(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 697 929**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **92 13726**

(51) Int Cl[5] : G 06 F 13/42, 15/21

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 10.11.92.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 13.05.94 Bulletin 94/19.

(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) :** *INNOVATRON (S.A.)* — FR.

(72) **Inventeur(s) :** Colnot Cédric.

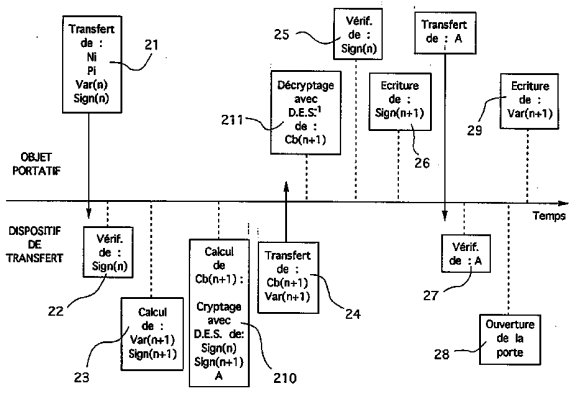
(73) **Titulaire(s) :**

(74) **Mandataire :** Vidon Patrice Cabinet Patrice Vidon.

(54) Protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif.

(57) L'invention concerne un protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif, chaque cycle d'échange de données consistant à:

- transférer vers le dispositif de transfert les données utiles courantes (Var(n)) et la signature courante (Sign(n)) mémorisées dans l'objet portatif, puis vérifier au dispositif de transfert l'intégrité des données utiles courantes (Var(n)) en vérifiant la signature courante (Sign(n));
- dans le dispositif de transfert, mettre à jour de nouvelles données utiles (Var(n+1)) et une nouvelle signature (Sign(n+1)), crypter sous la forme d'un certificat (Cb(N+1)) l'ensemble comprenant notamment la signature courante (Sign(n)), la nouvelle signature (Sign(n+1)) et un aléa (A), le cryptage étant effectué au moyen d'un algorithme public symétrique (DES) à clé secrète, puis transférer vers l'objet portatif les nouvelles données utiles (Vazr(n+1)) et le certificat (Cb(n+1));
- dans l'objet portatif, décrypter le certificat (Cb(n+1)) au moyen du même algorithme public symétrique (DES^{-1}), puis authentifier le dispositif de transfert en vérifiant la signature courante (Sign(n)), et écrire la nouvelle signature (Sign(n+1));
- renvoyer l'aléa (A) vers le dispositif de transfert puis écrire les nouvelles données utiles (Var(n+1)) dans l'objet portatif, l'objet portatif étant authentifié dans le dispositif de transfert en vérifiant l'aléa (A) renvoyé.



FR 2 697 929 - A1

Protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif.

Le domaine de l'invention est celui des échanges de données entre un dispositif de transfert et un objet portatif.

Plus précisément, l'invention concerne un protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif, l'objet portatif comportant des moyens de mémorisation des données échangées, ainsi que des moyens d'accès en lecture/écriture de la mémoire commandables par le dispositif de transfert.

Les données échangées mémorisées sont du type comprenant des données utiles variables mises à jour au cours de chaque cycle d'échange de données entre le dispositif de transfert et l'objet portatif, un cycle d'échange consistant à :

- transférer depuis l'objet portatif vers le dispositif de transfert les données utiles ;
- mettre à jour dans le dispositif de transfert de nouvelles données utiles ;
- transférer depuis le dispositif de transfert vers l'objet portatif les nouvelles données utiles.

Enfin, chaque cycle d'échange comporte en outre une opération d'authentification mutuelle du dispositif de transfert et de l'objet portatif.

L'invention a de nombreuses applications, telles que, par exemple, l'accès à un réseau de transports en commun. Dans ce cas, l'objet portatif représente le titre de transport de l'usager. Les données mémorisées dans cet objet portatif correspondent à des informations à caractère billétique :

- le descriptif des droits de transport (abonnement, réduction),
- le descriptif du voyage en cours,
- l'historique des voyages,

et des informations à caractère monétique (si l'objet portatif comporte un porte-monnaie électronique).

Le dispositif de transfert est par exemple une borne de péage (ou de

contrôle) commandant l'ouverture d'une porte d'accès au réseau de transports en commun, après avoir lu et vérifié les données mémorisées dans l'objet portatif, et, éventuellement, après avoir débité l'objet portatif d'un montant correspondant au trajet effectué.

De par les aspects monétiques, une telle application doit garantir un haut niveau de sécurité des échanges de données entre le dispositif de transfert et l'objet portatif.

Une application privilégiée du protocole de l'invention est la télébillétique, c'est-à-dire l'accès à un réseau de transport en commun grâce à un échange de données sans contact physique entre une borne de péage ou de contrôle (dispositif de transfert) et le titre de transport (objet portatif) de l'usager.

Plus généralement, l'invention peut s'appliquer dans tous les cas où le protocole d'échange de données du type décrit précédemment doit être sécurisé, une telle sécurisation signifiant d'une part que le dispositif de transfert et l'objet portatif doivent s'authentifier mutuellement, et d'autre part que les données utiles échangées ne peuvent être modifiées dans l'objet portatif que si cette authentification mutuelle a eu lieu.

Une solution connue permettant de réaliser une telle sécurisation d'un protocole d'échange de données entre un dispositif de transfert et un objet portatif est décrite dans le document "Système Opératoire dans les Cartes Microcircuits ou le COS en MOS, Manuel de Référence, Révision 3. Version 1, 25 novembre 1988, GEMPLUS CARD International".

Selon cette solution connue, le cycle d'échange de données entre le dispositif de transfert (appelé terminal) et l'objet portatif (appelé carte) est le suivant : authentification de la carte, authentification du terminal, lecture chiffrée puis écriture chiffrée de données dans l'objet portatif.

L'authentification de la carte par le terminal comprend les étapes suivantes:

- le terminal envoie à la carte un aléa A ;
- la carte calcule un résultat $R = DES(A, K_s) = R_g \| R_d$, avec DES

un algorithme public symétrique à clé secrète K_s, et R_g et R_d les 32 bits de gauche, respectivement de droite, du résultat R ;

- la carte envoie R_g au terminal ;
- le terminal calcule un résultat $R' = DES(A, K_s) = R'_g \| R'_d$ puis compare R'_g et R_g. S'il y a égalité, cela signifie que la carte possède K_s : le terminal a ainsi authentifié la carte.

L'authentification du terminal par la carte comprend les étapes suivantes:

- la carte calcule une clé de session $S = K_s \oplus V$, à partir de la clé secrète K_s et d'une valeur variable V (afin d'éliminer toute réutilisation du dialogue par un faux terminal) ;
- la carte envoie au terminal la valeur variable V et le terminal calcule la clé de session $S = Ks \oplus V$;
- le terminal crypte un code secret Cs à l'aide d'un algorithme public inverse DES^{-1} à clé secrète S (clé de session) et envoie à la carte le code secret crypté $M = DES^{-1}(Cs, S)$;
- la carte décrypte le code secret DES (M, S) = Cs' et le compare au code secret Cs qu'elle possède également. S'il y a égalité, cela signifie que le terminal possède le code secret Cs et la clé secrète Ks (qui lui a permis de calculer la clé de session S) : la carte a ainsi authentifié le terminal.

La lecture chiffrée de données dans l'objet portatif comprend les étapes suivantes:

- le terminal envoie à la carte une adresse de lecture AL ;
- la carte lit le mot Xl à l'adresse AL, le concatène deux fois à l'adresse de lecture AL, crypte la concaténation obtenue (Xl ‖ AL ‖ AL) à l'aide de l'algorithme public DES à clé secrète S, et envoie au terminal la concaténation chiffrée N = DES (Xl ‖ AL ‖ AL, D) ;
- le terminal décrypte la concaténation ($N' = DES^{-1}(N, S)$), et vérifie que la concaténation décryptée N' possède le format Xl' ‖ AL ‖ AL,

avec la redondance AL | AL. Si c'est le cas, le terminal récupère le mot lu Xl' et xconsidère qu'il est égal au mot Xl envoyé à la carte.

L'écriture chiffrée de données dans l'objet portatif comprend les étapes suivantes:

- le terminal calcule le nouveau mot X'e à écrire dans la carte à l'adresse AE, le concatène deux fois à l'adresse d'écriture AE, crypte la concaténation obtenue (Xe | AE | AE) à l'aide de l'algorithme public inverse DES^{-1} (Xe | AE | AE, S) ;
- la carte décrypte la concaténation (D'= DES (D, S)) et vérifie que la concaténation décryptée D' possède le format Xe' | AE | AE, avec la redondance AE | AE. Si c'est le cas, la carte écrit le mot Xe'= Xe à l'adresse AE et indique en retour au terminal que l'écriture a été effectuée.

Ainsi, les données sont échangées sous forme cryptée. Le cryptage/décryptage est effectué à l'aide d'un algorithme public (direct ou inverse) à clé secrète. Cette clé secrète est variable et prend une nouvelle valeur lors de chaque cycle d'échange (clé de session). De cette façon, l'échange de données est sécurisé et ne peut être réutilisé.

Toutefois, cette solution connue présente l'inconvénient majeur de nécessiter un triple cryptage/décryptage de données successivement pour authentifier le terminal, puis lire et enfin écrire des données dans la carte. Chaque cryptage/décryptage est effectué à l'aide d'un algorithme utilisé une fois dans le sens direct et une fois dans le sens inverse (par exemple DES et DES^{-1} respectivement), utilisant une même clé secrète dans les deux sens.

En d'autres termes, trois fois par cycle d'échange de données, des données sont cryptées par la carte (ou le terminal respectivement) à l'aide d'un algorithme public direct (ou inverse respectivement) utilisant une clé (une clé de session dans le cas de cette solution connue). Ces données cryptées sont envoyées au terminal (ou à la carte respectivement) qui les décrypte à l'aide de l'algorithme public

inverse (ou direct respectivement) utilisant la même clé que celle utilisée lors du cryptage.

Ces nombreux échanges de données ainsi que la triple utilisation de l'algorithme public dans les deux sens direct et inverse, avec une même clé secrète, lors de chaque cycle d'échange, se traduisent par un nombre élevé de calculs à effectuer (aussi bien par le terminal que par la carte).

Par conséquent, la durée de chaque cycle d'échange est assez longue, et tant le terminal que la carte doivent posséder d'importantes capacités de calcul.

Par ailleurs, cette solution présente un autre inconvénient lorsque le dispositif de transfert (c'est-à-dire le terminal) doit permettre l'ouverture d'une porte sous deux conditions, à savoir :

- si le dispositif de transfert et l'objet portatif (c'est-à-dire la carte) se sont authentifiés mutuellement ;
- si le dispositif de transfert est assuré qu'à l'issue du cycle d'échange, les données de l'objet portatif sont mises à jour.

Ceci correspond notamment au cas des transports en commun. Dans ce cas, la mise à jour des données mémorisées dans l'objet portatif (qui joue le rôle de titre de transport de l'usager) représente un débit d'un montant correspondant au trajet effectué par l'usager, la porte ouverte par le dispositif de transfert étant la porte d'accès au réseau de transport.

Or, un fraudeur peut interrompre le cycle d'échange après la lecture par le dispositif de transfert des données contenues dans l'objet portatif, mais avant l'écriture des données mises à jour, c'est-à-dire avant l'opération de débit.

Deux cas peuvent se présenter selon que l'échange de données entre le dispositif de transfert et l'objet portatif se fait avec ou sans contact physique.

Si les échanges de données entre le dispositif de transfert et l'objet portatif sont réalisés par contact physique (ou accouplement), une parade au type de fraude expliquée ci-dessus consiste à ne pas ouvrir la porte tant que l'objet portatif n'a pas indiqué au dispositif de transfert que l'opération d'écriture a été effectuée, et à interrompre immédiatement le cycle d'échange si le dispositif de transfert détecte

que l'objet portatif n'est plus en contact physique.

Cette solution, si elle présente l'avantage d'être hautement sécurisée, possède en contrepartie un inconvénient majeur à savoir la durée relativement longue du cycle d'échange, ceci étant dû au fait que l'écriture des données dans l'objet portatif est une opération relativement longue. Cette augmentation de la durée du cycle d'échange se traduit par une augmentation du temps d'attente des usagers aux lignes de péage.

Si les échanges de données entre le dispositif de transfert et la carte sont réalisés sans contact physique, la solution connue de protocole sécurisé d'échange de données ne permet en aucune façon de vérifier que l'usager n'a pas :

- d'une part désactivé son objet portatif pendant l'opération d'écriture des données mises à jour par le dispositif de transfert ; et
- d'autre part renvoyé un faux message indiquant que l'écriture a effectivement été réalisée.

Lors de l'utilisation suivante de l'objet portatif, le dispositif de transfert n'a aucun moyen de détecter cette fraude puisque rien dans les données mémorisées par l'objet portatif ne permet d'indiquer une fraude éventuelle.

L'invention a notamment pour objectif de pallier ces différents inconvénients de l'état de la technique.

Plus précisément, un objectif de l'invention est de fournir un protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif, chaque cycle d'échange de données comportant d'une part une opération d'authentification mutuelle du dispositif de transfert et de l'objet portatif et d'autre part une mise à jour des données échangées mémorisées dans l'objet portatif.

L'invention a également pour objectif de fournir un tel protocole présentant une durée de cycle d'échange réduite.

Un autre objectif de l'invention est de fournir un tel protocole limitant le nombre de calculs à effectuer, permettant ainsi de réduire les capacités de calcul du dispositif de transfert et surtout celles de l'objet portatif.

Un objectif complémentaire de l'invention est de fournir un tel protocole

empêchant toute tentative de fraude du type consistant à soustraire l'objet portatif à l'opération d'écriture, en particulier lorsque le dispositif de transfert permet l'ouverture d'une porte, l'échange de données entre le dispositif de transfert et l'objet portatif pouvant se faire avec ou sans contact.

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif,

ledit dispositif de transfert et ledit objet portatif comprenant chacun des moyens de communication l'un avec l'autre, pilotés par des moyens de mise en oeuvre dudit protocole,

ledit objet portatif comportant des moyens de mémorisation desdites données échangées et des moyens d'accès en lecture/écriture desdits moyens de mémorisation commandables par ledit dispositif de transfert, lesdites données échangées mémorisées comprenant des données utiles variables mises à jour au cours de chaque cycle d'échange de données entre ledit dispositif de transfert et ledit objet portatif, un cycle d'échange consistant à :

- dans un premier temps, transférer depuis l'objet portatif vers le dispositif de transfert les données utiles courantes mémorisées dans lesdits moyens de mémorisation dudit objet portatif ;
- dans un second temps, mettre à jour dans le dispositif de transfert de nouvelles données utiles destinées à se substituer auxdites données utiles courantes ;
- dans un troisième temps, transférer depuis le dispositif de transfert vers l'objet portatif lesdites nouvelles données utiles ;

chaque cycle comportant en outre une opération d'authentification mutuelle du dispositif de transfert et de l'objet portatif,

lesdites données mémorisées comprenant également une signature courante desdites données utiles courantes,

une nouvelle signature, destinée à se substituer à ladite signature courante, étant mise à jour au cours de chacun desdits cycles d'échange de données ;

et chaque cycle d'échange de données étant réalisé de la façon suivante :

- à l'issue dudit premier temps, on vérifie au dispositif de transfert l'intégrité des données utiles courantes transférées depuis l'objet portatif en s'assurant que ladite signature courante correspond auxdites données utiles courantes avec lesquelles ladite signature courante a été transférée;
- à l'issue dudit second temps, un nouveau couple données utiles/signature est mis à jour dans le dispositif de transfert ;
- ledit troisième temps est réalisé sous la forme de l'envoi d'une part des nouvelles données utiles mises à jour et d'autre part d'un certificat obtenu par cryptage de l'ensemble constitué notamment de ladite signature courante transférée depuis l'objet portatif, de la nouvelle signature mise à jour et d'un aléa, ledit cryptage étant effectué avec un algorithme public symétrique utilisant une clé secrète connue de l'objet portatif et du dispositif de transfert seuls, l'objet portatif authentifiant le dispositif de transfert en vérifiant, après avoir décrypté ledit certificat avec ledit algorithme public symétrique à clé secrète, que ladite signature décryptée correspond à ladite signature courante transférée lors du premier temps, la nouvelle signature mise à jour remplaçant la signature courante après que l'objet portatif a authentifié le dispositif de transfert ;
- dans un quatrième temps, ledit aléa décrypté par l'objet portatif est renvoyé au dispositif de transfert, le dispositif de transfert authentifiant l'objet portatif en vérifiant que ledit aléa reçu correspond audit aléa contenu dans le certificat envoyé lors dudit troisième temps, les nouvelles données utiles mises à jour remplaçant les données utiles courantes après que l'aléa a été renvoyé au dispositif de transfert par l'objet portatif.

De cette façon, le protocole selon l'invention permet une écriture chiffrée avec authentification mutuelle en ne mettant en oeuvre qu'un seul cryptage/décryptage de données au moyen d'un algorithme public symétrique utilisé dans les deux sens direct et inverse (par exemple DES et DES^{-1}) utilisant une clé secrète. En effet, cet unique cryptage/décryptage est utilisé pour transférer de façon sécurisée, du dispositif de transfert vers l'objet portatif, la signature précédente, la signature mise à jour et un aléa.

Il est important de noter que l'invention réalise en un seul calcul cryptographique (cryptage par le dispositif de transfert, décryptage par l'objet portatif) les trois opérations suivantes :

- authentification du dispositif de transfert par l'objet portatif,
- écriture de la nouvelle signature, et
- authentification de l'objet portatif par le dispositif de transfert.

Tout risque de fraude est évité puisque ces trois opérations sont imbriquées et il n'est pas possible à un éventuel fraudeur d'intervenir de façon intercalée entre deux opérations (alors que ces trois opérations étaient au contraire successives et indépendantes dans la solution connue de l'état de la technique).

Ainsi, les échanges lors de chaque cycle sont réduits et par conséquent la durée du cycle est plus courte.

Par ailleurs, les calculs, et notamment ceux effectués dans la carte, sont réduits. Les calculs étant réduits, les capacités de calcul du dispositif de transfert et de l'objet portatif sont également réduits. Ceci est particulièrement appréciable pour l'objet portatif qui peut ainsi être de dimensions plus faibles.

L'invention s'appuie sur le principe de variabilité des données : à l'issue de chaque cycle d'échange, le couple données utiles / signature doit être cohérent, la nouvelle signature étant calculée à partir des nouvelles données utiles (qui sont différentes des données utiles précédentes).

De plus, afin de réduire encore la durée du cycle d'échange, l'écriture des données utiles mises à jour, qui est une opération relativement longue, ne peut avoir lieu qu'une fois la communication entre le dispositif de transfert et l'objet portatif terminée.

En effet, l'intégrité des données est assurée par la signature qui elle a été mise à jour pendant la communication. Par conséquent, en empêchant la mise à jour des données utiles dans l'objet portatif, on rend cet objet portatif inutilisable puisque les données qu'il contient ne correspondent plus à la signature : le couple données utiles / signature n'est plus cohérent.

Si l'aléa est renvoyé par l'objet portatif mais n'est pas reçu par le dispositif

de transfert, le dispositif de transfert n'a pas authentifié l'objet portatif. Néanmoins, le couple données utiles/signature est cohérent puisque l'aléa ayant été renvoyé, la nouvelle signature a été écrite dans l'objet portatif. Par conséquent, un autre échange de données peut avoir lieu normalement. Si l'échange de données correspond à une opération de débit, un protocole de niveau inférieur permet d'éviter un double débit en vérifiant que, suite au premier échange de données, le couple données utiles/signature est effectivement cohérent bien que le dispositif de transfert n'a pas reçu l'aléa renvoyé par l'objet portatif.

Dans un mode de réalisation avantageux de l'invention, ledit échange de données s'effectue sans contact physique entre le dispositif de transfert et l'objet portatif,

et lesdits moyens de communication du dispositif de transfert et de l'objet portatif comprennent des moyens d'émission/réception.

Les données utiles mises à jour sont transmises en clair à l'objet portatif mais la signature mise à jour est transmise cryptée avec une clé que possèdent le dispositif de transfert et l'objet portatif seuls. Par conséquent, le protocole selon l'invention convient parfaitement aux protocoles d'échange de données sans contact physique qui sont plus exposés aux tentatives de fraudes que les protocoles d'échange de données avec contact physique.

Avantageusement, lesdites nouvelles données utiles sont élaborées en combinant aux données proprement dites une information représentative de la date ou de l'heure dudit cycle d'échange.

Dans un mode de réalisation préférentiel de l'invention, lorsque d'une part ladite authentification mutuelle du dispositif de transfert et de l'objet portatif est réalisée, et d'autre part ladite signature est mise à jour, le dispositif de transfert permet l'ouverture d'une porte.

Le protocole selon l'invention convient parfaitement aux systèmes de ce type puisque, comme expliqué auparavant, la fraude consistant à soustraire l'objet portatif à l'opération d'écriture des nouvelles données utiles est empêchée. En effet, une telle action rend l'objet portatif inutilisable par la suite en rendant incohérent

le couple données utiles/signature (la signature ayant été modifiée avant l'ouverture de la porte, et plus précisément, avant le renvoi de l'aléa au dispositif de transfert).

De plus, la porte peut être ouverte avant que l'opération d'écriture ait eu lieu puisque la nouvelle signature a été écrite et garantit l'intégrité des données.

Ainsi, la durée du cycle d'échange reste faible et permet de réduire les temps d'attente des usagers aux lignes de péage.

De façon avantageuse, ladite signature des données utiles est obtenue au moyen d'un algorithme public symétrique de cryptage à clé secrète.

En effet, cet algorithme (DES par exemple) présente le double avantage d'être peu coûteux en temps de calcul et disponible dans l'objet portatif puisqu'il est utilisé pour crypter le certificat.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de réalisation préférentiel de l'invention, donné à titre d'exemple indicatif et non limitatif, et des dessins annexés dans lesquels :

- la figure 1 présente un schéma simplifié d'un système d'accès à un réseau de transports en commun comprenant un dispositif de transfert et un objet portatif mettant en oeuvre le protocole sécurisé d'échange de données selon l'invention ;
- la figure 2 présente un exemple de déroulement d'un cycle d'échange du protocole selon l'invention ;
- la figure 3 présente un diagramme des temps correspondant au cycle d'échange de la figure 2.

L'invention concerne donc un protocole sécurisé d'échange de données entre un dispositif de transfert et un objet portatif, ce protocole permettant au dispositif de transfert de consulter des données variables mémorisées dans l'objet portatif et de les mettre à jour. Chaque cycle d'échange de ce protocole comporte en outre une opération d'authentification mutuelle du dispositif de transfert et de l'objet portatif.

Le protocole sécurisé décrit ci-dessous s'applique à un réseau de transports

en commun. Il est clair toutefois qu'il peut aisément être adapté à de nombreuses autres applications sans sortir du cadre de l'invention.

Dans cet exemple, chaque usager possède un objet portatif 11 qui constitue son titre de transport. L'usager accède au réseau de transport en mettant en communication son objet portatif 11 avec un dispositif de transfert 16. Ce dispositif de transfert 16 joue le rôle d'une borne de péage ou de contrôle, et commande un moyen 19 d'ouverture d'une porte 110.

Dans le cas d'un système de péage "main libre", tel que présenté sur la figure 1, l'objet portatif 11 peut être constitué d'un badge et d'une carte à microprocesseur, le badge assurant la transmission de données 15 par liaison immatérielle avec le dispositif de transfert.

Dans le cas d'un système de péage comprenant un dispositif de transfert 16 constitué d'un lecteur ISO (avec contact physique), l'objet portatif 11 est constitué uniquement d'une carte à microprocesseur.

Dans tous les cas, l'objet portatif 11 représente un support tarifaire universel, permettant tous les types de tarification, tout en simplifiant à l'usager le règlement de ses déplacements. Pour cela, l'objet portatif 11 comprend des moyens 12A de mémorisation de données échangées et des moyens 12B d'accès en lecture/écriture à cette mémoire 12A, ces moyens d'accès en lecture/écriture étant commandables par le dispositif de transfert 16.

Les données échangées mémorisées comprennent d'une part des données utiles variables Var(n) pour chaque cycle d'échange n, et d'autre part une signature de ces données utiles.

Les données utiles variables Var(n) concernent des informations à caractère billétique (descriptif des droits de transport (abonnement, réduction), descriptif du voyage en cours, historique des voyages (date et heure du dernier cycle d'échange), et des informations à caractère monétique (porte-monnaie électronique, qu'il soit privatif ou bancaire).

Afin de pouvoir échanger des données, l'objet portatif 11 et le dispositif de transfert 16 comprennent chacun des moyens 14, 18 de communication pilotés par

des moyens 13, 17 de mise en oeuvre du protocole selon l'invention, ce protocole devant garantir le haut niveau de sécurité des transactions liées au paiement du transport par l'usager.

Dans le cas de l'échange de données sans contact, les moyens de communication 14, 18 comprennent des moyens d'émission/réception de signaux radiofréquences.

La mise à jour des données utiles variables (c'est-à-dire le remplacement de Var(n) par Var(n+1)) est une opération de paiement qui consiste, par exemple, à débiter l'objet portatif 11 d'un nombre d'unités de transport fixe lors de l'entrée dans le réseau.

En résumé, l'accès au transport correspond au franchissement par l'usager d'une ligne de péage (ou porte 110). Celle-ci matérialise la frontière entre un mode de transport et le monde extérieur. Le passage d'une ligne de péage résulte d'un acte volontaire de l'usager, à savoir la mise en communication de son objet portatif 11 avec le dispositif de transfert 16. Cet acte volontaire a également pour fonction d'autoriser le transporteur à débiter l'objet portatif 11 du montant du voyage.

La figure 2 présente un exemple de déroulement d'un cycle d'échange du protocole selon l'invention. Ce cycle n + 1 fait suite au cycle n. La figure 3 présente un diagramme des temps correspondant à ce cycle d'échange.

Dans le cas d'un réseau de transports en commun tel que présenté en relation avec la figure 1, chaque accès de l'usager au réseau correspond à un cycle d'échange de données entre l'objet portatif et le dispositif de transfert.

Le protocole selon l'invention comprend l'ensemble des échanges de données entre l'objet portatif et le dispositif de transfert et correspond sensiblement à la couche session du modèle OSI.

Chaque cycle d'échange peut être décomposé en plusieurs phases successives, à savoir :

- l'identification 21 de l'objet portatif ;
- la vérification 22 de l'intégrité des données mémorisées transmises au dispositif de transfert par l'objet portatif ;

- le calcul 23 des nouvelles données par le dispositif de transfert ;
- le cryptage 210 de la nouvelle signature, de la signature courante et d'un aléa sous la forme d'un certificat ;
- le transfert 24 des nouvelles données vers l'objet portatif ;
- le décryptage 211 du certificat ;
- l'authentification 25 du dispositif de transfert par l'objet portatif ;
- l'écriture 26 de la nouvelle signature dans l'objet portatif ;
- l'authentification 27 de l'objet portatif par le dispositif de transfert;
- l'ouverture 28 de la porte par le dispositif de transfert ;
- l'écriture 29 des nouvelles données utiles dans l'objet portatif.

Avant le début du cycle d'échange n + 1, le dispositif de transfert et l'objet portatif possèdent des éléments invariables de calcul 212 (qui leur sont propres) ainsi que des données variables mémorisées lors du cycle d'échange précédent n.

Ces données variables comprennent des données utiles variables Var(n) (par exemple, le montant du porte-monnaie électronique et le lieu, la date et l'heure de la dernière transaction) et une signature Sign(n) de ces données utiles Var(n).

L'objet portatif possède les éléments invariables de calcul suivants :

- une clé secrète diversifiée Ki ;
- un numéro de série Ni ;
- une donnée fixe de profil Pi regroupant un ensemble de caractéristiques de l'usager, concernant par exemple le type d'abonnement (nombre de zones, période, nombre de déplacements, poucentage de réduction,...).

Le dispositif de transfert possède les éléments invariables de calcul suivants:

- une clé secrète de signature Ks ;
- une clé de diversification Kd.

Lors de la première phase 21 d'identification de l'objet portatif, l'objet portatif transmet au dispositif de transfert son numéro de série Ni et sa donnée fixe

de profil Pi, ainsi que les données variables (Var(n) et Sign(n)) correspondant à l'état courant de l'objet portatif après n cycles d'échange.

La phase suivante 22 consiste à vérifier l'intégrité des données transmises lors de la première phase 21.

Le dispositif de transfert calcule la clé secrète diversifiée Ki de l'objet portatif à partir du numéro de série Ni de l'objet portatif et de la clé de diversification Kd :

$$Ki = F (Ni, Kd)$$

où F est par exemple un algorithme public DES de cryptage utilisant la clé de diversification Kd comme clé secrète.

Cette clé secrète diversifiée Ki est utilisée par la suite comme clé secrète liée à un algorithme public de cryptage (DES par exemple) afin de sécuriser les échanges de données entre le dispositif de transfert et l'objet portatif.

La vérification proprement dite de l'intégrité des données est réalisée en comparant la signature Sign(n) (transmise par l'objet portatif) à une signature Sign'(n) recalculée par le dispositif de transfert à partir des données transmises par l'objet portatif :

$$Sign'(n) = F (Var(n), Pi, Ni, Ks)$$

où F est par exemple un algorithme public DES de cryptage utilisant la clé secrète de signature Ks. Plus généralement, la signature est calculée à l'aide d'une fonction irréversible, et permet de vérifier l'intégrité des données ayant permis de calculer cette signature.

L'intégrité des données est vérifiée si les deux signatures Sign(n) et Sign'(n) sont identiques.

Après avoir vérifié l'intégrité des données, le dispositif de transfert calcule (23) de nouvelles données.

D'une part, les nouvelles données utiles variables sont calculées : le dispositif de transfert applique la loi tarifaire g du transporteur en fonction de la donnée de profil Pi et des données utiles variables précédentes :

$$Var(n + 1) = g (Pi, Var(n)).$$

D'autre part, la nouvelle signature est calculée. La nouvelle signature Sign(n+1) est calculée à partir des nouvelles données utiles Var(n + 1), de la donnée de profil Pi et du numéro de série Ni :

$$\text{Sign } (n + 1) = F \text{ (Var } (n + 1), \text{ Pi, Ni, Ks).}$$

Enfin, on tire un aléa A, par exemple à partir d'un générateur pseudo-aléatoire.

L'étape suivante est le transfert 24 des nouvelles données vers l'objet portatif.

Les nouvelles données utiles Var (n + 1) sont transmises à l'objet portatif en clair. Par contre, la nouvelle signature Sign (n + 1) est transmise chiffrée.

Plus précisément, on transmet un certificat Cb (n + 1) crypté dans une étape précédente 210, à partir de la nouvelle signature Sign (n + 1), de la signature précédente Sign (n) et de l'aléa A :

$$Cb(n+1) = F \text{ (Sign}(n+1), \text{ Sign}(n), A, Ki)$$

où F est par exemple un algorithme public symétrique de cryptage (DES par exemple) utilisant la clé secrète diversifiée Ki.

L'objet portatif reçoit Var(n+1) et Cb(n+1), décrypte Cb(n+1) et obtient ainsi Sign"(n), Sign"(n+1) et A". Le décryptage 211 est effectué au moyen du même algorithme public symétrique, utilisé cette fois-ci en sens inverse (DES^{-1} dans cet exmple).

L'authentification 25 du dispositif de transfert par l'objet portatif consiste à comparer la signature Sign"(n) reçue par l'intermédiaire du certificat Cb(n+1) à la signature Sign(n) que possède cet objet portatif (et qui fait partie de l'état courant après n cycles d'échanges).

Si les deux signatures Sign"(n) et Sign(n) sont identiques, cela signifie que le dispositif de transfert possède la clé de diversification Kd ainsi que la clé secrète diversifiée Ki (calculée à partir de Kd). Par conséquent, le dispositif de transfert est authentifié par l'objet portatif.

Après que le dispositif de transfert a été authentifié, l'objet portatif peut mettre à jour la signature (26) : Sign"(n+1), c'est-à-dire Sign(n+1), remplace

Sign(n).

Avant d'ouvrir la porte (28), le dispositif de transfert doit authentifier (27) l'objet portatif.

Pour cela, l'objet portatif renvoie l'aléa A" au dispositif de transfert. Celui-ci compare l'aléa A" qu'il reçoit à l'aléa A d'origine utilisé pour le certificat Cb(n+1).

Si les deux aléa A et A" sont identiques, cela signifie que l'objet portatif a pu déchiffrer le certificat et donc que l'objet portatif possède Ki. Cet échange d'aléa interdit le rejeu des données par un badge factice ayant enregistré un cycle d'échange complet.

Ainsi, l'objet portatif est authentifié par le dispositif de transfert qui autorise l'ouverture 28 de la porte.

La dernière phase concerne la mise à jour 29 des données utiles dans l'objet portatif. Cette opération d'écriture consiste à remplacer Var(n) par Var(n+1). Cette opération étant relativement longue, elle n'a lieu effectivement qu'une fois la communication dispositif de transfert/objet portatif terminée.

La fraude consistant à empêcher cette opération d'écriture (correspondant à un débit) se traduit par un couple données utiles/signature (Var(n)/Sign(n+1)) incohérent dans l'objet portatif. Par conséquent, l'objet portatif devient inutilisable.

En effet, dans le cycle d'échange de données suivant (n+2), cette incohérence va être détectée lors de la phase de vérification de l'intégrité des données.

Le protocole décrit ci-dessus est mis en oeuvre dans un système d'accès à un réseau de transport en commun, le dispositif de transfert autorisant ou non l'ouverture d'une porte en fonction de données utiles lues dans un objet portatif.

Il est clair que l'invention n'est pas limitée à une telle application mais concerne également tous les systèmes dans lesquels un dispositif de transfert et un objet portatif s'authentifient mutuellement grâce à une signature des données utiles, le dispositif venant également lire et mettre à jour les données utiles mémorisées par l'objet portatif.

Enfin, il est important de noter que le protocole selon l'invention ne met en ouevre qu'un seul cryptage 210/décryptage 211 de données. Ceci permet notamment de réduire les capacités de calcul de l'objet portatif.

REVENDICATIONS

1. Protocole sécurisé d'échange de données entre un dispositif de transfert (16) et un objet portatif (11),

ledit dispositif de transfert et ledit objet portatif (11) comprenant chacun des moyens (14 , 18) de communication l'un avec l'autre, pilotés par des moyens (13 , 17) de mise en oeuvre dudit protocole,

ledit objet portatif (11) comportant des moyens (12A) de mémorisation desdites données échangées et des moyens (12B) d'accès en lecture/écriture desdits moyens (12A) de mémorisation commandables par ledit dispositif de transfert (16), lesdites données échangées mémorisées comprenant des données utiles variables (Var(n)) mises à jour au cours de chaque cycle d'échange de données entre ledit dispositif de transfert (16) et ledit objet portatif (11), un cycle d'échange consistant à :

- dans un premier temps, transférer depuis l'objet portatif (11) vers le dispositif de transfert (16) les données utiles courantes (Var(n)) mémorisées dans lesdits moyens (12A) de mémorisation dudit objet portatif (11) ;
- dans un second temps, mettre à jour dans le dispositif de transfert (16) de nouvelles données utiles (Var(n+1)) destinées à se substituer auxdites données utiles courantes (Var(n)) ;
- dans un troisième temps, transférer depuis le dispositif de transfert (16) vers l'objet portatif (11) lesdites nouvelles données utiles ;

chaque cycle comportant en outre une opération d'authentification mutuelle du dispositif de transfert (16) et de l'objet portatif (11),

caractérisé en ce que lesdites données mémorisées comprennent également une signature courante (Sign(n)) desdites données utiles courantes (Var(n)),

en ce qu'une nouvelle signature (Sign(n+1)), destinée à se substituer à ladite signature courante (Sign(n)), est mise à jour au cours de chacun desdits cycles d'échange de données ;

et en ce que chaque cycle d'échange de données est réalisé de la façon suivante :

- à l'issue dudit premier temps, on vérifie au dispositif de transfert (16) l'intégrité des données utiles courantes (Var(n)) transférées depuis l'objet portatif (11) en

s'assurant que ladite signature courante (Sign(n)) correspond auxdites données utiles courantes (Var(n)) avec lesquelles ladite signature courante (Sign(n)) a été transférée;

- à l'issue dudit second temps, un nouveau couple données utiles (Var(n+1))/-signature (Sign(n+1)) est mis à jour dans le dispositif de transfert (16) ;

- ledit troisième temps est réalisé sous la forme de l'envoi d'une part des nouvelles données utiles mises à jour (Var(n+1)) et d'autre part d'un certificat (Cb(n+1)) obtenu par cryptage de l'ensemble constitué notamment de ladite signature courante (Sign(n)) transférée depuis l'objet portatif (11), de la nouvelle signature (Sign(n+1)) mise à jour et d'un aléa (A), ledit cryptage étant effectué avec un algorithme public symétrique (F) utilisant une clé secrète (Ki) connue de l'objet portatif (11) et du dispositif de transfert (16) seuls, l'objet portatif (11) authentifiant le dispositif de transfert (16) en vérifiant, après avoir décrypté ledit certificat (Cb(n+1)) avec ledit algorithme public symétrique (F) à clé secrète (Ki), que ladite signature décryptée correspond à ladite signature courante (Sign(n)) transférée lors du premier temps, la nouvelle signature mise à jour (Sign(n+1) remplaçant la signature courante (Sign(n) après que l'objet portatif (11) a authentifié le dispositif de transfert (16) ;

- dans un quatrième temps, ledit aléa (A) décrypté par l'objet portatif (11) est renvoyé au dispositif de transfert (16), le dispositif de transfert (16) authentifiant l'objet portatif (11) en vérifiant que ledit aléa (A) reçu correspond audit aléa contenu dans le certificat (Cb(n+1)) envoyé lors dudit troisième temps, les nouvelles données utiles mises à jour (Var(n+1)) remplaçant les données utiles courantes (Var(n)) après que l'aléa (A) a été renvoyé au dispositif de transfert (16) par l'objet portatif (11).

2. Protocole sécurisé d'échange de données selon la revendication 1, caractérisé en ce que ledit échange de données s'effectue sans contact physique entre le dispositif de transfert (16) et l'objet portatif (11),

et en ce que lesdits moyens (14, 18) de communication du dispositif de transfert (16) et de l'objet portatif (11) comprennent des moyens d'émission/réception.

3. Protocole sécurisé d'échange de données selon l'une quelconque des revendications 1 et 2, caractérisé en ce que lesdites nouvelles données utiles (Var(n+1)) sont élaborées en combinant aux données proprement dites une information représentative de la date ou de l'heure dudit cycle d'échange.

4. Protocole sécurisé d'échange de données selon l'une quelconque des revendications 1 à 3, caractérisé en ce que lorsque d'une part ladite authentification mutuelle du dispositif de transfert (16) et de l'objet portatif (11) est réalisée, et d'autre part ladite signature (Sign(n)) est mise à jour, le dispositif de transfert (16) permet l'ouverture d'une porte (110).

5. Protocole sécurisé d'échange de données selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ladite signature (Sign(n)) des données utiles variables (Var(n)) est obtenue au moyen d'un algorithme public symétrique (F) de cryptage à clé secrète.

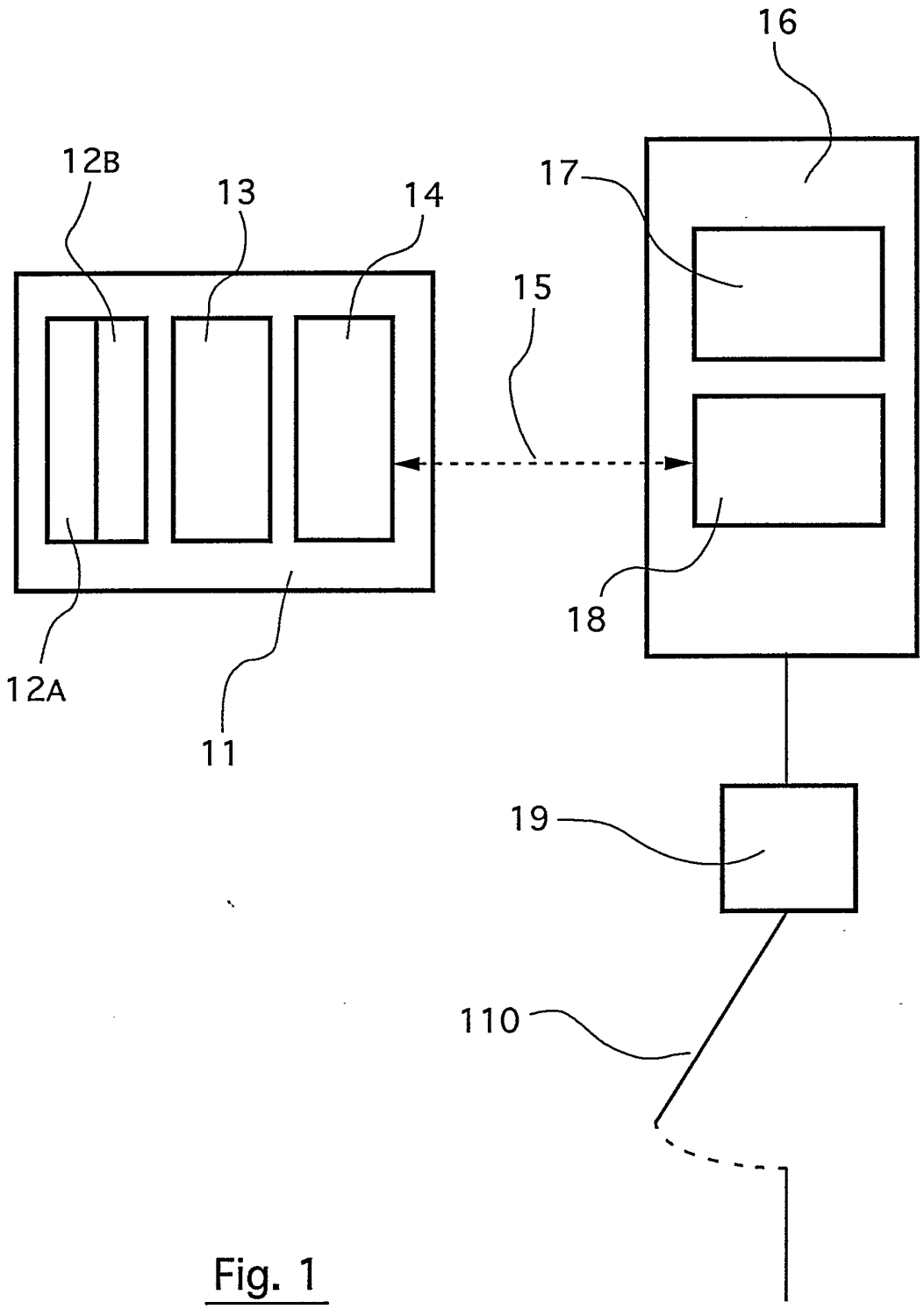


Fig. 1

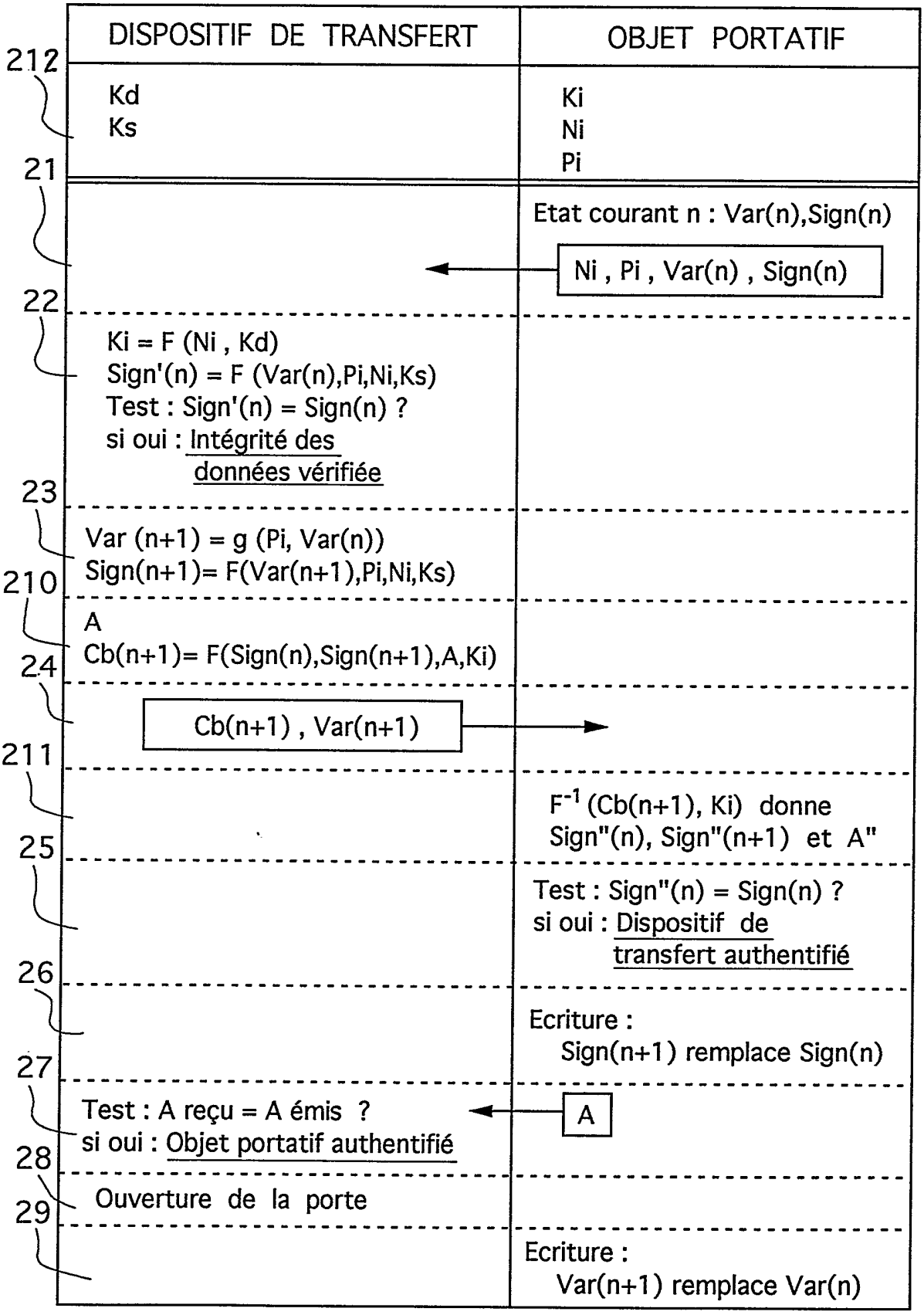

DISPOSITIF DE TRANSFERT
OBJET PORTATIF
212
Kd
Ks
Ki
Ni
Pi
21
Etat courant n : Var(n),Sign(n)
Ni , Pi , Var(n) , Sign(n)
22
Ki = F (Ni , Kd)
Sign'(n) = F (Var(n),Pi,Ni,Ks)
Test : Sign'(n) = Sign(n) ?
si oui : Intégrité des données vérifiée
23
Var (n+1) = g (Pi, Var(n))
Sign(n+1)= F(Var(n+1),Pi,Ni,Ks)
210
A
Cb(n+1)= F(Sign(n),Sign(n+1),A,Ki)
24
Cb(n+1) , Var(n+1)
211
F-1 (Cb(n+1), Ki) donne Sign"(n), Sign"(n+1) et A"
25
Test : Sign"(n) = Sign(n) ?
si oui : Dispositif de transfert authentifié
26
Ecriture :
Sign(n+1) remplace Sign(n)
27
Test : A reçu = A émis ?
A
si oui : Objet portatif authentifié
28
Ouverture de la porte
29
Ecriture :
Var(n+1) remplace Var(n)

Fig. 2

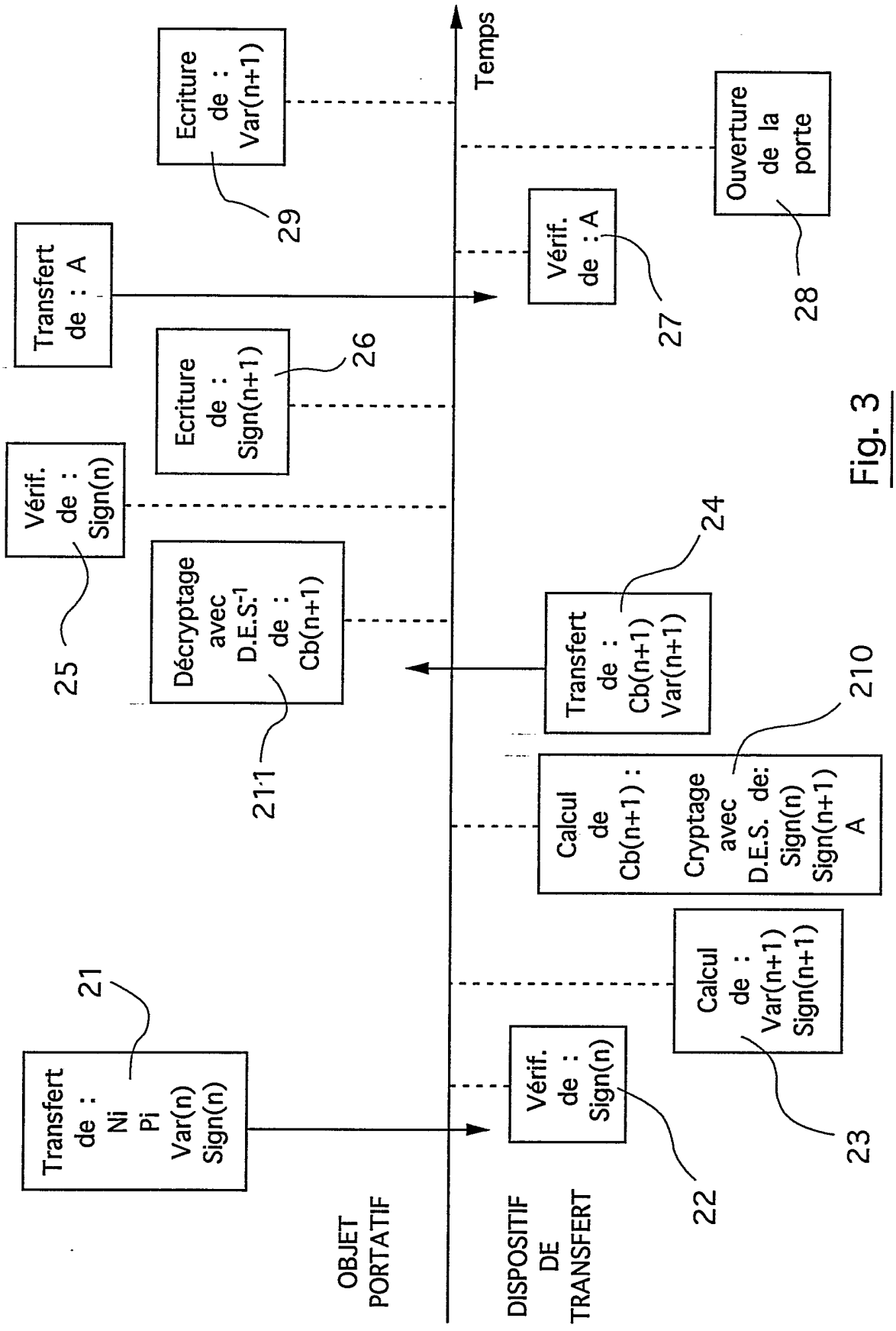

Temps
OBJET PORTATIF
DISPOSITIF DE TRANSFERT
Transfert de : Ni Pi Var(n) Sign(n)
21
Vérif. de : Sign(n)
22
Calcul de : Var(n+1) Sign(n+1)
23
Calcul de Cb(n+1) : Cryptage avec D.E.S. de: Sign(n) Sign(n+1) A
210
Transfert de : Cb(n+1) Var(n+1)
24
Décryptage avec D.E.S.-1 de : Cb(n+1)
211
Vérif. de : Sign(n)
25
Ecriture de : Sign(n+1)
26
Transfert de : A
Vérif. de : A
27
Ouverture de la porte
28
Ecriture de : Var(n+1)
29

Fig. 3

REPUBLIQUE FRANÇAISE

2697929

N° d'enregistrement national

FR 9213726
FA 479588

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

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

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
E	DE-A-4 119 924 (SIEMENS) * abrégé; figure 5 * * colonne 1, ligne 1 - colonne 2, ligne 53 * * colonne 10, ligne 41 - colonne 12, ligne 12 * * revendications 1-10 *	1-5	
Y	EP-A-0 253 722 (BULL CP8) * abrégé; figure 2 * * colonne 1, ligne 4 - colonne 2, ligne 55 * * colonne 5, ligne 14 - colonne 7, ligne 14 *	1-4	
Y	EP-A-0 414 314 (TRT TELECOMMUNICATIONS RADIOELECTRIQUES ET TELEPHONIQUES) * le document en entier *	1-4	
Y	US-A-4 757 185 (ONISHI) * abrégé; figure 1 *	2	DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
Y	US-A-4 910 776 (DYKE) * abrégé; figure 1 *	3	G07F G06F

Date d'achèvement de la recherche	Examinateur
02 AOUT 1993	POWELL D.

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 (P0413)