(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
26 février 2004 (26.02.2004)

PCT

(10) Numéro de publication internationale
WO 2004/017635 A1

(51) Classification internationale des brevets[7] : H04N 7/10, 7/16, 7/167

(21) Numéro de la demande internationale :
PCT/IB2003/003767

(22) Date de dépôt international : 14 août 2003 (14.08.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2002 1403/02 19 août 2002 (19.08.2002) CH

(71) Déposant *(pour tous les États désignés sauf US)* : **NAGRAVISION SA** [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **LE BUHAN, Corinne** [CH/CH]; Route des Vérollys 89, CH-1619 Les Paccots (CH). **KSONTINI, Rached** [CH/CH]; Av. de Riant-Mont 14, CH-1004 Lausanne (CH).

(74) Mandataire : **LEMAN CONSULTING SA**; Route de Clémenty 62, CH-1260 Nyon (CH).

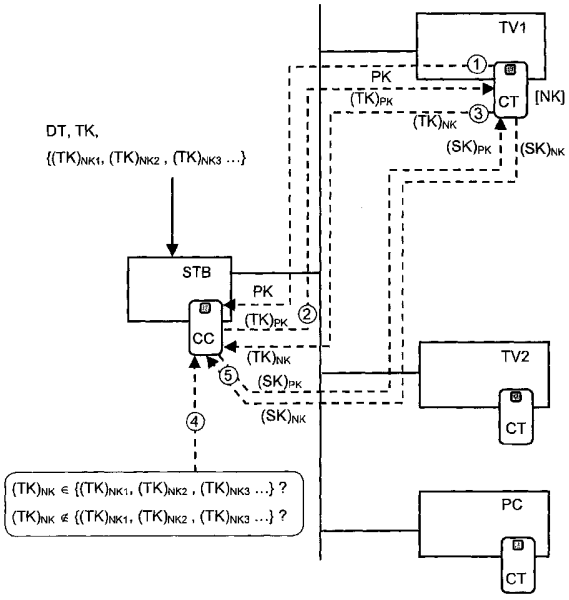
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) **Title:** METHOD FOR VERIFYING VALIDITY OF DOMESTIC DIGITAL NETWORK KEY

(54) **Titre :** MÉTHODE DE VÉRIFICATION DE LA VALIDITÉ D'UNE CLÉ POUR UN RÉSEAU DOMESTIQUE NUMÉRIQUE



(57) **Abstract:** The invention relates to a method for checking conformity of a network key (NK). The inventive method is used for transmitting data from a conditional access source to a domestic network and consists in verifying the authencity of a network key (NK) by means of pertinent control data provided by a verification centre in the form of a list { $(TK)_{NK1}$, $(TK)_{NK2}$, $(TK)_{NK3}$ }. The verification of the presence or absence of a cryptogram $(T K)_{NK}$ is carried out according to the list { $(TK)_{NK1}$, $(TK)_{NK2}$, $(TK)_{NK3}$ }. The cryptogram $(T K)_{NK}$ is produced on the basis of a test key (TK) delivered by the centre for verification of encryption, by the network key (NK) of the safety module (CT) of a device (TV1, TV2, PC) connected to the network.

[Suite sur la page suivante]

WO 2004/017635 A1

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Publiée :

— *avec rapport de recherche internationale*

(57) Abrégé : Le but de la présente invention est de proposer une méthode de contrôle de la conformité d'une clé de réseau (NK). Cette méthode s'applique lors du transfert de données provenant d'une source ô accès conditionnel vers un réseau domestique. Il s'agit de vérifier l'authenticité d'une clé de réseau (NK) par l'intermédiaire de données de contrôle pertinentes fournies par le centre de vérification en général sous forme d'une liste {(TK)NK1, (TK)NK2 , (TK)NK3 }. Une vérification de la présence ou de l'absence d'un cryptogramme (TK)NK est effectuée selon la liste {(TK)NK1, (TK)NK2 , (TK)NK3 }. Le cryptogramme (TK)NK est constitué ô partir d'une clé de test (TK) fournie par le centre de vérification encryptée par une clé de réseau (NK) d'un module de sécurité (CT) d'un appareil (TV1, TV2, PC) connecté au réseau.

MÉTHODE DE VÉRIFICATION DE LA VALIDITÉ D'UNE CLÉ POUR UN RÉSEAU DOMESTIQUE NUMÉRIQUE

La présente invention concerne une méthode de sécurisation dans un réseau domestique numérique. Plus particulièrement, la méthode de l'invention s'articule sur des réseaux uniques d'appareils dont les contenus sont personnalisés.

Un réseau domestique numérique est un ensemble d'appareils audio-visuels reliés par des interfaces numériques. Ces appareils incluent par exemple des décodeurs numériques, téléviseurs numériques, lecteurs / enregistreurs de DVD, appareils de stockage munis de disques durs, enregistreurs audio MP3, des livres électroniques, consoles de jeux, ordinateurs ou autres plate-formes permettant l'accès à Internet.

La technologie numérique donne la possibilité d'effectuer des copies de contenus (films, musique, jeux vidéos, logiciels...) qui sont de même qualité que l'original. Ces copies parfaites impliquent des conséquences néfastes pour l'industrie au niveau des droits d'auteurs si une protection efficace n'est pas disponible.

Le contenu original arrive dans la maison par diverses sources: il peut être transmis par voie hertzienne, par le satellite ou le câble, par l'Internet ou être enregistré sur une cassette numérique, un DVD ou même un disque dur. Avant de fournir leur contenu aux distributeurs, les détenteurs des droits spécifient certaines conditions d'accès concernant la protection du contenu qui doivent donc être mises en vigueur par un système de protection du contenu à l'intérieur de la maison.

Un contenu peut, par exemple, être associé à des droits comme: "Lecture seule", "Copie pour usage privé", "Copie libre".

Un système de protection des contenus numérique va permettre aux propriétaires et distributeurs de contenus de lutter contre les pertes de revenus dues au piratage. Il est basé sur l'utilisation de modules de sécurité permettant une identification de chaque appareil connecté sur le réseau domestique et le décodage des données.

L'avantage d'un tel système est que le contenu est toujours conservé crypté dans le réseau numérique domestique jusqu'à ce qu'il soit lu. Le décryptage est réalisé en collaboration avec le module de sécurité amovible inséré dans l'appareil de lecture. Cette méthode simple offre une sécurité complète de l'encryptage.

Un tel système de protection est qualifié de "bout en bout", c'est-à-dire depuis l'entrée du contenu sur le réseau domestique numérique jusqu'à sa restitution, en passant par son stockage éventuel.

Avec ce système, les fournisseurs de contenus peuvent facilement choisir des droits pour les utilisateurs de données encryptées qui seront appliqués au réseau domestique.

Une possibilité de dupliquer et de gérer des contenus numériques à l'intérieur de son réseau est ainsi offerte à l'utilisateur dans le cadre des droits définis par les fournisseurs de contenus. Elle permet à l'utilisateur de partager le contenu enregistré sur n'importe quel appareil numérique fixe ou portable connecté, tout en empêchant la redistribution de ce contenu à l'extérieur de son réseau personnel.

Le système crée un environnement sécurisé: il permet d'enregistrer des contenus cryptés, mais en interdit la lecture si le contenu n'est pas légitime. Un contenu illégitime est une copie non autorisée par le détenteur des droits associés. Par exemple, un disque copié à partir d'un original sur un appareil appartenant à un réseau A ne pourra pas être lu par un appareil connecté à un réseau B.

Tout contenu non gratuit est associé à un réseau domestique donné et, par conséquent, ne peut être utilisé que sur ce même réseau. L'identité au réseau est assurée par les modules de sécurité qui, du fait qu'ils sont amovibles, permettent une certaine mobilité.

Cependant, un réseau domestique peut également comprendre des appareils mobiles externes associés à ce réseau, par exemple un lecteur de musique portable ou un appareil dans une voiture, ainsi que des appareils dans une résidence secondaire qui appartient au propriétaire du réseau initial. Autrement dit, les contenus sont protégés par la même clé dès que les appareils externes ont été connectés au moins une fois au réseau de référence. Il n'est donc pas nécessaire d'avoir une connexion permanente. Tous ces appareils partagent une clé propre à un réseau privé domestique, sur lequel le contenu est disponible pour un usage privé, mais seulement selon les droits associés.

Le système de protection dont les principes sont évoqués ci-dessus est décrit dans le document de Thomson Multimedia SA: "SmartRight™, A Content Protection System for Digital Home Networks, White Paper" publié en octobre 2001.

Selon une configuration particulière, le point d'entrée d'un réseau domestique numérique est constitué d'un décodeur ("Set-Top-Box") qui reçoit un flux de données crypté à partir d'un satellite, d'un câble, voire par le biais d'Internet. Ce décodeur est muni d'un module de sécurité en général sous forme d'une carte à puce appelée module convertisseur. Le rôle de ce module consiste à traiter les conditions définies par le contrôle d'accès du fournisseur d'accès conditionnel donc à décrypter les messages de contrôle (ECM) contenant les mots de contrôle (CW) permettant le déchiffrement du contenu si les droits sont présents dans ce module. Dans l'affirmative, ce module réencrypte les mots de contrôle (CW) grâce à une clé de session générée aléatoirement par le module. Ce module joint aux mots de contrôle (CW) la clé de session encryptée par la clé de réseau pour former des messages de contrôle locaux (LECM).

Selon une deuxième possibilité, le point d'entrée est un lecteur de données tel qu'un lecteur DVD. Les données sont stockées sous forme encryptée et un module dans le lecteur dispose des capacités pour décrypter ces données. Une fois décryptées, elles sont re-encryptées selon le réseau local connecté et diffusées dans ce réseau. Selon le mode d'opération, il est possible de ne pas décrypter les données mais de traiter que la ou les clés d'encryption. En effet, une technique connue consiste à encrypter les données par un ou des clés de session (donc déterminée aléatoirement) et d'encrypter ces clés par une clé propre au système et connue du lecteur de DVD. Le lecteur décrypte l'ensemble des clés et re-encrypte cet ensemble grâce à la clé locale. Les données proprement dites ne sont pas traitées et restent sous leur forme originale. Dans cette forme d'exécution, le module convertisseur est le module qui contient les moyens pour décrypter l'ensemble des clés et les encrypter pour le réseau local.

Dans les deux cas cités ci-dessus, on parlera de dispositif de diffusion puisque sa fonction principale est de diffuser des données dans un réseau local.

La clé de réseau est une clé propre à un réseau donné. Elle est générée dans le réseau au moyen d'un module de sécurité appelée module terminal associée au premier appareil de visualisation du contenu se connectant au réseau. Ce dernier module est le seul capable d'initialiser le réseau. Un module terminal additionnel reçoit ensuite la clé de réseau de la part du premier appareil. Ce module terminal est en général sous forme d'une carte à puce ou peut être un circuit monté directement dans le dispositif de traitement.

Par contre, la clé de réseau n'est pas connue du module convertisseur afin d'éviter d'y concentrer tous les secrets, ce qui en ferait une cible privilégiée d'attaque pour les pirates. Par conséquent, un mécanisme de communication sécurisé doit être mis en place entre un module terminal et le module convertisseur pour que cette dernière puisse insérer la clé de session encryptée par la clé de réseau dans les messages de contrôle (LECM) qu'elle génère.

A cette fin, le module terminal échange avec le module convertisseur une clé publique connue du module terminal et une clé de session générée aléatoirement par le module convertisseur. Le module terminal transmet sa clé publique au module convertisseur qui retourne la clé de session cryptée avec la clé publique. Le module terminal décrypte alors la clé de session, puis retransmet au module convertisseur cette clé de session cryptée avec la clé de réseau.

Le module convertisseur encrypte d'une part les mots de contrôle (CW) à l'aide de la clé de session et d'autre part, elle y joint la clé de session cryptée avec la clé de réseau (provenant d'un des modules terminal) pour former les messages de contrôle locaux (LECM). Ces messages (LECM) sont alors transmis avec le contenu crypté aux différents appareils du réseau pour stockage ou visualisation.

Chaque appareil terminal connecté au réseau peut donc décrypter les messages (LECM) et en extraire les mots de contrôle (CW) car il possède la clé de réseau et il reçoit la clé de session cryptée par la clé de réseau. Il peut ensuite, à l'aide de ces mots de contrôle (CW), décrypter le flux de données. Ces appareils sont dit dispositif de traitement.

Ce procédé d'introduction d'une clé de réseau contenue dans une carte terminal présente un inconvénient par le fait qu'il est techniquement possible d'initialiser une

multitude de réseaux domestiques au moyen d'un module terminal falsifié. En effet, dans le système de protection connu, la clé de réseau n'est pas contenue en tant que telle dans le module convertisseur, mais seulement sous la forme d'une clé de session cryptée par la clé de réseau. Des réseaux non autorisés ainsi établis peuvent posséder donc tous la même clé et par conséquent, les contenus enregistrés dans les appareils peuvent être redistribués et exploités en dehors du nombre limité de membres tels que défini dans la norme d'un réseau domestique.

De plus, une clé de réseau tierce non reconnue par le fournisseur de contenu peut être introduite dans un module terminal permettant la création d'un réseau dont les droits attribués aux contenus ne sont plus gérés par le détenteur.

Le but de la présente invention est de pallier les inconvénients décrits ci-dessus en proposant une méthode de contrôle de la conformité de la clé de réseau.

Ce but est atteint par une méthode de vérification de la validité d'une clé de réseau dans un réseau domestique numérique comprenant au moins un dispositif de diffusion et un dispositif de traitement, le dispositif de diffusion disposant de données encryptées à diffuser vers le dispositif de traitement, ces données étant accessibles par le dispositif de traitement grâce à une clé de réseau inconnue du dispositif de diffusion, cette méthode comprenant les étapes suivantes:

- transmission par le dispositif de diffusion d'une clé de test au dispositif de traitement,

- calcul d'un cryptogramme résultant de l'encryption de la clé de test par la clé de réseau dans le dispositif de traitement,

- envoie du cryptogramme au dispositif de diffusion,

- détermination par le dispositif de diffusion de la validité de la clé de réseau en comparant le cryptogramme avec une liste de cryptogrammes valide et/ou invalide.

La méthode s'applique généralement lors de transfert de données provenant d'une source à accès conditionnel vers un réseau domestique. Il s'agit de vérifier l'authenticité d'une clé de réseau par l'intermédiaire de données de contrôle pertinentes fournies par un centre de vérification en général sous forme d'une liste.

La méthode est basée sur la vérification de la présence ou de l'absence d'un cryptogramme donné sur une liste de contrôle: le cryptogramme étant constitué à partir d'une clé de test, fournie par le centre de vérification, encryptée à l'aide d'une clé de réseau d'un module terminal d'un appareil connecté au réseau.

La liste de contrôle fournie par le centre de vérification contient des cryptogrammes créés soit avec des clés de réseau invalides ("black list"), soit avec des clés valides ("white list"). Une clé de réseau contenue dans un module terminal sera donc valide seulement si son cryptogramme correspondant est absent d'une "black list" ou présent dans une "white list".

Dans le cas d'un lecteur de DVD, les données du film par exemple sont accompagnées par un fichier de cryptogrammes invalides (ou valides) et la comparaison peut s'effectuer de la même manière que pour un décodeur.

Selon une première variante, les données permettant de vérifier une clé de réseau comprennent une clé de test et un ensemble de cryptogrammes, c'est-à-dire le résultat de l'encryption de la clé de test avec toutes les clés de réseau valides ou invalides. La clé de test est envoyée au dispositif de traitement et le cryptogramme renvoyé est comparé avec cette liste.

Selon une seconde variante, les données permettant de vérifier une clé de réseau comprennent l'ensemble des clés de réseau invalides. La clé de test est générée aléatoirement par le dispositif de diffusion et transmis au dispositif de traitement. Le cryptogramme renvoyé est stocké et comparé avec les cryptogrammes générés par le dispositif de diffusion en encryptant la clé de test avec chaque clé de réseau invalide.

Pour la suite de l'exposé, il sera fait plus particulièrement mention du module convertisseur localisé dans le dispositif de diffusion pour les opérations de vérification. De même, le module terminal effectue les opérations pour le compte du dispositif de traitement avec lequel ce module est relié.

Selon un mode de réalisation, une fois la vérification passée avec succès, le module convertisseur génère une clé de session, clé qui sera transmise de manière sécurisée au module terminal d'un des appareils. Cette clé de session est alors

encryptée par la clé de réseau du module terminal pour former un cryptogramme qui est renvoyé au module convertisseur. Le module convertisseur va utiliser cette clé de session pour encrypter les mots de contrôle (CW), et les transmettre soit vers un dispositif de traitement, soit vers un dispositif de stockage accompagné du cryptogramme.

Si la comparaison est négative, le module convertisseur stoppe la génération du flux de données de contrôle accompagnant le contenu et permettant son déchiffrement au sein du réseau domestique. Un message d'erreur invite l'utilisateur à changer de module terminal. Dans une variante où le décodeur possède un canal de retour, ce message peut être aussi transmis au centre de vérification pour signaler un module terminal non valide.

Selon cette méthode la clé de session est remplacée dans une phase de test, par une clé de test à valeur prédéfinie. La clé de test joue alors un rôle analogue à celui de la clé de session du procédé d'initialisation décrit plus haut.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux figures annexées servant d'exemple nullement limitatif, à savoir:

- La figure 1 représente une communication typique entre un module terminal et un module convertisseur selon la méthode de l'état de la technique.

- La figure 2 représente une communication typique entre un module terminal et un module convertisseur selon la méthode de l'invention.

Le réseau domestique numérique illustré par la figure 1 est composé d'un décodeur (STB), des téléviseurs (TV1, TV2) et d'un ordinateur (PC). Chaque appareil est muni d'une carte à puce amovible servant de module de sécurité chargé de l'encryptage / décryptage des données du réseau. Selon une variante particulière, le module de la carte à puce peut être directement monté dans l'appareil de manière permanente.

Selon une réalisation préférée, la carte associée au décodeur (STB) est un module convertisseur (CC) qui transforme des messages de contrôles ECM (Entitlement Control Message) reçus par le décodeur en ECM locaux (LECM) propres au réseau. Ces derniers contiennent les clés de décryptage ou mots de contrôle (CW) du flux de données (DT) provenant du centre de gestion encryptés par une clé de transmission

(TK). Les ECM locaux (LECM) contiennent également les mots de contrôle (CW) du flux de données (DT) encryptés avec une clé de session locale, mais ils contiennent aussi cette clé de session (SK)encryptée par la clé de réseau (NK).

Les cartes associées aux appareils de visualisation (TV1, TV2, PC) appartenant au réseau sont des modules terminal (CT) qui permettent le décryptage des données du réseau au niveau des appareils (TV1, TV2, PC) grâce à la clé de réseau (NK) stockée dans chaque module.

La liaison entre un réseau à accès conditionnel et un réseau domestique s'effectue par la connexion d'un appareil par exemple (TV1) au décodeur (STB). Lorsque le module convertisseur (CC) associée au décodeur (STB) doit transformer des messages de contrôles ECM (Entitlement Control Message) en des ECM locaux (LECM) propres au réseau, un dialogue s'établit entre le module terminal (CT) associée à l'appareil (TV1) et le module convertisseur (CC). Ce dialogue s'effectue de manière sécurisée en utilisant une paire de clés asymétriques (clé publique et clé privée) propre au module terminal (CT); il se résume en 3 étapes (1, 2, 3) comme suit:

1).- Le module terminal du premier appareil transmet sa clé publique (PK) au module convertisseur (CC) du décodeur (STB).

2).- Le module convertisseur (CC) génère aléatoirement une clé de session (SK) qu'elle crypte avec la clé publique (PK) précédemment reçue. Le module convertisseur (CC) transmet alors la clé encryptée $(SK)_{PK}$ au module terminal (CT).

3).- Le module terminal (CT) décrypte la clé de session (SK) en utilisant sa clé privée associée à la clé publique (PK). Elle encrypte ensuite la clé de session (SK) au moyen de la clé de réseau (NK) qu'elle stocke en permanence. Le message résultant $(SK)_{NK}$ est transmis au module convertisseur (CC).

Les messages de contrôle locaux (LECM) comprennent finalement des mots de contrôle (CW) encryptés par une clé de session (SK) et cette clé (SK) encryptée par la clé de réseau (NK).

Le téléviseur (TV1) muni de son module terminal (CT) est alors capable de décrypter les messages de contrôle locaux (LECM) grâce à la clé de réseau (NK) qui sert à

décrypter la clé de session (SK). Cette dernière permet ensuite la décryption de mots de contrôle (CW) servant à décrypter les données vidéo / audio destinées au téléviseur.

La figure 2 illustre le procédé d'initialisation de la communication selon l'invention dont les étapes se différencient par rapport aux précédentes par le fait que la clé de session (SK) est remplacée, dans une première phase, par une clé de test (TK). Pour cela, le décodeur (ou plus généralement le dispositif de diffusion) dispose d'une liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ de cryptogrammes et d'une clé de test; l'exemple ci-dessous concerne la variante avec une clé de test unique pour tous les cryptogrammes :

1).- Le module terminal (CT) du premier appareil transmet sa clé publique (PK) au module convertisseur (CC) du décodeur (STB).

2).- Le module convertisseur (CC) (ou le dispositif de diffusion grâce à sa mémoire plus étendue) dispose d'une liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ ainsi qu'une clé de test (TK). Le module convertisseur (CC) crypte la clé de test (TK) avec la clé publique (PK) reçue du module terminal (CT), ce qui donne un nouveau message $(TK)_{PK}$ qui sera retransmis au module terminal (CT).

3).- Le module terminal (CT) décrypte la clé de test (TK) en utilisant sa clé privée associée à la clé publique (PK). Elle encrypte ensuite la clé de test (TK) au moyen de la clé de réseau (NK) qu'elle stocke en permanence. Le cryptogramme résultant $(TK)_{NK}$ est transmis au module convertisseur (CC).

4).- Le module convertisseur compare le cryptogramme constitué par la clé de test cryptée par la clé de réseau $(TK)_{NK}$ avec ceux répertoriés dans la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ qui peut être soit une liste noire (black list) ou liste des valeurs non autorisées, soit une liste blanche (white list) ou liste des valeurs autorisées.

Un cryptogramme $(TK)_{NK}$ contenu dans une liste noire ou absente d'une liste blanche est invalide; cela signifie que la clé de réseau (NK) utilisée pour l'encryptage de la clé de test (TK) est refusée. Une signalisation adéquate, sous forme d'un message

d'erreur par exemple, invite l'utilisateur à changer de carte et à recommencer l'opération de connexion.

Un cryptogramme $(TK)_{NK}$ appartenant à une liste blanche ou absente d'une liste noire est par contre accepté. Dans ce cas, le module convertisseur (CC) génère aléatoirement une clé de session (SK) qu'elle crypte avec la clé publique (PK) précédemment reçue. Le module convertisseur transmet alors le clé encryptée $(SK)_{PK}$ au module terminal (CT).

5).- Le module terminal (CT) décrypte la clé de session (SK) en utilisant sa clé privée associée à la clé publique (PK). Elle encrypte ensuite la clé de session (SK) au moyen de la clé de réseau (NK) qu'elle stocke en permanence. Le message résultant $(SK)_{NK}$ est transmis au module convertisseur (CC).

En général, le module convertisseur (CC) vérifie l'authenticité des données de contrôle reçues au moyen d'une signature sécurisée provenant du centre de vérification.

Il est à noter que le traitement du cryptogramme reçu peut se faire postérieurement et dans l'intervalle, le module convertisseur autorise la diffusion de données vers le dispositif de traitement. L'exploitation des données comme par exemple la diffusion d'un film dure suffisamment longtemps pour permettre les opérations de comparaison avec un grand nombre de cryptogrammes. Ceci est particulièrement le cas où le module convertisseur dispose des clés de réseau à invalider et qu'il doit donc calculer pour chaque clé de réseau le cryptogramme correspondant.

Selon une variante de l'invention, la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est stockée dans une mémoire du décodeur après réception (ou plus généralement du dispositif de diffusion tel qu'un lecteur de DVD), car elle peut constituer un fichier trop important pour être stocké dans le module convertisseur (CC). La comparaison du cryptogramme $(TK)_{NK}$ avec ceux contenus dans la liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est effectuée par le décodeur (STB). Dans cette variante, en particulier pour un lecteur de DVD (LDVD), la liste peut être actualisée avec les DVD les plus récents. Ainsi, lorsqu'un ancien DVD est inséré, ce n'est plus la liste qui lui est attachée qui sera utilisée mais la liste la plus récente provenant d'un DVD récent, stockée dans le dispositif du diffusion.

Selon une autre variante le centre de vérification transmet, au lieu de la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$, une adresse indiquant où cette liste peut être téléchargée via Internet. Cette variante nécessite, soit un décodeur (STB) disposant d'un canal de retour, soit un ordinateur possédant une connexion Internet. Le fichier sera alors soit stocké directement dans la mémoire du décodeur, soit transmis depuis l'ordinateur vers le décodeur.

Selon une autre variante, la clé de test cryptée avec la clé de réseau $(TK)_{NK}$ est transmise de manière sécurisée par le module convertisseur (CC) via le décodeur (STB) vers un serveur adéquat ou vers le centre de vérification où la liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est stockée. La vérification de la validité de la clé $(TK)_{NK}$ est donc effectuée en ligne et seul un message d'acceptation ou de refus, avec éventuellement une signature de la clé, sera alors retourné au module convertisseur (CC). L'avantage de cette variante est de décharger le décodeur de tâches qui peuvent devenir importantes surtout avec une liste dont la longueur ne peut que croître avec le nombre de réseaux domestiques installés.

L'avantage de la variante de la liste des clés de réseau à invalider est de pouvoir définir localement la clé de test. En effet, si cette clé de test est connue, il est possible de programmer un module terminal pour répondre par une valeur aléatoire lorsqu'il reçoit une telle clé et donc passer avec succès l'étape de vérification quand bien même sa clé de réseau est invalidée.

Bien entendu, le centre de vérification peut générer des fichiers dans lesquels une clé de test différente est utilisée mais cela nécessite de télécharger ces informations régulièrement dans chaque décodeur, solution impossible pour le cas d'un lecteur DVD.

C'est pourquoi, dans le cadre de l'invention, la clé de session générée aléatoirement par le module convertisseur peut également servir de clé de test. Si le module terminal n'utilise pas la clé de réseau pour encrypter cette clé de session afin de contourner l'étape de vérification, les données ultérieurement encryptées par cette clé de session ne pourront jamais être exploitées par le réseau local relié à ce module convertisseur. Le module terminal est obligé d'utiliser la clé de réseau et la vérification pourra s'effectuer par le module convertisseur grâce au calcul par ce

dernier du cryptogramme de la clé de session avec toutes les clés de réseau invalidées.

Si l'on souhaite ne pas utiliser la clé de session comme clé de test, par exemple du fait que certains calculs sont exécutés dans le décodeur (ou lecteur DVD) et qu'il n'est pas souhaitable de sortir cette clé de session hors du module convertisseur, le protocole d'échange de données entre le module convertisseur et le module terminal peut comprendre l'envoi de plusieurs clés de session (par exemple trois) qui seront encryptées par la clé de réseau dans le module terminal. Les trois cryptogrammes sont renvoyés au module convertisseur qui va décider aléatoirement lequel va servir de clé de session, et lequel servira uniquement pour l'étape de vérification.

Bien qu'il soit sous-entendu que la méthode de vérification décrite ci-dessus est effectuée à chaque négociation d'une clé de session, il est possible de faire cette vérification à des intervalles plus grands. A cet effet, le module convertisseur mémorise l'identifiant du module terminal avec qui il a eu une liaison et n'a pas besoin de renouveler cette vérification tant que le module convertisseur diffuse des données vers le même module terminal.

REVENDICATIONS

1. Méthode de vérification de la validité d'une clé de réseau (NK) dans un réseau domestique numérique comprenant au moins un dispositif de diffusion (STB, LDVD) et un dispositif de traitement (TV1, TV2, PC), le dispositif de diffusion (STB, LDVD) disposant de données encryptées (DT) à diffuser vers le dispositif de traitement (TV1, TV2, PC), ces données étant accessibles par le dispositif de traitement grâce à une clé de réseau (NK) inconnue du dispositif de diffusion (STB, LDVD), cette méthode comprenant les étapes suivantes:

- transmission par le dispositif de diffusion (STB, LDVD) d'une clé de test (TK) au dispositif de traitement (TV1, TV2, PC),

- calcul d'un cryptogramme (TK_{NK}) résultant de l'encryption de la clé de test (TK) par la clé de réseau (NK) dans le dispositif de traitement (TV1, TV2, PC),

- envoi du cryptogramme (TK_{NK}) au dispositif de diffusion (STB, LDVD),

- détermination par le dispositif de diffusion de la validité de la clé de réseau en comparant le cryptogramme (TK_{NK}) avec une liste de cryptogrammes de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$.

2. Méthode de vérification selon la revendication 1, caractérisé en ce que la clé de test (TK) et la liste des cryptogrammes de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ constituent les données de contrôle et sont générées dans un centre de vérification et transférées dans le dispositif de diffusion.

3. Méthode de vérification selon la revendication 1, caractérisé en ce que la clé de test (TK) est déterminée par le dispositif de diffusion, la liste de cryptogrammes de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est calculée par le dispositif de diffusion sur la base d'une liste de clés de réseau prédéterminée (NK1, NK2, NK3 ...) transmise par un centre de vérification et constituant les données de contrôle, chaque cryptogramme de contrôle (TK_{NKn}) étant le résultat de l'encryption d'une clé de réseau listée (NKn) par la clé de test (TK).

4. Méthode de vérification selon la revendication 3, caractérisé en ce que la clé de test (TK) est générée aléatoirement et sert également de clé de session (SK) pour l'encryption des données encryptées (DT).

5. Méthode de vérification selon les revendications 4 ou 3, caractérisée en ce que le dispositif de diffusion génère au moins deux clés de test (TK1, TK2, TKn) et les transmet au dispositif de traitement (TV1, TV2, PC), qui lui renvoie les cryptogrammes correspondants, le dispositif de diffusion sélectionnant un cryptogramme ($TK1_{NK}$) et sa clé de test (TK1) associée pour les opérations de vérification et un autre cryptogramme ($TK2_{NK}$) et sa clé de test (TK2) associée comme clé de session (SK) pour l'encryption des données (DT).

6. Méthode de vérification selon les revendications 2 à 5, caractérisée en ce que la liste des cryptogrammes de contrôle consiste en une liste noire (black list) $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ contenant des cryptogrammes obtenus par l'encryption de la clé de test (TK) avec des clés de réseau invalides (NK1, NK2, NK3,...).

7. Méthode de vérification selon les revendications 2 à 5, caractérisée en ce que la liste des cryptogrammes de contrôle consiste en une liste blanche (white list) $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ contenant des cryptogrammes $(TK)_{NK}$ obtenus par l'encryption de la clé de test (TK) avec des clés de réseau valides (NK1, NK2, NK3,...).

8. Méthode de vérification selon les revendications 6 ou 7, caractérisée en ce qu'un cryptogramme présent $(TK)_{NK}$ dans la liste noire ou absent de la liste blanche est refusé lors de la comparaison, une signalisation d'erreur invitant l'utilisateur à changer de module terminal (CT) est alors générée.

9. Méthode de vérification selon l'une des revendications précédentes, caractérisée en ce que le dispositif de diffusion comprend un module convertisseur (CC) en charge des opérations de vérification.

10. Méthode de vérification selon l'une des revendications précédentes, caractérisée en ce que le dispositif de traitement comprend un module terminal (CT) stockant la clé de réseau (NK).

11. Méthode de vérification selon la revendication 9, caractérisée en ce que la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est stockée dans une mémoire du dispositif de diffusion (STB, LDVD), la comparaison avec le cryptogramme $(TK)_{NK}$ s'effectuant par ce dispositif.

12. Méthode de vérification selon les revendications 3 à 10, caractérisée en ce que les données de contrôle consistent en une adresse indiquant où la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ peut être téléchargée via Internet au moyen du dispositif de diffusion, ladite liste $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est alors stockée dans la mémoire du dispositif de diffusion (STB, LDVD).

13. Méthode de vérification selon les revendications 3 à 12, caractérisée en ce que le module convertisseur (CC) vérifie l'authenticité de la liste de contrôle au moyen d'une signature sur lesdites données.

14. Méthode de vérification selon la revendication 1 caractérisée en ce que la liste de contrôle $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$ est stockée par un centre de vérification, le dispositif de diffusion transmettant le cryptogramme audit centre pour effectuer la vérification.

15. Méthode de vérification selon les revendications 3 à 11, caractérisée en ce que le dispositif de diffusion est un lecteur de disque DVD, ce disque comprenant d'une part les données encryptées (DT) et d'autre part les données de contrôle.

16. Méthode de vérification selon les revendications 3 à 14, caractérisée en ce que le dispositif de diffusion est un décodeur de télévision à péage recevant les données encryptées et les données de contrôle d'un centre de gestion.

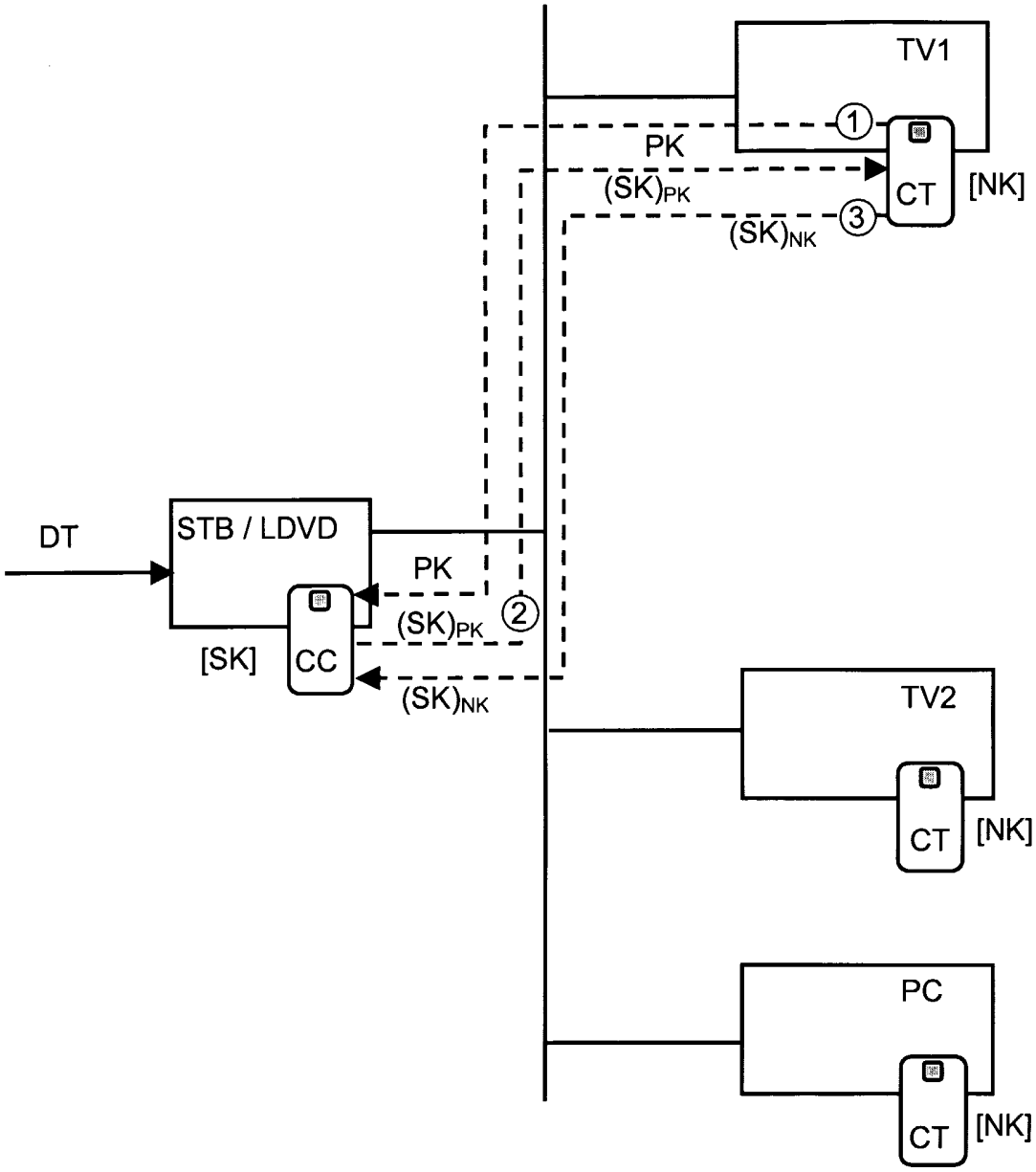

TV1
1
PK
(SK)PK
CT
[NK]
3
(SK)NK
DT
STB / LDVD
PK
2
(SK)PK
[SK]
CC
(SK)NK
TV2
CT
[NK]
PC
CT
[NK]

Fig. 1

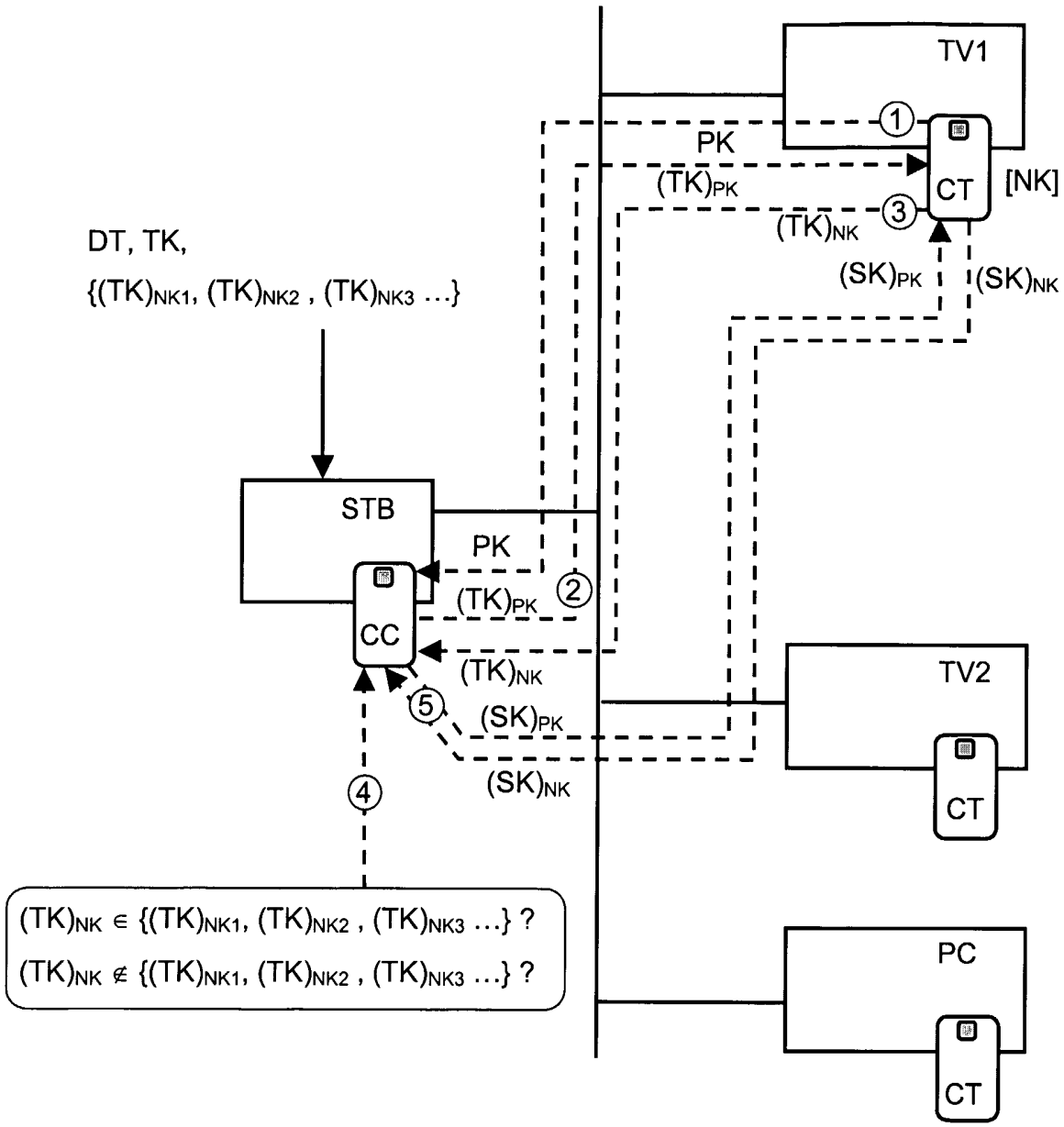

TV1
PK
(TK)PK
CT
[NK]
(TK)NK
DT, TK,
{(TK)NK1, (TK)NK2 , (TK)NK3 ...}
(SK)PK
(SK)NK
STB
PK
(TK)PK
CC
(TK)NK
TV2
(SK)PK
(SK)NK
CT
(TK)NK ∈ {(TK)NK1, (TK)NK2 , (TK)NK3 ...} ?
(TK)NK ∉ {(TK)NK1, (TK)NK2 , (TK)NK3 ...} ?
PC
CT

Fig. 2

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03767

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/10 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 56068 A (THOMSON LICENSING SA ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET M) 21 September 2000 (2000-09-21) page 7, line 8 -page 19, line 20 ---	1-16
A	WO 01 99422 A (SONY ELECTRONICS INC) 27 December 2001 (2001-12-27) page 6, line 12 -page 13, line 22 ---	1-16
A	EP 1 079 628 A (VICTOR COMPANY OF JAPAN) 28 February 2001 (2001-02-28) -----	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 November 2003	03/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

INTERNATIONAL SEARCH REPORT

PCT/IB 03/03767

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0056068 A	21-09-2000	AU 759546 B2	17-04-2003
		AU 3629100 A	04-10-2000
		CA 2366301 A1	21-09-2000
		CN 1343420 T	03-04-2002
		EP 1169856 A1	09-01-2002
		JP 2002539724 T	19-11-2002
		NZ 513903 A	28-09-2001
		WO 0056068 A1	21-09-2000
WO 0199422 A	27-12-2001	AU 1549602 A	02-01-2002
		WO 0199422 A1	27-12-2001
EP 1079628 A	28-02-2001	JP 2001060229 A	06-03-2001
		EP 1079628 A2	28-02-2001

RAPPORT DE RECHERCHE INTERNATIONALE

PCT/IB 03/03767

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/10 H04N7/16 H04N7/167

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 00 56068 A (THOMSON LICENSING SA ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET M) 21 septembre 2000 (2000-09-21) page 7, ligne 8 -page 19, ligne 20 ---	1-16
A	WO 01 99422 A (SONY ELECTRONICS INC) 27 décembre 2001 (2001-12-27) page 6, ligne 12 -page 13, ligne 22 ---	1-16
A	EP 1 079 628 A (VICTOR COMPANY OF JAPAN) 28 février 2001 (2001-02-28) -----	

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
27 novembre 2003	03/12/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

RAPPORT DE RECHERCHE INTERNATIONALE

PCT/IB 03/03767

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0056068 A	21-09-2000	AU 759546 B2	17-04-2003
		AU 3629100 A	04-10-2000
		CA 2366301 A1	21-09-2000
		CN 1343420 T	03-04-2002
		EP 1169856 A1	09-01-2002
		JP 2002539724 T	19-11-2002
		NZ 513903 A	28-09-2001
		WO 0056068 A1	21-09-2000
WO 0199422 A	27-12-2001	AU 1549602 A	02-01-2002
		WO 0199422 A1	27-12-2001
EP 1079628 A	28-02-2001	JP 2001060229 A	06-03-2001
		EP 1079628 A2	28-02-2001