(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 751 154**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **96 08916**

(51) Int Cl[6] : **H 04 L 9/32**, H 04 L 9/28

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 15.07.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 16.01.98 Bulletin 98/03.

(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) :** *SCHLUMBERGER INDUSTRIES SA SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** BRAHAMI LIONEL, OCQUET NATHALIE, DIETRICH CHRISTIAN et PHAN LY THANH.

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

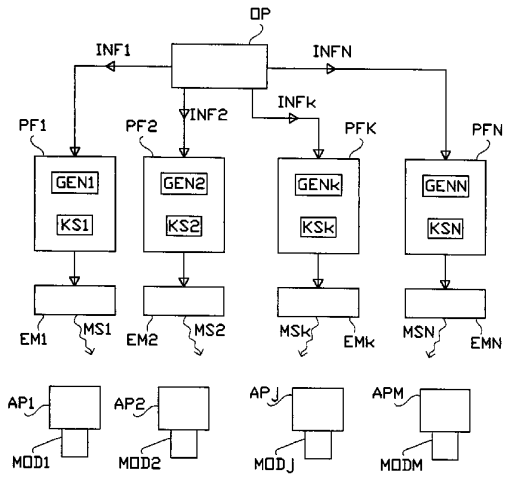
(74) **Mandataire :** SCHLUMBERGER INDUSTRIES.

(54) SYSTEME DE DIVERSIFICATION D'INFORMATIONS DANS UN RESEAU DE DISTRIBUTION DE PRODUITS OU DE SERVICES.

(57) Système de diversification d'informations transmises par un réseau vers des appareils délivrant des produits ou des services.

Selon l'invention, le réseau comprend une pluralité de plates-formes (PFk) aptes, chacune, à élaborer des messages (MSk) comportant une donnée (DDk) de diversification des informations (INFk) à transmettre, fournie par un générateur (GENk) de données de diversification, les appareils (APPj) comprennent, chacun, un module (MODj) de contrôle d'accès.

Application aux systèmes de transactions électroniques sécurisées, tels que les systèmes de paiement, les réseaux de téléphonie mobile, les réseaux informatiques, les systèmes de télévision à péage.



FR 2 751 154 - A1

2751154

SYSTEME DE DIVERSIFICATION D'INFORMATIONS DANS UN RESEAU DE DISTRIBUTION DE PRODUITS OU DE SERVICES

La présente invention concerne un système de diversification d'informations transmises par un réseau vers des appareils délivrant des produits ou des services.

L'invention trouve une application particulièrement avantageuse dans le domaine des systèmes de transactions électroniques sécurisées, tels que les systèmes de paiement, les réseaux de téléphonie mobile, les réseaux informatiques, les systèmes de télévision à péage, etc.

Ces réseaux de distribution de produits ou de services comprennent une ou plusieurs plates-formes, appelées aussi têtes de réseau, qui sont essentiellement des systèmes informatiques, PC ou gros ordinateurs, chargés d'élaborer, sur ordre de l'opérateur gestionnaire, des messages qui sont transmis, via un dispositif émetteur, aux divers appareils connectés au réseau considéré.

Ces messages peuvent comporter des informations relatives par exemple à l'autorisation pour l'utilisateur de l'appareil destinataire d'accéder à tel ou tel produit ou service comme un service de paiement, une communication téléphonique, l'accès à des fonctions informatiques (messagerie ou téléchargement d'un logiciel) ou à des programmes de télévision cryptée. A l'inverse, lesdites plates-formes peuvent également composer des messages de suppression de droits d'accès préalablement accordés, ou encore de modifier ces droits, notamment par leur extension à de nouveaux produits ou services proposés par le réseau à ses abonnés.

Les messages émis par les plates-formes sont captés par les récepteurs des appareils puis transmis à un module de sécurité présent dans chaque appareil et dont le but est de contrôler l'accès par l'appareil correspondant aux produits ou services distribués par le réseau.

Les modules de sécurité, qui seront appelés modules de contrôle d'accès dans la suite de ce mémoire, peuvent être

détachables, comme une carte à mémoire électronique ou similaire, ou non-détachables de l'appareil comme un composant de sécurité.

On comprendra que les messages provenant des plates-formes doivent absolument être sécurisés du fait même qu'ils permettent de créer, de modifier ou de supprimer des droits d'accès des appareils aux divers produits ou services du réseau.

A cet effet, on a recours à des systèmes de diversification qui ont pour objet d'empêcher, par exemple, qu'un message d'autorisation d'accès préalablement enregistré ne soit retransmis à l'appareil par un émetteur pirate après que l'accès ait été supprimé. De même, il y a lieu d'éviter tout détournement vers un appareil d'un message destiné à un autre appareil.

Un système de diversification connu consiste à inclure dans les messages élaborés par les plates-formes une donnée de diversification, propre à chaque message, qui, mélangée à une clé secrète propre à chaque plate-forme à l'aide d'un algorithme de cryptage, permet d'établir un certificat, ou signature, du message. Notons que pour éviter le détournement vers un appareil d'un message destiné à un autre appareil, il suffit pour composer le certificat d'utiliser non pas la clé secrète de la plate-forme mais une clé secrète diversifiée résultant du mélange par un autre algorithme de cryptage de la clé secrète de la plate-forme et d'un numéro d'identification du module de contrôle d'accès destinataire.

Le module de contrôle d'accès de l'appareil destinataire du message connaissant également la clé secrète de la plate-forme ainsi que l'algorithme de cryptage, peut à son tour reconstituer le certificat et le comparer à celui qui a été émis. Si la comparaison est positive, on en conclut que l'émetteur qui a transmis le message possède bien la clé secrète et que le message n'a pas été modifié.

Comme dans ce système de diversification, la donnée de diversification doit être propre à chaque message, les plates-formes, lorsqu'elles sont multiples, doivent être synchronisées, soit en étant reliées à un générateur de données de diversification unique qui distribue sur demande des plates-formes les données

de diversification, soit en ayant chacune son propre générateur avec compte-rendu aux autres générateurs à chaque message.

La donnée de diversification peut être un nombre aléatoire fourni par un générateur de nombres aléatoires. Dans ce cas, et pour éviter toute duplication de messages, les modules de contrôle d'accès doivent pouvoir stocker tous les nombres aléatoires des messages qu'ils reçoivent, ceci afin de pouvoir vérifier qu'un nombre aléatoire reçu ne l'a pas déjà été précédemment, ce qui signifierait que le message a déjà été reçu. Pour cela, il faudrait réserver dans le module de contrôle d'accès un espace très important. Par exemple, avec des nombres aléatoires de 4 octets par message, on atteint pour 1000 messages 4000 octects de réservation, soit la moitié de l'espace mémoire usuellement disponible dans les modules de contrôle d'accès.

Pour remédier à cet inconvénient, on a recours à une donnée de diversification constituée par le numéro d'ordre du message émis, généré par un compteur de messages qui s'incrémente d'une unité à chaque message émis par l'ensemble des plates-formes du réseau. Il suffit alors pour les modules de contrôle d'accès de stocker le numéro du dernier message reçu et de vérifier que ce numéro est bien postérieur au précédent reçu.

Toutefois, ce système présente l'inconvénient qu'en cas d'arrêt non contrôlé, il faudrait relancer le compteur à partir du nombre 1, ce qui conduirait à rejeter tout nouveau message car considéré comme antérieur et donc déjà reçu. Dans cette hypothèse, un moyen de sauvegarde serait pour chaque module de contrôle d'accès de stocker les numéros de tous les messages reçus, mais se pose alors le problème du coût de la sauvegarde.

Aussi, un premier problème technique à résoudre par l'objet de la présente invention est de proposer un système de diversification d'informations transmises par un réseau vers des appareils délivrant des produits ou des services, ledit réseau comprenant une pluralité de plates-formes aptes, chacune, à élaborer des messages comportant une donnée de diversification des informations à transmettre, fournie par un générateur de données de diversification, et lesdits appareils comprenant,

chacun, un module de contrôle d'accès, système qui permettrait d'éliminer les contraintes liées à la synchronisation des plates-formes entre elles.

La solution à ce premier problème technique consiste, selon la présente invention, en ce que chaque plate-forme dispose d'un générateur de données de diversification autonome, et en ce que ledit module de contrôle d'accès de chaque appareil comporte, d'une part, des moyens de stockage de la donnée de diversification transmise avec le dernier message fourni par chaque plate-forme, et, d'autre part, des moyens de comparaison de chaque nouvelle valeur de la donnée de diversification reçue de chaque plate-forme avec au moins la valeur précédente.

Ainsi, les modules de contrôle d'accès du réseau disposent d'autant de moyens de stockage que de plates-formes, chaque moyen de stockage étant affecté à un générateur de données de diversification d'une plate-forme.

Il résulte de l'autonomie des générateurs de données de diversification que les plates-formes n'ont plus besoin d'être synchronisées, d'où une simplification extrême du réseau qui n'est pas remise en cause par l'augmentation limitée du nombre de moyens de stockage des modules de contrôle d'accès.

Un autre problème technique que se propose de résoudre également l'invention est de permettre aux plates-formes de redevenir fonctionnelles après une défaillance quelconque tout en conservant une sécurité maximum.

A cet effet, il est prévu, selon la présente invention, que ledit générateur de données de diversification est une base de temps universel, ladite donnée de diversification étant par exemple la date d'émission du message par rapport à une origine t_0 arbitraire connue.

En cas de panne d'une plate-forme, l'origine t_0 n'étant pas perdue, le système pourra repartir à une date qui sera postérieure à la date du dernier message fournie par ladite plate-forme. Aucune disposition particulière de sauvegarde n'est donc à envisager.

Enfin, dans le but de réduire la taille des moyens de stockage des modules de contrôle d'accès, l'invention prévoit que ladite base de temps a une durée t_{max} limitée à au moins la durée de vie desdits modules de contrôle d'accès. En d'autres termes, au lieu de dimensionner les moyens de stockage sur la durée de vie du réseau, 40 ans par exemple, on les dimensionne légèrement supérieurs à la durée de vie des modules, 10 ans par exemple.

Mais alors, se pose le problème des modules qui auront été mis en service peu de temps avant t_{max} car, par hypothèse, ils ne pourront plus accepter de messages après cette date, la base de temps étant remise à zéro et les nouveaux messages présentant de ce fait une date apparente antérieure.

Pour résoudre cette difficulté, l'invention fournit un moyen de discrimination consistant en ce que chaque module de contrôle d'accès stocke en mémoire la date t_1 d'émission du premier message fourni par chaque plate-forme, et en ce que la validation d'un message émis à la date t_{n+1}, s'effectue par comparaison avec la date t_1 et la date t_n d'émission du message précédent :

- si $t_n > t_1$ le message à t_{n+1} est validé si $t_n + 1$ n'est pas compris dans $]t_1, t_n[$,
- si $t_n < t_1$ le message à t_{n+1} est validé si t_{n+1} est compris dans $]t_n, t_1[$

De cette manière, les modules de contrôle d'accès pourront être utilisés pendant toute la durée t_{max} quelle que soit la date de leur mise en service.

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est une vue schématique d'un réseau de distribution de produits ou de services muni d'un système de diversification d'informations conforme à l'invention.

La figure 2 est un schéma représentant la constitution d'un message fourni par les plates-formes du réseau de la figure 1.

La figure 3 est un schéma donnant la structure des modules de contrôle d'accès des appareils du réseau de la figure 1.

La figure 4 est un chronogramme d'une base de temps utilisée comme générateur de données de diversification des plates-formes de la figure 1.

La vue schématique de la figure 1 montre un réseau de distribution de produits ou de services comportant une pluralité de N plates-formes PF1, PF2,..., PFk, ..., PFN aptes à élaborer, sur instructions de l'opérateur OP du réseau, des messages, MS1 MS2, ... MSk, .. MSN à destination d'une pluralité de M appareils AP1, AP2, ... APj, ..., APM abonnés au réseau, tels que des téléphones mobiles par exemple. Lesdits messages MSk sont transmis aux divers appareils par des dispositifs émetteurs EM1, EM2, ..., EMk, EMN associées à chaque plate-forme.

Les messages MSk sont reçus par les appareils APj et transmis aux modules MODj de contrôle d'accès équipant respectivement lesdits appareils. Les modules de contrôle d'accès sont chargés d'authentifier et de valider les messages reçus avant prise en compte des informations qu'ils contiennent, comme des autorisations d'accès ou encore des modifications ou suppressions de droits d'accès accordés.

La figure 2 montre comment est typiquement constitué un message MSk destiné à un appareil APj. Ce message, que l'on notera ici MSk,j comprend les informations INFk proprement dites à transmettre à l'appareil APj. Il comprend également une donnée DDk de diversification fournie par un générateur GENk de données de diversification autonome, propre à la plate-forme PFk. Ladite plate-forme PFk est affectée d'une clé secrète KSk qui lui est également propre. A chaque module MODj de contrôle d'accès est attribué un code IDj d'identification, et l'ensemble de tous les codes d'identification est connu de chaque plate-forme. Ainsi, lorsqu'une plate-forme PFk doit fournir un message MSk,j à l'appareil APj, une clé secrète diversifiée KDk, j est constituée à partir de la clé secrète KSk, des informations INFk, du code IDj d'identification et d'un algorithme de cryptage qui peut être du type DES ou plus simplement un OU exclusif. La clé secrète diversifiée KDk,j est mélangée à la donnée DDk de diversification à l'aide d'un autre

algorithme de cryptage, DES par exemple, pour constituer un certificat CERk,j.

Ce système de diversification permet, du fait de la diversification de la clé secrète par rapport au module MODj destinataire, d'éviter qu'un message adressé à un appareil soit utilisé pour un autre.

A la réception, le module MODj de l'appareil APj qui, comme on peut le voir sur la figure 3, a stocké dans une mémoire les clés secrètes KSk de chaque plate-forme PFk, peut à son tour calculer un certificat de la même manière que la plate-forme PFk et vérifier l'authenticité du message MSk,j en comparant le certificat ainsi calculé au certificat CERk,j figurant dans ledit message.

De façon à supprimer toute synchronisation entre les plates-formes PFk, destinée à éviter que des plates-formes différentes envoient des message MSk ayant la même donnée DDk de diversification, les modules MODj de contrôle d'accès comportent, ainsi que le montre la figure 3, des moyens STk de stockage de la valeur de la donnée DDk de diversification transmise avec le dernier message MSk fourni par chaque plate-forme PFk. Comme les données de diversification sont stockées séparément pour chaque plate-forme, il n'y a plus de danger de collision et donc plus lieu de synchroniser les plates-formes entre elles, celles-ci deviennent alors autonomes : de plus, chaque module MODk est muni de moyens de comparaison de chaque nouvelle valeur de la donnée DDk de diversification reçue de chaque plate-forme PFk avec au moins la valeur précédente, ceci afin d'éviter qu'un message déjà envoyé, d'autorisation d'accès notamment, ne soit stocké et envoyé à nouveau à l'appareil de manière frauduleuse après suppression de l'accès par l'opérateur OP.

Les données DDk de diversification peuvent être, comme mentionné plus haut, des nombres aléatoires fournis par un générateur GENk de nombres aléatoires. Toutefois, il faudrait stocker dans les modules de contrôle d'accès tous les nombres aléatoires reçus par chaque plate-forme, ceci afin d'éviter toute répétition.

Dans ce cas, tout nouveau nombre aléatoire reçu est comparé à tous ceux déjà reçus de la même plate-forme.

On peut aussi choisir pour donnée DDk de diversification le numéro d'ordre des messages reçus de chaque plate-forme PFk, lequel s'incrémente d'une unité à chaque nouveau message. Le générateur GENk de données de diversification est alors un simple compteur. Dans chaque module MODj, les moyens STk de stockage enregistrent le numéro DDk du dernier message émis par la plate-forme PFk. Au message suivant provenant de la même plate-forme PFk, le module de contrôle d'accès vérifiera que le numéro DDk+1 du nouveau message est bien postérieur à DDk, auquel cas le message pourra être validé. ce système de diversification a l'avantage de n'avoir à stocker qu'une seule donnée dans lesdits moyens de stockage.

L'invention propose également un autre type de générateur de données de diversification dont le principe est illustré sur la figure 4.

Il s'agit d'un générateur constitué par une base de temps universel pour lequel la donnée DDk de diversification est la date t_K d'émission du message, cette date pouvant être prise par rapport à une origine t_0 arbitraire connue. En cas d'arrêt non contrôlé d'une plate-forme, celle-ci pourra repartir de manière automatiquement opérationnelle puisque to n'est pas perdu. Il n'y a donc aucune mesure de sauvegarde particulière à prévoir.

Afin de limiter la taille des moyens STk de stockage, on peut, au lieu de donner à la base de temps une durée t_{max} égale à la durée de vie du réseau, 40 ans par exemple, la limiter à une durée légèrement supérieure à la durée de vie moyenne des modules MODj de contrôle d'accès. Dans cette hypothèse, la donnée DDk de diversification de la plate-forme PFk repasse à zéro après avoir atteint t_{max}.

On comprend alors que, sans précaution particulière, les modules de contrôle d'accès devront rejeter tous les messages reçus après la date t_{max} car ayant une donnée DDk de diversification apparemment antérieure à la précédente, et ceci quelle que soit la date t_1 de mise en service du module. Cela

signifie que des modules qui auraient été fabriqués et stockés bien après la date t_0 auraient une durée de vie opérationnelle considérablement raccourcie.

C'est pourquoi, il est prévu des moyens de discrimination permettant d'éviter cet inconvénient. Ces moyens consistant en ce que chaque module MODj stocké en mémoire la date t_1 d'émission du premier message MS1 fourni par chaque plate-forme, la validation d'un message émis à la date t_{n+1} s'effectuant par comparaison avec la date t_1 et la date t_n d'émission de message précédent de la manière suivante :

- si $t_n > t_1$ le message à $t_n + 1$ est validé si t_{n+1} n'est pas compris dans $]t_1, t_n[$
- si $t_n < t_1$ le message à $t_n + 1$ est validé si t_{n+1} est compris dans $]t_n, t_1[$

Comme l'indique la figure 4, on peut ainsi prolonger la durée de vie des modules au-delà de t_{max} jusqu'à $t_{max} + t_1$ soit une durée totale de fonctionnement de t_{max}.

REVENDICATIONS

1. Système de diversification d'informations (INFk) transmises par un réseau vers des appareils (APPj) délivrant des produits ou des services, ledit réseau comprenant une pluralité de plates-formes (PFk) aptes, chacune, à élaborer des messages (MSk) comportant une donnée (DDk) de diversification des informations (INFk) à transmettre, fournie par un générateur (GENk) de données de diversification, et lesdits appareils (APPj) comprenant, chacun, un module (MODj) de contrôle d'accès, caractérisé en ce que chaque plate-forme (PFk) dispose d'un générateur (GENk) de données de diversification autonome, et en ce que ledit module (MODj) de contrôle d'accès de chaque appareil (APj) comporte, d'une part, des moyens (STk) de stockage de la valeur de la donnée (DDk) de diversification transmise avec le dernier message (MSk) fourni par chaque plate-forme (PFk), et, d'autre part, des moyens de comparaison de chaque nouvelle valeur de la donnée (DDk+1) de diversification reçue de chaque plate-forme (PFk) avec au moins la valeur précédente (DDk).
2. Système de diversification selon la revendication 1, caractérisé en ce que ledit générateur (GENk) de données de diversification est un générateur de nombres aléatoires.
3. Système de diversification selon la revendication 1, caractérisé en ce que ledit générateur (GENk) de données de diversification est un compteur de messages.
4. Système de diversification selon la revendication 1, caractérisé en ce que ledit générateur (GENk) de données de diversification est une base de temps universel.
5. Système de diversification selon la revendication 4, caractérisé en ce que la donnée (DDK) de diversification est la date t_n d'émission du message (MSk) par rapport à une origine t_o arbitraire connue.
6. Système de diversification selon l'une des revendications 4 ou 5, caractérisé en ce que ladite base de temps a une durée

t_{max} limitée à au moins la durée de vie desdits modules (MODj) de contrôle d'accès.

7. Système de diversification selon la revendication 6, caractérisé en ce que chaque module (MODj) de contrôle d'accès stocke en mémoire la date t_1 d'émission du premier message (MS1) fourni par chaque plate-forme (PFk), et en ce que la validation d'un message (MSk+1) émis à la date $t_n + 1$ s'effectue par comparaison avec la date t_1 et la date t_n d'émission du message précédent (MSk) :
   - si $t_n > t_1$ le message à $t_n + 1$ est validé si $t_n + 1$ n'est pas compris dans $]t_1, t_n[$
   - si $t_n < t_1$ le message à $t_n + 1$ est validé si $t_n + 1$ est compris dans $]t_n, t_1[$

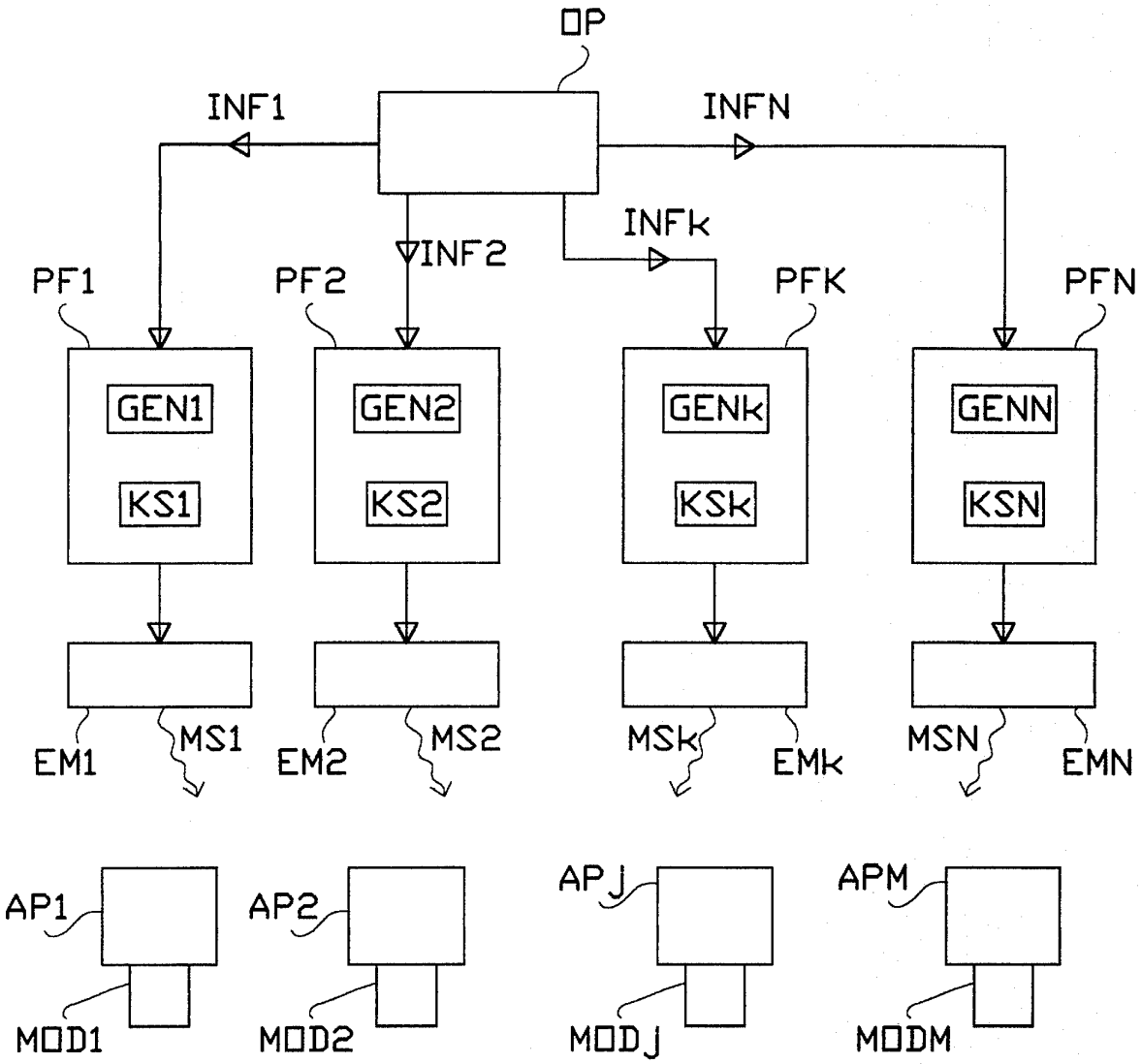

OP
INF1
INFN
INF2
INFk
PF1
PF2
PFK
PFN
GEN1
KS1
GEN2
KS2
GENk
KSk
GENN
KSN
EM1
MS1
EM2
MS2
MSk
EMk
MSN
EMN
AP1
AP2
APJ
APM
MOD1
MOD2
MODJ
MODM

Fig.1

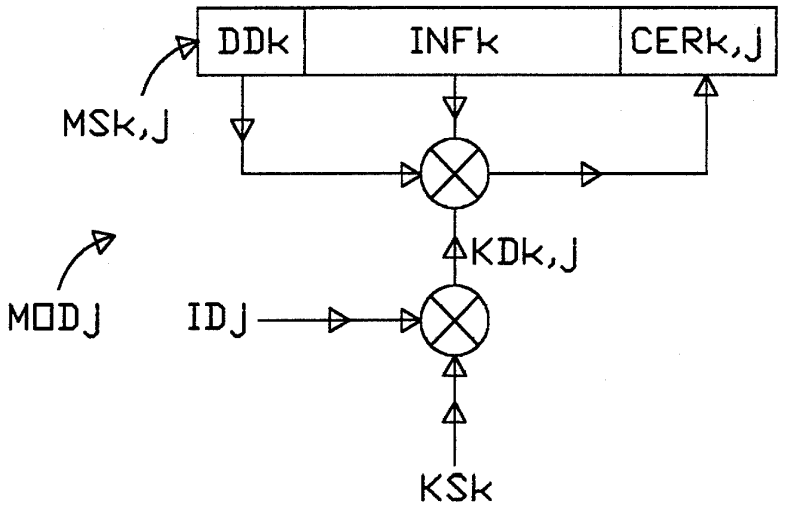

DDk
INFk
CERk,J
MSk,J
KDk,J
MODJ
IDJ
KSk

Fig.2

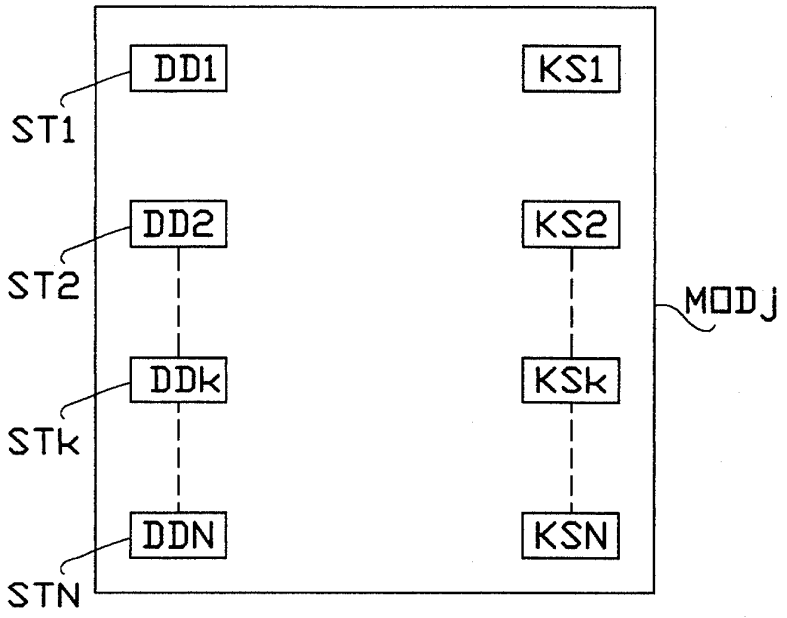

DD1
KS1
ST1
DD2
KS2
ST2
MODj
DDk
KSk
STk
DDN
KSN
STN

Fig.3

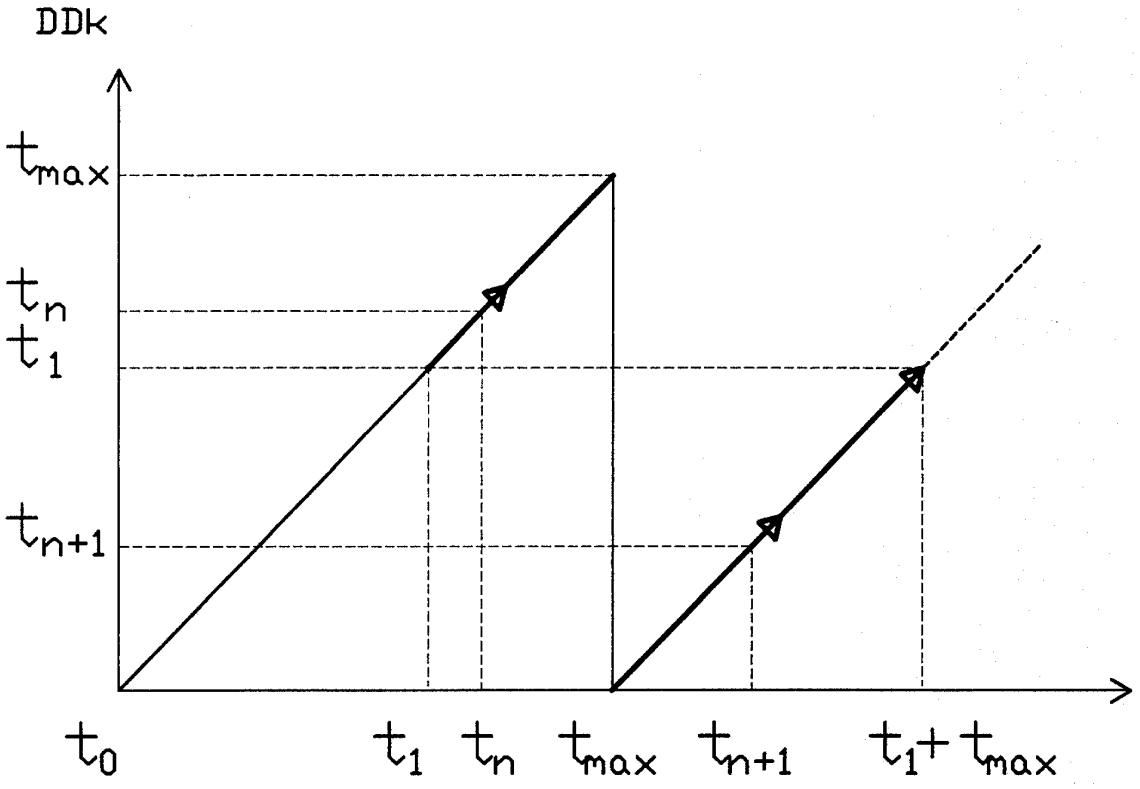

DDk
t_{max}
t_n
t_1
t_{n+1}
t_0
t_1
t_n
t_{max}
t_{n+1}
$t_1 + t_{max}$

Fig.4

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

2751154
N° d'enregistrement national

FA 530452
FR 9608916

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	WO 95 20280 A (FRANCE TELECOM) * page 13, ligne 33 - page 16, ligne 30 * * page 19, ligne 12 - page 21, ligne 27 * * figures 1-6 * ---	1
A	US 5 117 458 A (TAKARAGI ET AL.) * colonne 3, ligne 59 - colonne 4, ligne 49 * * colonne 7, ligne 4 - colonne 8, ligne 21 * * figure 2 * ---	1
A	WO 93 19549 A (SCIENTIFIC-ATLANTA INC) * page 8, ligne 3 - page 11, ligne 12 * * figures 1-3 * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
H04L

Date d'achèvement de la recherche	Examinateur
18 Avril 1997	Lydon, M

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)