(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 834 406**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 17139**

(51) Int Cl[7] : **H 04 L 9/32**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.12.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.07.03 Bulletin 03/27.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *THOMSON LICENSING S.A. Société anonyme* — FR.

(72) **Inventeur(s) :** DIEHL ERIC et DURAND ALAIN.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** THOMSON MULTIMEDIA.

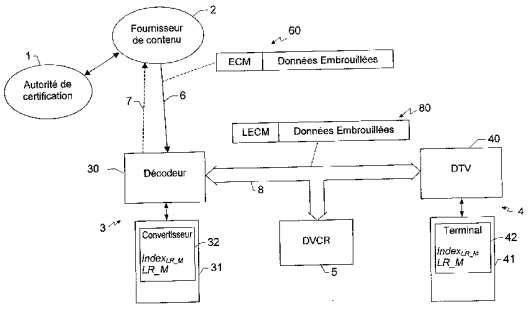
(54) PROCEDE DE MISE A JOUR D'UNE LISTE DE REVOCATION DE CLES, D'APPAREILS OU DE MODULES NON-CONFORMES DANS UN SYSTEME DE DIFFUSION SECURISE DE CONTENU.

(57) Le procédé consiste à recevoir dans un dispositif de réception (3) un contenu d'un fournisseur de contenu (2) auquel est attaché un identifiant unique de liste de révocation la plus récente, la liste de révocation contenant des identifiants de clés, d'appareils ou de modules considérés comme non conformes par un tiers de confiance (1).

L'identifiant de liste de révocation reçu ($Index_{LR\_C}$) est comparé avec un identifiant de liste de révocation mémorisé ($Index_{LR\_M}$) dans le dispositif de réception et, en cas de différence entre les identifiants:

- on télécharge la liste de révocation la plus récente dans ledit dispositif de réception; ou
- on attend la réception de la liste de révocation la plus récente avec un prochain contenu.

L'invention concerne aussi un procédé de présentation d'un contenu reçu selon le procédé ci-dessus.



FR 2 834 406 - A1

La présente invention se rapporte d'une manière générale au domaine de la protection contre la copie des contenus numériques. Elle concerne plus particulièrement un procédé de mise à jour d'une liste de révocation de clés, d'appareils ou de modules non-conformes dans un système de diffusion sécurisé de contenu.

La transmission de données numériques représentatives de contenus à travers un réseau de communication pose des problèmes de protection des données échangées et de gestion des autorisations ou interdictions de copie des données.

Pour remédier à ces problèmes, les fabricants de matériel multimedia ont proposé des solutions permettant de transmettre des contenus sous forme numérique tout en empêchant la copie illicite de ces contenus. Ces solutions impliquent généralement l'utilisation de systèmes cryptographiques à clés publiques, dans lesquels des paires de clés privées/publiques sont générées par un tiers de confiance (par exemple une autorité de certification), ainsi que l'utilisation d'appareils ou de modules dits conformes.

Malheureusement, il arrive qu'une paire de clés privée/publique soit piratée, c'est à dire qu'un « pirate » réussisse à se procurer la clé privée de la paire de clés, ou bien qu'un appareil ou un module conforme, contenant par exemple un secret, soit piraté, c'est à dire que le « pirate » se procure le secret.

C'est pourquoi, il est connu dans un système de diffusion sécurisée de contenu, de gérer une liste de révocation contenant des identifiants de clés, d'appareils ou de modules qui ne sont plus considérés comme conformes par le tiers de confiance car ce dernier a eu connaissance du fait qu'ils ont été piratés. Cette liste de révocation doit être communiquée à tous les acteurs du système de manière à ce que les clés, appareils ou modules qui ne sont plus conformes ne puissent plus être utilisés. Par exemple, les appareils conformes du système refuseront de communiquer avec un appareil non conforme ou avec un appareil transmettant une clé non-conforme.

Pour que ceci soit efficace, il est nécessaire que les appareils conformes aient toujours la dernière liste de révocation à jour.

Par ailleurs, il est courant aujourd'hui d'utiliser des appareils d'électronique grand public tels une télévision, un lecteur DVD (de l'anglais « Digital Versatile Disc » signifiant littéralement « disque polyvalent numérique »), un dispositif d'enregistrement numérique (notamment magnétoscope, enregistreur DVD ou disque dur) ou un ordinateur dans un réseau numérique domestique.

Dans ce cas, pour s'assurer que les divers appareils possèdent bien une liste de révocation à jour, il est connu de joindre systématiquement la dernière liste de révocation à jour à tout contenu qui entre dans le réseau domestique, le contenu étant envoyé par un fournisseur de contenu qui se procure la dernière liste de révocation à jour auprès du tiers de confiance.

Une autre solution connue consiste à ajouter une date de validité à toute liste de révocation qui est transmise au réseau. Après cette date, aucun contenu nouveau ne peut plus être reçu sur le réseau domestique tant qu'une nouvelle liste de révocation à jour n'a pas été reçue. Il est donc nécessaire qu'au moins un appareil du réseau domestique demande une mise à jour de la liste de révocation par exemple au fournisseur de contenu.

Ces techniques connues présentent cependant un certain nombre d'inconvénients.

Le fait d'envoyer systématiquement la dernière liste de révocation à jour avec tout contenu transmis augmentent le coût d'envoi du contenu puisqu'une partie de la bande passante est allouée à la transmission de la liste de révocation. De plus, un pirate pourrait toujours remplacer la liste de révocation transmise avec le contenu par une liste plus ancienne ne contenant pas les dernières mises à jour.

D'autre part, le fait d'ajouter une date de validité à la liste de révocation implique une gestion plus complexe au niveau des appareils du réseau domestique. Pour atteindre un bon niveau de sécurité, les listes de révocations doivent être mises à jour fréquemment. De plus, si une nouvelle liste de révocation est envoyée avant la fin de la période de validité de la précédente, elle pourra éventuellement être effacée par un pirate sans que les appareils du réseau domestique ne s'en aperçoivent car la date de validité de la liste de révocation mémorisée dans le réseau ne sera pas dépassée.

La présente invention vise à résoudre les problèmes précités.

Elle a pour objet un procédé de mise à jour d'une liste de révocation contenant des identifiants de clés, d'appareils ou de modules considérés comme non conformes par un tiers de confiance dans un système de diffusion sécurisé de contenu consistant à recevoir dans un dispositif de réception un contenu d'un fournisseur de contenu, caractérisé en ce qu'un identifiant unique est alloué à chaque mise à jour de la liste de révocation par le tiers de confiance, l'identifiant de la liste de révocation la plus récente étant attaché au contenu reçu dans le dispositif de réception, et en ce que le procédé comporte en outre une étape consistant à comparer l'identifiant de liste de révocation

reçu avec un identifiant de liste de révocation mémorisé dans ledit dispositif de réception et, en cas de différence entre lesdits identifiants :

- à télécharger la liste de révocation la plus récente dans ledit dispositif de réception ; ou
- à attendre la réception de la liste de révocation la plus récente avec un prochain contenu.

Ainsi, on évite de transmettre la liste de révocation entière à chaque envoi d'un nouveau contenu et une nouvelle liste de révocation n'est envoyée que lorsque cela est nécessaire, suite à une mise à jour de ladite liste.

L'invention concerne aussi un procédé de réception d'un contenu par un dispositif de réception dans un système de diffusion sécurisé de contenu dans lequel une liste de révocation, établie par un tiers de confiance, contient des identifiants de clés, d'appareils ou de modules considérés comme non conformes par ledit tiers de confiance, caractérisé en ce qu'un identifiant unique est alloué à chaque mise à jour de la liste de révocation, l'identifiant de la liste de révocation la plus récente étant attaché au contenu reçu par le dispositif de réception. Le procédé comporte en outre une étape consistant à comparer l'identifiant de liste de révocation reçu avec un identifiant de liste de révocation mémorisé dans le dispositif de réception, et en cas de différence entre lesdits identifiants : à télécharger la liste de révocation la plus récente dans le dispositif de réception; ou à attendre la réception de la liste de révocation la plus récente avec un prochain contenu.

Selon une caractéristique particulière de l'invention, l'identifiant unique de liste de révocation est un index de mise à jour de ladite liste de révocation.

Selon une autre caractéristique de l'invention, l'identifiant de liste de révocation la plus récente reçu avec le contenu est inclus dans une partie protégée par chiffrement ou par authentification dudit contenu. L'identifiant de liste de révocation ne peut donc pas être supprimé ou modifié facilement par un pirate.

Selon un mode de réalisation particulier de l'invention, la liste de révocation peut contenir un ou des élément(s) appartenant à l'ensemble comprenant :

- au moins un numéro de série de clé publique générée par le tiers de confiance et considérée comme non conforme par le tiers de confiance ;
- au moins un numéro de série d'un appareil considéré comme non conforme par le tiers de confiance ;

- au moins un numéro de série d'un module considéré comme non conforme par le tiers de confiance ;

- au moins un identifiant de clé secrète de réseau local servant à protéger des contenus contre la copie illicite ;

- au moins une clé secrète de réseau local servant à protéger des contenus contre la copie illicite ;

- au moins le résultat d'une fonction de calcul, notamment une fonction de hachage, appliquée à une clé secrète de réseau local servant à protéger des contenus contre la copie illicite.

Selon une autre caractéristique avantageuse de l'invention, on mémorise en outre, pour chaque élément de la liste de révocation son index de révocation correspondant à l'index de mise à jour de ladite liste au moment de l'insertion de l'élément dans la liste de révocation.

L'invention a également pour objet un procédé de présentation d'un contenu, reçu conformément au procédé tel que décrit ci-dessus, qui comprend les étapes consistant pour un dispositif de présentation de contenu à : vérifier si la liste de révocation la plus récente à la disposition du dispositif de réception ne contient pas d'élément relatif à au moins une clé, un module ou un appareil utilisé par ledit dispositif de réception ; et si la liste de révocation ne contient aucun desdits éléments, continuer le procédé pour présenter le contenu à un utilisateur, sinon, arrêter le procédé.

En variante du procédé ci-dessus, si la liste de révocation contient au moins un desdits éléments (c'est à dire un élément relatif à au moins une clé, un module ou un appareil utilisé par le dispositif de réception), le procédé se poursuit par les étapes consistant à : comparer l'index de mise à jour de la liste de révocation attaché au contenu avec l'index de révocation dudit élément ; et si l'index de mise à jour de la liste de révocation attaché au contenu est inférieur à l'index de révocation dudit élément, continuer le procédé pour présenter ledit contenu à un utilisateur, sinon, arrêter le procédé.

L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés sur lesquels :

- la figure 1 représente schématiquement un système de diffusion sécurisé de contenu dans un réseau numérique domestique dans lequel est mise en œuvre l'invention ;

- les figures 2 et 3 représentent schématiquement des procédés mis en œuvre, selon l'invention, dans des dispositifs de la figure 1.

Sur la figure 1, nous avons représenté un système de diffusion sécurisé de contenu comprenant une autorité de certification 1, qui constitue le tiers de confiance dans le procédé de l'invention, un fournisseur de contenu 2 et un réseau numérique domestique comportant un dispositif de réception de contenu 3, un dispositif de présentation de contenu 4 et un dispositif d'enregistrement 5, reliés entre eux par un bus numérique 8, qui est par exemple un bus selon la norme IEEE 1394.

L'autorité de certification 1 génère notamment les paires de clés privées/publiques utilisées par les différents dispositifs du système, les clés publiques étant contenues dans des certificats signés par l'autorité de certification comme cela est connu de l'homme du métier.

L'autorité de certification 1 est reliée au fournisseur de contenu 2, qui est par exemple un diffuseur de programmes télévisés payants. Un seul fournisseur de contenu 2 est représenté sur la figure 1 mais naturellement, l'invention s'applique aussi au cas où plusieurs fournisseurs de contenus différents sont reliés à l'autorité de certification pour délivrer des contenus à des utilisateurs. Un autre fournisseur de contenu peut notamment être un distributeur de programmes musicaux diffusés via Internet.

Selon l'invention, l'autorité de certification 1 tient à jour une liste de révocation qui contient des identifiants de clés, d'appareils de ou de modules qui ne sont plus considérés comme sûrs et auxquels l'autorité de certification ne fait plus confiance, notamment parce qu'elle a détecté que les clés, appareils ou modules ont été piratés. A chaque nouvelle mise à jour de cette liste de révocation, un index est incrémenté et la liste de révocation ainsi que l'index de mise à jour sont transmis par l'autorité de certification à tous les fournisseurs de contenus auxquels elle est raccordée.

Préférentiellement, la liste de révocation contient des numéros de série, de modules, d'appareils ou de clés (notamment des clés qu'elle a émises) qui ne sont plus considérés comme sûrs par l'autorité de certification. Elle peut également contenir des informations relatives à des clés secrètes (utilisées en cryptographie dite symétrique) utilisées dans le système de diffusion sécurisé de contenu lorsque l'autorité de certification a eu connaissance d'un piratage (par exemple d'une diffusion publique d'une clé secrète) d'une de ces clés.

De plus, la liste de révocation contient également, de manière préférentielle, pour chaque élément de la liste, son index de révocation, c'est à dire l'index de mise à jour de la liste de révocation au moment de l'insertion de

l'élément dans la liste. Ceci permet avantageusement de gérer le moment à partir duquel une clé, un appareil ou un module n'est plus considéré comme conforme et fiable par l'autorité de certification.

Dans le réseau numérique domestique représenté sur la figure 1, le dispositif de réception 3 comprend un décodeur numérique 30 doté d'un lecteur de carte à puce muni d'une carte à puce 31. Ce décodeur reçoit des contenus numériques du fournisseur de contenu 2 via une liaison 6. Il peut s'agir d'une liaison hertzienne, par câble, satellite ou encore d'une liaison utilisant le réseau Internet. De manière préférentielle, le décodeur 30 comporte également une voie de retour 7 vers le fournisseur de contenu. Cette voie de retour peut notamment utiliser le réseau téléphonique commuté.

Le dispositif de réception 3 du réseau domestique joue également le rôle de dispositif source dans le réseau, c'est à dire qu'il émet les contenus reçus à destination des autres dispositifs du réseau, notamment le dispositif de présentation de contenu 4 ou le magnétoscope numérique (DVCR) 5. Le dispositif de présentation de contenu 4 comprend un récepteur de télévision numérique (DTV) 40 doté d'un lecteur de carte à puce muni d'une carte à puce 41.

Les données numériques représentant le contenu diffusé par le fournisseur de contenu 2 vers le dispositif de réception 3 sont en général des données embrouillées selon le principe de la télévision payante ou « à accès conditionnel ». Les données sont embrouillées à l'aide de mots de contrôle (CW) qui sont eux-mêmes transmis dans le flux de données sous forme chiffrée à l'aide d'une clé de chiffrement K en étant contenus dans des messages de contrôle (ECM, de l'anglais « Entitlement Control Message »). La clé de chiffrement K est mise à la disposition des utilisateurs qui ont payé pour recevoir les données, notamment en étant stockée dans une carte à puce.

Dans l'exemple de la figure 1, on suppose que la carte à puce 31 contient une telle clé K. Nous avons également représenté un exemple de paquet de données 60 tels qu'ils sont reçus par le dispositif de réception 3.

Naturellement, l'invention s'applique également au cas où les données numériques sont protégées par un système dit DRM (de l'anglais « Digital Rights Management », signifiant littéralement « Gestion des droits numériques »).

Selon un mode de réalisation préféré de l'invention, lorsque les données représentatives d'un contenu sont reçues par le décodeur 30, elles sont ensuite mises en forme par le dispositif 3 avant d'être diffusées sur le réseau numérique. Pour cela, les messages ECM contenant les mots de

contrôle CW chiffrés à l'aide de la clé K sont transformés, par un module convertisseur 32 contenu dans la carte à puce 31, en messages LECM (de l'anglais « Local Entitlement Control Message ») contenant les mots de contrôle déchiffrés, les messages LECM étant eux-même protégés à l'aide d'une clé spécifique au réseau domestique, notamment une clé secrète. Un exemple de paquet de données 80 circulant sur le bus 8 du réseau domestique est représenté à la figure 1.

Selon le principe de l'invention, lorsque le fournisseur de contenu 2 transmet un contenu au dispositif de réception 3, il attache au contenu l'index de mise à jour de la liste de révocation que lui a transmis l'autorité de certification en dernier lieu.

Cet index $Index_{LR\_C}$ est préférentiellement contenu dans le message ECM en étant protégé par la clé K. Notamment, l'index pourra être chiffré par la clé K.

Le dispositif de réception 3 contient quant à lui une liste de révocation *LR_M* ainsi qu'un index de mise à jour de cette liste $Index_{LR\_M}$ qui sont préférentiellement mémorisés dans le module convertisseur 32 contenu dans la carte à puce 31.

Dans une première variante préférée de l'invention, les cartes à puces telles la carte 31 sont livrées par l'autorité de certification aux utilisateurs en contenant entre autres la dernière liste de révocation à jour *LR_M* ainsi que l'index correspondant $Index_{LR\_M}$. Dans une deuxième variante de réalisation, les cartes ne contiennent aucune liste de révocation ni d'index lorsqu'elles sont livrées aux utilisateurs.

Nous allons maintenant décrire, en liaison avec la figure 2, le procédé qui est mis en œuvre lorsqu'un nouveau contenu est reçu dans le réseau domestique par le dispositif de réception 3.

La première étape 100 consiste à détecter dans le contenu reçu l'index de mise à jour de la liste de révocation $Index_{LR\_C}$.

La deuxième étape 101, qui n'est mise en œuvre que dans la deuxième variante de réalisation mentionnée ci-dessus, consiste à vérifier la présence dans le dispositif de réception 3 d'un index de mise à jour de liste de révocation mémorisé $Index_{LR\_M}$. Si un index $Index_{LR\_M}$ est mémorisé, alors on passe à l'étape 102 consistant à vérifier si l'index reçu dans le contenu $Index_{LR\_C}$ est inférieur ou égal à l'index mémorisé $Index_{LR\_M}$. Si $Index_{LR\_C} \leq Index_{LR\_M}$, alors le procédé se termine.

Sinon, on passe à l'étape 103 consistant à remplacer la valeur de l'index de mise à jour de la liste de révocation mémorisé $Index_{LR\_M}$ par l'index reçu dans le contenu $Index_{LR\_C}$. De même, si la réponse au test de l'étape 101 est négative (pas d'index mémorisé dans le dispositif de réception), alors on passe à l'étape 103 et l'index mémorisé $Index_{LR\_M}$ est initialisé à la valeur de l'index reçu dans le contenu $Index_{LR\_C}$.

Suite à l'étape 103, il faut également mettre à jour la liste de révocation mémorisée *LR_M* dans le dispositif de réception 3. Ceci est schématisé à la figure 2 par l'étape 104 qui peut consister, soit en un téléchargement de la liste de révocation la plus récente en utilisant la voie de retour 7 du décodeur 30 vers le fournisseur de contenu 2, soit en une attente de réception de cette liste avec un prochain contenu. Dans ce cas, on prévoit que le fournisseur de contenu envoie périodiquement la liste de révocation la plus récente avec des contenus.

Lorsque l'index de liste de révocation mémorisé $Index_{LR\_M}$ ainsi que la liste de révocation *LR_M* correspondante ont été mis à jour dans le dispositif de réception 3, celui-ci les communique aux autres dispositifs du réseau, à l'exception des dispositifs d'enregistrement tels le DVCR 5 à la figure 1. Notamment dans l'exemple de la figure 1, il les communique au dispositif de présentation 4 qui les mémorise dans un module terminal 42 contenu dans la carte à puce 41.

Ce module terminal 42 contient notamment une clé secrète spécifique au réseau domestique et il est chargé de traiter les messages LECM inclus dans les paquets de données 80 reçus par le dispositif de présentation 4. Grâce à cette clé secrète du réseau domestique, le module terminal 42 est capable de récupérer dans le message LECM les mots de contrôle CW ayant servi à embrouiller les données numériques. Le dispositif de présentation 4 peut alors désembrouiller les données pour les présenter à l'utilisateur.

On notera que l'invention s'applique également au cas où le réseau numérique domestique comporte une paire de clés asymétriques spécifique à ce réseau pour protéger les messages LECM.

En revenant au dispositif de réception 3, lorsque celui-ci a effectué les étapes 100 à 104 décrites précédemment, il transforme le message ECM inclus dans les données numériques reçues en un message LECM qui contient en outre l'index de mise à jour de la liste de révocation $Index_{LR\_C}$ reçu avec le contenu.

Si ce contenu, qui circule sur le réseau numérique domestique sous forme de paquets de données tels le paquet 80 représenté à la figure 1, est enregistré par le dispositif d'enregistrement 5, il sera donc enregistré avec l'index de mise à jour de la liste de révocation le plus récent au moment de l'enregistrement, cet index étant inclus dans les messages LECM des paquets qui composent le contenu. De cette manière, le contenu pourra toujours être visualisé ou joué dans le réseau même si plus tard une clé ou un appareil du réseau sont révoqués.

De manière préférentielle, l'index $Index_{LR\_C}$ inséré dans le message LECM par le module convertisseur 32 est inséré dans une partie « en clair » de ce message.

Le message LECM comprend en effet une partie A en clair, contenant notamment des informations sur le type de contenu (audio/video...) ou sur l'autorisation ou non de copier ce contenu, et une partie B protégée contenant notamment les mots de contrôle ayant servi à embrouiller les données numériques représentant le contenu. Cette partie B est protégée par chiffrement, c'est à dire que le message LECM contient une version chiffrée de la partie B à l'aide d'une clé qui est soit la clé spécifique du réseau, soit une clé qui peut être retrouvée en connaissant la clé spécifique du réseau. Le message LECM contient également de manière préférentielle un champ d'intégrité qui est le résultat d'une fonction de hachage appliquée à la partie A et à la partie B (avant chiffrement) du message.

Rappelons qu'une fonction de hachage, souvent notée « Hash(x) », est une fonction mathématique qui transforme un ensemble de données « x » en un ensemble de données « y » de taille fixe, souvent nettement inférieure à la taille des données d'entrées, et que cette fonction est à sens unique (« one way function » en anglais), c'est à dire que connaissant « y », il est impossible de retrouver « x », tel que y=Hash(x).

Dans une variante de réalisation, notamment lorsque le message LECM ne comporte pas de champ d'intégrité, l'index $Index_{LR\_C}$ inséré dans le message LECM par le module convertisseur 32 est inséré dans la partie B protégée du message LECM.

Nous allons maintenant décrire, en liaison avec la figure 3, le procédé qui est mis en œuvre par le dispositif de présentation 4 lorsqu'un contenu provenant du réseau numérique domestique doit être présenté à un utilisateur, et plus précisément lorsque chaque paquet de données 80 du contenu est reçu par le dispositif de présentation 4.

Lors d'une première étape 200, le dispositif de présentation vérifie l'intégrité du message LECM inclus dans le paquet de données reçu. Pour cela, il retrouve la partie B du message LECM grâce à la clé secrète spécifique du réseau domestique puis il calcule le résultat de la même fonction de hachage que celle mentionnée plus haut, appliquée aux parties A et B du message LECM, pour le comparer au champ d'intégrité du message LECM reçu.

Si cette vérification est positive, alors le procédé se poursuit par l'étape 201 lors de laquelle on vérifie si la liste de révocation *LR_M* mémorisée dans le module terminal 42 contient au moins un élément relatif à une clé, un module ou un appareil utilisé dans le dispositif de présentation. Il peut s'agir du numéro de série d'une clé publique utilisée par le dispositif de présentation (et mémorisée préférentiellement dans le module terminal 42), ou bien du numéro de série de l'appareil récepteur de télévision 40 ou du module terminal 42, ou encore d'une information relative à la clé sécrète du réseau domestique, mémorisée dans le module terminal 42 également (cette information pourra être un numéro de série de la clé secrète, la clé elle-même ou bien le résultat d'un fonction de hachage ou d'une fonction de chiffrement appliquée à la clé).

Si la liste de révocation *LR_M* ne contient aucun élément relatif à une clé, un module ou un appareil utilisé dans le dispositif de présentation 4, alors ce dernier peut présenter le contenu à l'utilisateur lors de l'étape 203.

Par contre, si la liste de révocation contient au moins un desdits éléments, alors le procédé se poursuit par l'étape 202 consistant à vérifier si l'index de révocation de cet élément (l'index de révocation de l'élément étant contenu dans la liste *LR_M*) est supérieur à l'index $Index_{LR\_C}$ inclus dans le contenu reçu (plus précisément, inclus dans le message LECM du paquet reçu). Ceci peut se produire quand un contenu, enregistré avant qu'un élément ne soit inséré dans la liste de révocation, est ensuite rejoué dans le réseau domestique après que l'élément ait été inséré dans la liste.

Si la vérification ci-dessus est positive, alors le dispositif de présentation peut présenter le contenu à l'utilisateur à l'étape 203.

Sinon, le procédé est arrêté (étape 204) et le contenu n'est pas présenté à l'utilisateur. Le procédé est également arrêté lorsque la vérification de l'intégrité du message LECM à l'étape 200 est négative. Le procédé peut également être arrêté, en variante non préférée, lorsque au moins un élément relatif à une clé, un module ou un appareil utilisé dans le dispositif de présentation est inclus dans la liste de révocation *LR_M* (flèche pointillée représentée à partir de l'étape 201).

L'invention ne se limite pas aux modes de réalisation qui ont été décrits ci-dessus. En particulier, l'invention s'applique également au cas où un contenu est reçu par un seul dispositif formant dispositif de réception et de présentation de contenu, sans que ce dispositif soit forcément inclus dans un réseau numérique domestique.

REVENDICATIONS

1. Procédé de mise à jour d'une liste de révocation contenant des identifiants de clés, d'appareils ou de modules considérés comme non conformes par un tiers de confiance (1) dans un système de diffusion sécurisé de contenu consistant :

à recevoir dans un dispositif de réception (3) un contenu d'un fournisseur de contenu (2),

caractérisé en ce qu'un identifiant unique est alloué à chaque mise à jour de la liste de révocation par le tiers de confiance (1), l'identifiant de la liste de révocation la plus récente ($Index_{LR\_C}$) étant attaché au contenu reçu dans ledit dispositif de réception, et

en ce que le procédé comporte en outre une étape (102) consistant à comparer l'identifiant de liste de révocation reçu ($Index_{LR\_C}$) avec un identifiant de liste de révocation mémorisé ($Index_{LR\_M}$) dans ledit dispositif de réception et, en cas de différence entre lesdits identifiants :

- à télécharger la liste de révocation la plus récente dans ledit dispositif de réception ; ou
- à attendre la réception de la liste de révocation la plus récente avec un prochain contenu.

2. Procédé de réception d'un contenu par un dispositif de réception (3) dans un système de diffusion sécurisé de contenu dans lequel une liste de révocation, établie par un tiers de confiance (1), contient des identifiants de clés, d'appareils ou de modules considérés comme non conformes par ledit tiers de confiance,

caractérisé en ce qu'un identifiant unique est alloué à chaque mise à jour de la liste de révocation, l'identifiant de la liste de révocation la plus récente ($Index_{LR\_C}$) étant attaché au contenu reçu par ledit dispositif de réception,

le procédé comportant en outre une étape consistant à

comparer (102) l'identifiant de liste de révocation reçu ($Index_{LR\_C}$) avec un identifiant de liste de révocation mémorisé ($Index_{LR\_M}$) dans ledit dispositif de réception, et en cas de différence entre lesdits identifiants :

- à télécharger la liste de révocation la plus récente dans ledit dispositif de réception; ou
- à attendre la réception de la liste de révocation la plus récente avec un prochain contenu.

3. Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce que l'identifiant unique de liste de révocation est un index de mise à jour de ladite liste de révocation.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'identifiant de liste de révocation la plus récente reçu avec le contenu ($Index_{LR\_C}$) est inclus dans une partie protégée par chiffrement ou par authentification dudit contenu.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que la liste de révocation contient au moins un élément appartenant à l'ensemble comprenant :

- au moins un numéro de série de clé publique générée par ledit tiers de confiance et considérée comme non conforme par ledit tiers de confiance ;
- au moins un numéro de série d'un appareil considéré comme non conforme par ledit tiers de confiance ;
- au moins un numéro de série d'un module considéré comme non conforme par ledit tiers de confiance.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que la liste de révocation contient au moins un élément appartenant à l'ensemble comprenant :

- au moins un identifiant de clé secrète de réseau local servant à protéger des contenus contre la copie illicite ;
- au moins une clé secrète de réseau local servant à protéger des contenus contre la copie illicite ;
- au moins le résultat d'une fonction de calcul, notamment une fonction de hachage, appliquée à une clé secrète de réseau local servant à protéger des contenus contre la copie illicite.

7. Procédé selon l'une des revendications 5 ou 6, caractérisé en ce qu'on mémorise en outre, pour chaque élément de la liste de révocation son index de révocation correspondant à l'index de mise à jour de ladite liste au moment de l'insertion de l'élément dans la liste de révocation.

8. Procédé de présentation d'un contenu reçu conformément au procédé selon l'une des revendications 2 à 7, les revendications 3 à 7 étant

dépendantes de la revendication 2, caractérisé en ce qu'il comprend les étapes consistant pour un dispositif de présentation de contenu (4) à :

- vérifier (201) si la liste de révocation la plus récente (*LR_M*) à la disposition du dispositif de réception ne contient pas d'élément relatif à au moins une clé, un module ou un appareil utilisé par ledit dispositif de réception ; et

- si la liste de révocation ne contient aucun desdits éléments, continuer le procédé pour présenter ledit contenu à un utilisateur (203),

- sinon, arrêter (204) le procédé.

9. Procédé de présentation d'un contenu reçu conformément au procédé selon la revendication 7 prise dans sa dépendance des revendications 2 et 3, caractérisé en ce qu'il comprend les étapes consistant pour un dispositif de présentation de contenu à :

- vérifier (201) si la liste de révocation la plus récente (*LR_M*) à la disposition du dispositif de réception ne contient pas d'élément relatif à au moins une clé, un module ou un appareil utilisé par ledit dispositif de réception ; et

- si la liste de révocation contient au moins un desdits éléments :

  - comparer (202) l'index de mise à jour de la liste de révocation attaché au contenu ($Index_{LR\_C}$) avec l'index de révocation dudit élément ; et

  - si l'index de mise à jour de la liste de révocation attaché au contenu est inférieur à l'index de révocation dudit élément, continuer le procédé pour présenter ledit contenu à un utilisateur (203),

  - sinon, arrêter (204) le procédé.

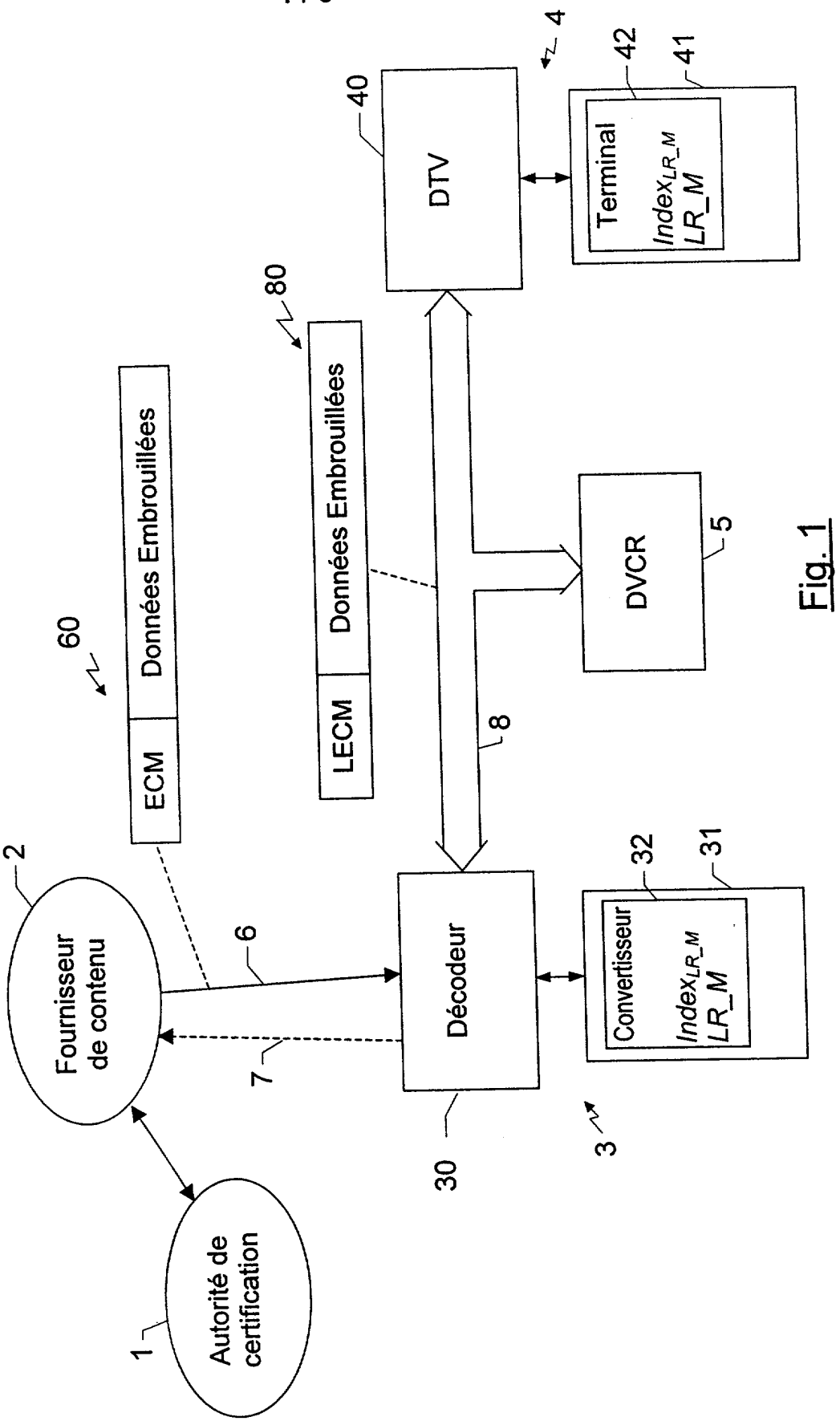

Autorité de certification
1
Fournisseur de contenu
2
Décodeur
30
Convertisseur
32
$Index_{LR\_M}$
LR_M
31
3
6
7
8
ECM
Données Embrouillées
60
LECM
Données Embrouillées
80
DTV
40
Terminal
42
$Index_{LR\_M}$
LR_M
41
4
DVCR
5

Fig. 1

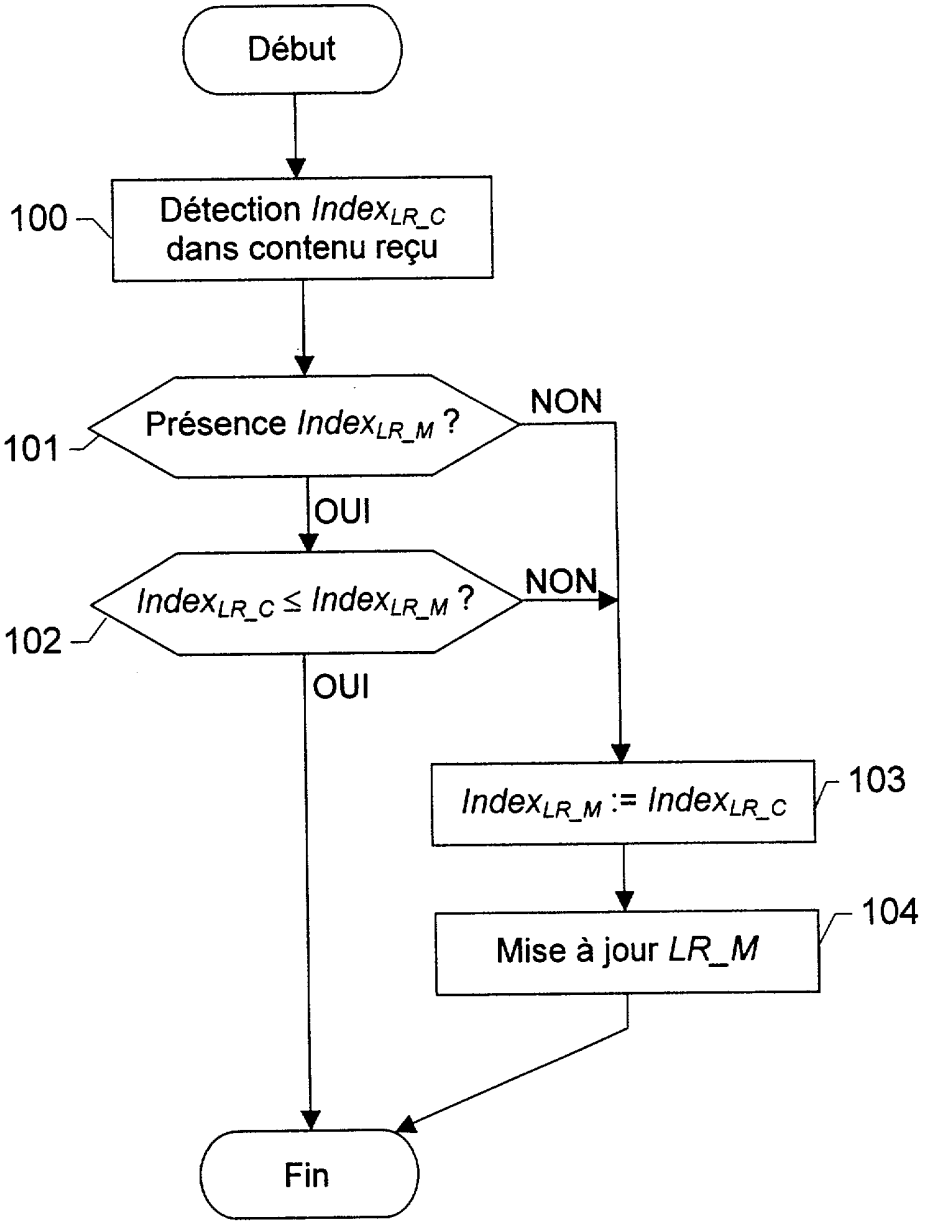

Début
100
Détection $Index_{LR\_C}$ dans contenu reçu
101
Présence $Index_{LR\_M}$?
NON
OUI
102
$Index_{LR\_C} \leq Index_{LR\_M}$?
NON
OUI
$Index_{LR\_M} := Index_{LR\_C}$
103
Mise à jour *LR_M*
104
Fin

Fig. 2

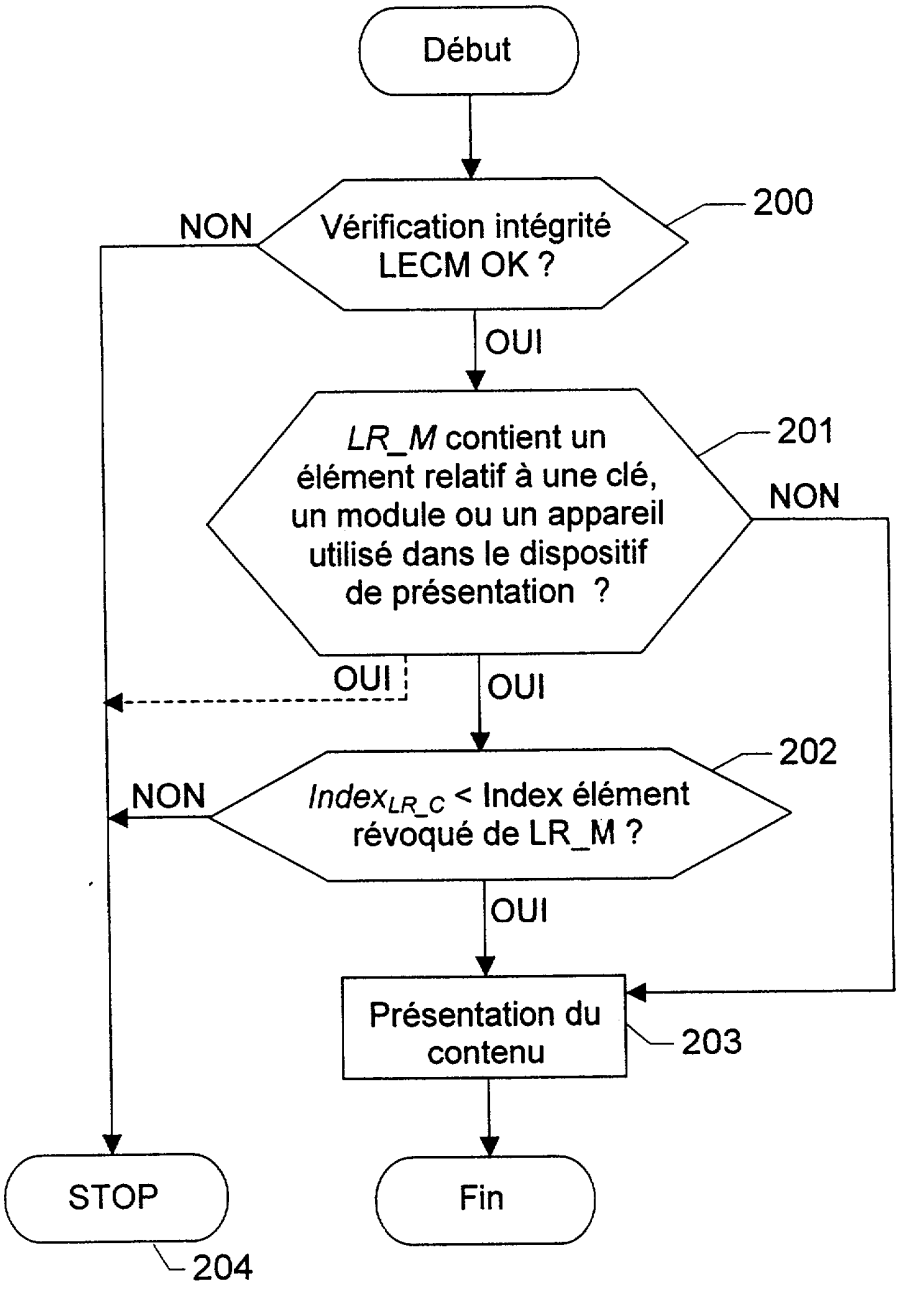

Début
Vérification intégrité LECM OK ?
NON
200
OUI
LR_M contient un élément relatif à une clé, un module ou un appareil utilisé dans le dispositif de présentation ?
201
NON
OUI
OUI
202
NON
Index$_{LR_C}$ < Index élément révoqué de LR_M ?
OUI
Présentation du contenu
203
STOP
204
Fin

Fig. 3

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2834406

N° d'enregistrement national

FA 612960
FR 0117139

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 01 99422 A (SONY ELECTRONICS INC) 27 décembre 2001 (2001-12-27) * page 6, ligne 12 - page 13, ligne 22 *	1-6	H04L9/32
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 décembre 1995 (1995-12-21), pages 64-77, XP000559450 Grand- Saconnex, CH ISSN: 0251-0936 * page 65, colonne de gauche, ligne 1 - colonne de droite, ligne 67 * * page 67, colonne de droite, ligne 34 - page 71, colonne de droite, ligne 12 *	1-8	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04N

1

Date d'achèvement de la recherche	Examinateur
5 novembre 2002	Van der Zaal, R

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0117139 FA 612960

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 05-11-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0199422 A	27-12-2001	AU 1549602 A	02-01-2002
		WO 0199422 A1	27-12-2001

EPO FORM P0465