(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
21 août 2003 (21.08.2003)

PCT

(10) Numéro de publication internationale
WO 03/069450 A2

(51) Classification internationale des brevets[7] : G06F 1/00

(21) Numéro de la demande internationale :
PCT/IB03/00436

(22) Date de dépôt international : 7 février 2003 (07.02.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0233/02 12 février 2002 (12.02.2002) CH
0698/02 24 avril 2002 (24.04.2002) CH

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

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : BRIQUE, Olivier [CH/CH]; Chemin de la Perrause 39, CH-1052 Le Mont-sur-Lausanne (CH). HILL, Michael, John [CH/CH]; Route de Commugny 10, CH-1296 Coppet (CH). JOLY, Stéphane [CH/CH]; Port Roulant 10, CH-2000 Neuchâtel (CH). COCHARD, Jimmy [CH/CH]; Chemin d'En-Quettolla 41, CH-1616 Attalens (CH).

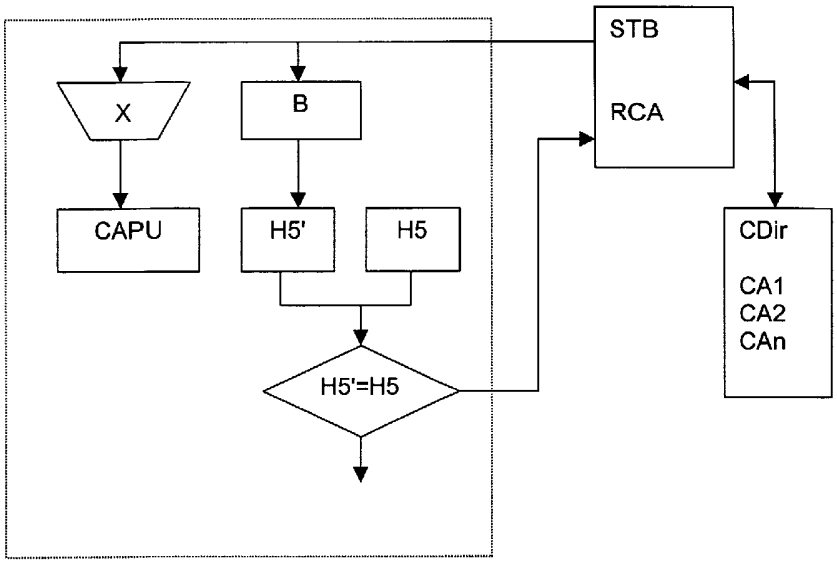
(74) Mandataire : LEMAN CONSULTING SA; Route de Clémenty 62, CH-1260 Nyon (CH).

(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, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[Suite sur la page suivante]

(54) Title: METHOD FOR STORAGE AND TRANSPORT OF AN ELECTRONIC CERTIFICATE

(54) Titre : METHODE DE STOCKAGE ET DE TRANSPORT D'UN CERTIFICAT ELECTRONIQUE



(57) Abstract: The aim of the invention is to ensure the transportability of an electronic certificate and the security of the private key which forms part of a certificate of type X509, wherein it is important that said certificate is not used for unauthorised purposes by the bearer, such as assuming identity, authorisation of undesired transactions and the reproduction of transactions (replay). Said aim is achieved by means of a method for storage and transport of an electronic certificate, said certificate comprising an authorisation section dedicated to the issuing authority, a bearer section dedicated to the bearer of the certificate and a signature section fixed by the issuing authority, characterised in that all or part of the bearer section is contained in a detachable security module and that at least the authorisation section is contained in a host computer.

[Suite sur la page suivante]

WO 03/069450 A2

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

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

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.

(57) Abrégé : Le but de la présente invention est d'assurer la transportabilité d'un certificat électronique et la sécurité de la clé privée faisant partie d'un certificat du type X509.En effet, il est important que ce certificat ne soit pas utilisé ô des fins non contrôlées par le titulaire, telles que l'usurpation d'identité, l'autorisation de transactions non souhaitées ou la reproduction de transactions (replay).Ce but est atteint par une méthode de stockage et de transport d'un certificat électronique, ledit certificat comprenant une section autorité propre ô l'autorité émettrice, une section titulaire propre au titulaire du certificat et une section signature déterminée par l'autorité émettrice, caractérisée en ce que tout ou partie de la section titulaire est contenue dans un module de sécurité amovible et ce qu'au moins la section autorité est contenue dans un ordinateur hôte.

MÉTHODE DE STOCKAGE ET DE TRANSPORT D'UN CERTIFICAT ÉLECTRONIQUE

La présente invention concerne une méthode de stockage et de transport d'un certificat de type X.509.

Le certificat électronique, tel que par exemple de type X.509, est une collection d'information pour tout ce qui concerne l'authentification d'un titulaire par voie électronique. Ce certificat est délivré par une autorité reconnue qui s'engage sur l'identité du titulaire possédant un tel certificat. C'est pourquoi, selon le niveau d'engagement de l'autorité délivrant le certificat, celle-ci peut exiger que le titulaire présente des garanties de son identité, par exemple qu'un notaire confirme son identité.

Ce certificat est schématiquement composé d'une partie propre à l'autorité émettrice et une partie propre au titulaire du certificat qui est dénommée "explicite".

La partie propre à l'autorité peut être identique pour tous les certificats délivrés par cette autorité. Cette partie est dénommée "implicite".

Pour rendre indissociable ces deux parties, un certificat comprend une signature effectuée sur ces deux parties et par l'intermédiaire de la clé privée de l'autorité.

Lorsqu'un tel certificat est reçu d'un serveur de stockage, la signature est vérifiée grâce à la clé publique de l'autorité émettrice. Cette clé peut se trouver dans le certificat racine de l'autorité émettrice. Comme indiqué plus haut, la signature permet de vérifier l'authenticité du contenu du certificat.

Ces certificats sont généralement stockés sur une unité de stockage d'un ordinateur, ainsi que le certificat racine qui est le certificat de l'autorité émettrice.

Il existe donc un intérêt à disposer d'un certificat stocké sur un support amovible et permettant de jouer de ce fait le rôle de module d'authentification. Pour cela, une simple disquette suffit pour transporter son certificat, support parfois utilisé pour communiquer un tel certificat à un utilisateur. Néanmoins ce principe n'offre pas de sécurité suffisante pour le stockage de la clé privée qui est aussi nécessaire aux opérations de transactions en ligne.

C'est pourquoi le but de la présente invention est d'assurer la transportabilité d'un certificat électronique et la sécurité de la clé privée.

En effet, il est important que ce certificat ne soit pas utilisé à des fins non contrôlées par le titulaire, telles que l'usurpation d'identité, l'autorisation de transactions non souhaitées ou la reproduction de transactions (replay).

Ce but est atteint par une méthode de stockage et de transport d'un certificat électronique, ledit certificat comprenant une section autorité propre à l'autorité émettrice, une section titulaire propre au titulaire du certificat et une section signature déterminée par l'autorité émettrice, caractérisée en ce que tout ou partie de la section titulaire est contenue dans un module de sécurité amovible et ce qu'au moins la section autorité est contenue dans un ordinateur hôte.

Cette méthode a également l'avantage de diminuer la quantité d'information stockées dans le module de sécurité. Ce module peut avoir la forme d'une carte à puce, un module avec interface PCMCIA ou USB, ou voire un module à transmission sans contact.

Les programmes de transactions sur Internet requièrent une authentification par certificat de type X.509. Il a été constaté qu'une partie de ce certificat peut être commune à un grand nombre d'utilisateurs et représente la section propre à l'autorité (implicite) émettant de tels certificats.

Il est ainsi avantageux, grâce à la présente invention, de ne stocker que la partie propre à chaque utilisateur (explicite) dans le support amovible, dans notre exemple cette unité de sécurité est une carte à puce. Cela évite une redondance d'informations donc une meilleure utilisation de la mémoire.

En effet, dans ces modules, on privilégie le stockage d'informations ayant un contenu de type contractuel tels que les transactions effectuées par le titulaire.

Bien que ce certificat soit fractionné, la signature de l'autorité émettrice sur l'ensemble des sections autorité et titulaire permet de rétablir la relation entre ces deux entités. Dès lors qu'une des deux parties est modifiée, l'image unique ne pourra être identique à la valeur de l'authentification calculée avec la clé publique de l'autorité émettrice sur cette signature.

Par signature, on entend le processus qui consiste à déterminer une image unique des données considérée pour cette signature (par une fonction Hash par exemple) et d'encrypter cette image unique par la clé privée de l'entité qui signe. L'algorithme utilisé pour l'établissement de cette signature est une encryption est de type asymétrique.

Pour la vérification d'une telle signature, on utilise la clé publique de cette entité pour décrypter la signature reçue et cette valeur est comparée avec le résultat de l'image unique effectué sur les données à authentifier. Si la valeur décryptée et l'image unique sont égales, les données sont intègres et authentique.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux dessins annexés qui sont donnés à titre d'exemple nullement limitatif, dans lesquels:

- la figure 1 représente la vérification du certificat de l'autorité émettrice,

- la figure 2 représente la configuration montrant les deux supports du certificat,

- la figure 3 représente l'authentification du certificat reconstitué,

- la figure 4 illustre la méthode de traitement d'une transaction,

- la figure 5 représente la méthode d'authentification du temps,

- la figure 6 illustre la signature finale sur l'ensemble des données,

- la figure 7 illustre le message envoyé.

La figure 1 représente l'extraction de la clé publique du certificat racine par l'unité de sécurité SM. Le certificat racine RCA est le certificat de l'autorité émettrice. Cette unité demande à l'unité hôte STB l'envoi du certificat racine RCA associé au certificat du titulaire TCI1. Ce certificat racine contient la clé publique CAPU de l'autorité émettrice. Cette clé permet d'authentifier le certificat du titulaire reconstitué avec la partie implicite et la partie explicite du certificat du titulaire. L'unité hôte STB envoie ce certificat racine vers le module de sécurité SM pour en extraire la clé publique CAPU. Lors de l'installation du certificat du titulaire dans l'unité de sécurité, cette dernière conserve l'image H5 qui est le résultat de la fonction Hash sur le certificat racine RCA.

Parallèlement à l'extraction de la clé publique CAPU (voir module X), la fonction Hash est effectuée par le bloc B sur les données explicites et implicites du certificat racine (explicite = partie propre à l'autorité émettrice, implicite = partie propre à l'autorité ayant certifié l'autorité émettrice) et le résultat H5' est comparé avec la valeur de référence H5 stockée initialement. Si les deux valeurs diffèrent, les opérations d'authentification sont stoppées et l'unité hôte en est informée.

Dans le cas où les deux valeurs H5 et H5' sont égales, la clé publique de l'autorité émettrice est sauvegardée et pourra être utilisée pour des opérations d'authentification du certificat reconstitué du titulaire.

Si l'unité hôte STB ne dispose pas du certificat racine, il peut en faire la requête sur le réseau Internet auprès par exemple d'un site disposant d'un répertoire (CDir) permettant d'accéder aux certificats souhaités (CA1, CA2, CAn).

Sur la figure 2, est représenté une première carte à puce SM1 dans laquelle la partie explicite TCE1 du titulaire ainsi que sa clé secrète TS1 sont stockées.

Du côté de l'unité hôte STB, se trouve un logiciel d'accès à Internet BR appelé couramment navigateur. Pour ce qui concerne les fonctions d'authentification, ce programme fait appel à un logiciel de sécurité SA qui réalise l'interface avec la carte à puce. Il est également en charge de transmettre le certificat dans son ensemble et pour cela, contient les données de la section autorité TCI1.

L'unité hôte STB est reliée au reste du monde par Internet par exemple pour accéder les prestataires de services PS1, PS2, les sites pour obtenir les informations de l'autorité émettrice CauD, les informations de l'heure TSAu et les informations sur le certificat racine CDir.

Lors du transfert entre l'unité de sécurité SM1 et l'unité hôte STB, les données concernant la section titulaire TCE1 sont envoyées à l'unité hôte selon une procédure mettant en œuvre l'unité de sécurité de manière prépondérante. Cette opération sera décrite plus en détail plus avant.

La vérification de l'intégrité de ce certificat est fait par le processus illustré à la figure 3. L'unité multimédia ou unité hôte, représentée ici par le bloc STB, transmet les données du certificat contenues dans l'unité hôte à destination de l'unité de sécurité SM. A ce propos, si la partie "autorité"

(implicite) est contenue dans son ensemble dans l'unité hôte STB, il est possible de stocker une partie des informations "utilisateur" (explicite) dans l'unité hôte également, le reste étant placé dans l'unité de sécurité SM.

Ces données sont organisées dans le module A alimenté d'une part par l'unité hôte STB, et d'autre part par les données TCE1 de la mémoire de l'unité de sécurité.

Il est important de noter ici que les données TCE1 de l'unité de sécurité ne sont pas simplement envoyées à l'unité hôte STB pour traitement mais que c'est l'unité de sécurité SM qui pilote l'opération.

Les données reconstituées par le module A, sont redirigées vers l'unité hôte STB et forment le certificat CERT en vue de l'envoi vers un prestataire de service. Le module A fonctionne comme un synchronisateur et recompose le certificat selon le format prédéfini et illustré par le bloc composé des éléments TCE, TCI, SCAT.

Dans le certificat reconstitué dans le module A, on extrait la signature SCAT du certificat du titulaire provenant de l'unité hôte STB (voir module X).

Les données réunies, à l'exclusion de la signature SCAT, sont envoyées au module B qui est en charge de la détermination d'une image unique de l'ensemble de ces données. Cette image est obtenue par une fonction Hash (unidirectionnelle et sans collision) qui est effectuée sur l'ensemble des données dans un ordre précis H= f (TCE1, TCI1). Il est admis qu'il n'existe pas d'ensemble de données différent qui donne le même résultat de cette fonction. Cette image est produite par une fonction unidirectionnelle et sans collision de type Hash. L'algorithme utilisé peut être de type SHA-1 ou MD5 et cette image exprime l'ensemble des données d'une manière unique. Le type d'algorithme à utiliser est spécifié dans le certificat.

Cette image est sauvegardée dans le module B1 pour usage futur.

Pour vérifier si les deux parties du certificat sont intègres et authentiques, l'unité de sécurité SM extrait la signature SCAT du certificat et décrypte cette dernière dans le module C grâce à la clé publique de l'autorité CAPU.

Pour cette opération, il est tenu compte des paramètres contenu dans le certificat qui décrivent le type de signature et la longueur des clés.

Dans le module D, la valeur de référence B1' est calculée et comparée avec l'image unique B1. Si les deux valeurs correspondent, le certificat est authentique et pourra servir pour des opérations futures illustrées par le module E. Dans la négative, la carte à puce SM refusera toute opération de transaction et informera l'unité hôte STB.

La figure 4 montre l'opération suivante qui consiste à autoriser une transaction. Si le test précédent sur l'authentification du certificat est positif (voir modules D et E de la figure 3), le module hôte STB va pouvoir envoyer la transaction signée à un prestataire de service PS1, PS2.

Une transaction Q peut être filtrée par le module F de l'unité de sécurité SM, module qui contient les règles d'acceptation. En effet, il est possible de déterminer un montant maximum ou énumérer une liste des instituts qui sont acceptés par le titulaire de l'unité de sécurité SM. Ces conditions peuvent inclure une date de limite de validité du certificat du titulaire.

Une fois que la transaction a passé avec succès le filtre du module F, elle est présentée au module B qui calcule une fonction Hash H2 sur l'ensemble de la transaction Q. Le résultat B2 est stocké pour utilisation subséquente. Cette valeur H2 est ensuite signée par la clé privée TS1 du titulaire pour former la signature de transaction SQTM. Le module A2 assemble les données de la transaction Q et la signature de la transaction SQTM pour les envoyer vers l'unité hôte STB.

Selon une variante de l'invention, il est possible d'ajouter à la transaction Q, une limite de validité de la transaction qui est schématisé par le temps TM. Une manière de déterminer ce temps est d'utiliser le temps courant T et d'ajouter la durée de validité ΔT. Ainsi ce temps TM est représenté par :

$$TM = T + \Delta T.$$

Cette limite de validité TM est ajoutée à la transaction Q lors de la détermination de la fonction Hash dans le module B et lors de l'assemblage des données dans le module A2. Lorsque la transaction sera reçue par le prestataire de service, il vérifiera que cette limite n'est pas dépassée.

Selon une variante de l'invention, l'utilisation d'une limite de validité TM peut être rendue obligatoire si un certain montant de transaction est atteint.

Sur la figure 5 est décrite l'opération d'authentification du temps fourni par l'unité hôte STB. Ces données temps comprennent le temps T proprement dit, une partie aléatoire R et une signature sur les deux précédentes données. Les données du temps T ainsi que la partie aléatoire R et la signature STA sont transmis à l'unité de sécurité SM. A partir du temps T, on détermine la limite de validité TM en ajoutant la durée de validité ΔT. Cette limite sert à définir une durée maximale durant laquelle une transaction pourra être marquée par ce temps.

L'authentification se fait d'une manière analogue aux opérations décrites précédemment, à savoir le calcul d'une fonction Hash sur les données temps T et l'aléa R dans le module B après leur assemblage dans le module A. Le résultat intermédiaire H3 est stocké dans le module B3 pour utilisation subséquente. Pour la détermination de la valeur B3' (module C) on utilise la clé TSPU qui est la clé publique de l'autorité délivrant le temps.

Dans le cas où la clé TSPU n'est pas disponible dans l'unité de sécurité SM, une requête est transmise via l'unité hôte STB pour rechercher le

certificat correspondant à l'autorité émettrice du temps T qui contient cette clé.

On compare (module D) ensuite cette valeur calculé B3' avec l'image unique B3 des données T et R, pour déterminer si le temps est authentique.

Sur la figure 6 est indiqué l'opération de liaison du certificat et de la transaction, et optionnellement le temps ainsi que d'autres informations concernant la transaction. Les valeurs précédentes B1 du certificat, B2 de la transaction et B3 du temps sont organisées dans le module A et envoyées au module B pour déterminer la fonction Hash. Cette valeur est ensuite signée par la clé secrète du titulaire TS1. Le résultat est la signature SETM de l'enveloppe comprenant l'ensemble certificat, transaction et temps.

Cette enveloppe est illustrée à la figure 7.

Du fait que la gestion de la mémoire est un aspect important dans une unité de sécurité, la signature de l'enveloppe SETM est déterminée sur la base des valeurs résultant des fonctions Hash de chaque étape. Cette manière de procéder permet de relier toutes les données et garantir que toutes chaque partie du message n'a pas été altérée.

Il serait également possible de calculer une signature d'enveloppe en prenant chaque élément séparément et de calculer la fonction Hash sur ceux-ci. Néanmoins cette méthode implique la mémorisation de tout le message pour effectuer cette opération.

REVENDICATIONS

1. Méthode de stockage et d'exploitation par une unité hôte (STB) connectée à un module de sécurité amovible (SM), d'un certificat électronique, ledit certificat comprenant une section autorité (TCI) propre à l'autorité émettrice, une section titulaire (TCE) propre au titulaire du certificat et une section signature (SCAT) déterminée par l'autorité émettrice, caractérisée en ce que tout ou partie de la section titulaire (TCE) est contenue dans le module de sécurité amovible (SM) et ce qu'au moins la section autorité est contenue dans l'unité hôte (STB).

2. Méthode de stockage et d'exploitation d'un certificat électronique selon la revendication 1, comprenant les étapes suivantes:

- transmettre la section autorité (TCI) au module de sécurité (SM),
- reconstituer le certificat dans le module de sécurité (SM) en joignant la section titulaire (TCE) contenue dans le module de sécurité (SM),
- déterminer une image (B1) unique sur les sections autorité et titulaire,
- décrypter la signature (SCAT) grâce à la clé publique (CAPU) de l'autorité émettrice du certificat pour obtenir une valeur de référence (B1') sur,
- comparer cette valeur de référence (B1') avec l'image (B1) unique sur les sections autorité et titulaire,
- informer l'unité hôte (STB) si les deux valeurs divergent et arrêter l'exploitation.

3. Méthode selon la revendication 2, caractérisée en ce que le module de sécurité (SM) traite des données d'une transaction à autoriser selon les étapes suivantes:

- réception d'une demande de transaction (Q) par l'unité de sécurité (SM),
- filtrage de cette transaction selon des paramètres de filtrage par un module de filtrage (F),

- détermination d'une image unique (B2) de la transaction acceptée (Q) et calcul d'une signature (SQTM) par la clé privé (TS1) du titulaire,

- transmission des données de la transaction (Q) et de la signature (SQTM) à l'unité hôte (STB).

4. Méthode selon la revendication 3, caractérisée en ce qu'elle consiste à ajouter à la transaction (Q) une limite de validité (TM) pour la détermination de l'image unique (B2) et de la signature de transaction (SQTM), et à transmettre à l'unité hôte (STB) cette limite de validité (TM) avec les données de la transaction (Q) et la signature de transaction (SQTM).

5. Méthode selon les revendications 1 à 4, caractérisée en ce que le module de sécurité (SM) reçoit une information temporelle (T) et une données aléatoire (R) qui sont signées par une autorité certificatrice du temps et en ce que le module de sécurité (SM) authentifie l'intégrité de ces informations (T , R) et informe d'unité hôte (STB) si l'exploitation peut continuer.

6. Méthode selon la revendication 5, caractérisée en ce que le module de sécurité amovible (SM) génère la limite de validité (TM) à partir de l'information temporelle (T) selon une durée (ΔT) propre ä l'unité de sécurité (SM).

7. Méthode selon l'une des revendications précédentes, caractérisée en ce que le module de sécurité (SM) détermine une signature générale (SETM) grâce à sa clé privée (TS1) sur les images uniques du certificat (B1) de la transaction (B2) et des informations temporelles (B3).

8. Méthode selon l'une des revendications précédentes, caractérisée en ce que le module de sécurité amovible (SM) est une carte à puce.

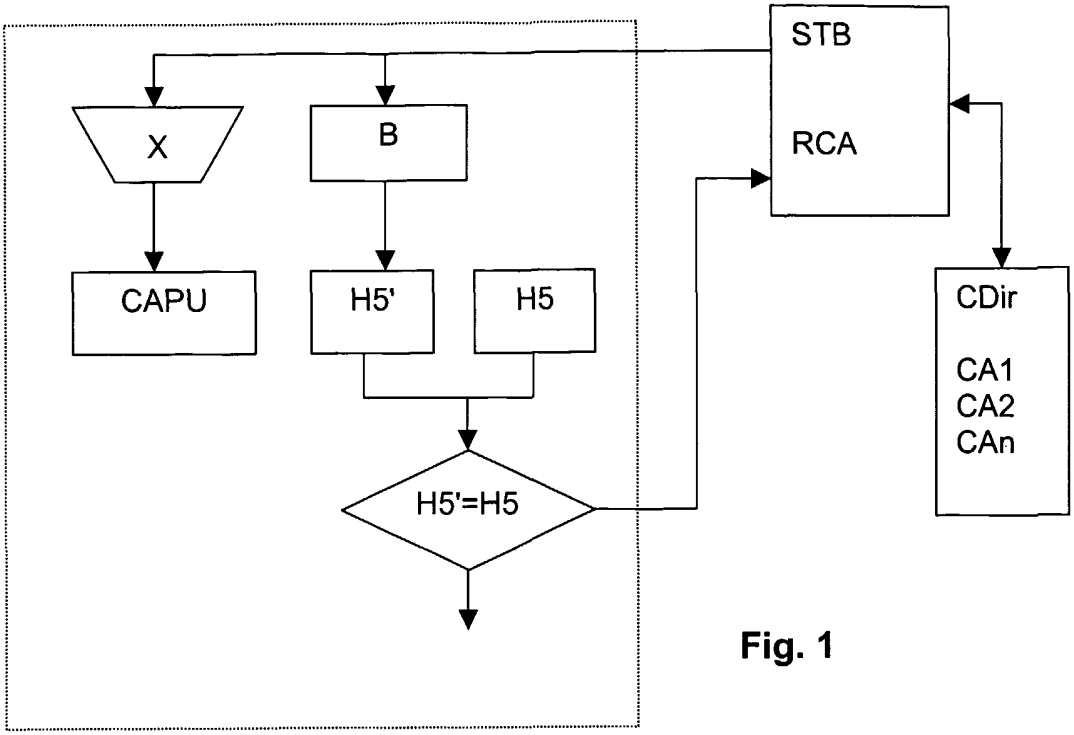

STB
RCA
X
B
CAPU
H5'
H5
H5'=H5
CDir
CA1
CA2
CAn

Fig. 1

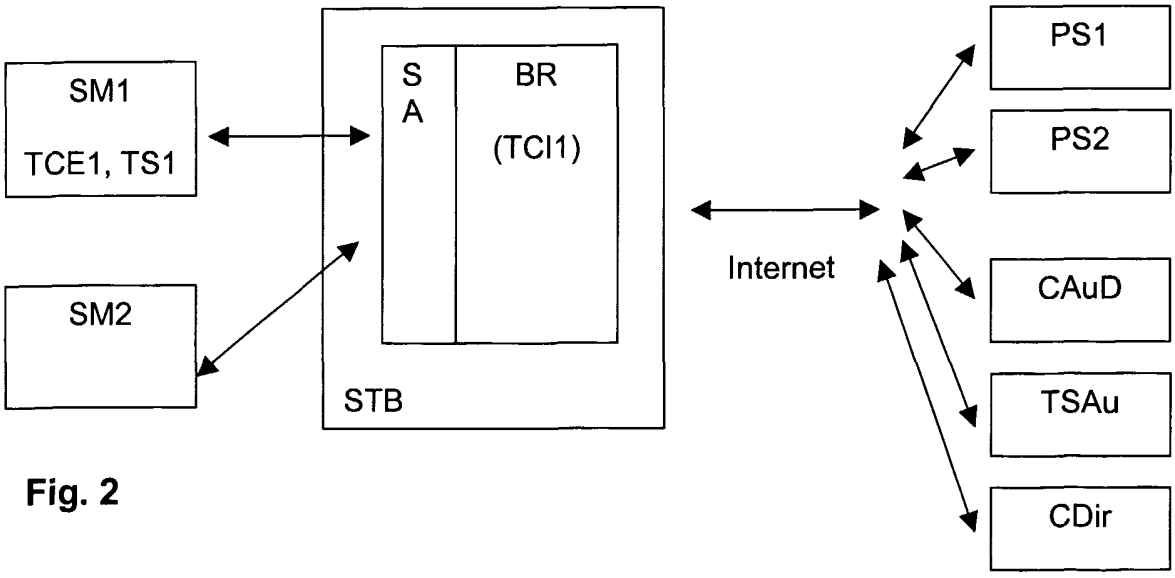

SM1
TCE1, TS1
SM2
S
A
BR
(TCI1)
STB
Internet
PS1
PS2
CAuD
TSAu
CDir

Fig. 2

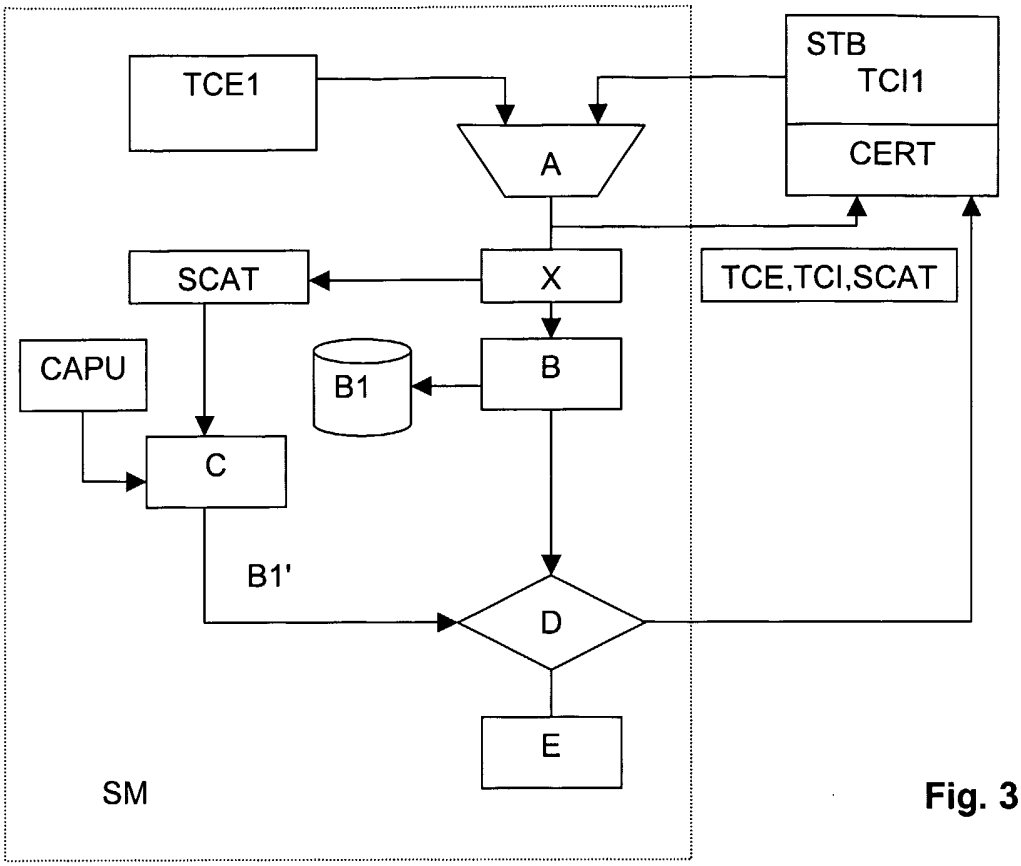

TCE1
STB
TCI1
CERT
A
SCAT
X
TCE,TCI,SCAT
CAPU
B1
B
C
B1'
D
E
SM

Fig. 3

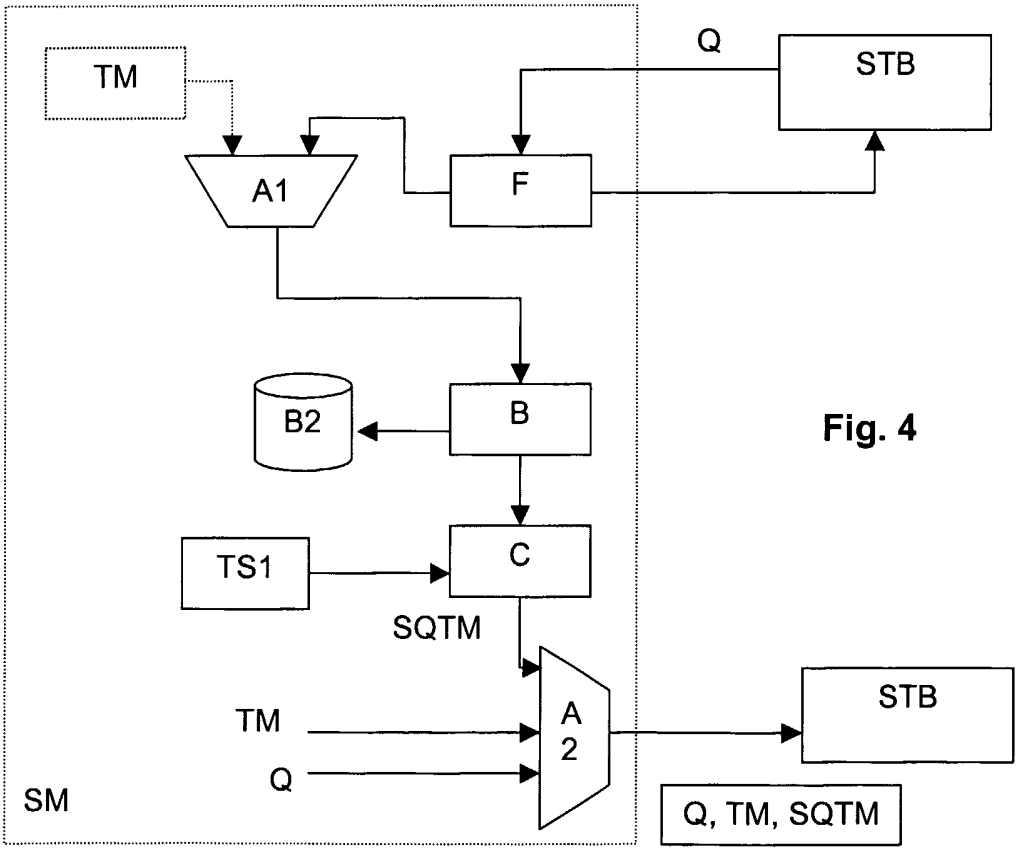

TM
Q
STB
A1
F
B2
B
TS1
C
SQTM
TM
Q
A
2
STB
SM
Q, TM, SQTM

Fig. 4

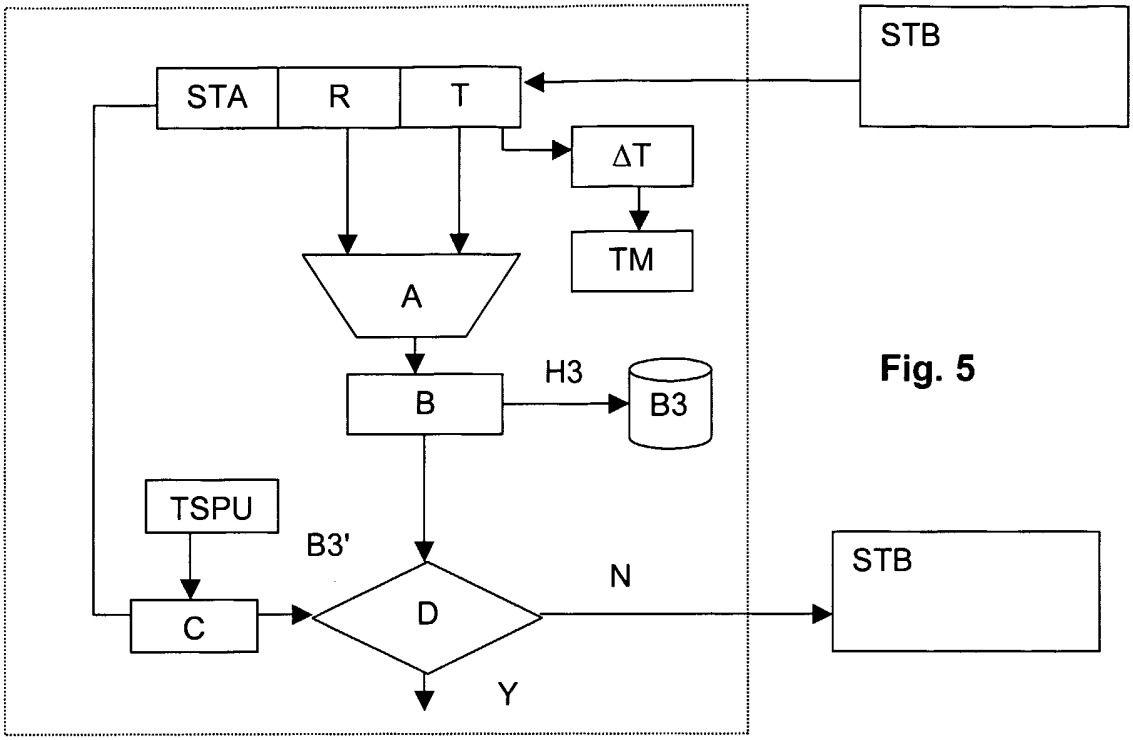

STB
STA
R
T
ΔT
TM
A
B
H3
B3
TSPU
B3'
C
D
N
STB
Y

Fig. 5

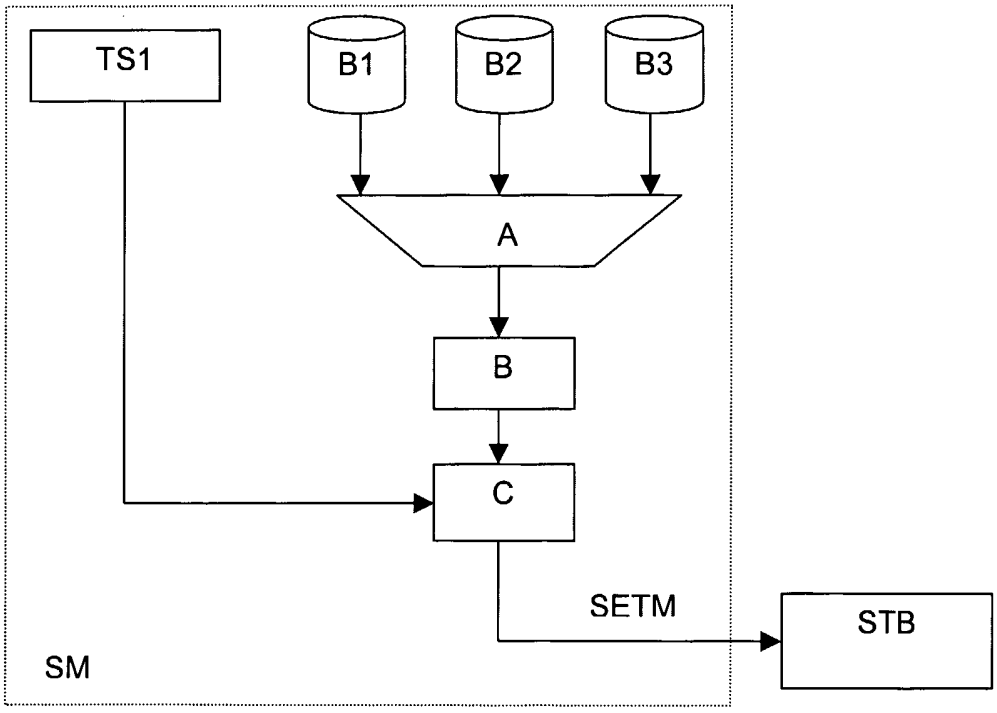

TS1
B1
B2
B3
A
B
C
SETM
STB
SM

Fig. 6

Fig. 7