le temps de cumul dépasse le temps de coupure maximal (non-détection du filigrane), selon ce qui se produit en premier (détection du cumul de trames). De plus, comme l'algorithme choisit des signaux de façon qu'ils soient indépendants les uns des autres, la variance du signal cumulé peut être calculée comme une fonction de la racine carrée du nombre d'échantillons *f*, et donc le comportement du signal cumulé:

$$S_f = \sum_{1}^{f} R_i$$

peut être estimé à l'aide de la fonction de densité de probabilité normale:

$$\varepsilon_B = \mathrm{P}(|\frac{S_f}{\sqrt{f}}| > T) = 2\int_{T}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$$

Comme l'algorithme effectue un test de détection indépendant en même temps que le cumul, le taux total de fausse détection pour chaque bit peut être exprimé comme suit:

$$\varepsilon' = 1 - (1 - \varepsilon)^f$$

où ε est le taux de fausse détection pour un échantillon et *f* est le nombre d'échantillons. Le Tableau II.6 indique quelques seuils *T* ainsi que les taux correspondants de fausse détection ε′, où le nombre maximal d'échantillons est fixé à 40.

Tableau II.6/J.95 – Taux de fausse détection en fonction du seuil

Taux cible (ε′) de fausse détection	Seuil (*T*) pour une détection de 8 bits
10^{-8}	1,85878
10^{-9}	1,98372
10^{-10}	2,10306
10^{-11}	2,21752
10^{-12}	2,32729
10^{-13}	2,44118

II.7 Technologie et système d'incorporation

Dans la technologie Galaxy, l'incorporation est un double processus:

1) analyse du contenu de l'image;

2) processus de modification de la luminance.

Ce double processus permet un contrôle automatique de la tenue à l'incorporation afin de satisfaire la transparence, la robustesse et le taux de fausse détection requis. Huit bits de données CCI sont incorporés comme marque primaire dans chaque sous-trame de bande vidéonumérique non comprimée.

Le système d'incorporation en studio est un système DSP sur ordinateur, capable de fonctionner en temps réel avec des trames de retard. Son entrée et sa sortie constituent l'interface vidéonumérique UIT-R-656. Le système est prévu pour être équipé d'un moniteur en temps réel permettant de confirmer l'intensité du signal des clips insérés et de proposer une interface utilisateur conviviale pour les paramètres d'incorporation réglables. Le système propose également des fonctions de sécurité telles que le contrôle de l'accès des opérateurs non autorisés et la prévention de toute réincorporation fortuite ou délibérée.

II.8 Abréviations

A/N	Conversion analogique-numérique
APS	Système de protection analogique (*analogue protection system*)
CCI	Informations relatives au contrôle de la copie (*copy control information*)
CFP	Appel de propositions (*call for proposal*)
CM	Marque de copie (*copy mark*)
CPAC	Comité consultatif antipiratage (*copy protection advisory committee*)
CSS	Système d'embrouillage de contenu (*contents scramble system*)
DHSG	Sous-groupe de dissimulation de données (*data-hiding sub-group*)
DSP	Processeur de signaux numériques (*digital signal processor*)
DVD ROM	Vidéodisque numérique à mémoire fixe (*digital versatile disc read-only memory*)
DVNR	Réduction numérique du bruit vidéo (*digital video noise reduction*)
FPGA	(Réseau) prédiffusé programmable (*field programmable gate array*)
ICPAC	Comité CPAC intérimaire (*interim CPAC*)
MPEG-2	Groupe 2 d'experts pour les images animées (*moving pictures expert group 2*)
N/A	Conversion numérique-analogique
PM	Marque primaire (*primary mark*)
WM	Filigrane (*water mark*)

II.9 Informations de contact

Contact au Japon

IBM Corporation
Tokyo Research Laboratory
1623-14, Shimotsuruma, Yamato-shi
Kanagawa-ken, 242-8502
Japon

NEC Corporation
1-10, Nisshincho, Fuchu-shi
Tokyo, 183-8501
Japon

Hitachi Ltd.
292, Yoshidacho, Totsuka-ku
Yokohama-shi
Kanagawa-ken, 244-0817
Japon

Pioneer Electronic Corporation
1-1, Fujimi 6 chome, Tsurugashima-shi
Saitama-ken, 350-2288
Japon

Sony Corporation
6-7-35, Kitashinagawa, Shinagawa-ku
Tokyo, 141-0001
Japon

Contact aux Etats-Unis d'Amérique

Director of Licensing Development
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
Etats-Unis

NEC Research Institute Inc.
4 Independence Way
Princeton, NJ
Etats-Unis

Appendice III

Proposition 5C de protection antipiratage de la propriété intellectuelle de la vidéo MPEG

Propriété intellectuelle

L'implémentation de la présente spécification nécessite l'attribution d'une licence par l'administrateur d'attribution de licences dans le domaine des transmissions numériques (DTLA, *digital transmission licensing administrator*).

Informations de contact

Il convient d'adresser les informations de retour sur cette spécification à l'adresse électronique suivante: spec-comments@dtcp.com.

L'administrateur d'attribution de licences dans le domaine des transmissions numériques peut être consulté à l'adresse suivante: dtla@intel.com.

L'adresse URL du site de l'administrateur d'attribution de licences dans le domaine des transmissions numériques est la suivante: http://www.dtcp.com.

NOTE – Les documents sources pour le matériel indiqué dans le présent appendice ne peuvent être obtenus auprès des détenteurs de droits d'auteur que par l'application d'un accord de non-divulgation (NDA, *non-disclosure agreement*). Contacter l'administrateur d'attribution de licences dans le domaine des transmissions numériques pour les sources appropriées de ces informations.

III.1 Introduction

III.1.1 Objet et domaine d'application

La *Spécification 5C de protection du contenu de transmissions numériques (DTCP, digital transmission content protection)* définit un protocole cryptographique de protection des contenus de divertissement audio/vidéo contre toute copie, interception et violation non autorisées, lorsque celles-ci transitent par des mécanismes de transmission numérique tels qu'un bus série à haute performance conforme à la norme IEEE 1394-1995. Seul un contenu de divertissement légitime, acheminé vers un dispositif source par l'intermédiaire d'un autre système de protection antipiratage agréé (tel que le système d'embrouillage de contenu de DVD), sera protégé par ce système de protection antipiratage.

L'utilisation de la présente spécification et l'accès à la propriété intellectuelle et aux matériels cryptographiques requis pour implémenter ladite spécification feront l'objet d'une licence. L'administrateur d'attribution de licences dans le domaine des transmissions numériques (DTLA) est responsable de la définition et de l'administration du système de protection de contenu décrit dans la présente spécification.

Alors que la protection DTCP a été conçue pour être utilisée par des dispositifs reliés à des bus série comme défini par la norme IEEE 1394-1995, les développeurs prévoient qu'elle pourra être utilisée avec des extensions futures de la présente norme, avec d'autres systèmes de transmission et avec d'autres types de contenu, sur autorisation de l'administrateur DTLA.

III.1.2 Aperçu général

La présente spécification s'applique à quatre couches de protection antipiratage:

- **Informations relatives au contrôle de copie (CCI)**

  Les détenteurs de contenus ont besoin de spécifier la façon dont lesdits contenus peuvent être utilisés ("copie de première génération", "pas de copie", etc.). Ce système de protection du contenu est capable de communiquer en toute sécurité les informations relatives au contrôle des copies (CCI) entre des dispositifs, et ce de deux manières différentes:

  – l'indicateur du mode de cryptage (EMI, *encryption mode indicator*) permet une transmission facilement accessible et non moins sûre des informations CCI par le biais des deux bits de poids fort du champ sy de l'en-tête de paquet isochrone;

  – les informations CCI sont incorporées dans le flux de contenu (par exemple MPEG). Cette forme d'informations CCI est traitée uniquement par les dispositifs qui reconnaissent le format de contenu spécifique.

- **Authentification des dispositifs et échange de clé (AKE, *authentication and key exchange*)**

  Avant de procéder au partage des informations dignes d'intérêt, un dispositif connecté doit d'abord vérifier qu'un autre dispositif connecté est authentique. Afin d'équilibrer les prescriptions de protection des industries de production de contenus (des matériels audio/vidéo) au regard des prescriptions du monde réel des utilisateurs d'ordinateurs et de dispositifs électroniques grand public (CE, *consumer electronics*), cette spécification comprend deux niveaux d'authentification, à savoir un niveau intégral et un niveau restreint:

  – l'authentification intégrale peut être utilisée avec tous les contenus protégés par le système;

  – l'authentification restreinte permet uniquement de protéger les contenus avec "copie de première génération" et avec "plus de copies". Les dispositifs de copie tels que les magnétoscopes numériques utilisent ce type d'authentification.

- **Cryptage du contenu**

  Les dispositifs comportent un sous-système de chiffrage par canal qui crypte et décrypte les contenus protégés par le droit d'auteur. Afin de garantir une interopérabilité, tous les dispositifs doivent prendre en charge le cryptogramme spécifique stipulé comme le cryptogramme de référence. Le sous-système peut également prendre en charge d'autres cryptogrammes complémentaires dont l'utilisation fait l'objet de négociations lors de l'authentification.

- **Aptitude du système au renouvellement [MP1]**

  Les dispositifs qui prennent en charge une authentification intégrale peuvent recevoir et traiter les messages d'aptitude du système au renouvellement (SRM, *system renewability messages*) créés par l'administrateur DTLA et distribués avec les contenus et les nouveaux dispositifs. L'aptitude du système au renouvellement garantit son intégrité à long terme par le rejet des dispositifs compromis.

La Figure III.1 donne un aperçu général de la protection du contenu. Dans cet aperçu général, il a été indiqué au dispositif source de transmettre un flux de contenu à protection antipiratage. Dans ce diagramme et dans les diagrammes ultérieurs, un dispositif source est un dispositif qui peut transmettre un flux de contenu. Un dispositif récepteur est un dispositif qui peut recevoir un flux de contenu. Les dispositifs multifonctions tels que les ordinateurs et les dispositifs d'enregistrement/lecture comme les enregistreurs-lecteurs numériques peuvent être à la fois des dispositifs sources et récepteurs.

1) Le dispositif source déclenche la transmission d'un flux de contenu crypté marqué selon l'état de protection antipiratage approprié (par exemple "copie de première génération", "pas de copie", ou "plus de copies") par l'intermédiaire des bits EMI.[1]

2) Dès réception du flux de contenu, le dispositif récepteur examine les bits EMI afin de déterminer l'état de protection antipiratage du contenu. Si le contenu est marqué "pas de copie", le dispositif récepteur demande au dispositif source qu'il déclenche un échange AKE intégral. Si le contenu est marqué "copie de première génération" ou "plus de copies", le dispositif récepteur requiert un échange AKE intégral, s'il peut être pris en charge, ou un échange AKE restreint. Si le dispositif récepteur a déjà procédé à l'authentification appropriée, il peut immédiatement passer à la phase 4.

---

[1] Si le contenu requis par un dispositif récepteur est protégé, le dispositif source peut choisir de transmettre un flux de contenu vide jusqu'à ce qu'au moins un dispositif ait exécuté la procédure d'authentification appropriée, requise pour accéder au flux de contenu.

3) Lorsque le dispositif source reçoit la demande d'authentification, il procède au type d'authentification requis par le dispositif récepteur, à moins qu'un échange AKE intégral ne soit requis; mais le dispositif source ne peut prendre en charge qu'un échange AKE restreint, auquel cas il procède à un échange AKE restreint.

4) Une fois que les dispositifs ont exécuté la procédure d'échange AKE requise, une clé de cryptage par canal de contenu peut être échangée entre eux. Cette clé est utilisée pour crypter le contenu au niveau du dispositif source et pour le décrypter au niveau du dispositif récepteur.

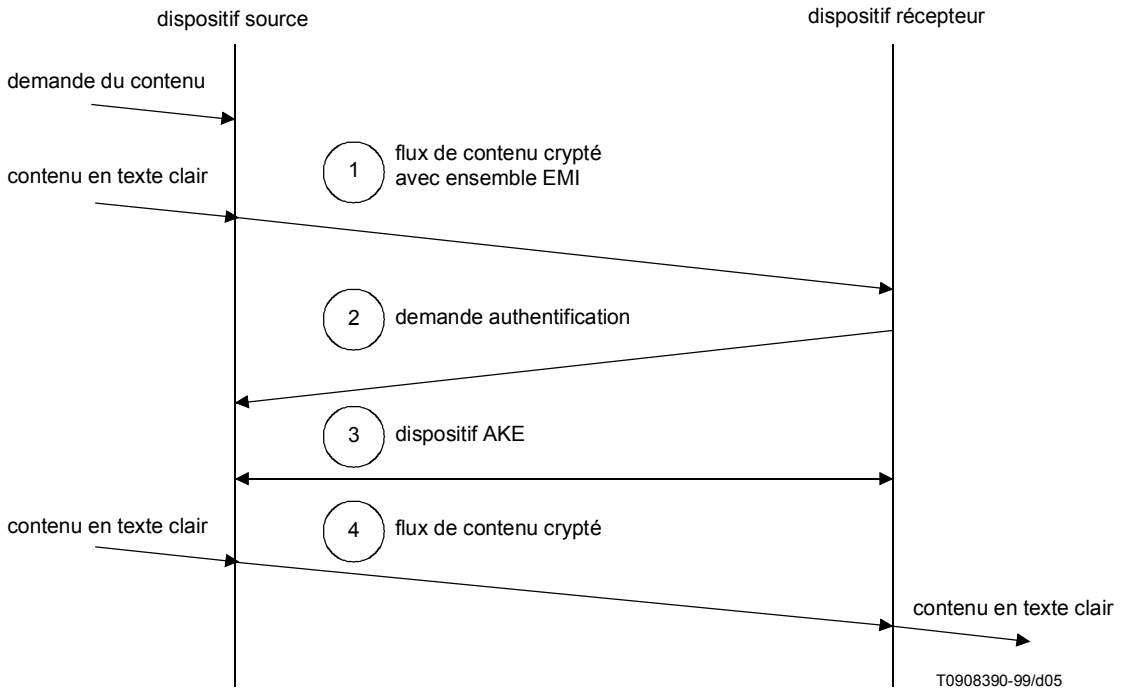


Figure III.1/J.95 – Aperçu général de la protection du contenu

III.1.3 Références

La présente spécification doit être utilisée conjointement avec les publications suivantes. Lorsque les publications sont remplacées par une révision approuvée, ladite révision s'applique.

– Digital Transmission Protection License Agreement, *Development and Evaluation License*, Digital Transmission Licensing Authority.

– 1394 Association commerciale, *Specification for AV/C Digital Interface Command Set*.

– Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 1, Version 0.91.

– Digital Transmission Licensing Administrator, *5C Digital Transmission Content Protection Specification*, Volume 2, Version 0.90.

– Digital Transmission Protection License Agreement, *Development and Evaluation License*, Digital Transmission Licensing Authority.

– IEEE Std 1394-1995, *Norme en matière de bus en série à hautes performances*.

– IEEE P1363, *Editorial Contribution to Standard for Public Key Cryptography*, Preliminary Draft, P1363/D3 (11 mai 1998).

– Publication de la CEI 61883-1 (1998), *Interface numérique pour matériel audio/vidéo grand public – Partie 1: Généralités.*

– National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS Publication 180-1, 17 avril 1995.

– Toshiba Corporation, *Efficient Implementation of an Elliptic Curve Cryptosystem,* disponible sur http://www.dtcp.com/

III.1.4 Organisation du présent appendice

L'organisation du présent appendice est la suivante:

- le sous-paragraphe III.1 donne un aperçu général de la protection du contenu;
- le sous-paragraphe III.2 énumère les termes et les abréviations utilisés dans le présent appendice;
- le sous-paragraphe III.3 décrit le fonctionnement du système global de protection des transmissions numériques comme un automate à états;
- le sous-paragraphe III.4 traite des détails du niveau intégral d'authentification des dispositifs et de l'échange des clés;
- le sous-paragraphe III.5 traite des détails du niveau d'authentification restreint des dispositifs et de l'échange des clés;
- le sous-paragraphe III.6 décrit de manière détaillée l'établissement des canaux de contenu après exécution du processus d'authentification intégral ou restreint;
- le sous-paragraphe III.7 décrit les capacités de renouvellement du système;
- le sous-paragraphe III.8 couvre les extensions de la commande AV/C.

III.1.5 Notation de l'automate à états

Les automates à états sont utilisés dans le présent appendice afin d'indiquer les différents états de fonctionnement. Ces automates utilisent le style représenté à la Figure III.2.

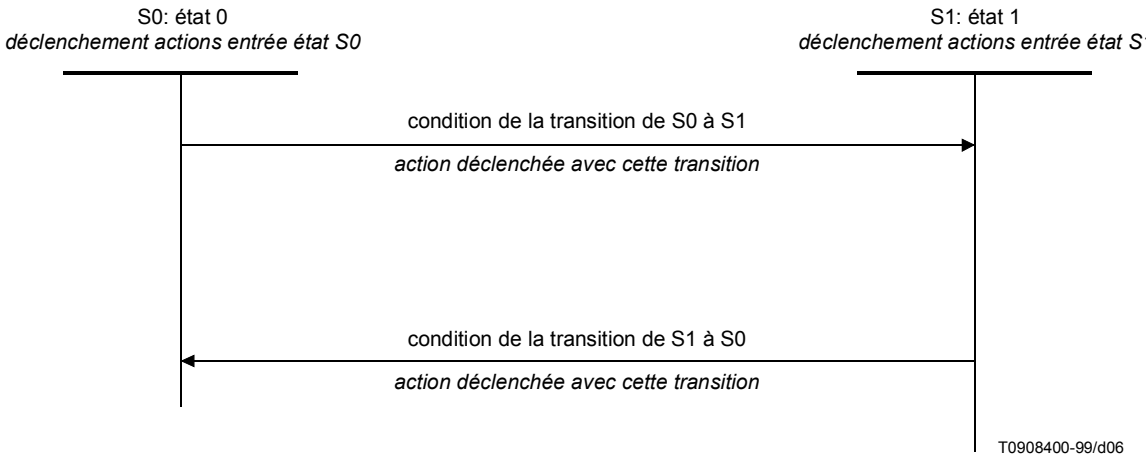


Figure III.2/J.95 – Exemple d'automate à états

Les automates à états posent trois hypothèses:

1) le temps s'écoule uniquement par états discrets;

2) les passages d'un état à un autre sont instantanés, de sorte que les seules actions effectuées au cours d'une transition sont le positionnement des fanions, la valuation des variables et la transmission de signaux;

3) chaque fois qu'on passe à un état, les actions de cet état se déclenchent. Une transaction qui retourne au même état reprendra ces actions depuis le début.

III.1.6 Notation

La notation suivante est utilisée:

$[X]_{msb\_z}$ = les z bits de plus fort poids de X

$[X]_{lsb\_z}$ = les z bits de plus faible poids de X

$S_{X^{-1}}[M]$ = signe M utilisant l'algorithme EC-DSA avec la clé privée X^{-1} (les détails de l'algorithme de signature figurent au III.4)

$V_{X^1}[M]$ = vérifier la signature de M en utilisant l'algorithme EC-DSA avec une clé publique X^1 (les détails de l'algorithme de vérification figurent au III.4)

$X \,||\, Y$ = concaténation ordonnée de X avec Y

$X \oplus Y$ = opération OU exclusif bit à bit (XOR, *exclusive-OR*) de deux chaînes X et Y.

III.1.7 Valeurs numériques

Trois différentes représentations de nombres sont utilisées dans la présente spécification. Les nombres décimaux sont représentés sans aucune notation particulière. Les nombres binaires sont représentés comme une chaîne de chiffres binaires (0, 1) suivie d'un indice 2 (par exemple, 1010_2). Les nombres hexadécimaux sont représentés comme une chaîne de chiffres hexadécimaux (0..9, A..F) suivie d'un indice 16 (par exemple, $3C2_{16}$).

III.1.8 Ordonnancement des bits

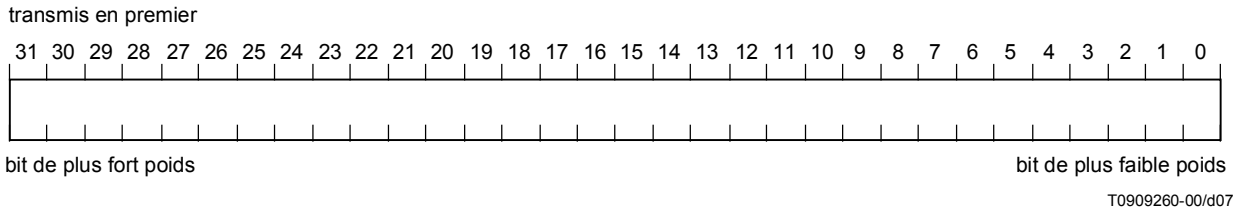


Figure III.3/J.95 – Ordonnancement des bits

III.1.9 Format des paquets

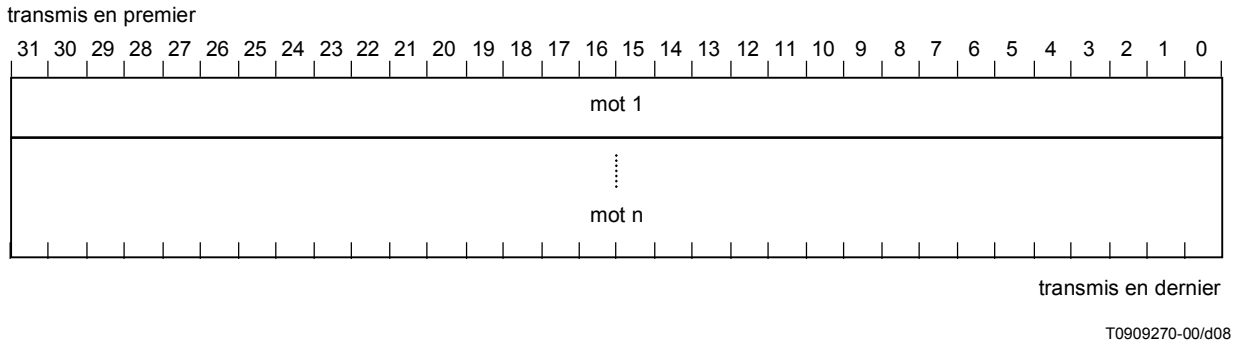


Figure III.4/J.95 – Format des paquets

III.1.10 Traitement des parties facultatives de la présente spécification

Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'exploitation n'a pas encore été établie par l'administrateur DTLA.

III.2 Termes et abréviations

A étudier.

III.3 Le système 5C de protection du contenu de transmissions numériques

III.3.1 Dispositif source de contenu

La Figure III.5 représente les différents états de fonctionnement d'un dispositif qui est une source de contenu.

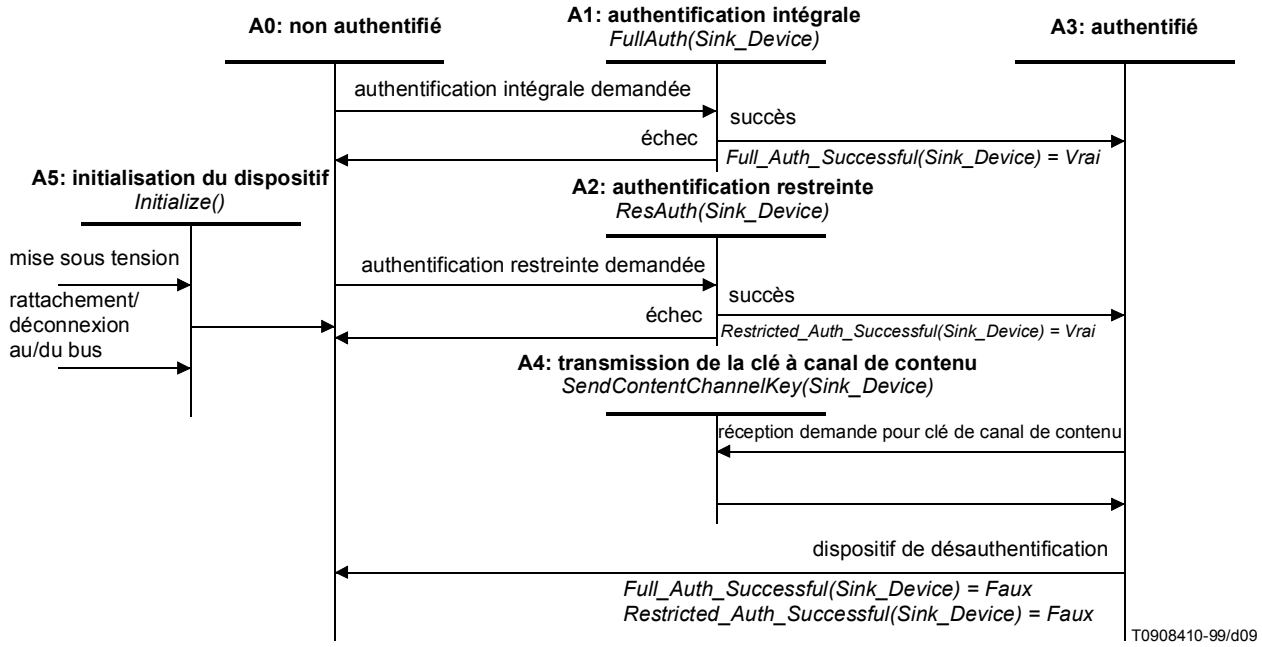


Figure III.5/J.95 – Automate à états du dispositif source de contenu

Un événement de mise sous tension ou de rattachement/déconnexion au/du bus rétablit l'automate à états à l'**état A5: initialisation du dispositif**.

Etat A5: initialisation du dispositif. Cet état est l'état d'initialisation du dispositif.

Transition A5:A0. Cette transition à l'**état A0: non authentifié** se produit suite à l'achèvement du processus d'initialisation.

Etat A0: non authentifié. Un dispositif est réglé à l'état non authentifié et attend l'ordre d'exécuter la procédure d'authentification intégrale ou restreinte.

Transition A0:A1. Cette transition s'effectue lorsque le dispositif reçoit l'ordre d'exécuter la procédure d'authentification intégrale avec un dispositif récepteur *(Sink_Device)*.

Etat A1: authentification intégrale. Cet état permet l'exécution du processus *FullAuth(Sink_Device)*. Ce processus est décrit en détail au III.4.

Transition A1:A3. Cette transition s'effectue lorsque la relation *FullAuth(Sink_Device)* a été exécutée de manière satisfaisante.

Etablir Full_Auth_Successful(Sink_Device) = Vrai

Transition A1:A0. Cette transition s'effectue lorsque la relation *FullAuth(Sink_Device)* n'a pas été exécutée de manière satisfaisante.

Transition A0:A2. Cette transition s'effectue lorsque le dispositif reçoit l'ordre d'exécuter la procédure d'authentification restreinte avec un dispositif récepteur *(Sink_Device)*.

Etat A2: authentification restreinte. Cet état est l'état auquel le dispositif exécute le processus *ResAuth(Sink_Device)*. Cette procédure est décrite en détail au III.5.

Transition A2:A3. Cette transition s'effectue lorsque la relation *ResAuth(Sink_Device)* a été exécutée de manière satisfaisante.

Etablir Restricted_Auth_Successful(Sink_Device) = Vrai

Transition A2:A0. Cette transition s'effectue lorsque la relation *ResAuth(Sink_Device)* n'a pas été exécutée de manière satisfaisante.

Etat A3: authentifié. Lorsqu'un dispositif a atteint cet état, il a exécuté de manière satisfaisante la procédure d'authentification intégrale ou restreinte.

Transition A3:A4. Un dispositif authentifié reçoit l'ordre de transmettre à un dispositif récepteur les valeurs nécessaires à la création d'une clé de contenu.

Etat A4: transmission de la clé à canal de contenu. Dans cet état, le dispositif source transmet à un dispositif authentifié les valeurs nécessaires à la création d'une clé de contenu par l'exécution du processus S*endContentChannelKey(Sink_Device)*. Ce processus est décrit au III.6.

Transition A4:A3. Cette transition s'effectue à l'exécution du processus *SendContentChannelKey(Sink_Device)*.

Transition A3:A0.

Etablir Full_Auth_Successful(Sink_Device) = Faux

Etablir Restricted_Auth_Successful(Sink_Device) = Faux

III.3.2 Dispositif récepteur de contenu

La Figure III.6 représente les différents états de fonctionnement d'un dispositif récepteur de contenu.

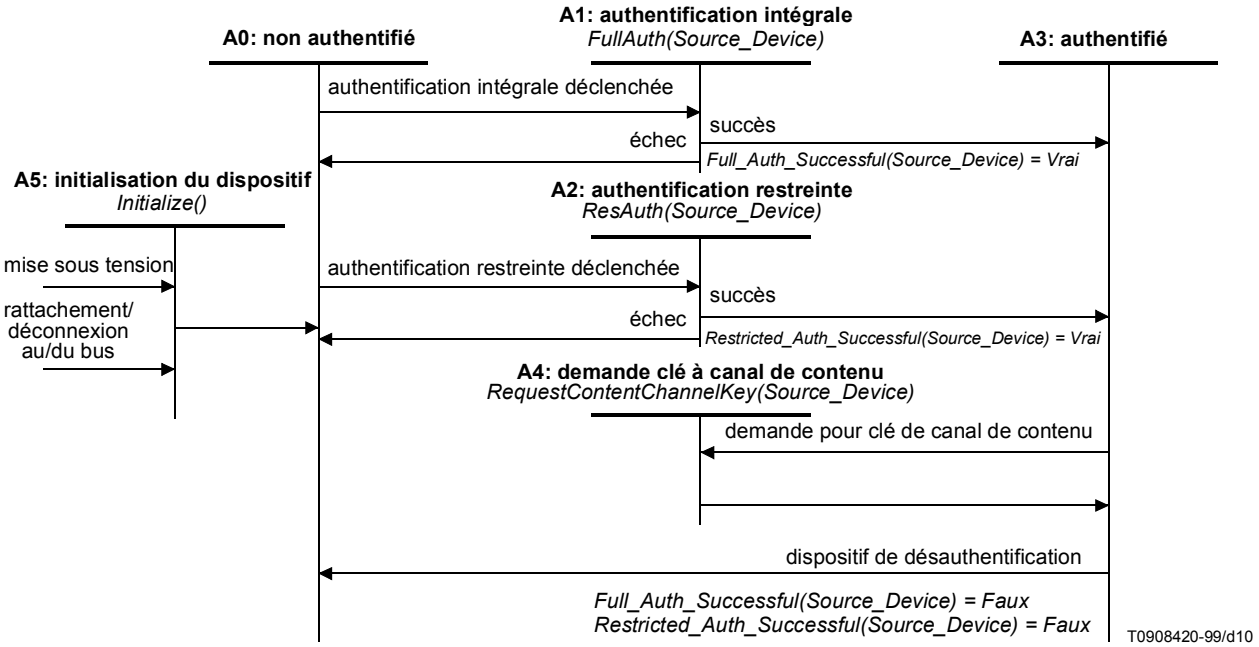


Figure III.6/J.95 – Automate à états du dispositif récepteur de contenu

Un événement de mise sous tension ou de rattachement/déconnexion au/du bus rétablit cet automate à états à l'**état A5: initialisation du dispositif**.

Etat A5: initialisation du dispositif. Cet état est l'état d'initialisation du dispositif.

Transition A5:A0. La transition à l'**état A0: non authentifié** s'effectue suite à l'exécution du processus d'initialisation.

Etat A0: non authentifié. Un dispositif, à l'état non authentifié, attend le déclenchement de l'ordre d'exécuter la procédure d'authentification intégrale ou restreinte.

Transition A0:A1. Cette transition s'effectue lorsque le dispositif déclenche l'ordre d'exécuter la procédure d'authentification intégrale avec un autre dispositif *(Source_Device)*.

Etat A1: authentification intégrale. Cet état est l'état d'exécution du processus *FullAuth(Source_Device)*. Ce processus est décrit en détail au III.4.

Transition A1:A3. Cette transition s'effectue lorsque le processus *FullAuth(Source_Device)* a été exécuté de manière satisfaisante.

Etablir Full_Auth_Successful(Source_Device) = Vrai

Transition A1:A0. Cette transition s'effectue lorsque le processus *FullAuth(Source_Device)* n'a pas été exécuté de manière satisfaisante.

Transition A0:A2. Cette transition s'effectue lorsque le dispositif déclenche l'ordre d'exécuter la procédure d'authentification restreinte avec un autre dispositif *(Source_Device)*.

Etat A2: authentification restreinte. A cet état, le dispositif exécute le processus *ResAuth(Source_Device)*. Cette procédure est décrite en détail au III.5.

Transition A2:A3. Cette transition s'effectue lorsque le processus *ResAuth(Source_Device)* a été exécuté de manière satisfaisante.

Etablir Restricted_Auth_Successful(Source_Device) = Vrai

Transition A2:A0. Cette transition s'effectue lorsque le processus *ResAuth(Source_Device)* n'a pas été exécuté de manière satisfaisante.

Etat A3: authentifié. Le dispositif, lorsqu'il a atteint cet état, a exécuté de manière satisfaisante la procédure d'authentification intégrale ou restreinte.

Transition A3:A4. Un dispositif authentifié a besoin d'une clé de contenu pour avoir accès au contenu protégé contre le piratage.

Etat A4: demande de la clé à canal de contenu. A cet état, un dispositif récepteur authentifié requiert les valeurs nécessaires à la création d'une clé de contenu en exécutant le processus *RequestContentChannelKey(Source_Device)*. Ce processus est décrit au III.6.

Transition A4:A3. Cette transition s'effectue à l'exécution du processus *RequestContentChannelKey(Source_Device)*.

Transition A3:A0.

Etablir Full_Auth_Successful(Source_Device) = Faux

Etablir Restricted_Auth_Successful(Source_Device) = Faux

III.4 Authentification intégrale

III.4.1 Introduction

Le présent sous-paragraphe traite des détails du niveau d'authentification intégrale des dispositifs et de l'échange de clé. L'authentification intégrale utilise l'algorithme de signature numérique à courbe elliptique établi sur la clé publique (EC-DSA, *elliptic curve digital signature*) pour toute signature et toute vérification. Elle utilise également l'algorithme d'échange de clé Diffie-Hellman à courbe elliptique (EC-DH, *elliptic curve Diffie-Hellman*) pour produire une clé d'authentification partagée.

III.4.2 Notation

La notation présentée dans le présent sous-paragraphe est utilisée pour décrire les procédés cryptographiques. Toutes les opérations effectuées dans le domaine de la courbe elliptique sont calculées sur une courbe elliptique E définie sur GF(p).

III.4.2.1 Courbe définie par l'administrateur DTLA

Les paramètres, clés, constantes et certificats suivants sont produits par l'administrateur DTLA.

III.4.2.1.1 Généralités

p = un nombre premier supérieur à 3.

GF(p) = le champ fini de p éléments, représenté comme le modulo p des nombres entiers.

E = la courbe elliptique sur le corps GF(p).

a, b = les coefficients définissant la courbe elliptique E, éléments de GF(p).

G = le point de référence de la courbe elliptique.

r = l'ordre de G.

L^{-1}, L^{1} = la paire de clés DTLA EC-DSA se compose d'une clé privée EC L^{-1} qui est un nombre entier dans la plage [1, r – 1] et d'une clé publique EC L^{1} qui est un point sur la courbe E, où $L^{1} = L^{-1}G$.

Ces constantes, à l'exception de L^{-1}, figurent dans la spécification DTCP disponible sous licence délivrée par l'administrateur DTLA.

III.4.2.1.2 Pour le dispositif X

X^{-1}, X^{1} = la paire de clés EC-DSA du dispositif se compose d'une clé privée EC X^{-1} qui est un nombre entier dans la plage [1, r – 1] et d'une clé publique EC X^{1} qui est un point sur la courbe E, où $X^{1} = X^{-1}G$.

X_{Cert} = certificat propre à un dispositif attribué au dispositif conforme X par l'administrateur DTLA et utilisé au cours du processus d'authentification (voir le sous-paragraphe suivant pour plus de détails).

Les points de la courbe elliptique consistent en la concaténation de la coordonnée x et de la coordonnée y, respectivement; pour un point de courbe elliptique $P = (x_P, y_P)$ qui n'est pas égal au point de la courbe elliptique à l'infini, $P = x_P \| y_P$.

Tableau III.1/J.95 – Longueur des clés et des paramètres de la courbe elliptique produits par l'administrateur DTLA (authentification intégrale)

Clés et paramètres de la courbe elliptique	Taille (bits)
Clé publique DTLA (L^{1})	320
Clé privée du dispositif (X^{-1})	160
Clé publique du dispositif (X^{1})	320
Point de référence (G)	320
Coefficient du polynôme (a, b) de la courbe elliptique	160 (chacun)
Nombre premier (p) du corps fini GF(p)	160
Ordre du point de référence (r)	160

III.4.2.2 Notation utilisée au cours du processus d'authentification intégrale

Les valeurs complémentaires suivantes sont produites et utilisées par les dispositifs au cours du processus d'authentification intégrale:

X_n = mot de circonstance (interrogation aléatoire produite par RNG_F).

X_k = valeur aléatoire utilisée dans l'échange de clés EC-DH produit par RNG_F dans le dispositif (entier dans la plage [1, r – 1]).

X_V = valeur de première phase EC-DH (X_kG) calculée dans le dispositif (point sur la courbe elliptique E).

X_{SRMV} = numéro de version du message d'aptitude du système au renouvellement (SRMV) mis en mémoire par le dispositif (voir III.7).

X_{SRMC} = indique le nombre de la ou des parties du message SRM actuellement stockées dans la mémoire non volatile du dispositif. Une valeur de SRMC indique que les premières générations SRMC+1 de messages SRM sont actuellement mises en mémoire par le dispositif (voir III.7).

K_{Auth} = clé d'authentification qui représente les 96 bits de plus faible poids des données partagées créées par l'intermédiaire de l'échange de clés EC-DH.

Tableau III.2/J.95 – Longueur des clés et variables produites par le dispositif (authentification intégrale)

Clé ou variable	Taille (bits)
Mot de circonstance (interrogation aléatoire X_n)	128
Valeur aléatoire pour EC-DH (X_k)	160
Valeur de première phase EC-DH (X_V)	320
X_{SRMV}	16
X_{SRMC}	4
Clé d'authentification créée par l'intermédiaire de l'échange de clés EC-DH (K_{Auth})	96

III.4.2.3 Formats des certificats propres aux dispositifs

Un certificat propre à un dispositif est attribué à chaque dispositif conforme par l'administrateur DTLA. Ce certificat est stocké dans le dispositif conforme et est utilisé au cours du processus d'authentification.

III.4.2.3.1 Format de référence

La Figure III.7 montre le format de référence du certificat propre à un dispositif:

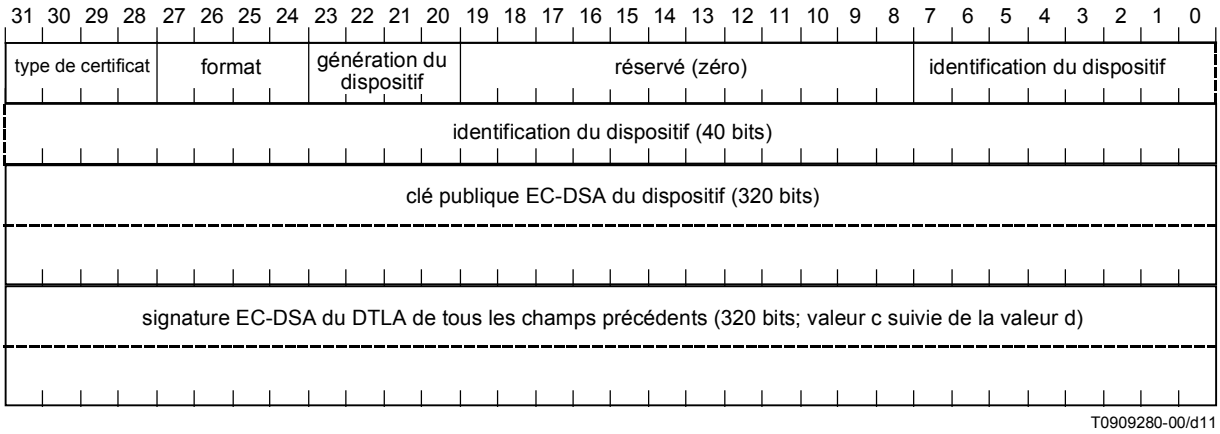


Figure III.7/J.95 – Format de référence du certificat propre à un dispositif

Les certificats propres à un dispositif se composent des champs de format de référence suivants:

- **type de certificat** (4 bits). Le seul codage actuellement défini est 0, ce qui indique que le certificat est destiné à la norme IEEE 1394 de protection du contenu. D'autres codages sont actuellement réservés;
- **format de certificat** (4 bits). Ce champ spécifie le format d'un type spécifique de certificat. Trois formats sont actuellement définis:

  format 0 = format du certificat propre à un dispositif à authentification restreinte (décrit au III.5);

  format 1 = format de référence du certificat propre à un dispositif à authentification intégrale;

  format 2 = format élargi du certificat propre à un dispositif à authentification intégrale (facultatif[2]).

---

[2] Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.

D'autres codages sont actuellement réservés:

- **génération du dispositif** (X_{SRMG}) (4 bits). Ce champ indique la capacité de mémoire non volatile et par conséquent la génération maximale des messages d'aptitude au renouvellement que ce dispositif peut prendre en charge (voir III.7). Le codage 0 indique une taille maximale de 128 octets alors que les autres codages sont actuellement réservés;
- champ réservé (12 bits). Ces bits, réservés pour une définition future, sont actuellement définis comme ayant une valeur égale à zéro;
- numéro **identificateur (ID) du dispositif** (X_{ID}, 40 bits) attribué par l'administrateur DTLA;
- **clé publique EC-DSA** du dispositif (X^1, 320 bits);
- **signature EC-DSA de l'administrateur** DTLA des composantes énumérées ci-dessus (320 bits).

La taille globale d'un certificat de format de référence propre à un dispositif est de 88 octets.

III.4.2.3.2 Champs de format élargi (composantes facultatives du certificat propre à un dispositif)

Outre les champs de format de référence, chaque certificat propre à un dispositif peut, à titre facultatif, inclure les champs suivants de format élargi[3]:

- **masque de capacité du dispositif** indiquant les propriétés du dispositif et les cryptogrammes à codage par canal acceptés (X_{Cap_Mask}, 32 bits);
- **signature EC-DSA** de l'administrateur DTLA de toutes les composantes mentionnées précédemment dans le certificat propre au dispositif (320 bits).

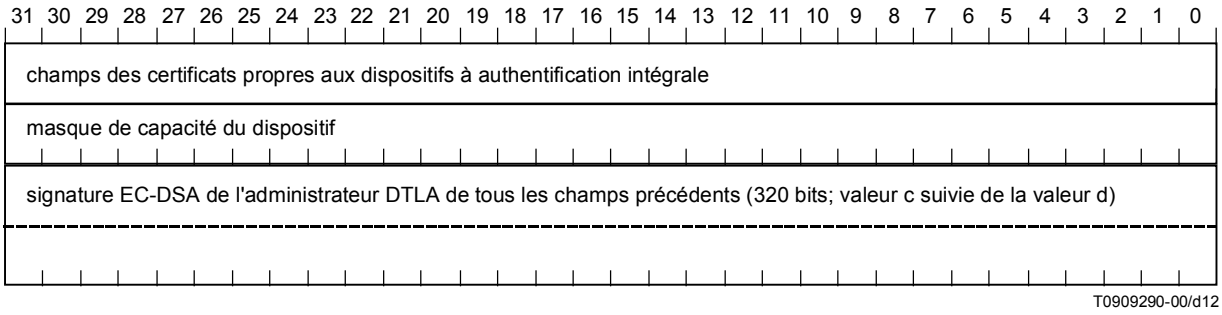


Figure III.8/J.95 – Champs de format élargi du certificat propre à un dispositif

Masque de capacité du dispositif

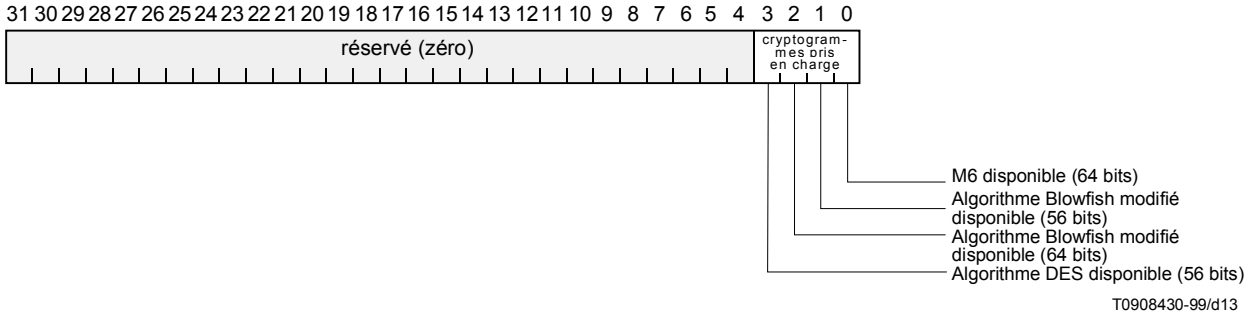


Figure III.9/J.95 – Masque de capacité du dispositif

Le masque de capacité du dispositif est fourni pour décrire les caractéristiques d'élargissement prises en charge par un dispositif donné. Le format du masque est représenté à la Figure III.9.

Il est supposé que les dispositifs qui ne prennent pas en charge le masque de capacité prennent uniquement en charge les caractéristiques cryptographiques obligatoires définies par ce système de protection du contenu (par exemple, le cryptogramme de référence M6 de 56 bits).

---

[3] Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.

III.4.3 Fabrication de dispositifs conformes

Tous les dispositifs conformes qui prennent en charge une authentification intégrale (c'est-à-dire chaque élément fabriqué, indépendamment de la marque et du type) se verront attribuer un identificateur de dispositif unique (X_{ID}) ainsi qu'une paire de clés publique/privée EC-DSA (X^1, X^{-1}) produites par l'administrateur DTLA. La clé X^{-1} doit être stockée au sein du dispositif de manière à ne pas pouvoir être divulguée. Les dispositifs conformes doivent également se voir attribuer un certificat propre (X_{Cert}) par l'administrateur DTLA. Ce certificat est stocké dans le dispositif conforme et est utilisé au cours du processus d'authentification. De plus, le dispositif conforme devra stocker les autres constantes et clés nécessaires à la mise en application des protocoles cryptographiques.

III.4.4 Fonctions cryptographiques

III.4.4.1 SHA-1 (algorithme de hachage sûr, révision 1)

SHA-1, comme décrit dans la norme FIPS PUB 180-1[4], est l'algorithme utilisé par la norme DSS pour produire une compilation de messages d'une longueur de 160 bits. Une compilation de messages est une valeur calculée à partir d'un message. Son concept est similaire à un mot de contrôle, mais sa contrefaçon est impossible sur le plan informatique.

III.4.4.2 Générateur de nombres aléatoires

Un générateur de nombres aléatoires de grande qualité est requis pour une authentification intégrale. La production de ce générateur de nombres aléatoires est indiquée par la fonction RNG_F décrite dans la spécification de protection DTCP disponible sous licence attribuée par l'administrateur DTLA.

III.4.4.3 Cryptographie à courbe elliptique (ECC)

Ces algorithmes cryptographiques sont fondés sur les principes cryptographiques sur les primitives et sur les méthodes de codage décrits dans la norme IEEE P1363/D3 (11 mai 1998). Le document IEEE P1363/D3 est un projet non approuvé sujet à modification. Des changements, susceptibles d'intervenir dans les versions ultérieures de ce projet, pourraient alors nuire à la conformité à la norme finale IEEE 1363 des algorithmes cryptographiques décrits ici.

Le système cryptographique à courbe elliptique (ECC, *elliptic curve cryptosystem*) est utilisé comme base cryptographique des algorithmes DH et DSA.

Le corps de définition classe les implémentations ECC. Pour ce système, le corps de définition utilisé est GF(p) où p est un nombre premier élevé supérieur à trois. Une courbe elliptique E sur le champ GF(p), où $p > 3$, est définie par les paramètres a et b et l'ensemble de solutions (x, y) à l'équation de la courbe elliptique ainsi que par un point supplémentaire souvent appelé *point à l'infini*. Ce point à l'infini est l'élément d'identité du groupe abélien, (E, +). L'équation de la courbe elliptique utilisée est la suivante:

$$y^2 = x^3 + ax + b \quad \text{où } 4a^3 + 27b^2 \neq 0$$

où a, b, x, y, sont les éléments de GF(p). Un point P sur la courbe elliptique se compose de la coordonnée x et de la coordonnée y d'une solution à cette équation, ou du point à l'infini, et est désigné par $P = (x_p, y_p)$.

Pour les algorithmes EC-DSA et EC-DH, on sélectionne un point de référence G sur la courbe elliptique. Toutes les opérations effectuées dans le domaine de la courbe elliptique sont calculées sur une courbe elliptique E définie sur GF(p). La clé publique Y^1 (point sur la courbe elliptique) et la clé privée Y^{-1} (valeur scalaire satisfaisant $0 < Y^{-1} < r$) pour chaque entité concernée satisfont l'équation suivante:

$$Y^1 = Y^{-1} G$$

Pour la spécification de la courbe elliptique utilisée:

- l'ordre du point de référence G aura un facteur premier élevé;
- le système résistera face à toute attaque par réduction de variable MOV, étant donné que l'on évite l'emploi de supercourbes elliptiques singulières.

---

4 National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", FIPS Publication 180-1, 17 avril 1995.

III.4.4.3.1 Algorithme de signature numérique à courbe elliptique (EC-DSA)

Signature

L'algorithme de signature suivant est fondé sur le principe de signature numérique ECSSA qui utilise la primitive de signature DLSP-DSA et la méthode de codage EMSA-SHA-1 définies au IEEE P1363/D3.

Entrée:

- M = données devant être signées
- X^{-1} = clé privée du dispositif de signature (doit être gardée secrète)
- p, a, b, G et r = paramètres de la courbe elliptique associés à X^{-1}

Sortie:

- $S_{X^{-1}}[M]$ = signature de 320 bits de données, M, fondée sur la clé privée, X^{-1}

Algorithme:

Etape 1: produire une valeur aléatoire, u, satisfaisant $0 < u < r$, en utilisant $\mathbf{RNG_F}$. Une nouvelle valeur de u est produite pour chaque signature et ne doit pas pouvoir être déterminée par un concurrent pour chaque calcul de signature. Calculer également le point sur la courbe elliptique, $V = uG$.

Etape 2: calculer $c = x_V \bmod r$ *(coordonnée x de V réduit modulo r)*. Si $c = 0$, passer alors à l'**étape 1**.

Etape 3: calculer $f = [\text{SHA-1}(M)]_{\text{msb\_bits\_in\_r}}$. Il s'agit de calculer le hachage SHA-1 de M puis de prendre les bits de plus fort poids de la compilation de messages, c'est-à-dire le même nombre de bits que la taille de r.

Etape 4: calculer $d = [u^{-1}(f + cX^{-1})] \bmod r$ *(il est à noter que u^{-1} est l'inverse modulaire de u mod r alors que X^{-1} est la clé privée du dispositif de signature)*. Si $d = 0$, passer alors à l'**étape 1**.

Etape 5: établir que les 160 premiers bits de $S_{X^{-1}}[M]$ sont égaux à la représentation gros-boutiste de c, et que les 160 bits suivants de $S_{X^{-1}}[M]$ sont égaux à la représentation gros-boutiste de d. $S_{X^{-1}}[M] = c \parallel d$).

Vérification

L'algorithme de vérification suivant est fondé sur le principe de signature numérique ECSSA qui utilise la primitive de signature DLVP-DSA et la méthode de codage EMSA-SHA-1 définies dans la norme IEEE P1363/D3.

Entrée:

- $S_{X^{-1}}[M]$ = signature présumée de 320 bits ($c \parallel d$) des données, M, fondée sur la clé privée, X^{-1}
- M = données associées à la signature
- X^1 = clé publique du dispositif de signature
- p, a, b, G, et r = paramètres de la courbe elliptique associés à X^{-1}

Sortie:

- "valide" ou "non valide", indique si la signature présumée est déterminée comme valide ou non valide, respectivement

Algorithme:

Etape 1: établir que c est égal aux 160 premiers bits de $S_{X^{-1}}[M]$ interprété comme faisant partie d'une représentation gros-boutiste, et que d est égal aux 160 bits suivants de $S_{X^{-1}}[M]$ interprété comme faisant partie d'une représentation gros-boutiste. Si c ne figure pas dans la plage $[1, r - 1]$ ou si d ne figure pas dans la plage $[1, r - 1]$, déclarer le résultat "non valide" et arrêter (le calcul).

Etape 2: calculer $f = [\text{SHA-1}(M)]_{\text{msb\_bits\_in\_r}}$. Il s'agit de calculer le hachage SHA-1 de M et de prendre ensuite les bits de plus fort poids de la compilation de messages, c'est-à-dire le même nombre de bits que la taille de r.

Etape 3: calculer $h = d^{-1} \bmod r$, $h_1 = (fh) \bmod r$, et $h_2 = (ch) \bmod r$.

Etape 4: calculer le point de la courbe elliptique $P = (x_P, y_P) = h_1G + h_2X^1$. Si P est égal au point à l'infini de la courbe elliptique, déclarer alors le résultat "non valide" et arrêter (le calcul).

Etape 5: calculer $c' = x_P \bmod r$. Si $c' = c$, déclarer alors le résultat "valide"; dans le cas contraire, déclarer le résultat "non valide".

III.4.4.3.2 Courbe elliptique Diffie-Hellman (EC-DH)

L'algorithme suivant de dérivation secrète partagée est fondé sur la primitive ECSVDP-DH définie dans la norme IEEE P1363/D3.

Entrée:

- Y_V = la valeur Diffie-Hellman de première phase produite par l'autre dispositif (point de courbe elliptique)
- p, a, b, G, et r = les paramètres de la courbe elliptique associés à X^{-1}

Sortie:

- X_V = la valeur Diffie-Hellman de première phase (point de courbe elliptique)
- la coordonnée x de $X_K Y_V$ = le secret partagé produit par cet algorithme (doit être gardé secret vis-à-vis des tiers)

Algorithme:

Etape 1: produire un entier aléatoire, X_K, dans la plage [1, r – 1] en utilisant $\mathbf{RNG_F}$. Une nouvelle valeur de X_K est produite pour chaque secret partagé et ne doit pas pouvoir être déterminée par un concurrent. Calculer également le point de la courbe elliptique, $X_V = X_K G$.

Etape 2: obtenir X_V.

Etape 3: calculer $X_K Y_V$. Obtenir la coordonnée x de $X_K Y_V$ comme valeur de secret partagé.

III.4.4.3.3 Implémentation du système cryptographique à courbe elliptique

Il est possible d'avoir une série d'implémentations du système cryptographique à courbe elliptique qui soient compatibles avec les primitives IEEE P1363 décrites dans le présent sous-paragraphe.

Une implémentation effective d'un système cryptographique à courbe elliptique peut consister à effectuer des calculs dans l'espace de Montgomery en utilisant les nouvelles définitions des opérations arithmétiques de base que sont l'addition, la soustraction, la multiplication et l'inverse[5].

III.4.5 Flux de protocoles

III.4.5.1 Aperçu général du flux de protocoles

Au cours du processus d'authentification intégrale:

1) le dispositif récepteur requiert l'exécution du processus d'authentification en transmettant une interrogation aléatoire et son propre certificat. Cela peut être le résultat du dispositif récepteur dans sa tentative d'accéder à un flux de contenu protégé (dont la valeur EMI est fixée à l'un des états suivants: "pas de copie", "plus de copies", ou "copie de première génération"). Le dispositif récepteur peut requérir l'exécution d'un processus d'authentification hypothétique, avant de tenter d'accéder à un flux de contenu. Si un dispositif récepteur tente de procéder à une authentification hypothétique, la demande peut être rejetée par la source;

2) le dispositif A renvoie alors une interrogation aléatoire ainsi que son certificat. Si la valeur des champs de format ou de type de certificat propre à l'autre dispositif est réservée, il convient d'abandonner immédiatement le processus d'authentification. A l'issue de l'échange de l'interrogation aléatoire et du certificat propre au dispositif, chaque dispositif vérifie l'intégrité du certificat de l'autre dispositif en utilisant EC-DSA. Si l'on détermine que la signature DTLA est valide, les dispositifs examinent la liste de révocation des certificats incorporée dans leurs messages d'aptitude du système au renouvellement (voir III.7) afin de vérifier que l'autre dispositif n'a pas été rejeté. Si l'autre dispositif n'a pas été rejeté, chaque dispositif calcule une valeur de première phase d'échange de clés EC-DH (voir III.4.4.3.2);

3) les dispositifs échangent alors les messages contenant la valeur de première phase de l'échange de clés EC-DH, le numéro de version du message d'aptitude au renouvellement et la génération du message d'aptitude du système au renouvellement mis en mémoire par le dispositif, ainsi que la signature du message contenant l'interrogation aléatoire de l'autre dispositif concaténée aux composantes précédentes.

---

5 Numéro de dépôt de demande japonais: à déterminer.

Les dispositifs vérifient les messages signés et reçus en contrôlant la signature du message au moyen de l'algorithme EC-DSA et de la clé publique de l'autre dispositif. Cela permet de vérifier que le message n'a pas été trafiqué. Si la signature ne peut être vérifiée, le dispositif refuse de poursuivre sa fonction.

De plus, grâce à la comparaison des numéros de version échangés, les dispositifs peuvent ultérieurement faire appel aux mécanismes de renouvellement du système (voir III.7.2 pour les détails de cette procédure).

Chaque dispositif calcule une clé d'authentification (K_{Auth}) en procédant à l'échange de clés EC-DH.

Une description détaillée du protocole d'authentification intégrale et des automates à états associés est donnée dans la spécification de protection DTCP disponible sous licence attribuée par l'administrateur DTLA.

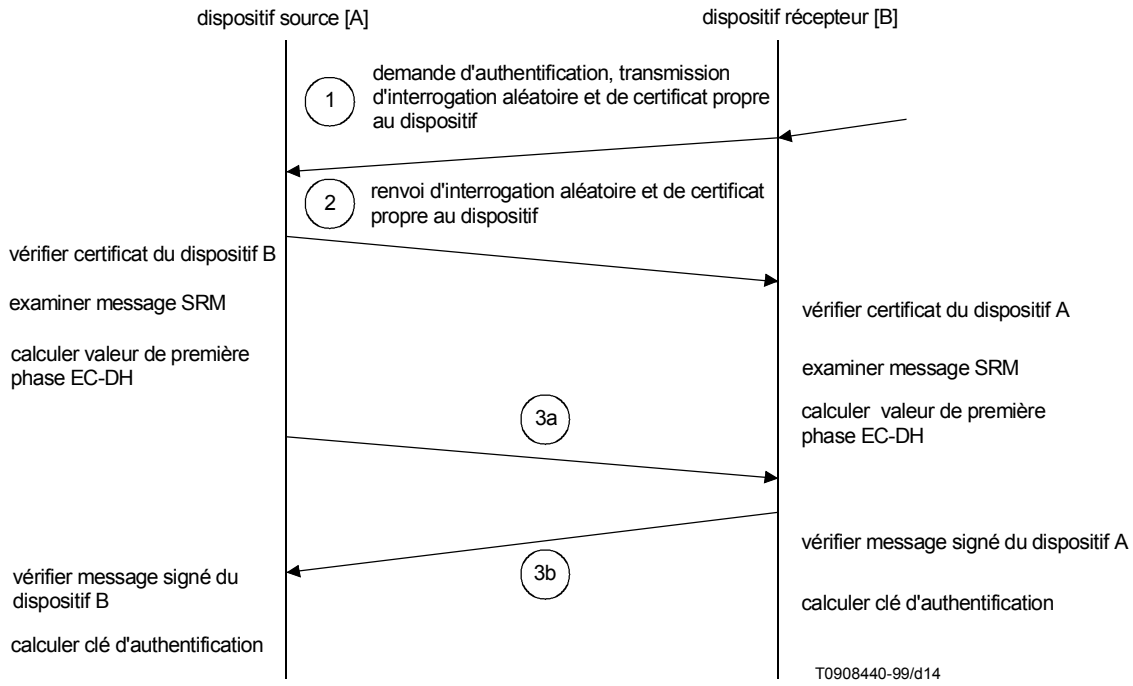


Figure III.10/J.95 – Aperçu général du flux de protocoles à authentification intégrale

III.5 Authentification restreinte

III.5.1 Introduction

Le présent sous-paragraphe décrit l'authentification et l'échange de clés entre les dispositifs source et récepteur qui font appel à une gestion de clés asymétrique et à une cryptographie commune de clés pour les contenus ayant les états suivants: "copie de première génération" et "plus de copies". Ces types de dispositifs, qui disposent généralement de ressources de calcul limitées, suivent un protocole d'authentification restreinte au lieu d'un protocole d'authentification intégrale. L'authentification restreinte repose sur l'utilisation des secrets partagés et de la fonction de hachage pour répondre à une interrogation aléatoire.

La méthode d'authentification restreinte est fondée sur la capacité d'un dispositif à démontrer qu'il détient un secret partagé avec d'autres dispositifs. Un dispositif authentifie un autre dispositif par la formulation d'une interrogation aléatoire à laquelle il répond en la modifiant avec le secret partagé et le hachage.

III.5.2 Notation

La notation indiquée dans le présent sous-paragraphe est utilisée pour décrire le processus et le protocole cryptographiques utilisés pour l'authentification restreinte.

III.5.2.1 Définis par l'administrateur DTLA

Les paramètres, clés, constantes et certificats suivants doivent être produits par l'administrateur DTLA.

III.5.2.1.1 Généralités

Les paramètres définis au III.4.2.1 sont également utilisés au cours du processus d'authentification restreinte par les dispositifs source qui prennent également en charge le processus d'authentification intégrale.

III.5.2.1.2 Pour le dispositif X

X_{Cert} = certificat propre à un dispositif attribué au dispositif conforme X par l'administrateur DTLA et utilisé au cours du processus d'authentification (voir III.5.2.2 pour plus de détails).

$X_{Kcosrc1}…X_{Kcosrc12}$ = chaque dispositif source de contenus dont l'état est "copie de première génération" reçoit des clés de douze 64 bits fournies par l'administrateur DTLA.

$X_{Kcosnk1}…X_{Kcosnk12}$ = chaque dispositif récepteur de contenus dont l'état est "copie de première génération" reçoit des clés de douze 64 bits fournies par l'administrateur DTLA.

$X_{Knmsrc1}…X_{Knmsrc12}$ = chaque dispositif source de contenus dont l'état est "plus de copies" reçoit des clés de douze 64 bits fournies par l'administrateur DTLA.

$X_{Knmsnk1}…X_{Knmsnk12}$ = chaque dispositif récepteur de contenus dont l'état est "plus de copies" reçoit des clés de douze 64 bits fournies par l'administrateur DTLA.

X_{KSV} = ce vecteur de sélection de clés (KSV, *key selection vector*) détermine les clés qui seront utilisées avec ce dispositif au cours de la procédure d'authentification restreinte. Seul un vecteur KSV est requis pour les dispositifs qui peuvent être à la fois un dispositif source et récepteur de contenus.

Tableau III.3/J.95 – Longueur des clés et constantes créées par l'administrateur DTLA (authentification restreinte)

Clé ou variable	Taille (bits)
Clés du dispositif récepteur "copie de première génération" ($X_{Kcosnk1}… X_{Kcosnk12}$)	64 (chacune)
Clés du dispositif source "copie de première génération" ($X_{Kcosrc1}… X_{Kcosrc12}$)	64 (chacune)
Clés du dispositif récepteur "plus de copies" ($X_{Knmsnk1}… X_{Knmsnk12}$)	64 (chacune)
Clés du dispositif source "plus de copies" ($X_{Knmsrc1}… X_{Knmsrc12}$)	64 (chacune)
Vecteur de sélection des clés (X_{KSV})	12

Les dispositifs contiennent les clés appropriées au type de contenu ainsi qu'aux fonctions qu'ils exécutent.

Notation utilisée au cours du processus d'authentification restreinte

Les valeurs complémentaires suivantes sont produites et utilisées par les dispositifs au cours du processus d'authentification restreinte:

X_n = mot de circonstance (interrogation aléatoire produite par RNG_R)

K_V, K'_V = clés de vérification

R, R′ = réponses aux mots de circonstance

K_{Auth}, K'_{Auth} = clés d'authentification

Tableau III.4/J.95 – Longueur des clés et variables produites par le dispositif (authentification restreinte)

Clé ou variable	Taille (bits)
Mot de circonstance (A_n, B_n)	64
Clés de vérification (K_v, K'_v)	64
Réponses (R, R')	64
Clés d'authentification (K_{Auth}, K'_{Auth})	96

III.5.2.2 Format du certificat propre à un dispositif

Le processus d'authentification restreinte utilise le certificat propre à un dispositif à authentification restreinte. Chaque certificat propre à un dispositif à authentification restreinte est attribué par l'administrateur DTLA et inclut un identificateur du dispositif ainsi qu'une signature, tous deux produits par l'administrateur DTLA. Tous les dispositifs récepteurs conformes qui prennent uniquement en charge une authentification restreinte doivent disposer de ce certificat.

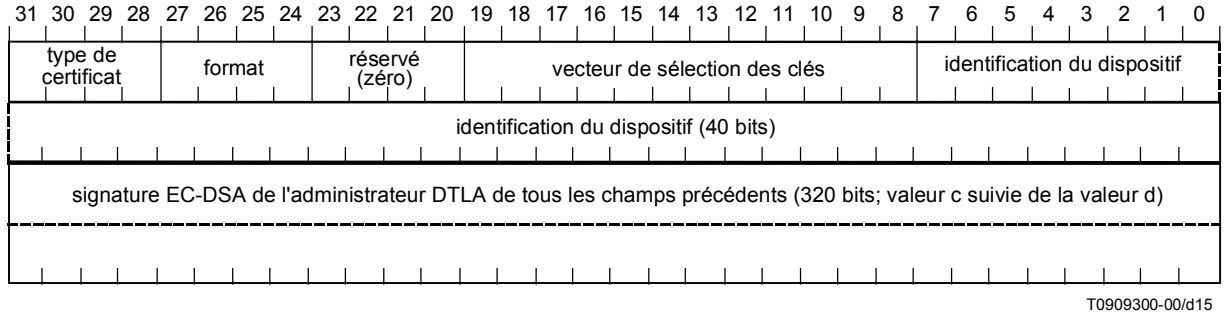


Figure III.11/J.95 – Format du certificat propre à un dispositif à authentification restreinte

Le certificat propre à un dispositif à authentification restreinte comprend les champs suivants (voir Figure III.11):

- **type du certificat** (4 bits) (voir III.4.2.3.1 pour une description du codage);
- **format du certificat** (4 bits) (voir III.4.2.3.1 pour une description du codage);
- **champ réservé** (4 bits). Ces bits sont réservés pour une définition future et sont actuellement définis comme ayant une valeur égale à zéro;
- **vecteur de sélection des clés** (X_{KSV}, 12 bits) attribué par l'administrateur DTLA (voir Figure III.12). Ce vecteur détermine les clés qui seront utilisées avec ce dispositif au cours de la procédure d'authentification restreinte. Ce vecteur KSV est utilisé sans tenir aucun compte de la valeur EMI du flux à traiter, ni du fait que le dispositif est utilisé comme un dispositif source ou récepteur de contenus. Le codage de ce champ est le suivant:
- le numéro **identificateur (ID) du dispositif** (X_{ID}, 40 bits) attribué par l'administrateur DTLA;
- la **signature EC-DSA** de l'administrateur DTLA des composantes énumérées ci-dessus (320 bits).

La taille globale du format du certificat propre à un dispositif à authentification restreinte est de 48 octets.

III.5.2.3 Générateur de nombres aléatoires

Le processus d'authentification restreinte requiert un générateur de nombres aléatoires. Le résultat obtenu avec ce générateur de nombres aléatoires est indiqué par la fonction RNG_R. Soit la fonction RNG_R soit la fonction RNG_F comme décrit dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA peut être utilisée pour l'authentification restreinte.

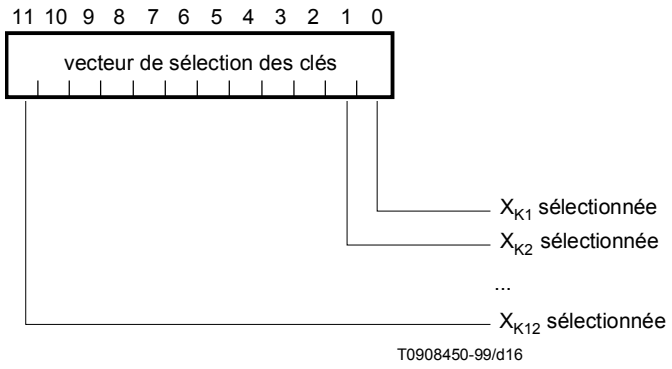


Figure III.12/J.95 – Vecteur de sélection des clés

III.5.3 Flux de protocoles

III.5.3.1 Aperçu général du flux de protocoles

La Figure III.13 donne un aperçu général du flux de protocoles à authentification restreinte.

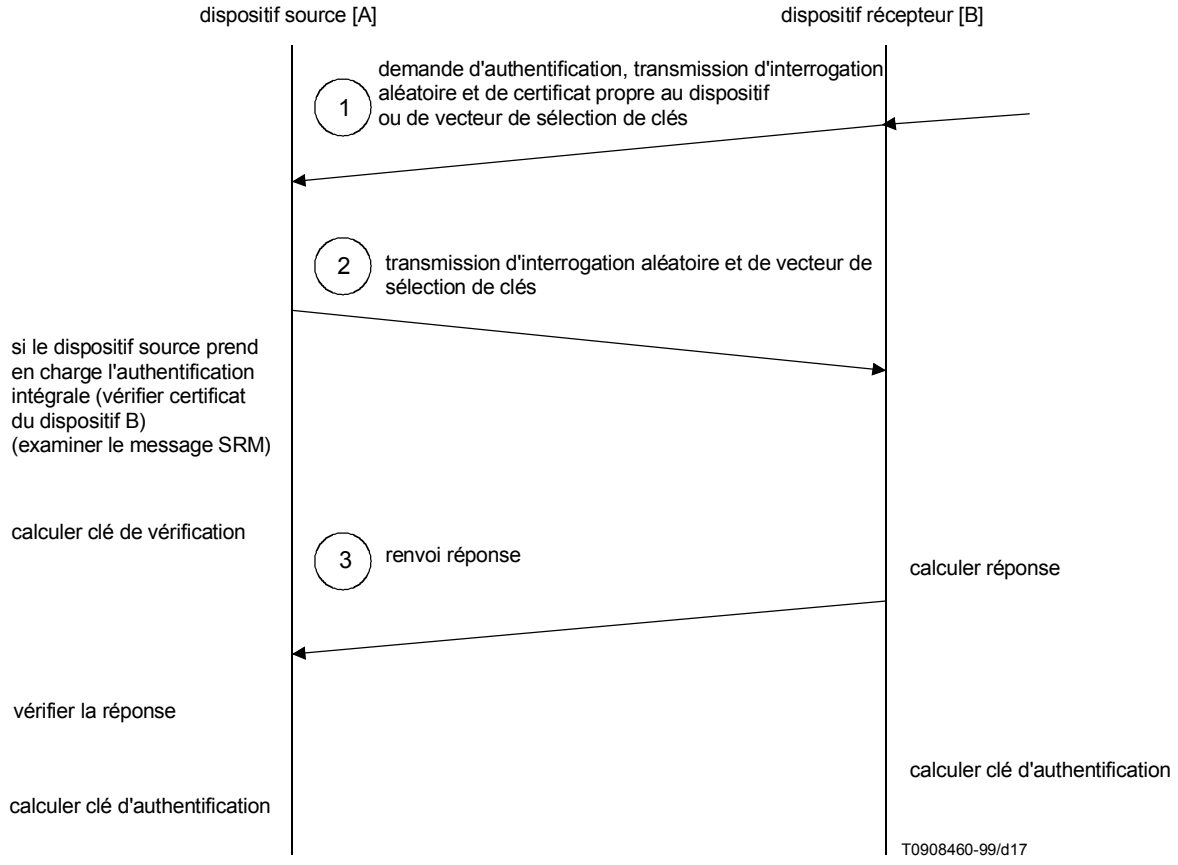


Figure III.13/J.95 – Aperçu général du flux de protocoles à authentification restreinte

Au cours du processus d'authentification restreinte:

1) le dispositif récepteur déclenche le protocole d'authentification en adressant une requête interrogative asynchrone au dispositif source. Cette requête contient le type de clé d'échange que les dispositifs source et récepteur doivent se partager ainsi qu'un nombre aléatoire produit par le dispositif récepteur à l'aide de la fonction RNG_R. Si le dispositif récepteur sait que le dispositif source n'est pas en mesure de prendre en charge une authentification intégrale, il transmet son vecteur KSV à ce dernier; dans le cas contraire, le dispositif récepteur transmet son certificat propre à un dispositif à authentification restreinte;

2) le dispositif source produit une interrogation aléatoire à l'aide de la fonction RNG_R et la transmet au dispositif récepteur. Si le dispositif source prend en charge une authentification intégrale, il extrait l'identificateur du dispositif récepteur du certificat transmis par celui-ci. Il vérifie ensuite:

   a) que le certificat transmis par le récepteur est valide;

   b) que l'identificateur du dispositif récepteur ne figure pas dans la liste de révocation de certification contenue dans le message d'aptitude du système au renouvellement, lui-même stocké dans le dispositif source.

   Ainsi, si la valeur des champs types ou de format du certificat de l'autre dispositif est réservée, il convient d'abandonner immédiatement le processus d'authentification. Si ces vérifications sont effectuées de manière satisfaisante, le dispositif source poursuit le protocole en calculant la clé de vérification;

3) après réception de l'interrogation aléatoire en provenance du dispositif source, le dispositif récepteur calcule une réponse à l'aide d'une clé de vérification qu'il a lui-même calculée et la transmet au dispositif source;

4) après que le dispositif récepteur a répondu, le dispositif source compare cette réponse avec les informations similaires produites côté source, à l'aide de sa clé de vérification. Si la comparaison correspond à son propre calcul, le dispositif récepteur a été vérifié et authentifié. Si la comparaison ne correspond pas à son calcul, le dispositif source doit rejeter le dispositif récepteur. Enfin, chaque dispositif calcule la clé d'authentification.

Une description détaillée du protocole d'authentification restreinte et des automates à états associés figure dans la spécification de protection DTCP disponible sous licence attribuée par l'administrateur DTLA.

III.6 Gestion et protection des canaux de contenus

III.6.1 Introduction

Le présent sous-paragraphe décrit en détail les mécanismes utilisés pour:

1) partager une clé d'échange entre un dispositif source et un dispositif récepteur;

2) établir et gérer le canal isochrone crypté par lequel circule le contenu protégé.

Le processus d'authentification intégrale ou restreinte (selon les capacités du dispositif) doit être mené à son terme avant de définir un canal de contenu.

III.6.2 Clés de gestion du contenu

III.6.2.1 Clé d'échange (K_x, *exchange key*)

Un jeu commun de clés d'échange (K_x) est établi entre un dispositif source et tous les dispositifs récepteurs qui ont exécuté la procédure d'authentification appropriée (intégrale ou restreinte) avec le dispositif source requis pour traiter les contenus avec une valeur EMI spécifique (voir III.6.4.2). De plus, si des cryptogrammes de contenus facultatifs[6] sont mutuellement pris en charge, on définit des clés d'échange pouvant être utilisées avec lesdits cryptogrammes pour les contenus de type "pas de copie".

La procédure d'établissement d'une clé d'échange est décrite au III.6.3.1.

III.6.2.2 Clé de contenu (K_c, *content key*)

La **clé de contenu** (K_c) est utilisée comme clé du moteur de cryptage du contenu. K_c est calculée à partir des trois valeurs indiquées ci-dessous:

- clé d'échange K_x attribuée au mode EMI et à la taille du cryptogramme/la longueur de la clé utilisés pour protéger le contenu;

---

6 Uniquement applicables aux clés d'échange établies à la suite d'une authentification intégrale entre les deux dispositifs qui prennent en charge le masque de capacité facultatif du certificat propre au dispositif.

- nombre aléatoire N_c produit par le dispositif source (à l'aide de la fonction RNG_F pour les dispositifs qui prennent en charge une authentification intégrale ou à l'aide de la fonction RNG_R pour les dispositifs qui prennent en charge uniquement une authentification restreinte) et transmis sous forme de texte en clair à tous les dispositifs récepteurs à l'intérieur de paquets asynchrones;
- valeur constante C_a, ou C_b, ou C_c, qui correspond au mode de cryptage EMI dans l'en-tête d'un paquet.

La clé de contenu est produite de la manière suivante:

$$K_c = J[K_x, N_c, f[\text{EMI}]]$$

où:

$f[\text{EMI}] = C_a$ si EMI est le mode A

$f[\text{EMI}] = C_b$ si EMI est le mode B

$f[\text{EMI}] = C_c$ si EMI est le mode C

C_a, C_b et C_c sont des constantes secrètes universelles attribuées par l'administrateur DTLA. Les valeurs de ces constantes sont spécifiées dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA. La définition de la fonction J [] est également décrite dans le présent appendice.

III.6.2.3 Longueur des clés

Le Tableau III.5 donne la liste des longueurs des clés et des constantes décrites ci-dessus:

Tableau III.5/J.95 – Longueur des clés et des constantes (gestion des canaux de contenus)

Clé, variable, ou constante	Taille (bits)
Clés d'échange (K_x)	96
Clés d'échange chiffrées (K_{sx})	96
Constantes (C_a, C_b, C_c)	24
Clé de contenu pour le cryptogramme de référence (K_c)	56
Clé de contenu pour les cryptogrammes facultatifs[a)] (K_c)	56-64
Mot de circonstance pour le canal de contenu (N_c)	64

a) Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.

III.6.3 Flux de protocoles

III.6.3.1 Définition de la clé d'échange

Après exécution du processus d'authentification intégrale ou restreinte, le dispositif source définit la ou les clés d'échange décrites au III.6.2.1. La procédure suivante est utilisée pour chaque clé:

1) le dispositif source a attribué une valeur aléatoire pour la clé d'échange spécifique (K_x) définie;
2) il attribue ensuite un chiffre (chiffrement) à la clé K_x en utilisant K_{Auth}, ce qui donne K_{sx} selon la fonction décrite dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA;
3) le dispositif source transmet K_{sx} au dispositif récepteur;
4) le dispositif récepteur déchiffre la clé K_{sx} à l'aide de K'_{Auth} afin de déterminer la clé d'échange partagée K_x selon la fonction décrite dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA.

Le dispositif source répète les étapes précédentes pour toutes les clés d'échange requises entre lui-même et le dispositif récepteur.

Enfin, les dispositifs mettent à jour le message SRM (message d'aptitude du système au renouvellement) si cela est jugé nécessaire au cours du processus d'authentification intégrale (voir III.4).

Les dispositifs demeurent authentifiés aussi longtemps qu'ils maintiennent valides les clés d'échange. La clé d'échange peut être utilisée de manière répétée pour fixer et gérer la sécurité des flux de contenus protégés par droit d'auteur sans autre authentification. Il est recommandé que les clés d'échange des dispositifs source ne soient plus valides lorsque ces derniers cessent toutes sorties isochrones. De plus, les clés d'échange des dispositifs ne sont plus valides au moment où ces derniers sont déconnectés du bus.

III.6.3.2 Définition des clés de contenus

Le présent sous-paragraphe décrit le mécanisme de définition des clés de contenus (K_c) utilisées pour crypter/décrypter le contenu échangé entre les dispositifs source et récepteur (voir Figure III.14).

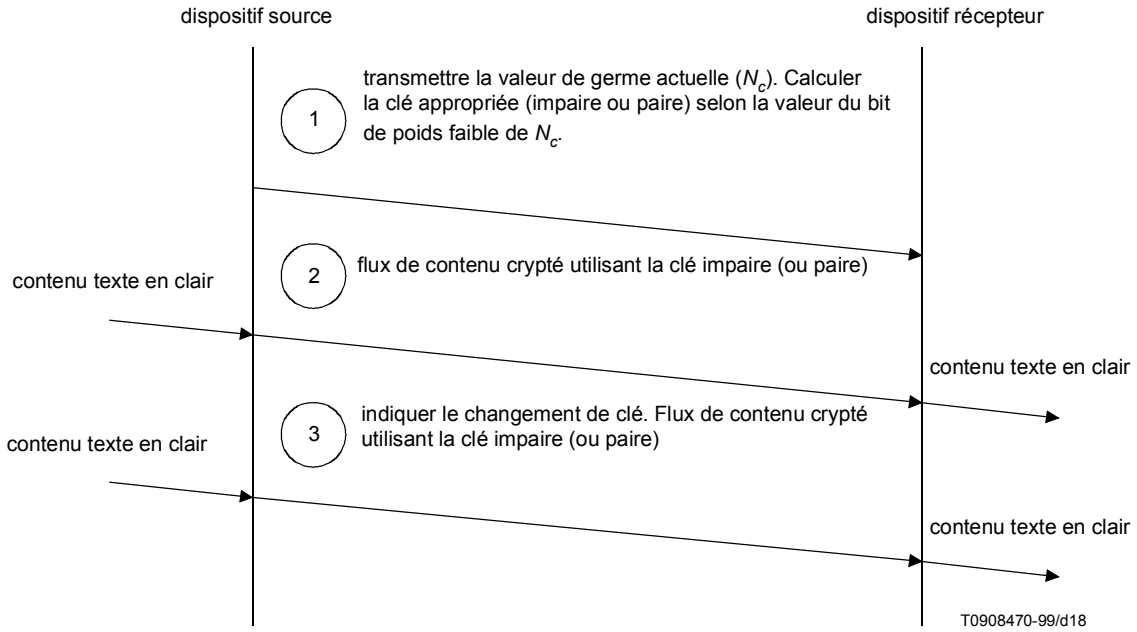


Figure III.14/J.95 – Aperçu général du flux de protocoles de définition et de gestion d'un canal de contenu

Les clés de contenus sont définies entre le dispositif source et le dispositif récepteur de la manière suivante:

1) lorsque le dispositif source commence à transmettre un contenu, il produit un nombre aléatoire de 64 bits comme valeur initiale du germe (N_c) de la clé de contenu. Le germe initial est classé comme germe impair ou pair sur la base de son bit de plus faible poids. Si d'autres canaux de contenus sont définis, la valeur actuelle de N_c obtenue à partir du ou des canaux de contenus actifs peut être utilisée comme germe;

2) le dispositif source commence à transmettre le contenu à l'aide de la clé de contenu impaire ou paire (K_c) correspondant à la référence susmentionnée du germe initial afin de crypter le contenu. La clé de contenu est calculée par le dispositif source à l'aide de la fonction *J*, de la clé d'échange K_x, du germe (N_c) ainsi que de la fonction *f[EMI]*. Un bit de l'en-tête de paquet IEEE 1394 est utilisé pour indiquer la clé (impaire ou paire) qui est utilisée pour crypter un paquet spécifique de contenus. Si le germe initial est impair, le bit pair/impair de l'en-tête de paquet IEEE 1394 est déterminé comme impair; dans le cas contraire, il est déterminé comme pair.

A réception du germe N_c, le dispositif récepteur vérifie si le bit de plus faible poids de la valeur N_c correspond à l'état du bit impair/pair. Si les deux bits sont identiques, le dispositif récepteur calcule la clé de contenu actuelle à l'aide de la fonction *J*, de K_x, de *f[EMI]*, et de N_c. Si ces bits sont différents, il indique que la clé a été modifiée et le dispositif récepteur calcule la clé de contenu actuelle à l'aide de la méthode suivante:

a) calculer $N_c + 1 \ mod \ 2^{64}$ comme nouveau germe;

b) calculer la clé de contenu à l'aide de la méthode ci-dessus en utilisant le nouveau germe en lieu et place du germe original transmis par le dispositif source.

Le dispositif source prépare la prochaine clé de contenu en calculant K_c au moyen du même processus employé pour le calcul initial à l'exception du fait que la valeur du germe (N_c) augmente.

Régulièrement, le dispositif source doit modifier les clés de contenus afin de maintenir une protection robuste du contenu. Pour modifier les clés, le dispositif source commence le cryptage avec la nouvelle clé calculée ci-dessus et indique ce changement en commutant l'état du bit impair/pair de l'en-tête de paquet IEEE 1394. La période minimale de modification de la clé de contenu est définie à 30 s. La période maximale est définie à 120 s. La durée relative à K_c est comprise entre 30 s et 2 min. Il convient que le dispositif source n'augmente pas le rythme de fonctionnement du compteur de la clé de contenu lorsqu'il ne produit que des contenus marqués d'une valeur EMI (voir III.6.4.2) de copie autorisée. Lorsqu'un dispositif suspend toutes les données isochrones produites, il convient qu'il réinitialise son compteur.

Le flux de protocoles nécessaire à la définition de la clé de contenu à l'aide des transactions IEEE 1394 est représenté au III.8.

III.6.3.3 Bit impair/pair

Le bit impair/pair (le 3e bit du champ synchrone de l'en-tête de paquet isochrone IEEE 1394) est utilisé pour indiquer la clé de contenu (K_c) actuellement utilisée pour protéger le canal de contenu (voir Figure III.15). Le bit impair/pair n'existe que lorsque la valeur du champ étiqueté est 01A; "0" indique qu'il convient d'utiliser la clé paire tandis que "1" indique qu'il convient d'utiliser la clé impaire. La clé impaire et la clé paire sont utilisées et mises à jour alternativement. Le bit impair/pair ne peut être modifié que sur des paquets isochrones qui contiennent le début d'une nouvelle trame de cryptage ou qui constituent un paquet au repos entre des trames de cryptage. Si un paquet isochrone contient des parties de plusieurs trames de cryptage, la modification apportée à la clé s'applique à la première trame de cryptage au début du paquet.

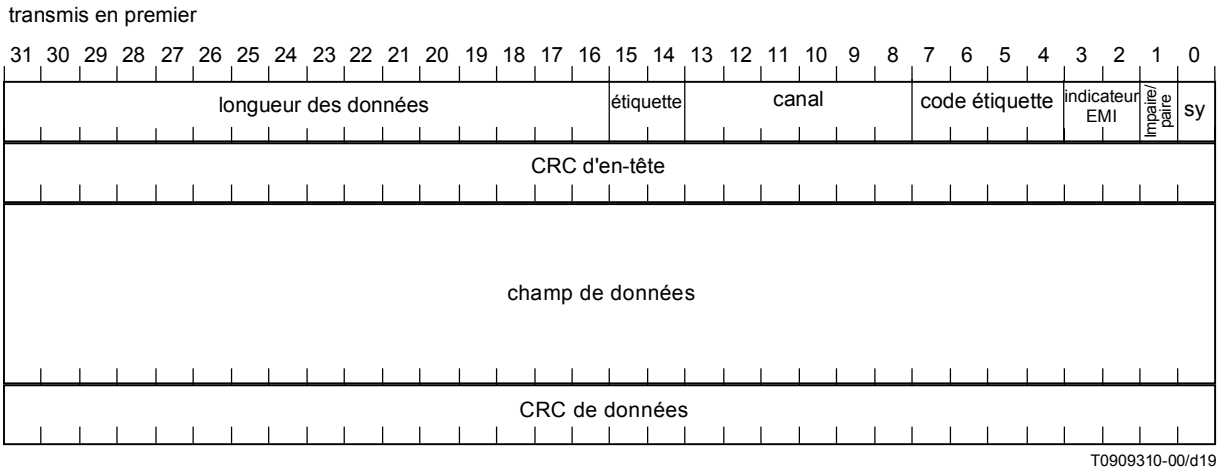


Figure III.15/J.95 – Emplacement du bit impair/pair dans l'en-tête de paquet

III.6.4 Informations relatives au contrôle des copies (CCI)

Les **informations relatives au contrôle des copies (CCI, *copy control information*)** spécifient les attributs du contenu eu égard à ce système de protection du contenu. Deux mécanismes CCI sont admis: informations CCI incorporées et indicateur de mode de cryptage.

III.6.4.1 Informations CCI incorporées

Les informations CCI incorporées sont véhiculées comme partie du flux de contenu. De nombreux formats de contenu y compris le format MPEG ont des champs alloués à la transmission des informations CCI associées au flux. L'intégrité des informations CCI incorporées est garantie dans la mesure où la falsification du flux de contenu entraîne un mauvais décryptage dudit contenu.

III.6.4.2 Indicateur du mode de cryptage (EMI)

L'indicateur du mode de cryptage (EMI) garantit un mécanisme d'accès facile et non moins sûr qui permet d'indiquer les informations CCI associées à un flux de contenu numérique. Pour les bus série IEEE 1394, l'indicateur EMI est placé dans les deux bits de plus fort poids du champ synchrone de l'en-tête de paquet comme représenté à la Figure III.16. Les bits de l'indicateur EMI n'existent que lorsque la valeur du champ étiqueté est 01. En plaçant l'indicateur EMI sur un site d'accès facile, les dispositifs peuvent déterminer immédiatement les informations CCI du flux de contenu sans devoir décoder le format de transport du contenu pour extraire les informations CCI incorporées. Cette disposition est importante pour faciliter la tâche des dispositifs d'enregistrement à flux binaire (par exemple enregistreur-lecteur numérique) qui ne reconnaissent pas et qui ne peuvent pas décoder des formats de contenu spécifiques.

Les bits EMI ne peuvent être modifiés qu'avec les paquets isochrones qui contiennent le début d'une nouvelle trame de cryptage ou qui constituent des paquets inactifs entre des trames de cryptage. Si un paquet isochrone contient des parties de plusieurs trames de cryptage, la modification apportée à l'indicateur EMI s'applique alors à la première trame de cryptage au début du paquet.

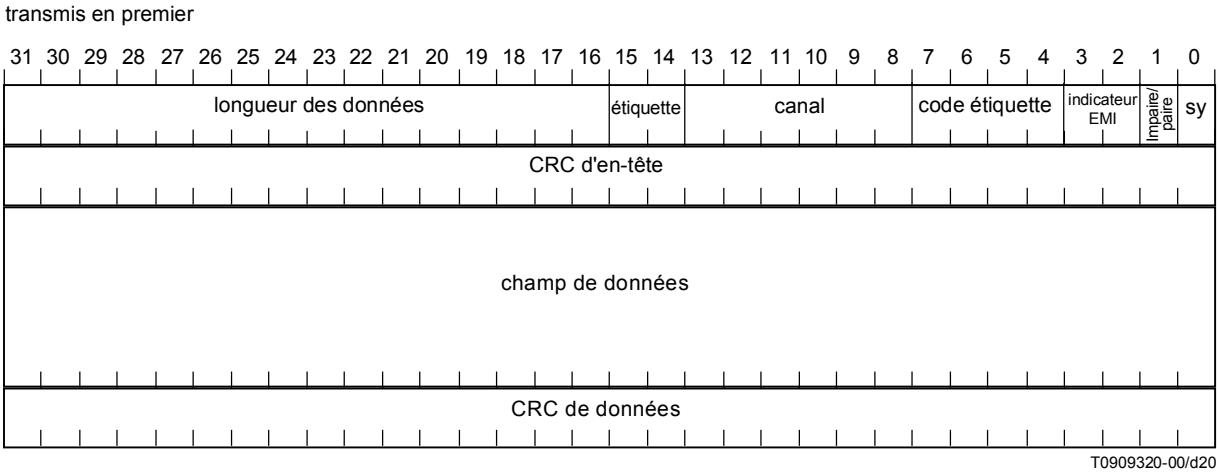


Figure III.16/J.95 – Emplacement de l'indicateur EMI

L'indicateur EMI indique le mode de cryptage appliqué à un flux:

- les dispositifs source sous licence choisiront le mode de cryptage approprié en fonction des caractéristiques du flux de contenu et régleront son indicateur EMI en conséquence. Si le flux de contenu se compose de flux secondaires multiples avec différentes informations CCI incorporées, les informations CCI incorporées les plus strictes seront utilisées pour régler l'indicateur EMI;

- les dispositifs récepteurs sous licence choisiront le mode de décryptage approprié, comme indiqué par l'indicateur EMI.

Si les bits de l'indicateur EMI sont falsifiés, les modes de cryptage et de décryptage ne correspondront pas, entraînant de ce fait un mauvais décryptage du contenu.

Tableau III.6/J.95 – Codage EMI

Mode EMI	Valeur EMI	Signification	Authentification requise
Mode A	11	Pas de copie	Intégrale
Mode B	10	Copie de première génération	Restreinte ou intégrale
Mode C	01	Plus de copies	Restreinte ou intégrale
N.A.[a)]	00	Copie autorisée	Aucune, non cryptée
[a)] Non applicable. Aucun mode EMI n'est défini pour un codage de 00.			

- Un codage 00 est utilisé pour indiquer que la copie du contenu peut être autorisée. Aucune authentification ni aucun cryptage n'est requis pour protéger ce contenu.

- Pour les contenus qui ne doivent jamais être copiés [par exemple contenus de supports préenregistrés avec une valeur de système de gestion des générations de copies (CGMS, *copy generation management system*) égale à 11], un codage EMI de valeur 11 est utilisé. Ce contenu peut être échangé uniquement entre des dispositifs qui ont exécuté avec succès la procédure d'authentification intégrale.

- Un codage EMI de 10 indique que l'on peut procéder à une génération de copies (par exemple contenus de supports préenregistrés avec une valeur CGMS de 10). Les dispositifs qui échangent ce contenu peuvent faire appel soit à l'authentification intégrale, soit à l'authentification restreinte.

- Si un contenu dont l'indicateur EMI = 10 est reproduit, les échanges futurs par l'intermédiaire d'une interconnexion numérique sont marqués d'un codage EMI de 01, ce qui indique qu'une copie à génération unique a déjà été faite.

III.6.4.3 Relation entre les informations CCI incorporées et l'indicateur EMI

Un flux de contenu protégé peut se composer d'un ou de plusieurs programmes. Chacun de ces programmes peut se voir attribuer un niveau différent d'informations CCI incorporées. Dans la mesure où l'indicateur EMI est associé au flux global de contenu, il est possible que ce dernier soit composé de programmes multiples et que l'indicateur EMI ne corresponde pas à la valeur des informations CCI incorporées dans chacun des programmes protégés. En cas de conflit, la valeur la plus restrictive des informations CCI incorporées sera utilisée pour l'indicateur EMI.

Tableau III.7/J.95 – Relation entre l'indicateur EMI et les informations CCI incorporées

EMI	Informations CCI incorporées pour chaque programme			
	00	01	10	11
Mode A (pas de copie)	Autorisées	Autorisées[a)]	Autorisées	Autorisées
Mode B (copie de première génération)	Autorisées	Interdites	Autorisées	Interdites
Mode C (plus de copies)	Autorisées	Autorisées	Autorisées	Interdites
N.A. (copie autorisée)	Autorisées	Interdites	Interdites	Interdites
[a)] N'est pas particulièrement utilisé.				

III.6.4.4 Traitement de l'indicateur EMI/des informations CCI incorporées pour les fonctions courantes des dispositifs

Le présent sous-paragraphe présente le comportement des fonctions courantes des dispositifs selon leur capacité à transmettre/recevoir l'indicateur EMI et à détecter/modifier les informations CCI incorporées. Les autres fonctions non reprises dans le présent sous-paragraphe peuvent être admises dans la mesure où elles sont cohérentes avec les dispositions de la présente spécification.

III.6.4.4.1 Fonction source de reconnaissance du format

Une fonction source de reconnaissance du format (voir Tableau III.8) peut reconnaître les informations CCI incorporées d'un flux de contenu en cours de transmission.

Tableau III.8/J.95 – Traitement des informations CCI relatives à la fonction source de reconnaissance du format

Informations CCI de programme incorporées				EMI
00	**01**	**10**	**11**	
Aucune importance	(Note)	Aucune importance	Présentes	Mode A (pas de copie)
Aucune importance	Ne peuvent être présentes	Présentes	Ne peuvent être présentes	Mode B (copie de première génération)
Aucune importance	Présentes	Ne peuvent être présentes	Ne peuvent être présentes	Mode C (plus de copies)
Présentes	Ne peuvent être présentes	Ne peuvent être présentes	Ne peuvent être présentes	N.A. (copie autorisée)
Autres combinaisons				Transmission interdite
NOTE – Sans aucune importance, mais n'est pas particulièrement utilisé.				

III.6.4.4.2 Fonction source de non-reconnaissance du format

Une fonction source de non-reconnaissance du format (voir Tableau III.9) n'a pas besoin de reconnaître les informations CCI incorporées d'un flux de contenu en cours de transmission.

Tableau III.9/J.95 – Traitement des informations CCI relatives à la fonction source de non-reconnaissance du format

EMI ou informations CCI enregistrées[a)] d'un contenu source	EMI utilisé pour une transmission
Pas de copie	Mode A (pas de copie)
Copie de première génération	Mode B (copie de première génération)
Plus de copies	Mode C (plus de copies)
Copie autorisée	N.A. (copie autorisée)

a) Les informations CCI enregistrées sont des informations relatives au contrôle des copies qui ne sont pas incorporées dans le programme de contenu et qui ne nécessitent pas de connaître le format de contenu à extraire.

III.6.4.4.3 Fonction d'enregistrement à reconnaissance du format

Une fonction d'enregistrement à reconnaissance du format (voir Tableau III.10) reconnaît les informations CCI incorporées d'un programme de contenus reçu avant de les inscrire sur des supports inscriptibles.

Tableau III.10/J.95 – Traitement des informations CCI de la fonction d'enregistrement à reconnaissance du format

EMI	Informations CCI de programme incorporées			
	00	01	10	11
Mode A (pas de copie)	Inscriptible	Ne pas enregistrer	(Note 1)	Ne pas enregistrer
Mode B (copie de première génération)	Inscriptible	Ignorer le flux entier de contenu (Note 2)	(Note 1)	Ignorer le flux entier de contenu (Note 2)
Mode C (plus de copies)	Inscriptible	Ne pas enregistrer	Ne pas enregistrer	Ignorer le flux entier de contenu (Note 2)
NOTE 1 – Si la fonction d'enregistrement prend en charge l'enregistrement de la valeur CCI de l'état "plus de copies", ladite valeur doit alors être consignée avec le programme. Dans le cas contraire, les informations CCI de l'état "pas de copie" doivent être consignées avec le programme. NOTE 2 – Si la fonction détecte cette combinaison d'informations CCI parmi les programmes qu'elle enregistre, le flux entier de contenu est ignoré.				

III.6.4.4.4 Fonction de réception à reconnaissance du format

Une fonction de réception à reconnaissance du format peut reconnaître les informations CCI incorporées du contenu reçu.

Le Tableau III.11 indique les informations CCI de programme incorporées, contenues dans le flux de contenu qui peut être reçu.

Tableau III.11/J.95 – Traitement des informations CCI relatives à la fonction de réception à reconnaissance du format

EMI	Informations CCI de programme incorporées			
	00	01	10	11
Mode A (pas de copie)	Peuvent être traitées	Peuvent être traitées (Note 2)	Peuvent être traitées	Peuvent être traitées
Mode B (copie de première génération)	Peuvent être traitées	Ignorer le flux entier de contenu (Note 1)	Peuvent être traitées	Ignorer le flux entier de contenu (Note 1)
Mode C (plus de copies)	Peuvent être traitées	Peuvent être traitées	Peuvent être traitées (Note 3)	Ignorer le flux entier de contenu (Note 1)
NOTE 1 – Si la fonction détecte cette combinaison d'informations CCI parmi les programmes qu'elle enregistre, le flux entier de contenu est ignoré. NOTE 2 – N'est pas particulièrement utilisé. NOTE 3 – Si le dispositif dispose d'une règle de traitement de l'état "plus de copies", ce programme doit être traité selon la règle. Dans le cas contraire, le programme doit être traité comme l'état "pas de copie".				

III.6.4.4.5 Fonction d'enregistrement à non-reconnaissance du format

Une fonction d'enregistrement à non-reconnaissance du format (voir Figure III.12) peut enregistrer un contenu avec un indicateur EMI approprié sur des supports inscriptibles.

Tableau III.12/J.95 – Traitement des informations CCI relatives à la fonction d'enregistrement à non-reconnaissance du format

EMI du flux reçu	Les informations CCI enregistrées[a)] doivent être inscrites sur des supports utilisateur inscriptibles
Mode A (pas de copie)	Le flux ne peut être enregistré
Mode B (copie de première génération)	Plus de copies
Mode C (plus de copies)	Le flux ne peut être enregistré

a) Les informations CCI sont des informations relatives au contrôle des copies qui ne sont pas incorporées dans le programme de contenu et qui ne nécessitent pas de connaître le format de contenu à extraire.

III.6.4.4.6 Fonction de réception à non-reconnaissance du format

Pour cette fonction, le contenu doit être traité d'une manière qui soit cohérente avec son indicateur EMI 6.5 Catégories courantes de dispositifs.

Les dispositifs peuvent prendre en charge aucune ou plusieurs fonctions parmi les fonctions décrites au III.6.4.4.

Les types courants de dispositifs de fonction fixes incluent, sans toutefois s'y limiter, les dispositifs suivants:

1) **le dispositif source à contenu préenregistré et à reconnaissance du format** a une fonction source de reconnaissance du format (par exemple lecteur DVD);

2) **le dispositif source/de décodage du contenu acheminé en temps réel et à reconnaissance du format** a une fonction source de reconnaissance du format et une fonction réception de reconnaissance du format (par exemple boîtier adaptateur ou TV numérique);

3) **l'enregistreur-lecteur à reconnaissance du format** a une fonction source de reconnaissance du format, une fonction réception de reconnaissance du format, et une fonction enregistrement de reconnaissance du format (par exemple DV-VCR);

4) **l'enregistreur-lecteur à non-reconnaissance du format** a une fonction source de non-reconnaissance du format et une fonction enregistrement de non-reconnaissance du format (par exemple D-VHS VCR);

5) **le pont de bus à non-reconnaissance du format** a une fonction source de non-reconnaissance du format et une fonction réception à non-reconnaissance du format (par exemple, IEEE 1394 à IEEE 1394, pont de bus).

III.6.5 Cryptogrammes propres au canal de contenu

Tous les dispositifs conformes prennent en charge le cryptogramme de référence et éventuellement d'autres cryptogrammes facultatifs pour la protection du contenu[7].

III.6.5.1 Cryptogramme de référence

Tous les dispositifs et applications doivent, au minimum, prendre en charge le cryptogramme de référence afin de garantir l'interopérabilité. Le chiffrement par bloc M6-S56 qui utilise le mode de chaînage de blocs de cryptogrammes convertis (C-CBC, *converted cipher-block-chaining*) est le cryptogramme de référence. Ce cryptogramme est décrit en détail dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA.

---

7 Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.

III.6.5.2 Formats de cryptage du contenu

Le Tableau III.13 donne les formats de cryptage du contenu qui seront utilisés avec les cryptogrammes propres au canal de contenu.

Tableau III.13/J.95 – Formats de cryptage du contenu

Format des données	Trame de cryptage	Taille
Flux de transport MPEG	Paquet du flux de transport CEI 61883-4	188 octets
DV (format SD)	Unité de transfert isochrone CEI 61883-2	480 octets
Audio	Données conformes à CEI 61883-6 (CEI-PAS) CEI 958 pour 2 canaux	8 octets

III.6.5.3 Support des cryptogrammes facultatifs propres au canal de contenu

Le support est défini au III.4 (masque de capacité des dispositifs), à la Section A.6 (détermination de valeurs K_X multiples), à la Section A.8 (codage de la sélection de cryptogrammes dans l'ensemble de commandes d'interface numérique AV/C). Les algorithmes à cryptogrammes facultatifs propres au canal de contenu utilisant le mode de chaînage de blocs de cryptogrammes (C-CBC) convertis sont décrits dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA[8].

III.7 Aptitude du système au renouvellement

III.7.1 Introduction

Les dispositifs conformes qui prennent en charge une authentification intégrale peuvent recevoir et traiter les messages d'aptitude du système au renouvellement (SRM) créés par l'administrateur DTLA et distribués avec le contenu. Ces messages sont utilisés pour garantir l'intégrité à long terme du système.

III.7.1.1 Composantes et présentation d'un message d'aptitude du système au renouvellement

Plusieurs composantes constituent le message d'aptitude du système au renouvellement (SRM):

- un champ définissant le **type** de message (4 bits). Ce champ a le même codage que celui qui est utilisé pour le champ définissant le type de certificat dans le cas des certificats propres aux dispositifs. Voir III.4.2.3.1 pour une description. Le seul codage actuellement défini est 0, ce qui indique que le message est destiné à la protection du contenu IEEE 1394;
- un champ de **génération** du message (SRMM) (4 bits). Ce champ spécifie la génération du message SRM. Il est utilisé pour garantir l'extension du mécanisme SRM. Actuellement, le seul codage défini est 0, qui indique un message SRM de première génération avec une taille maximale définie dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA. D'autres codages sont actuellement réservés. Cette valeur reste inchangée même si seule une partie du message SRM peut être mise en mémoire par le dispositif (par exemple X_{SRMC} <= SRMM);
- champ réservé (8 bits). Ces bits sont réservés pour une définition future et sont actuellement définis comme ayant une valeur zéro;
- un numéro de version du message d'aptitude du système au renouvellement à croissance monotone (SRMV, *system renewability message version number*) (16 bits). Cette valeur est échangée comme valeur X_{SRMV} au cours de l'authentification intégrale. Cette valeur n'est pas réinitialisée lorsque le champ de génération du message est modifié;
- longueur de la liste de révocation des certificats (CRL, *certificate revocation list*) (16 bits). Ce champ spécifie la taille (en octets) de la liste CRL y compris le champ définissant sa longueur (deux octets), ses entrées (longueur variable), et la signature de l'administrateur DTLA (40 octets);
- entrées CRL (à taille variable). La liste CRL sert à la révocation des certificats des dispositifs dont la sécurité a été compromise. Son format est décrit dans le sous-paragraphe suivant;
- la signature DTLA EC-DSA de ces composantes qui utilisent L^{-1} (320 bits).

---

[8] Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.

La structure des messages SRM de première génération est indiquée dans la Figure III.17. Les champs définis dans les 4 premiers octets du message SRM comprennent l'en-tête SRM.

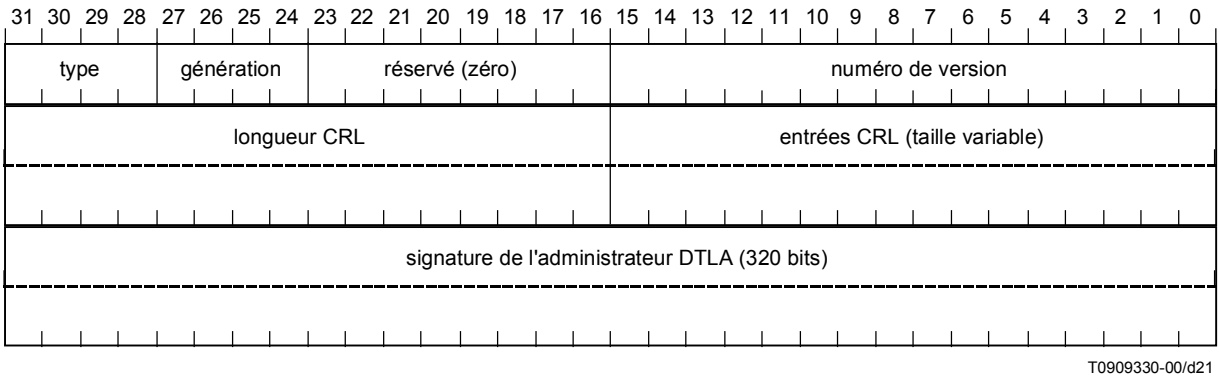


Figure III.17/J.95 – Structure du message de première génération d'aptitude du système au renouvellement

III.7.1.1.1 Liste de révocation des certificats (CRL)

La **liste de révocation des certificats (CRL)** identifie les dispositifs qui ne sont plus conformes. Elle se compose du champ de longueur CRL qui spécifie la longueur de la liste CRL en octets. Ce champ est suivi d'une séquence de blocs du type entrée (1 octet) suivis à leur tour du nombre d'entrées CRL spécifié par le bloc de type entrée. Deux types de blocs d'entrée sont pris en charge. Un type de bloc permet la révocation des dispositifs individuels tandis que le second bloc permet la révocation de blocs de dispositifs dont le nombre peut atteindre 65 535.

III.7.1.1.2 Signature DTLA EC-DSA

Le champ de signature DTLA EC-DSA est une signature de 320 bits calculée sur l'ensemble des champs précédents du message SRM à l'aide de la clé privée DTLA EC-DSA L^{-1}. Ce champ est utilisé pour vérifier l'intégrité du message SRM à l'aide de la clé publique DTLA EC-DSA L^{1}.

III.7.1.2 Echelonnabilité du message SRM

Afin de garantir l'échelonnabilité de cette solution de renouvellement, le format du message SRM est extensible (voir Figure III.18). Les extensions de génération suivante (listes CRL et éventuellement d'autres mécanismes) à un format de message SRM de génération actuelle doivent être annexées au message SRM de génération actuelle afin de garantir une compatibilité rétroactive avec les dispositifs qui ne prennent en charge que les messages SRM de génération précédente. Les dispositifs sont tenus uniquement de prendre en charge la génération du message SRM requis par l'administrateur DTLA au moment de leur fabrication. Les conditions dans lesquelles l'administrateur DTLA autorisera des messages SRM de nouvelle génération sont spécifiées dans le contrat de licence de l'administrateur DTLA.

III.7.2 Mise à jour des messages SRM

Les messages d'aptitude du système au renouvellement peuvent être mis à jour à partir:

- d'autres dispositifs conformes (raccordés par l'intermédiaire du support de transmission numérique) qui disposent d'une liste plus récente;
- des supports de contenu préenregistré;
- des flux de contenu par l'intermédiaire de dispositifs conformes temps réel qui peuvent communiquer de manière externe (par exemple par l'intermédiaire du réseau Internet, d'une ligne téléphonique, d'un système câblé, d'un satellite de diffusion directe, etc.).

La procédure générale de mise à jour des messages SRM est la suivante:

1) Examen du numéro de version du nouveau message SRM.
2) Vérifier que le numéro de version du message SRM est supérieur à celui qui est stocké dans la mémoire non volatile.
3) Vérifier l'intégrité avec la clé publique DTLA (L^{1}).
4) Si le message SRM est valide et nouveau, mettre alors en mémoire la plus grande partie possible de la version la plus récente du message dans la mémoire non volatile du dispositif.

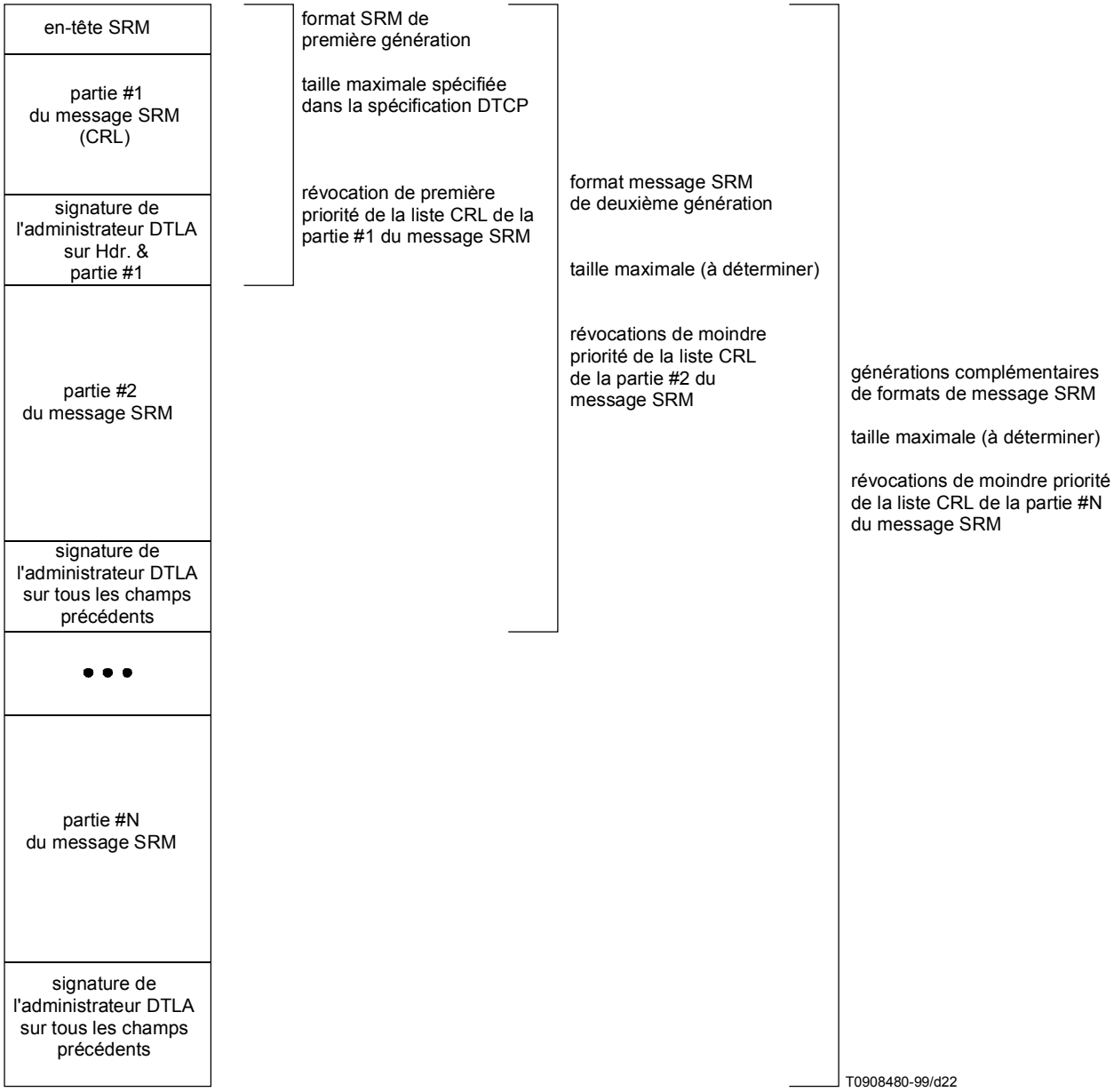


Figure III.18/J.95 – Extension du message SRM

III.8 Extensions de l'ensemble de commandes d'interface numérique AV/C

III.8.1 Introduction

Les dispositifs audio/vidéo qui échangent des contenus par l'intermédiaire du bus série IEEE 1394 sont typiquement conformes à la CEI 61883 et à l'ensemble de commandes d'interface numérique AV/C. Il est important de revoir les Sections A.5, A.6, et A.7 de la *Spécification pour l'ensemble de commandes d'interface numérique AV/C* (spécification générale) en ce qui concerne les règles générales relatives aux commandes et aux réponses AV/C.

Ces spécifications définissent l'utilisation de paquets asynchrones IEEE 1394 pour le contrôle et la gestion des dispositifs ainsi que l'utilisation de paquets isochrones IEEE 1394 pour l'échange de contenus. Ce chapitre décrit les extensions de l'ensemble de commandes AV/C qui prennent en charge les protocoles d'authentification DTCP et d'échange de clés. Les extensions du format de paquet isochrone IEEE 1394 sont décrites à la Section A.6.

III.8.2 Commande SÉCURITÉ

Une nouvelle commande de sécurité est définie pour la commande AV/C. Cette commande est destinée à protéger les contenus y compris le système DTCP. Le format général de la commande SÉCURITÉ est le suivant:

	bit de plus fort poids		bit de plus faible poids
Code d'opération	SÉCURITÉ ($0F_{16}$)		
Opérande[0]	catégorie	(bit de plus fort poids)	
Opérande[1]	champ dépendant de la catégorie		
:			
Opérande[X]			(bit de plus faible poids)

La valeur du code d'opération de la commande de sécurité est $0F_{16}$ (commande commune d'unité et de sous-unité).

Le champ **catégorie** de la commande SÉCURITÉ est défini comme suit:

Valeur	Catégorie
0	Prise en charge de DTCP AKE. Cette commande est appelée commande AKE
$1\text{-}D_{16}$	Réservée pour une extension future
E_{16}	Vendor_dependent (en fonction du fournisseur)
F_{16}	Extension du champ de catégorie

La valeur 0 du champ catégorie spécifie que cette commande est utilisée pour prendre en charge les protocoles d'authentification DTCP et d'échange de clés.

La commande AKE est définie pour le *ctype* de CONTROL ("commande contrôle") et de STATUS ("commande état"). Les dispositifs qui prennent en charge la commande AKE doivent accepter les deux *ctype*s.

La valeur E_{16} du champ catégorie spécifie que cette commande est utilisée par les fournisseurs pour définir leurs propres commandes de sécurité pour une utilisation sous licence.

III.8.3 Commande AKE

Cette commande est destinée au dispositif récepteur lui-même. Par conséquent, le champ subunit_type de 5 bits d'une trame de commande/réponse AV/C est égal à 11111_2 et le champ subunit_ID de 3 bits de la trame est égal à 111_2.

III.8.3.1 Commande de contrôle AKE

La commande de contrôle AKE est utilisée pour échanger les messages nécessaires à l'implémentation des protocoles d'authentification et d'échange de clés. Le format de cette commande est présenté ci-dessous:

Les deux trames de commande et de réponse AKE ont le même code d'opération et les mêmes 9 premiers opérandes (opérandes[0-8]). La valeur de chaque champ de la trame de réponse est identique à celle de la trame de commande à l'exception des champs status (état) et data (données). Si l'un des champs définis dans les 9 premiers opérandes contient des valeurs réservées, il convient que la réponse NOT_IMPLEMENTED (non appliquée) soit renvoyée.

Si une trame de commande donnée inclut un champ data, la trame de réponse correspondante n'a pas de champ data (données). Les commandes de contrôle AKE permettent de transmettre les informations utilisées pour la procédure d'authentification exécutée entre le dispositif source et le dispositif récepteur. Ces informations, qui sont transmises au champ data (données), sont appelées *informations AKE*. Il convient d'ignorer les valeurs non nulles définies dans les champs Reserved_zero (réservé zéro) des informations AKE

Le champ AKE_ID ("identification AKE") spécifie le format du champ AKE_ID dependant (champ dépendant d'identification AKE). Actuellement, seul le codage AKE_ID = 0 est défini. Le champ dépendant de AKE_ID propre à ce codage est décrit au III.8.3.3. Les autres valeurs, de 1_{16} à F_{16}, sont réservées pour une définition future.

	bit de plus fort poids		bit de plus faible poids
Code d'opération	$0F_{16}$		
Opérande[0]	catégorie = 0000_2 (AKE)	AKE_ID	
Opérande[1]	(bit de plus fort poids)		
Opérande[2]	champ dépendant de AKE_ID		
Opérande[3]			
Opérande[4]			(bit de plus faible poids)
Opérande[5]	AKE_label ("étiquette AKE")		
Opérande[6]	nombre (facultatif)	état	
Opérande[7]	blocks_remaining ("blocs restants")		(bit de plus fort poids)
Opérande[8]	data_length ("longueur des données") (bit de plus faible poids)		
Opérande[9]	données		
:			
Opérande[8 + data_length] ("longueur des données")			

Le champ AKE_label est une étiquette unique utilisée pour identifier une séquence de commandes AKE associées à un processus d'authentification donné. L'initiateur d'une procédure d'authentification peut sélectionner une valeur arbitraire pour le champ AKE_label. Il convient que la valeur sélectionnée soit différente des autres valeurs AKE_label actuellement utilisées par le dispositif qui déclenche l'authentification. La même valeur AKE_label sera utilisée pour toutes les commandes de contrôle associées à une procédure d'authentification spécifique entre un dispositif source et un dispositif récepteur. Il convient de vérifier l'identification du champ AKE_label et du nœud source de chaque commande de contrôle afin de s'assurer qu'elle provient du contrôleur approprié.

Le champ nombre facultatif[9] number spécifie le nombre d'étapes d'une commande de contrôle spécifique afin d'identifier sa position dans la séquence de commandes de contrôle constituant une procédure d'authentification. L'initiateur d'une procédure d'authentification fixe la valeur de ce champ à 1 pour la commande de contrôle AKE initiale. On augmente cette valeur pour chaque commande ultérieure qui fait partie intégrante du même processus d'authentification. Lorsqu'une commande AKE doit être fragmentée pour une transmission (voir la description du champ blocks_remaining ci-dessous), chaque fragment utilisera la même valeur pour le champ propre au nombre. Les dispositifs qui ne prennent pas en charge ce champ doivent fixer sa valeur à 0000_2.

Le champ status est utilisé pour signifier au dispositif qui émet la commande la raison pour laquelle ladite commande entraîne une réponse REJECTED (refusée). Le dispositif qui émet la commande fixe la valeur de ce champ à 1111_2. Si le dispositif qui apporte une réponse rejette la commande, il écrase le champ status (état) avec un code indiquant la raison du refus. Le codage du champ status est le suivant:

Valeur	Etat	Code de réponse
0000_2	Aucune erreur	Acceptée
0001_2	La prise en charge pour des procédures ne nécessitant plus d'authentification est actuellement disponible	Refusée
0010_2	Aucun signal isochrone	Refusée
0011_2	Aucune connexion point à point	Refusée
0111_2	Toute autre erreur	Refusée
1111_2	Aucune information	Réservée pour utilisation temporaire INTERIM[a)]

a) Réservé pour une utilisation future. Il convient de ne pas utiliser actuellement de réponse avec le code de réponse "temporaire".

9 Les caractéristiques de la présente spécification étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.

Les codes d'état suivants sont uniquement destinés aux essais. Les produits ne doivent pas renvoyer ces codes, mais doivent en revanche renvoyer la valeur 0111_2 (toute autre erreur) si ces conditions sont réunies.

Valeur	Etat	Code de réponse
1000_2	Ordre de commande incorrect (uniquement pour essai)	Refusée
1001_2	Echec de l'authentification (uniquement pour essai)	Refusée
1010_2	Erreur de syntaxe du champ de données (uniquement pour essai)	Refusée

Le champ blocks_remaining est utilisé lorsque la commande dépasse la taille maximale de la trame de commande que le dispositif récepteur peut recevoir (le dispositif produisant une commande peut déterminer la taille du champ de données que le dispositif récepteur peut prendre en charge en utilisant la commande d'état AKE). Lorsque cela se produit, le champ data est fragmenté en N blocs transmis de manière séquentielle, chacun d'entre eux figurant dans l'une de N commandes séparées, chaque commande étant suffisamment petite pour pouvoir convenir à la mémoire tampon de la commande du dispositif récepteur. La mémoire tampon doit au minimum être capable de contenir une commande ayant au moins un champ de données de 32 octets[10]. La taille du champ de données dans les premiers fragments N – 1 doit être la même et être supérieure ou égale à 32 octets, selon un multiple de 16 octets.

Chacune des N trames de commande est identique aux autres trames de même commande à l'exception des valeurs des champs blocks_remaining, data_length, et data. Pour la première commande, le champ blocks_remaining est fixé à la valeur N – 1. Pour chaque commande successive, la valeur du champ blocks_remaining est diminuée d'une unité jusqu'à ce qu'elle atteigne zéro, valeur qui indique le dernier fragment de commande. Si la valeur du champ blocks_remaining n'est pas correcte (par exemple, ordre incorrect), il convient que le récepteur adresse une réponse REJECTED (refusée) avec un champ status de valeur 0111_2 (toute autre erreur).

Dans la mesure où la taille des trames de commande et de réponse ne peut dépasser la limite de 512 octets imposée par le transport FCP sous-jacent, le cas où une commande doit être fragmentée ne peut se produire que lorsque la capacité de la mémoire tampon de la trame de commande du dispositif récepteur est inférieure à 512 octets. Généralement, la taille de la commande est comprise dans la capacité de la mémoire tampon de la trame de commande du dispositif récepteur et la commande est transmise sans fragmentation et avec une valeur du champ blocks_remaining égale à zéro.

Lorsqu'un champ AKE_Info est transmis à l'aide de plusieurs commandes de contrôle, le contrôleur ne doit transmettre chaque commande qu'après réception d'une réponse ACCEPTED (acceptée) pour la commande précédente.

Le champ data_length spécifie la longueur du champ data en octets. Les réponses à une commande utiliseront la même valeur pour leurs champs data_length respectifs même lorsque la réponse ne comporte aucune donnée. Si la réponse comporte un certain nombre de données lorsque le code de réponse est ACCEPTED (accepté), la commande correspondante ne comportera aucune donnée mais la valeur du champ data_length doit être la même que la valeur de la réponse.

Le champ data contient les données à transférer. Le contenu du champ data dépend du champ AKE_ID et du champ dépendant de celui-ci. Les réponses dont le code de réponse est REJECTED (refusé) n'ont pas de champ data.

[10] Si des générations futures de messages d'aptitude du système au renouvellement (SRMM > 0) ont une taille maximale supérieure à 4096 octets, les nouveaux dispositifs devront prendre en charge l'augmentation de la taille minimale.

III.8.3.2 Commande d'état AKE

Le format de la commande d'état AKE est le suivant:

	bit de plus fort poids							bit de plus faible poids
Code d'opération	$0F_{16}$							
Opérande[0]	catégorie = 0000_2 (AKE)				AKE_ID			
Opérande[1]	(bit de plus fort poids)							
Opérande[2]	champ dépendant de AKE_ID							
Opérande[3]								
Opérande[4]								(bit de plus faible poids)
Opérande[5]	FF_{16}							
Opérande[6]	F_{16}				état			
Opérande[7]	$7F_{16}$							(bit de plus fort poids)
Opérande[8]	champ data_length (bit de plus faible poids)							

Les deux trames de commande et de réponse ont la même structure. Les valeurs de chaque champ des trames de commande et de réponse sont identiques à l'exception des valeurs du champ dépendant de AKE_ID, status, et data_length.

Le champ AKE_ID spécifie le format du champ AKE_ID dependant. Le champ AKE_ID dependant pour ce codage est décrit au III.8.3.3. Actuellement, seul le codage de AKE_ID = 0 est défini. Les autres valeurs, de 1_{16} à F_{16}, sont réservées pour une définition future.

Le champ status ("état") est utilisé par un dispositif pour consulter l'état d'un autre dispositif. Lorsque la commande est exécutée, la valeur de ce champ est fixée à 1111_2. Dans sa réponse, le dispositif récepteur écrase ce champ avec une valeur indiquant sa situation actuelle.

Valeur	Etat	Code de réponse
0000_2	Aucune erreur	Stable
0001_2	La prise en charge pour des procédures ne nécessitant plus d'authentification est actuellement disponible	Stable
0010_2	Aucun signal isochrone	Stable
0011_2	Aucune connexion point à point	Stable
0111_2	Toute autre erreur	Stable
1111_2	Aucune information[a)]	Refusée

a) Il est recommandé que les réalisateurs n'utilisent pas la réponse "Absence d'information".

Les codes d'état suivants sont destinés uniquement aux essais. Les produits ne doivent pas renvoyer ces codes, mais doivent en revanche renvoyer la valeur 0111_2 (toute autre erreur) si ces conditions sont réunies.

Valeur	Etat	Code de réponse
1001_2	Echec de l'authentification (uniquement pour essai)	Stable

Le champ data_length spécifie la capacité maximale du champ data du dispositif récepteur en octets. Lorsque la commande "status" ("état") est exécutée, la valeur de ce champ est fixée à $1FF_{16}$. Dans sa réponse, le dispositif récepteur écrase ce champ avec une valeur indiquant sa situation actuelle. La valeur minimale pouvant être prise en charge est 020_{16} (32 octets).

III.8.3.3 Champ dépendant de AKE_ID (AKE_ID = 0)

Lorsque AKE_ID = 0, le format de son champ dépendant est le suivant:

	bit de plus fort poids		bit de plus faible poids
Opérande[1]	champ subfunction		
Opérande[2]	champ AKE_procedure		
Opérande[3]	champ exchange_key		
Opérande[4]	champ subfunction_dependent		

Le champ subfunction ("sous-fonction") spécifie l'exécution des commandes de contrôle. Le bit de plus fort poids du champ subfunction indique si la commande de contrôle contient ou non des données.

- Si la valeur du *bit de plus fort poids* est 0, la commande concernée contient certaines données et le champ data_length indique sa longueur.
- Si la valeur du *bit de plus fort poids* est 1, la commande concernée ne contient pas de données et le champ data_length indique la longueur du champ de données dans la trame de réponse dont le code de réponse est ACCEPTED (accepté).

Les sous-fonctions sont entièrement décrites dans la spécification DTCP disponible sous licence attribuée par l'administrateur DTLA. Le tableau ci-dessous résume les six sous-fonctions actuellement définies:

Valeur	Sous-fonction	Commentaires
01_{16}	CHALLENGE (interrogation)	Envoi d'une valeur aléatoire. Cette sous-fonction, lorsqu'elle provient d'un dispositif récepteur, déclenche la procédure AKE.
02_{16}	RESPONSE (réponse)	Renvoyer les données calculées avec la valeur aléatoire reçue.
03_{16}	EXCHANGE_KEY	Envoi d'une clé d'échange cryptée (K_x) au dispositif authentifié récepteur du contenu.
04_{16}	SRM	Envoi d'un message SRM à un dispositif ayant un message périmé ou de moindre importance.
$C0_{16}$	AKE_CANCEL	Signifier au dispositif que la procédure actuelle d'authentification ne peut se poursuivre.
80_{16}	CONTENT_KEY_REQ	Demande des données requises pour la création de la clé de contenu (K_c).

Pour les commandes d'état, la valeur du champ subfunction doit être fixée à FF_{16}.

Chaque bit du champ AKE_procedure correspond à un type de procédure d'authentification, comme décrit dans le tableau ci-dessous.

Bit	AKE_procedure
0 (bit de plus faible poids)	Procédure d'authentification restreinte (rest_auth)
1	Procédure d'authentification restreinte améliorée (en_rest_auth) (Note 1)
2	Procédure d'authentification intégrale (full_auth)
3	Procédure d'authentification intégrale étendue (Note 2) (ex_full_auth, facultative) (Note 3)
4-7 (bit de plus fort poids)	Réservée pour une extension future et sa valeur doit être égale à zéro
NOTE 1 – Les dispositifs source qui prennent en charge la procédure d'authentification intégrale doivent vérifier le certificat du dispositif récepteur et examiner le message SRM même dans le cadre de la procédure d'authentification restreinte. Le présent sous-paragraphe fait référence à cette procédure d'authentification comme procédure d'authentification restreinte améliorée. NOTE 2 – Les dispositifs qui prennent en charge les certificats de dispositifs étendus utilisent la procédure d'authentification intégrale étendue décrite dans le présent sous-paragraphe. NOTE 3 – Les caractéristiques de cette spécification qui sont étiquetées comme "facultatives" décrivent les capacités dont l'emploi n'a pas encore été établi par l'administrateur DTLA.	

Pour la commande de contrôle, l'initiateur de la procédure d'authentification définit un bit dans ce champ afin de préciser le type d'authentification exécuté. La valeur du champ reste alors constante pendant toute la partie restante de cette procédure d'authentification.

Pour la commande d'état, l'initiateur doit fixer la valeur initiale de ce champ à FF_{16}. Le dispositif récepteur écrasera le champ, en effaçant les bits qui indiquent les procédures d'authentification non prises en charge par le récepteur en sa qualité de dispositif source. Par exemple, si un dispositif source prend en charge à la fois les procédures d'authentification intégrale et d'authentification restreinte améliorée, les valeurs du champ AKE_procedure doivent alors être fixées à 06_{16}.

Il convient que les dispositifs récepteurs déterminent, à l'aide de la commande d'état, les procédures d'authentification qui sont prises en charge par un dispositif source, avant de procéder au protocole d'authentification. Le tableau ci-dessous montre comment sélectionner la procédure d'authentification appropriée:

Procédure d'authentification prise en charge par le dispositif récepteur / Procédure d'authentification prise en charge par le dispositif source	Rest_auth et En_rest_auth	Rest_auth et Full_auth	Rest_auth, Full_auth, et Ex_full_auth
Rest_auth	Authentification restreinte	Authentification restreinte	Authentification restreinte
En_rest_auth et Full_auth	Authentification restreinte améliorée	Authentification intégrale	Authentification intégrale
En_rest_auth, Full_auth, et Ex_full_auth	Authentification restreinte améliorée	Authentification intégrale	Authentification intégrale étendue

Chaque bit du champ exchange_key correspond à une ou plusieurs clés comme décrit dans le tableau ci-dessous:

Bit	exchange_key
0 (bit de plus faible poids)	Clé(s) d'échange pour un contenu "pas de copie" [nécessite une authentification intégrale ou intégrale étendue (Note)]
1	Clé d'échange pour un contenu destiné à une "copie de première génération" (toute authentification acceptable)
2	Clé d'échange pour le contenu "plus de copies" (toute authentification acceptable)
3-7 (bit de plus fort poids)	Réservée pour une extension future et sa valeur doit être égale à zéro
NOTE – Si l'on fait appel à la procédure d'authentification intégrale étendue, toutes les clés d'échange destinées aux cryptogrammes facultatifs de prise en charge mutuelle, seront transmises à l'issue de la procédure d'authentification intégrale.	

Pour la commande de contrôle, le dispositif récepteur fixe la valeur de ce champ au début de la procédure d'authentification afin d'indiquer la ou les clés d'échange qui seront fournies par le dispositif source après exécution satisfaisante de la procédure. Pour la procédure d'authentification intégrale, n'importe quel bit peut être déterminé. Pour la procédure d'authentification restreinte, un seul bit doit être fixé pour les contenus "copie de première génération" ou pour les contenus "plus de copies". Ce champ reste constant pour le reste de la procédure d'authentification sauf lorsque la sous-fonction EXCHANGE_KEY est exécutée.

Pour la commande d'état, l'initiateur doit fixer la valeur FF_{16} dans ce champ et le récepteur doit effacer chaque bit du champ qui correspond à une clé d'échange que le récepteur ne peut fournir.

Par exemple, si le récepteur peut fournir trois clés qui correspondent aux valeurs bit0 à bit2 dans le tableau susmentionné, la valeur du champ exchange_key sera fixée à 07_{16}.

Il convient que le dispositif récepteur détermine la ou les clés dont il aura besoin en obtenant ces informations antérieurement à la procédure d'authentification.

La définition du champ subfunction_dependent varie. La spécification DTCP disponible sous licence attribuée par l'administrateur DTLA décrit les définitions des commandes de contrôle. Pour les commandes d'état, la valeur de ce champ est fixée à FF_{16} pour les trames de commande et de réponse.

III.8.4 Comportement de réinitialisation du bus

Si le dispositif source continue à transmettre un contenu sur un canal isochrone suite à la réinitialisation du bus, les clés d'échange et de contenu utilisées doivent être les mêmes que celles qui ont été utilisées avant la réinitialisation.

Si la réinitialisation du bus se produit au cours de la procédure d'authentification, les dispositifs source et récepteur doivent immédiatement arrêter la procédure d'authentification. Suite à la réinitialisation, le champ d'identification du nœud source (SID, *source node ID*) de l'en-tête du paquet isochrone commun peut être modifié, obligeant ainsi le dispositif récepteur à recommencer la procédure d'authentification en utilisant la nouvelle identification SID.

III.8.5 Action exécutée lorsqu'un dispositif non autorisé est détecté lors de l'authentification

Après renvoi de la réponse ACCEPTED (acceptée) à l'initiateur d'une commande, le récepteur examine les informations AKE. Si le récepteur détermine que l'initiateur est un dispositif non autorisé, il doit alors arrêter immédiatement la procédure AKE sans aucune notification.

III.8.6 Authentification des flux de commande AV/C

Les Figures III.19 et III.20 illustrent les flux de commande AV/C utilisés pour une authentification intégrale, restreinte améliorée/restreinte.

III.8.6.1 Notation des figures

Les lignes pleines indiquent les paires commande/réponse exécutées dans tous les cas.

Les lignes pointillées indiquent les paires commande/réponse exécutées sur la base de conditions définies.

III.8.6.2 Flux de la commande pour authentification intégrale

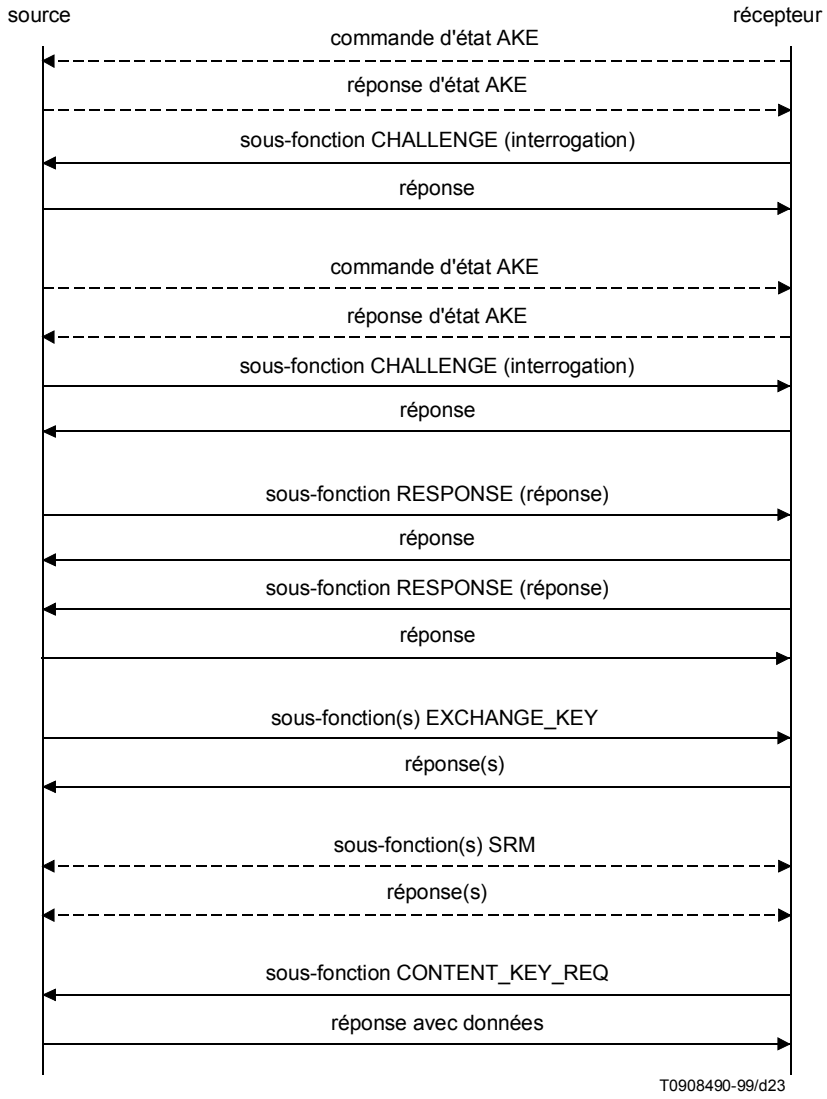


Figure III.19/J.95 – Flux de commande pour authentification intégrale

III.8.6.3 Flux de commande pour authentification restreinte améliorée/restreinte

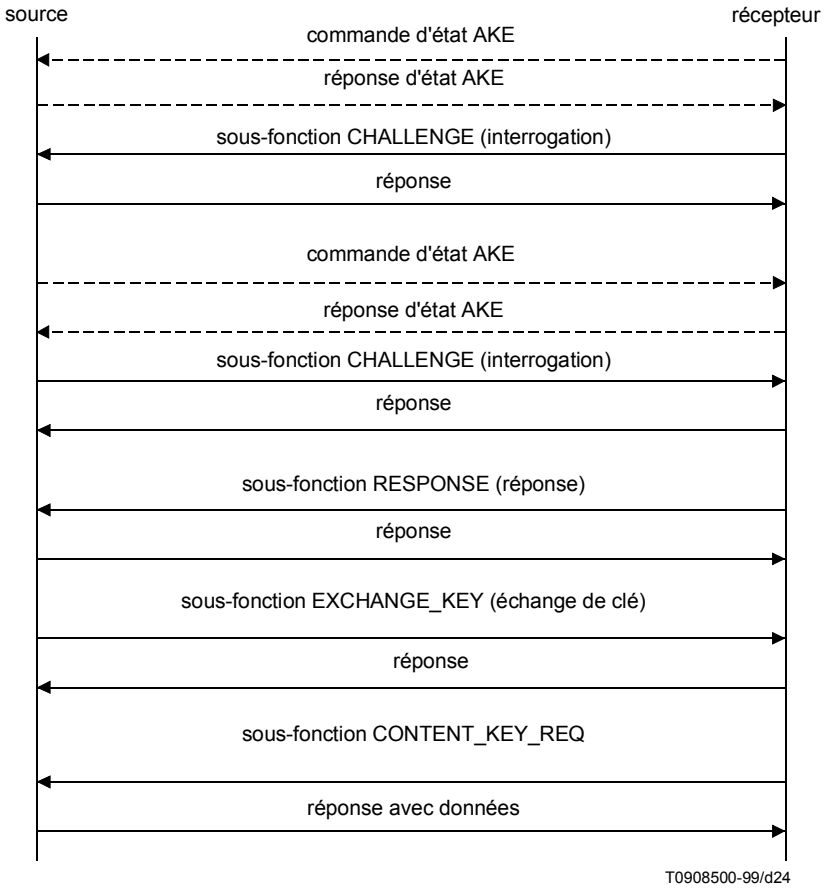


Figure III.20/J.95 – Flux de commande pour authentification restreinte améliorée/restreinte

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 de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication

Genève, 2001