(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 792 482**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **99 04767**

(51) Int Cl[7] : **H 04 L 12/28,** H 04 L 9/18

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.04.99.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.10.00 Bulletin 00/42.

(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 MULTIMEDIA Société anonyme* — FR.

(72) **Inventeur(s) :** QUES FLORENCE, ANDREAUX JEAN PIERRE et FURON TEDDY.

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

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

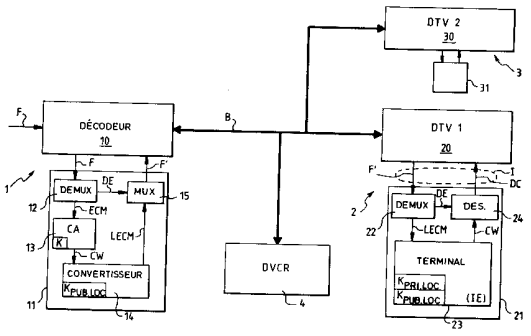
(54) RESEAU NUMERIQUE LOCAL, NOTAMMENT RESEAU NUMERIQUE DOMESTIQUE, ET PROCEDE DE CREATION ET DE MISE A JOUR D'UN TEL RESEAU.

(57) Le réseau numérique local comprend:

- des dispositifs passerelles (1), pour recevoir des données en provenance de l'extérieur du réseau et les émettre en un point du réseau; et
- des dispositifs récepteurs (2, 3), pour recevoir les données circulant dans le réseau et les présenter en un point du réseau.

Les données circulent dans le réseau sous forme chiffrée et tous les dispositifs du réseau utilisent pour le chiffrement et le déchiffrement des données une unique clé: la clé locale du réseau. Préférentiellement, la clé locale du réseau est formée par une paire de clés publique et privée.

Le but de ce réseau est de permettre la copie des données dans le réseau local tout en prévenant les copies pirates à destination d'autres réseaux locaux.



FR 2 792 482 - A1

La présente invention se rapporte d'une manière générale au domaine des réseaux numériques locaux et plus particulièrement au domaine des réseaux numériques domestiques.

Un tel réseau est constitué d'un ensemble de dispositifs reliés entre eux par un bus numérique, par exemple un bus selon la norme IEEE 1394. Il comprend deux types principaux de dispositifs :

- des dispositifs passerelles capables de recevoir des données en provenance de l'extérieur du réseau local et de les émettre en un point du réseau auquel ils sont raccordés, et

- des dispositifs récepteurs, adaptés à recevoir les données circulant dans le réseau pour les présenter en un autre point du réseau auquel ils sont raccordés. Ce deuxième type de dispositif n'a aucun lien avec l'extérieur du réseau local.

Ainsi, si on prend l'exemple d'un réseau numérique domestique destiné à véhiculer des données audio et/ou vidéo dans différentes pièces d'une maison, les dispositifs passerelles sont par exemple des décodeurs numériques recevant des programmes vidéo de l'extérieur du réseau, via une antenne satellite ou via une connexion au câble, ou bien des lecteurs de disques optiques diffusant sur le réseau, sous forme numérique, des données (audio et/ou vidéo) lues sur un disque (le disque contient dans ce cas des données provenant de l'extérieur du réseau). Les dispositifs récepteurs sont par exemple des récepteurs de télévision permettant de visualiser des programmes vidéo reçus du réseau ou, d'une manière plus générale tout type d'appareil capable de convertir une information numérique reçue en signal analogique pour diffuser ce signal vers un utilisateur final.

Un réseau domestique du type mentionné ci-dessus peut également comporter un troisième type de dispositif n'ayant aucun lien avec l'extérieur du réseau et ayant pour fonction d'enregistrer les données circulant dans le réseau. A titre d'exemple d'appareils de ce troisième type, on peut notamment citer les magnétoscopes numériques ou les appareils capables d'enregistrer des disques optiques, du type DVD (l'abréviation "DVD" venant de l'anglais "Digital Versatile Disc" signifiant littéralement : Disque Numérique Polyvalent).

Il est à noter qu'un même appareil peut appartenir à deux, voire trois catégories différentes de dispositifs mentionnés ci-dessus. Par exemple, un appareil enregistreur de disques optiques peut également être capable de lire

des disques pré-enregistrés du commerce et appartenir ainsi en même temps à la première et à la troisième catégorie de dispositifs mentionnés plus haut.

Si on se place du point de vue des fournisseurs de contenu qui fournissent les données en provenance de l'extérieur du réseau local, notamment des prestataires de services diffusant des programmes télévisés payants ou bien des éditeurs de disques optiques par exemple, il est nécessaire d'éviter que ces données transmises ne soient copiées et puissent circuler facilement (par exemple en étant copiées sur un disque optique ou tout autre support d'enregistrement) d'un réseau local à l'autre.

Pour cela, il est connu de transmettre les données sous forme secrète en les chiffrant à l'aide d'algorithmes de cryptographie utilisant des clés qui sont connues au préalable des appareils autorisés à recevoir ces données ou bien qui sont échangées selon des protocoles particuliers sécurisés entre le fournisseur de contenu et ces appareils.

Si on se place maintenant du point de vue d'un utilisateur qui possède un réseau numérique domestique, il est souhaitable que lorsque l'un des appareils du réseau est autorisé à recevoir des données d'un fournisseur de contenu, ces données puissent être transmises à tous les autres appareils du réseau. Ainsi, un utilisateur qui est abonné à un service de télévision payante et reçoit des programmes (transmis sous forme chiffrée) sur un décodeur numérique situé dans son salon (autorisé à les déchiffrer), souhaitera pouvoir regarder ces programmes par exemple sur un téléviseur situé dans sa chambre. D'autre part, il est intéressant pour l'utilisateur d'enregistrer des programmes reçus et de pouvoir ensuite les visualiser sur plusieurs appareils du réseau même lorsqu'il n'est plus abonné au service de télévision payante.

Pour tenir compte à la fois des souhaits des fournisseurs de contenu et des utilisateurs, un but de l'invention est de fournir un moyen pour que des données reçues par un réseau numérique local puissent circuler aisément entre les différents appareils du réseau tout en empêchant leur circulation d'un réseau local à un autre.

A cet effet, l'invention propose un réseau numérique local, notamment un réseau numérique domestique, comprenant au moins un dispositif passerelle, capable de recevoir des données en provenance de l'extérieur dudit réseau et de les émettre en un point du réseau ; et au moins un dispositif récepteur, adapté à recevoir des données circulant dans le réseau

pour les présenter en un point du réseau ; dans lequel les données sont adaptées à ne circuler que sous forme chiffrée. Selon l'invention, tous les dispositifs dudit réseau utilisent pour le chiffrement et le déchiffrement des données circulant dans le réseau une unique clé de chiffrement, spécifique audit réseau : la clé locale du réseau.

Comme chaque réseau local possède sa propre clé locale qui est différente de celle des autres réseaux locaux, toute information qui entrera dans ledit réseau pourra être lue indifféremment par tous les appareils du réseau mais ne pourra pas être copiée pour être lue sur un autre réseau local. Plus exactement, l'information pourra être copiée, sous sa forme chiffrée, mais elle ne pourra pas être relue dans un réseau local différent de celui dans lequel elle a été copiée. Ainsi, l'invention répond à la fois au souhait des fournisseurs de contenu et des utilisateurs.

Selon un aspect préféré de l'invention, les données sont chiffrées en utilisant un système cryptographique à clés publiques. La clé locale du réseau est formée dans ce cas par une paire de clés publique et privée : la clé publique locale et la clé privée locale du réseau.

Préférentiellement, la clé privée locale est connue uniquement par les dispositifs récepteurs raccordés audit réseau.

Selon un mode de réalisation particulier, à un instant donné, un seul dispositif récepteur du réseau est autorisé à transmettre la clé privée locale à un nouveau dispositif récepteur susceptible d'être raccordé audit réseau. Ce dispositif sera appelé ultérieurement le géniteur du réseau.

Ainsi, si ce géniteur est retiré du réseau local, notamment pour créer un réseau local pirate possédant la même clé locale que le réseau local initial, ce dernier ne pourra plus évoluer puisque plus aucun dispositif du réseau initial ne sera capable de transmettre la clé privée locale du réseau à un nouveau dispositif récepteur susceptible d'être raccordé au réseau local initial.

Selon un autre aspect de l'invention, à un instant donné, un dispositif récepteur ne peut se trouver que dans l'un des états suivants :

i) un premier état, l'état vierge, lorsque le dispositif récepteur est raccordé pour la première fois audit réseau ;

ii) un deuxième état, l'état géniteur, dans lequel le dispositif récepteur est autorisé à transmettre la clé privée locale du réseau à tout nouveau dispositif récepteur susceptible d'être raccordé audit réseau ;

iii) un troisième état, l'état stérile, dans lequel le dispositif récepteur n'est plus autorisé à transmettre la clé privée locale du réseau à aucun nouveau dispositif récepteur susceptible d'être raccordé audit réseau.

Un dispositif récepteur ne peut changer d'état que pour passer à un état de rang supérieur, c'est à dire de l'état vierge à l'état géniteur ou de l'état géniteur à l'état stérile, ou encore de l'état vierge à l'état stérile.

Selon un aspect préféré de l'invention, un seul dispositif récepteur du réseau se trouve dans le deuxième état, l'état géniteur : le géniteur du réseau.

Selon un mode de réalisation particulier, à un instant donné, le géniteur du réseau est le dispositif récepteur qui a été raccordé en dernier lieu audit réseau.

Ainsi, la qualité de "géniteur" du réseau est transmise à chaque nouvel appareil raccordé au réseau local. Ceci permet d'éviter qu'un pirate ne puisse, à partir d'un unique dispositif récepteur géniteur, créer en série des réseaux locaux ayant tous les mêmes clés locales.

L'invention concerne également un dispositif récepteur adapté à être raccordé à un réseau numérique tel que décrit ci-dessus et qui, à un instant donné, ne peut se trouver que dans l'un des états qui ont été mentionnés plus haut, à savoir : l'état vierge, l'état géniteur ou l'état stérile, ledit dispositif récepteur n'étant adapté à changer d'état que pour passer à un état de rang supérieur.

Selon un aspect de l'invention, lorsque ledit dispositif récepteur se trouve dans l'état vierge, il possède sa propre paire de clés publique et privée et il est autorisé à recevoir la paire de clés locales d'un réseau auquel il est susceptible d'être raccordé pour les mémoriser à la place de sa propre paire de clés.

Selon un autre aspect de l'invention, lorsque ledit dispositif récepteur se trouve dans l'état stérile, il n'est plus autorisé à recevoir la paire de clés locales d'un réseau auquel il est susceptible d'être raccordé.

Selon un autre aspect de l'invention, le dispositif récepteur comporte un moyen de mémorisation de l'état dans lequel il se trouve, ce moyen de mémorisation étant intégré dans une carte à puce.

Selon encore un autre aspect de l'invention, la paire de clés locales du réseau est contenue dans une carte à puce dont est muni ledit dispositif.

L'invention concerne également un procédé de création et de mise à jour d'un réseau tel que ci-dessus qui seront décrits ultérieurement.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de réalisation particulier, non limitatif, de l'invention faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente un réseau numérique local selon l'invention ;
- la figure 2 illustre un procédé de création d'un réseau numérique tel que celui de la figure 1 ; et
- la figure 3 illustre un procédé pour raccorder un nouveau dispositif récepteur à un réseau numérique local créé selon le procédé de la figure 2 par exemple.

Sur les figures, seuls les éléments indispensables à la compréhension de l'invention et du mode de réalisation particulier qui va être décrit ont été représentés.

Sur la figure 1, on a représenté un réseau numérique domestique comprenant un dispositif passerelle 1, deux dispositifs récepteurs 2 et 3 ainsi qu'un magnétoscope numérique 4, appelé communément DVCR (l'abréviation DVCR étant issue de l'anglais "Digital Video Cassette Recorder" signifiant littéralement : Enregistreur de Cassette Vidéo Numérique). L'ensemble des dispositifs 1, 2, 3 et 4 est raccordé à un bus numérique domestique B qui est par exemple un bus selon la norme IEEE 1394.

Le dispositif passerelle 1 comprend un décodeur numérique 10 doté d'un lecteur de carte à puce muni d'une carte à puce 11. Ce décodeur numérique 10 est raccordé, soit à une antenne satellite, soit à un réseau câblé pour recevoir des programmes vidéo distribués par un prestataire de service. Ces programmes sont reçus dans un flux F de données par exemple au format MPEG-2. D'une manière connue en soi, ils sont transmis sous une forme embrouillée par des mots de contrôles CW, ces mots de contrôle étant eux-mêmes transmis, dans le flux de données F, sous une forme chiffrée à l'aide d'une clé K selon un algorithme de cryptage donné de manière à rester secrets pendant la transmission.

Ainsi, seuls les utilisateurs autorisés par le prestataire de service sont habilités à désembrouiller les données transmises (contre le paiement d'un abonnement par exemple). Pour cela, le prestataire fournit aux utilisateurs autorisés la clé K servant à déchiffrer les mots de contrôle CW. Bien souvent, l'autorisation de recevoir les programmes n'est que temporaire, tant que

l'utilisateur paie son abonnement. La clé K est donc modifiée régulièrement par le prestataire de service.

Grâce à l'invention, et comme on le verra ci-dessous, l'utilisateur pourra néanmoins enregistrer des programmes transmis pendant qu'il est abonné et les relire autant de fois qu'il le souhaite sur son propre réseau, même lorsqu'il ne sera plus abonné. Par contre, comme les données sont enregistrées sous forme embrouillée, elles ne pourront être relue que sur le réseau de l'utilisateur qui les a enregistrées.

Sur la figure 1, le réseau est représenté dans l'état dans lequel il se trouve lorsque tous les appareils ont été raccordés selon les procédés qui seront décrits ultérieurement en liaison avec les figures 2 et 3.

Nous allons maintenant décrire comment sont traitées les données qui sont transmises dans le flux F reçu par le décodeur 10. Comme cela est connu de l'homme de l'art, dans le cas de données transmises selon le format MPEG-2, le flux de données F comprend une succession de paquets de données vidéo, de paquets de données audio et de paquets de données de gestion. Les paquets de données de gestion comprennent notamment des messages de contrôles notés ECM (l'abréviation "ECM" venant de l'anglais "Entitlement Control Message" signifiant littéralement Message de Contrôle des Droits) dans lesquels sont transmis, sous une forme chiffrée à l'aide d'une clé K, les mots de contrôle CW ayant servis à embrouiller les données transmises dans les paquets de données vidéo et audio.

Ce flux de données F est transmis à la carte à puce 11 pour y être traité. Il est reçu par un circuit démultiplexeur (DEMUX) 12, lequel circuit transmet, d'une part à un circuit de contrôle d'accès (CA) 13 les ECM et, d'autre part à un circuit de multiplexage (MUX) 15 les paquets de données vidéo et audio embrouillées, notés DE. Le circuit CA contient la clé K et peut ainsi déchiffrer les mots de contrôle CW qui sont contenus dans les ECM. Le circuit CA transmet ces mots de contrôle CW à un circuit convertisseur 14 qui contient, selon l'invention la clé publique locale du réseau $K_{PUB\ LOC}$. Le convertisseur 14 utilise la clé $K_{PUB\ LOC}$ pour chiffrer les mots de contrôles CW et transmet au circuit de multiplexage 15 ces mots de contrôles, chiffrés à l'aide de la clé publique locale, dans des messages de contrôle notés LECM. Ces messages LECM ont la même fonction que les messages ECM reçus dans le flux de données F initial, à savoir transmettre les mots de contrôle CW, mais dans les messages LECM, les mots de contrôle CW y sont chiffrés à l'aide de

la clé publique locale $K_{PUB\ LOC}$ au lieu d'être chiffrés à l'aide de la clé K du fournisseur de service.

Le circuit de multiplexage 15 transmet ensuite les paquets de données DE et les messages de contrôle convertis LECM dans un flux de données F' qui est reçu par le décodeur 10. C'est ce flux de données F' qui circulera ensuite dans le bus domestique B pour être reçu, soit par un des dispositifs récepteurs 2 ou 3, soit par le magnétoscope numérique 4 pour être enregistré. Selon l'invention, les données circulent donc toujours sous forme chiffrée dans le bus B, et seuls les appareils contenant la clé locale privée $K_{PRI\ LOC}$ du réseau sont capables de déchiffrer les mots de contrôles CW et donc de déchiffrer lesdites données DE. Ceci empêche donc la diffusion vers d'autres réseaux locaux de toute copie effectuée dans le réseau domestique de la figure 1.

Dans l'exemple de la figure 1, les circuits 12 à 15 se trouvent intégrés dans la carte à puce 11 mais dans une variante de réalisation, il est possible de placer les circuits DEMUX et MUX dans le décodeur 10, seuls les circuits 13 et 14 restant intégrés dans la carte à puce. En effet, comme le circuit CA 13 et le convertisseur 14 contiennent des clés de déchiffrement et de chiffrement, ils doivent être intégrés dans un support sécurisé tel qu'une carte à puce.

Le dispositif récepteur 2 comprend un récepteur de télévision numérique (DTV1) 20 doté d'un lecteur de carte à puce muni d'une carte à puce 21. Le récepteur 20 reçoit le flux de données F' provenant, soit du décodeur 10, soit du magnétoscope numérique 4, à travers le bus B. Le flux de données F' est transmis à la carte à puce 21. Il est reçu par un circuit démultiplexeur (DEMUX) 22, lequel transmet, d'une part les paquets de données vidéo et audio embrouillées DE à un circuit de désembrouillage (DES.) 24, et d'autre part les messages de contrôle convertis LECM à un module terminal 23. Le module terminal contient la paire de clés publique ($K_{PUB\ LOC}$) et privée ($K_{PRI\ LOC}$) du réseau. Comme les messages de contrôle LECM contiennent les mots de contrôle CW qui ont été chiffrés à l'aide de la clé publique locale $K_{PUB\ LOC}$ du réseau, le module terminal peut déchiffrer ces mots de contrôle avec l'aide de la clé privée locale $K_{PRI\ LOC}$ pour obtenir les mots de contrôle CW en clair. Ces mots de contrôle CW sont alors transmis au circuit de désembrouillage 24 qui les utilise pour désembrouiller les paquets de données

DE et fournir, en sortie, des paquets de données claires DC au récepteur de télévision 20.

Afin de sécuriser la transmission en dernier lieu des données claires DC entre la carte à puce 21 et les circuits d'affichage du récepteur de télévision 20, l'interface I entre ladite carte à puce et le lecteur de carte du récepteur 20 est par exemple sécurisée selon la norme américaine NRSS (NRSS étant l'acronyme de National Renewable Security Standard) de sécurisation des cartes à puces.

Le deuxième dispositif récepteur 3, comprenant un récepteur de télévision numérique (DTV2) 30 doté d'un lecteur de carte à puce muni d'une carte à puce 31 fonctionne exactement de la même manière que le dispositif récepteur 2 et ne sera pas décrit plus avant.

Grâce au réseau numérique local qui vient d'être décrit, le flux de données F provenant d'un fournisseur de contenu est transformé par le dispositif passerelle qui le reçoit en un flux de données F' grâce à la clé publique locale du réseau $K_{PUB\,LOC}$. Ce flux de données F' contient ainsi des données ayant un format spécifique au réseau local qui ne peuvent être déchiffrées que par les dispositifs récepteurs du réseau local qui contiennent tous la clé privée locale du réseau.

Nous allons maintenant décrire comment le réseau numérique local de la figure 1 est créé et comment est géré le raccordement de nouveaux appareils audit réseau pour garantir que tous les appareils du réseau partagent tous la paire de clés locale unique du réseau.

Sur la figure 2, le procédé de création du réseau numérique représenté à la figure 1 est illustré schématiquement.

Pour créer un réseau numérique selon l'invention, il est nécessaire de raccorder ensemble un dispositif passerelle et un dispositif récepteur.

Sur la figure 2, on suppose qu'au départ, le réseau est créé en raccordant le dispositif passerelle 1 et le dispositif récepteur 2 par l'intermédiaire du bus numérique B. On a représenté les différentes étapes du procédé de création du réseau le long d'un axe des temps t qui est dédoublé de manière à illustrer les échanges qui ont lieu entre les deux dispositifs.

A la première étape 100 du procédé, lorsque l'on raccorde les deux dispositifs ensemble, le dispositif récepteur contient une paire de clés publique K_{PUB2} et privée K_{PRI2} et se trouve, selon l'invention, dans l'état vierge.

L'état du dispositif est mémorisé préférentiellement par un indicateur d'état IE qui est un registre de 2 bits se trouvant dans le module terminal 23 (Figure 1) du dispositif récepteur. Par convention, on suppose que lorsque le dispositif se trouve dans l'état vierge, l'indicateur d'état IE est égal à 00; lorsque le dispositif se trouve dans l'état géniteur, IE = 01 et lorsque le dispositif se trouve dans l'état stérile, IE = 10.

L'indicateur d'état IE est contenu dans un circuit intégré dans une carte à puce pour garantir son inviolabilité.

Lorsqu'un dispositif récepteur est vendu par un fabricant, il doit pouvoir être raccordé à n'importe quel réseau numérique local, du type de l'invention, existant. Il doit également être capable d'être raccordé à un dispositif passerelle pour créer un nouveau réseau. C'est pourquoi, tout dispositif récepteur qui est fabriqué selon l'invention comporte systématiquement une paire de clés publique et privée, cette paire de clés étant unique et différente d'un dispositif à l'autre, ceci afin de garantir le fait que chaque réseau local créé selon l'invention possède également une paire de clés unique. De plus, afin de garantir la sécurité des échanges, toutes les paires de clés privées / publiques utilisées sont certifiées selon une méthode connue de l'homme de l'art.

Les dispositifs passerelles, par contre, sont fabriqués et vendus sans contenir aucune clé de chiffrage/déchiffrage. Ils contiennent néanmoins préférentiellement un circuit convertisseur selon l'invention (contenu dans une carte à puce), tel que décrit précédemment en liaison avec la figure 1, qui est capable de mémoriser une clé locale de réseau auquel ils sont susceptibles d'être raccordés.

En se reportant à nouveau à la figure 2, l'étape 101 du procédé consiste, pour le dispositif récepteur 2, à envoyer sur le bus B sa clé publique K_{PUB2} à destination de tous les dispositifs passerelles susceptible d'être raccordé au bus B, en l'espèce le dispositif passerelle 1.

L'étape 102 consiste, pour le dispositif passerelle 1, à recevoir la clé publique K_{PUB2} et à la mémoriser en tant que nouvelle clé publique locale du réseau ($K_{PUB\,LOC} = K_{PUB2}$).

A l'étape 103, le dispositif passerelle 1 envoie sur le bus B un signal de changement d'état à destination du dispositif récepteur 2. Cette étape a pour but d'indiquer au dispositif récepteur 2 qu'il est le premier à être raccordé au réseau et qu'il doit donc devenir le géniteur du réseau, c'est à dire le seul

dispositif récepteur autorisé à transmettre sa clé privée K_{PRI2} (qui devient la clé privée locale du réseau $K_{PRI\,LOC}$) à tout nouveau dispositif récepteur susceptible d'être raccordé au réseau.

L'étape 104 consiste donc, pour le dispositif récepteur 2 à recevoir le signal de changement d'état et à modifier son indicateur d'état pour passer à l'état géniteur (IE = 01).

A la fin du procédé, on dispose donc d'un réseau numérique local conforme à l'invention qui comprend une clé publique locale $K_{PUB\,LOC}$ unique (égale à la clé publique initiale K_{PUB2} du dispositif récepteur 2), connue des deux dispositifs du réseau, et une clé privée locale $K_{PRI\,LOC}$ unique connue uniquement du dispositif récepteur 2. Le réseau comporte également, conformément à l'invention, un dispositif récepteur géniteur qui est capable de le faire évoluer en permettant le raccordement de nouveaux dispositifs récepteurs.

Le procédé de raccordement d'un nouveau dispositif récepteur, en l'espèce le dispositif récepteur 3, au réseau créé conformément au procédé de la figure 2, va maintenant être décrit en liaison avec la figure 3.

A la première étape 200, 200', 200" du procédé, qui consiste à raccorder le dispositif récepteur 3 au réseau local existant par l'intermédiaire du bus numérique B, le dispositif récepteur 3 contient sa propre paire de clés publique K_{PUB3} et privée K_{PRI3} et il se trouve dans l'état vierge (IE = 00). Les dispositifs passerelle 1 et récepteur 2 se trouvent respectivement dans le même état qu'à la fin du procédé de la figure 2, c'est à dire que le dispositif passerelle 1 contient la clé publique locale du réseau $K_{PUB\,LOC}$ et que le dispositif récepteur est le géniteur du réseau (IE = 01) et contient la paire de clés locales ($K_{PUB\,LOC}$, $K_{PRI\,LOC}$) du réseau.

La seconde étape 201 consiste, pour le dispositif récepteur 3, à envoyer sur le bus B sa clé publique K_{PUB3} à destination de tous les dispositifs passerelles susceptibles d'être raccordés au bus B, en l'espèce le dispositif passerelle 1. Cette étape est la même que l'étape 101 (Figure 2) du procédé de création.

L'étape 202 consiste, pour le dispositif passerelle 1, à recevoir la clé publique K_{PUB3} et à vérifier s'il contient déjà une clé publique ou non (VERIF. PRESENCE $K_{PUB\,LOC}$).

En cas de vérification positive, ce qui est le cas en l'espèce, l'étape suivante 203 consiste, pour le dispositif passerelle 1, à envoyer la clé publique locale $K_{PUB\ LOC}$ sur le bus B à destination du nouveau dispositif récepteur 3.

A l'étape 204, le dispositif récepteur 3 reçoit la clé publique locale $K_{PUB\ LOC}$ et il la mémorise, préférentiellement dans son module terminal.

L'étape suivante 205 consiste, pour le dispositif récepteur 3, à envoyer un signal sur le bus B, adressé à tous les dispositifs récepteurs du réseau, sous la forme d'un message (GENITEUR ?) demandant au dispositif géniteur du réseau de lui répondre.

A l'étape 206, le dispositif géniteur du réseau, en l'espèce le dispositif récepteur 2, reçoit ce message et, une fois la communication établie de manière sûre entre les dispositifs récepteurs 2 et 3, il change d'état pour passer à l'état stérile (IE = 10).

L'étape 207 consiste ensuite, pour le dispositif récepteur 2, à envoyer la clé privée locale du réseau sous une forme chiffrée ($E(K_{PRI\ LOC})$) déchiffrable par le dispositif récepteur 3. Notamment, cette transmission sécurisée de la clé privée locale entre les dispositifs récepteurs 2 et 3 peut être effectuée en utilisant la clé publique initiale K_{PUB3} du dispositif récepteur 3 pour chiffrer la clé privée locale, le dispositif récepteur 3 étant capable de déchiffrer ce message à l'aide de sa clé privée K_{PRI3}. La clé K_{PUB3} est par exemple transmise au dispositif récepteur 2 lors de l'étape 205.

A l'étape 208, le dispositif récepteur 3 reçoit et déchiffre la clé privée locale et il la mémorise, préférentiellement dans son module terminal, intégré dans la carte à puce 31 (Figure 1).

L'étape 209 consiste, pour le dispositif récepteur 3, à envoyer un signal d'accusé de réception de la clé privée locale (ACCUSE-RECEPTION ($K_{PRI\ LOC}$)) sur le bus B à destination du dispositif récepteur 2.

A l'étape 210, le dispositif récepteur 2 reçoit ce signal d'accusé de réception et envoie, en réponse , un signal de changement d'état au nouveau dispositif récepteur 3 et à l'étape 211, le dispositif récepteur 3 reçoit ce signal et change d'état pour devenir le nouveau géniteur du réseau (IE = 01).

Comme le dispositif récepteur 2 se trouve désormais à l'état stérile, il n'est plus autorisé à transmettre la clé publique locale du réseau à un autre dispositif récepteur. Ceci permet d'éviter que ce dispositif 2 soit enlevé du réseau pour créer un autre réseau local pirate possédant la même paire de clés locales que le réseau qui vient d'être décrit.

A la fin du procédé, il y a donc deux dispositifs récepteurs 2 et 3 et un dispositif passerelle 1 raccordés au réseau local. Ils partagent tous la paire de clé locale du réseau $K_{PUB\ LOC}$, $K_{PRI\ LOC}$. Il y a toujours un unique géniteur dans le réseau qui est le dispositif récepteur qui a été raccordé en dernier lieu au réseau.

Le raccordement d'un nouveau dispositif passerelle au réseau local est quant à lui beaucoup plus simple car tout dispositif passerelle conforme à l'invention est vendu sans contenir de clé. On peut notamment envisager que lorsqu'un nouveau dispositif passerelle est connecté au réseau, il envoie un message sur le bus B demandant à recevoir la clé publique du réseau. On peut prévoir ensuite que, soit le premier dispositif de réseau qui reçoit ce message, soit seulement le dispositif géniteur, envoie, en réponse à ce message, la clé publique du réseau au nouveau dispositif passerelle.

REVENDICATIONS

1. Réseau numérique local, notamment réseau numérique domestique, comprenant :

- au moins un dispositif passerelle (1), capable de recevoir des données en provenance de l'extérieur dudit réseau et de les émettre en un point du réseau ; et

- au moins un dispositif récepteur (2, 3), adapté à recevoir des données circulant dans le réseau pour les présenter en un point du réseau ;

dans lequel les données sont adaptées à ne circuler que sous forme chiffrée, caractérisé en ce que tous les dispositifs dudit réseau utilisent pour le chiffrement et le déchiffrement des données circulant dans le réseau une unique clé de chiffrement, spécifique audit réseau : la clé locale ($K_{PUB\ LOC}$, $K_{PRI\ LOC}$) du réseau.

2. Réseau numérique selon la revendication 1, dans lequel les données sont chiffrées en utilisant un système cryptographique à clés publiques, caractérisé en ce que la clé locale du réseau est formée par une paire de clés publique et privée : la clé publique locale ($K_{PUB\ LOC}$) et la clé privée locale ($K_{PRI\ LOC}$) du réseau.

3. Réseau numérique selon la revendication 2, caractérisé en ce que seuls les dispositifs récepteurs (2, 3) raccordés audit réseau contiennent la clé privée locale ($K_{PRI\ LOC}$).

4. Réseau numérique selon la revendication 3, caractérisé en ce qu'à un instant donné, un seul dispositif récepteur du réseau est autorisé à transmettre la clé privée locale ($K_{PRI\ LOC}$) à un nouveau dispositif récepteur susceptible d'être raccordé audit réseau.

5. Réseau numérique selon la revendication 3, caractérisé en ce qu'à un instant donné, un dispositif récepteur ne peut se trouver que dans l'un des états suivants :

i) un premier état, l'état vierge (IE = 00), lorsque le dispositif récepteur est raccordé pour la première fois audit réseau ;

ii) un deuxième état, l'état géniteur (IE = 01), dans lequel le dispositif récepteur est autorisé à transmettre la clé privée locale du réseau à tout nouveau dispositif récepteur susceptible d'être raccordé audit réseau ;

iii) un troisième état, l'état stérile (IE = 10), dans lequel le dispositif récepteur n'est plus autorisé à transmettre la clé privée locale du réseau à aucun nouveau dispositif récepteur susceptible d'être raccordé audit réseau,

un dispositif récepteur n'étant adapté à changer d'état que pour passer à un état de rang supérieur.

6. Réseau numérique selon la revendication 5, caractérisé en ce qu'un seul dispositif récepteur du réseau se trouve dans le deuxième état, l'état géniteur : le géniteur du réseau.

7. Réseau numérique selon la revendication 6, caractérisé en ce qu'à un instant donné, le géniteur du réseau est le dispositif récepteur qui a été raccordé en dernier lieu audit réseau.

8. Dispositif récepteur adapté à être raccordé à un réseau numérique selon l'une des revendications 2 à 7, caractérisé en ce qu'à un instant donné, ledit dispositif récepteur ne peut se trouver que dans l'un des états suivants :

i) un premier état, l'état vierge (IE = 00), lorsque le dispositif récepteur est raccordé pour la première fois à un réseau ;

ii) un deuxième état, l'état géniteur (IE = 01), dans lequel le dispositif récepteur est autorisé à transmettre la clé privée locale du réseau à tout nouveau dispositif récepteur susceptible d'être raccordé audit réseau ;

iii) un troisième état, l'état stérile (IE = 10), dans lequel le dispositif récepteur n'est plus autorisé à transmettre la clé privée locale du réseau à aucun nouveau dispositif récepteur susceptible d'être raccordé audit réseau,

ledit dispositif récepteur n'étant adapté à changer d'état que pour passer à un état de rang supérieur.

9. Dispositif récepteur selon la revendication 8, caractérisé en ce que lorsque ledit dispositif récepteur se trouve dans l'état vierge, il contient sa propre paire de clés publique et privée et il est autorisé à recevoir la paire de clés locales d'un réseau auquel il est susceptible d'être raccordé pour les mémoriser à la place de sa propre paire de clés.

10. Dispositif récepteur selon l'une des revendications 8 ou 9, caractérisé en ce que lorsque ledit dispositif récepteur se trouve dans l'état stérile, il n'est plus autorisé à recevoir la paire de clés locales d'un réseau auquel il est susceptible d'être raccordé.

11. Dispositif récepteur selon l'une des revendication 8 à 10, caractérisé en ce qu'il comporte un moyen de mémorisation (IE) de l'état dans lequel se trouve ledit dispositif récepteur, ce moyen de mémorisation étant intégré dans une carte à puce (21, 31).

12. Dispositif récepteur selon l'une des revendications 8 à 11, caractérisé en ce que la paire de clés locales du réseau est contenue dans une carte à puce (21, 31) dont est muni ledit dispositif.

13. Procédé de création d'un réseau numérique local selon l'une des revendications 5 à 7, caractérisé en ce qu'il comprend les étapes consistant successivement :

a) à raccorder ensemble par l'intermédiaire d'un bus numérique (B) un dispositif passerelle (1) et un dispositif récepteur (2) se trouvant dans l'état vierge et contenant une paire de clés publique (K_{PUB2}) et privée (K_{PRI2}) ;

b) pour le dispositif récepteur (2), à envoyer sur ledit bus (B) sa clé publique (K_{PUB2}) ;

c) pour le dispositif passerelle (1), à recevoir ladite clé publique (K_{PUB2}), à la mémoriser en tant que nouvelle clé publique locale du réseau ($K_{PUB\ LOC} = K_{PUB2}$) et à envoyer sur ledit bus un signal de changement d'état du dispositif récepteur ;

d) pour le dispositif récepteur (2), à recevoir ledit signal de changement d'état et à passer à l'état géniteur (IE = 01).

14. Procédé pour raccorder un nouveau dispositif récepteur (3) se trouvant dans l'état vierge (IE = 00) et contenant une paire de clés publique (K_{PUB3}) et privée (K_{PRI3}) à un réseau numérique local selon l'une des revendications 5 à 7, caractérisé en ce qu'il comprend les étapes consistant successivement :

e) à raccorder le nouveau dispositif récepteur (3) audit réseau local par l'intermédiaire d'un bus numérique (B) ;

f) pour le nouveau dispositif récepteur (3), à envoyer sur ledit bus sa clé publique (K_{PUB3}) ;

g) pour au moins un des dispositifs passerelle (1) dudit réseau, à recevoir la clé publique (K_{PUB3}) du nouveau dispositif récepteur, à vérifier que ledit dispositif passerelle contient déjà une clé publique, la clé publique locale ($K_{PUB\ LOC}$) du réseau, et en cas de vérification positive, à envoyer sur le bus (B) ladite clé publique locale du réseau;

h) pour le nouveau dispositif récepteur (3), à recevoir la clé publique locale ($K_{PUB\ LOC}$) du réseau, à la mémoriser et à envoyer sur ledit bus un signal, adressé à tous les dispositifs récepteurs du réseau, de demande de réponse du dispositif récepteur se trouvant dans l'état géniteur;

i) pour le dispositif récepteur géniteur du réseau (2), à recevoir ledit signal de demande de réponse, à passer à l'état stérile (IE = 10), et à envoyer en réponse au nouveau dispositif récepteur (3) la clé privée locale ($K_{PRI\ LOC}$) du réseau sous une forme chiffrée déchiffrable par le nouveau dispositif récepteur (3) ;

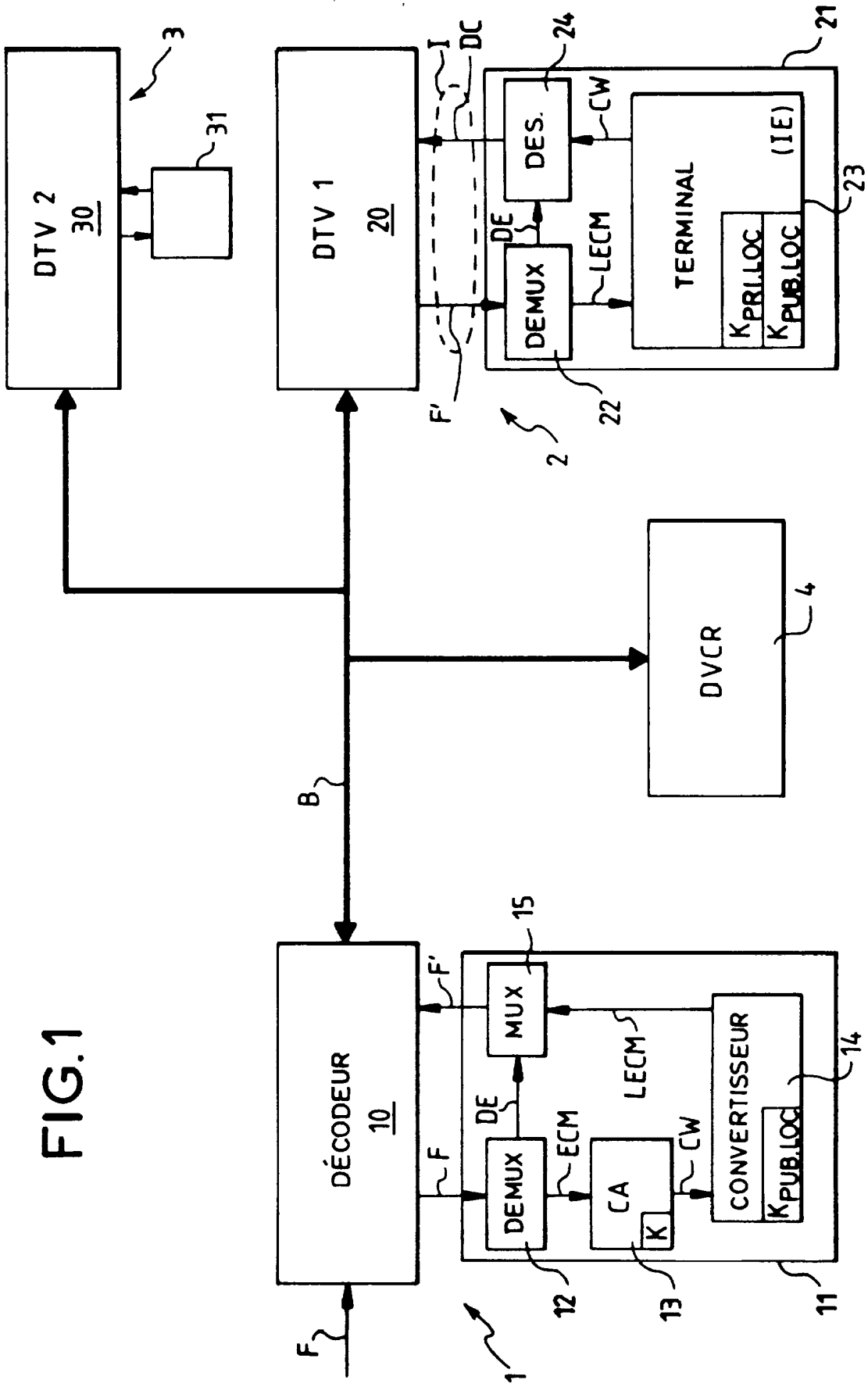
j) pour le nouveau dispositif récepteur (3), à recevoir ladite clé privée locale ($K_{PRI\ LOC}$) du réseau, à la mémoriser et à envoyer un signal d'accusé de réception au dispositif récepteur anciennement géniteur du réseau (2) ;

k) pour le dispositif récepteur anciennement géniteur du réseau (2), à recevoir ledit signal d'accusé de réception et à envoyer au nouveau dispositif récepteur (3) un signal de changement d'état ;

l) pour le nouveau dispositif récepteur (3), à recevoir ledit signal de changement d'état et à passer à l'état géniteur (IE = 01).

2792482

FIG.1



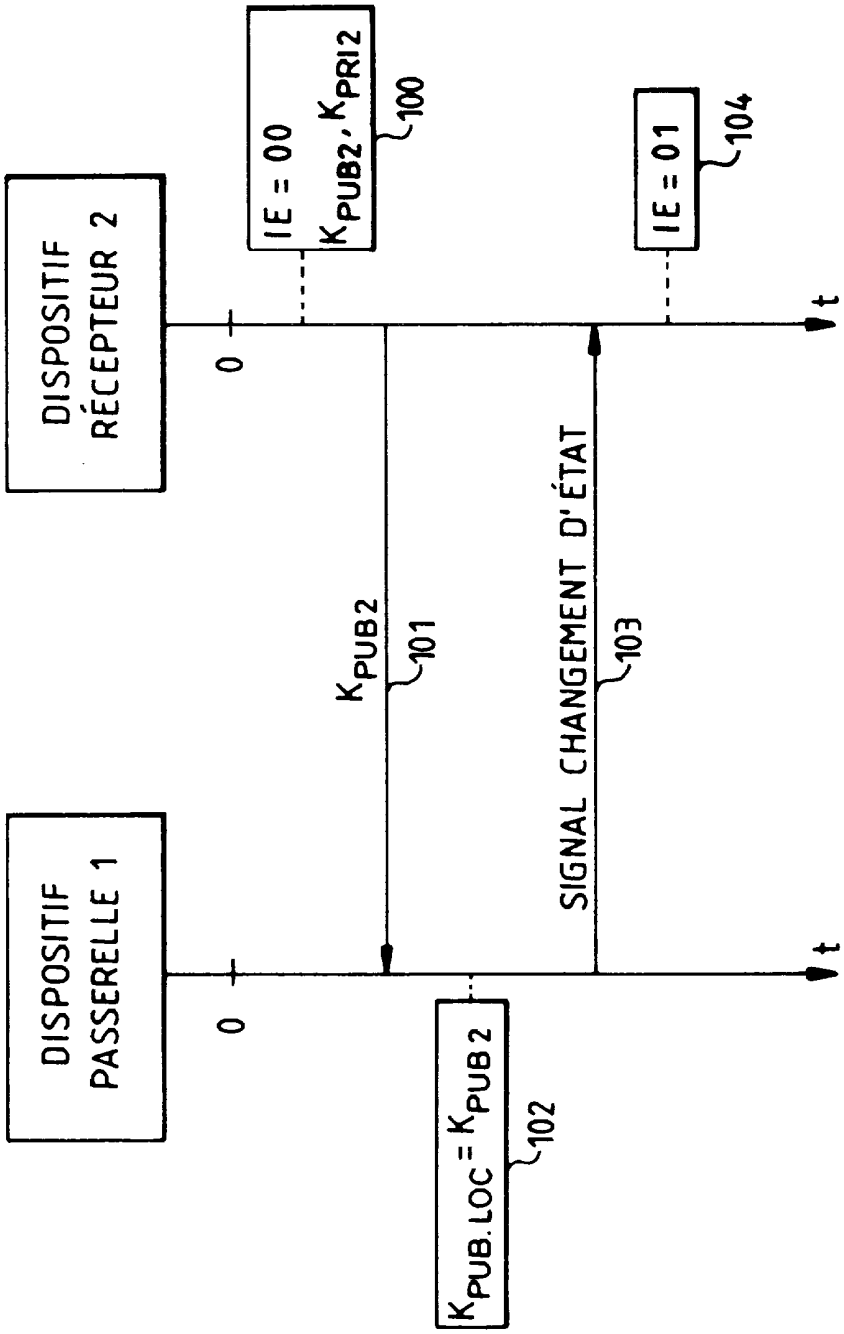

DISPOSITIF RÉCEPTEUR 2
DISPOSITIF PASSERELLE 1
0
0
IE = 00
K_{PUB2}, K_{PRI2}
100
IE = 01
104
K_{PUB2}
101
SIGNAL CHANGEMENT D'ÉTAT
103
$K_{PUB.LOC} = K_{PUB2}$
102
t
t

FIG.2

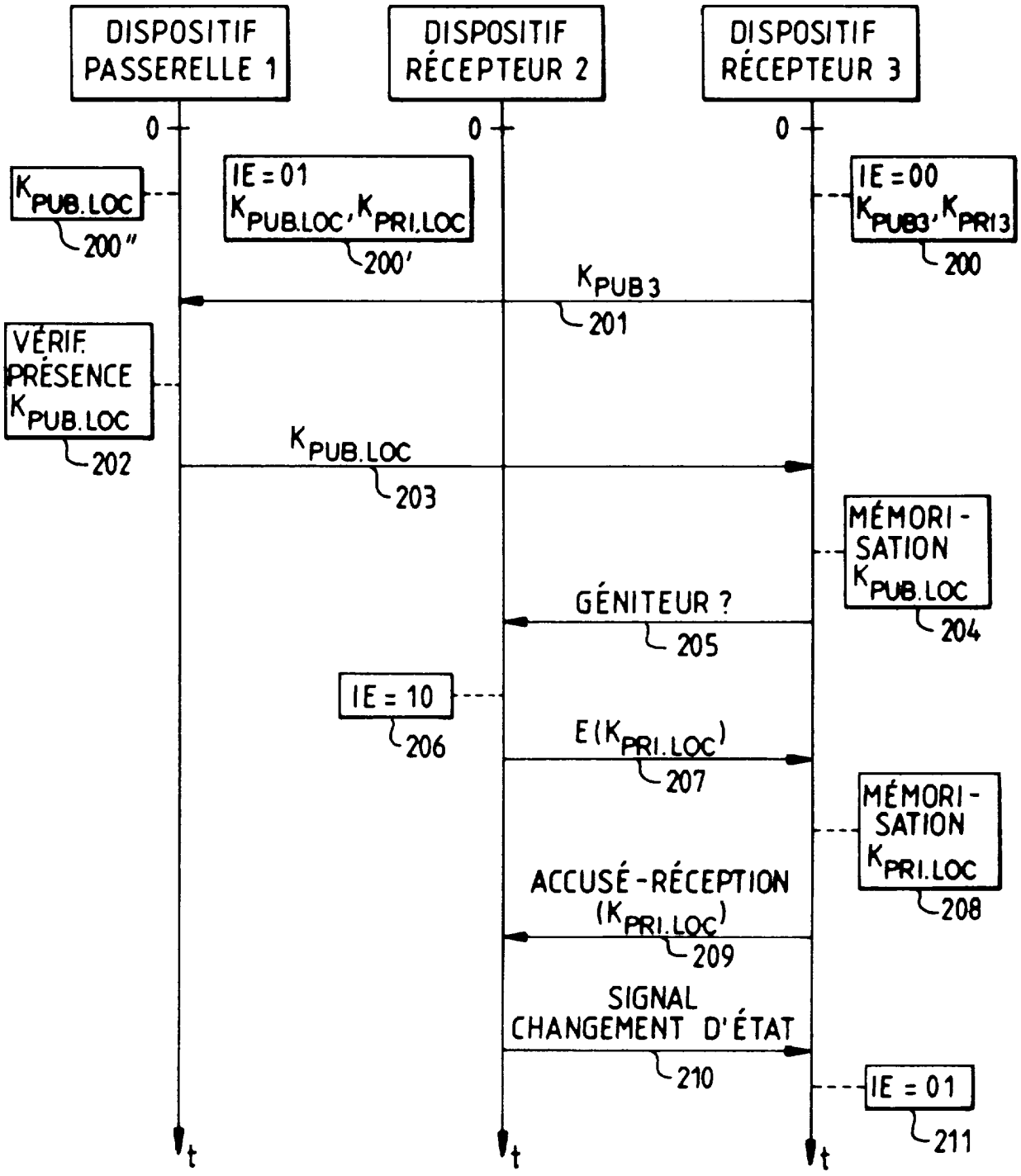

DISPOSITIF PASSERELLE 1
DISPOSITIF RÉCEPTEUR 2
DISPOSITIF RÉCEPTEUR 3
0
0
0
$K_{PUB.LOC}$
200"
IE = 01
$K_{PUB.LOC}$, $K_{PRI.LOC}$
200'
IE = 00
K_{PUB3}, K_{PRI3}
200
K_{PUB3}
201
VÉRIF. PRÉSENCE $K_{PUB.LOC}$
202
$K_{PUB.LOC}$
203
MÉMORI-SATION $K_{PUB.LOC}$
204
GÉNITEUR ?
205
IE = 10
206
$E(K_{PRI.LOC})$
207
MÉMORI-SATION $K_{PRI.LOC}$
208
ACCUSÉ-RÉCEPTION ($K_{PRI.LOC}$)
209
SIGNAL CHANGEMENT D'ÉTAT
210
IE = 01
211
t
t
t

FIG.3

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

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

2792482
N° d'enregistrement national

FA 575559
FR 9904767

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X	EP 0 382 296 A (N.V. PHILIPS GLOEILAMPENFABRIEKEN) 16 août 1990 (1990-08-16)	1
A	* colonne 2, ligne 2-37 * * colonne 3, ligne 12-29 * * colonne 4, ligne 40-44 * * colonne 4, ligne 55 - colonne 5, ligne 34 * * colonne 6, ligne 57 - colonne 7, ligne 5 * * colonne 8, ligne 56 - colonne 9, ligne 42 *	2-14
A	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 octobre 1995 (1995-10-25) * page 2, ligne 22-41 * * page 3, ligne 31-34 * * page 3, ligne 47-50 * * page 7, ligne 34-57 * * page 9, ligne 46-57 *	1-14

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)

H04L
H04N

1

Date d'achèvement de la recherche	Examinateur
25 janvier 2000	Lázaro Lõpez, M.L.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
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 03.82 (P04C13)