(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 841 020**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **02 07298**

(51) Int Cl[7] : **G 06 K 7/08,** H 04 L 9/28

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.06.02.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 19.12.03 Bulletin 03/51.

(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) :** *STMICROELECTRONICS SA* *Société anonyme* — FR.

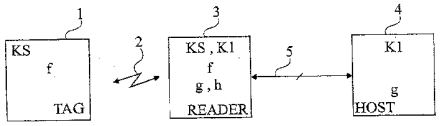
(72) **Inventeur(s) :** MOREAUX CHRISTOPHE et ANGUILLE CLAUDE.

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

(74) **Mandataire(s) :** CABINET MICHEL DE BEAUMONT.

(54) AUTHENTIFICATION D'UNE ETIQUETTE ELECTRONIQUE.

(57) L'invention concerne un procédé et système d'authentification d'une étiquette électronique (1) par un serveur (4), consistant: à calculer, côté étiquette, une première signature numérique (St) à l'aide d'une première fonction (f) partagée par l'étiquette et un lecteur communicant avec le serveur, en prenant en compte une première clé secrète (KS) connue seulement de l'étiquette et du lecteur; à transmettre la première signature au lecteur; à calculer, côté lecteur, une deuxième signature numérique (SIGN) à l'aide d'une deuxième fonction (g), partagée par le lecteur et le serveur, en tenant compte de la première signature; à transmettre la deuxième signature au serveur; et à vérifier, côte serveur (4), la cohérence entre la deuxième signature et une grandeur de validation (VAL) calculée à partir de ladite deuxième fonction et d'une deuxième clé secrète (K1) connue du serveur et d'un seul élément choisi parmi l'étiquette et le lecteur.



FR 2 841 020 - A1

AUTHENTIFICATION D'UNE ÉTIQUETTE ÉLECTRONIQUE

La présente invention concerne de façon générale les systèmes d'authentification d'un circuit intégré porté par un élément distant (par exemple une étiquette électronique à poser sur un produit quelconque). L'invention concerne plus particulièrement les systèmes qui requièrent, pour une authentification, trois éléments distincts à savoir le circuit intégré à authentifier, un lecteur d'informations contenues dans ce circuit, et un serveur communiquant avec le lecteur.

Un exemple d'application de la présente invention concerne le marquage par étiquette radio fréquence (TAG) de consommables de systèmes de distribution. Par exemple, il peut s'agir de recharges d'une "machine à café" ou de cartouches d'imprimante. L'authentification sert alors à garantir que seules les cartouches autorisées par le fabriquant soient utilisées par une imprimante donnée. Dans une telle application, le circuit intégré à authentifier est porté par la cartouche d'imprimante sous la forme d'une étiquette électronique susceptible de communiquer, sans contact et sans fil, avec un lecteur, à la manière d'un transpondeur électromagnétique. Le lecteur est relié au serveur au moyen d'une liaison d'un autre type, par exemple, une interface électrique de type I2C ou analogue.

On désignera par la suite par "application", l'ensemble des tâches effectuées par le système (par exemple, l'imprimante) une fois l'étiquette authentifiée.

Pour que l'application fonctionne correctement, l'étiquette électronique doit avoir au préalable été authentifiée afin de s'assurer que le produit (par exemple, une cartouche ou une recharge) qui la porte est un produit autorisé (par exemple, s'assurer que la marchandise marquée par l'étiquette n'a pas été remplacée par une contrefaçon).

Le rôle du serveur (constitué par exemple d'un micro-contrôleur, d'un ordinateur distant ou de tout autre système électronique adapté) est de contrôler l'application, c'est-à-dire le programme d'authentification ainsi que les actions appropriées suite à la détection (par exemple, blocage de l'imprimante ou de la machine à café en cas d'absence d'authentification). Dans ces domaines, le serveur sera préférentiellement un microcontrôleur équipant la machine de distribution automatique ou l'imprimante. Il pourra toutefois également s'agir d'un serveur distant communiquant, par exemple par liaison téléphonique ou par ligne dédiée, avec différents lecteurs.

La communication entre le serveur et le lecteur est basée sur des protocoles accessibles et répandus afin de permettre une utilisation de lecteurs différents avec un même serveur équipé du contrôleur d'application. Toutefois, cela engendre une faiblesse en terme de sécurité, surtout si le serveur est distant du lecteur (même faiblement en étant dans le même appareil). Or c'est au serveur qu'appartient la décision finale d'authentifier l'étiquette pour autoriser l'exécution correcte de l'application.

Les systèmes d'authentification connus font appel à des algorithmes de cryptographie pour authentifier une étiquette électronique à partir d'une clé secrète spécifique. Par exemple, on a recours à des algorithmes de type DES (Data Encryptions Standard).

Un inconvénient de tels algorithmes de cryptographie est qu'ils requièrent une étiquette électronique pourvue de moyens de calcul performants, en l'espèce, généralement un microprocesseur. Le coût engendré par de tels moyens de calcul rend ces systèmes mal adaptés à des recharges ou marchandises de type consommable pour lesquelles on souhaite minimiser le coût de l'étiquette électronique en raison du fait que celle-ci n'est pas durable.

La présente invention sera décrite par la suite en relation avec un exemple particulier de transmission radiofréquence entre le circuit intégré à authentifier et son lecteur. On notera toutefois qu'elle s'applique plus généralement à tout système d'authentification faisant intervenir trois éléments distincts (une étiquette électronique à authentifier, un lecteur et un serveur) et où la communication entre le lecteur et le serveur s'effectue par des moyens différents de la communication entre l'étiquette et le lecteur.

La présente invention vise à proposer un nouveau procédé et système d'authentification d'un dispositif électronique dans un système comprenant au moins ce dispositif à authentifier, un lecteur du dispositif et un serveur chargé de contrôler l'exécution d'une application en fonction de l'authentification du dispositif.

L'invention vise plus particulièrement à proposer une solution adaptée à des étiquettes électroniques ou analogues de faible taille et coût, en particulier, sans nécessiter le recours à un microprocesseur dans l'étiquette.

L'invention vise également à permettre une authentification alors que la communication entre le lecteur et le serveur s'effectue sur une liaison non protégée contre d'éventuels piratages.

Selon un premier aspect, l'invention prévoit des étiquettes électroniques ayant toutes une même clé secrète pour des étiquettes de même type.

Selon un deuxième aspect, l'invention prévoit d'individualiser la clé secrète au niveau de chaque étiquette électronique.

Pour atteindre ces objets et d'autres, la présente invention prévoit un procédé d'authentification d'une étiquette électronique par un serveur communiquant avec cette étiquette par l'intermédiaire d'un lecteur, consistant :

à calculer, côté étiquette, une première signature numérique à l'aide d'au moins une première fonction partagée par l'étiquette et le lecteur, en prenant en compte au moins une première clé secrète connue seulement de l'étiquette électronique et du lecteur ;

à transmettre la première signature au lecteur ;

à calculer, côté lecteur, une deuxième signature numérique à l'aide d'au moins une deuxième fonction, différente de la première fonction et partagée par le lecteur et le serveur, en tenant compte de la première signature ;

à transmettre la deuxième signature au serveur ; et

à vérifier, côté serveur, la cohérence entre la deuxième signature et une grandeur de validation calculée à partir de ladite deuxième fonction et d'une deuxième clé secrète connue du serveur et d'un seul élément choisi parmi l'étiquette et le lecteur.

Selon un mode de mise en oeuvre de la présente invention, la deuxième clé secrète est connue seulement du lecteur et du serveur, cette deuxième clé étant prise en compte dans le calcul, par le lecteur, de la deuxième signature transmise au serveur.

Selon un mode de mise en oeuvre de la présente invention, la deuxième clé secrète est connue seulement de l'étiquette électronique et du serveur et est mémorisée dans l'étiquette lors d'une première utilisation associée au serveur.

Selon un mode de mise en oeuvre de la présente invention, on utilise, pour les calculs de la deuxième signature

et de la grandeur de validation, une troisième clé connue seulement du lecteur et du serveur.

Selon un mode de mise en oeuvre de la présente invention, le procédé d'authentification comprend les étapes successives suivantes :

extraire de l'étiquette électronique des données à transmettre au serveur ;

transmettre ces données au serveur par l'intermédiaire du lecteur, en mémorisant ces données côté serveur et côté lecteur ;

générer, côté serveur, un nombre aléatoire ou pseudo-aléatoire, et le transmettre à l'étiquette par l'intermédiaire du lecteur, en mémorisant ce nombre côté serveur, côté lecteur et côté étiquette ;

calculer, côté étiquette électronique, une signature intermédiaire par application de ladite première fonction avec comme opérandes ledit nombre, lesdites données et ladite première clé secrète ; et

côté lecteur, calculer une grandeur intermédiaire par application de la première fonction avec comme opérandes ledit nombre, lesdites données et ladite première clé secrète.

Selon un mode de mise en oeuvre de la présente invention, ladite grandeur intermédiaire constitue ladite première signature, et le procédé comporte, côté lecteur, les étapes suivantes :

comparer ladite première signature à ladite grandeur intermédiaire calculée par le lecteur ; et

calculer ladite deuxième signature en prenant en compte ledit nombre, lesdites données, ladite deuxième clé secrète et le résultat de la comparaison précédente.

Selon un mode de mise en oeuvre de la présente invention, le calcul de la deuxième signature consiste à utiliser la deuxième fonction ou une troisième fonction selon le résultat de ladite comparaison.

Selon un mode de mise en oeuvre de la présente invention, le calcul de la deuxième signature consiste à utiliser la deuxième fonction avec comme opérandes ledit nombre, lesdites données, ladite deuxième clé secrète et le résultat de ladite comparaison.

Selon un mode de mise en oeuvre de la présente invention, le procédé comporte les étapes suivantes :

côté étiquette électronique, calculer une première combinaison de type OU-Exclusif de ladite signature intermédiaire avec ladite deuxième clé secrète, pour obtenir ladite première signature à transmettre au lecteur ; et

côté lecteur :

calculer une deuxième combinaison de type OU-Exclusif de la première signature reçue avec ladite grandeur intermédiaire ; et

calculer ladite deuxième signature par application de ladite deuxième fonction avec comme opérandes le résultat de la deuxième combinaison, ledit nombre et desdites données.

Selon un mode de mise en oeuvre de la présente invention, ladite deuxième fonction est une fonction de génération d'un nombre pseudoaléatoire, commune au lecteur et au serveur.

Selon un mode de mise en oeuvre de la présente invention, ladite fonction de génération pseudoaléatoire utilise comme graines lesdites données, ledit nombre et, respectivement côté lecteur et côté serveur, ladite deuxième combinaison de type OU-Exclusif et ladite deuxième clé secrète.

Selon un mode de mise en oeuvre de la présente invention, ladite étiquette électronique est un transpondeur électromagnétique.

L'invention prévoit également une étiquette électronique, comportant un circuit intégré et des moyens de mémorisation d'une première clé secrète et d'exécution d'une première fonction algorithmique.

L'invention prévoit également un lecteur d'étiquette électronique.

Selon un mode de réalisation de la présente invention, le lecteur comporte un générateur pseudoaléatoire propre à fournir ladite deuxième signature.

L'invention prévoit en outre un microcontrôleur d'authentification d'une étiquette électronique.

Selon un mode de réalisation de la présente invention, le microcontrôleur comporte un générateur pseudoaléatoire propre à fournir ladite grandeur de validation.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de mise en oeuvre et de réalisation particuliers, faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 représente, de façon très schématique et sous forme de blocs, un système exploitant une étiquette électronique selon un mode de réalisation du premier aspect de l'invention ;

la figure 2 est un organigramme d'un mode de mise en oeuvre de l'invention selon son premier aspect ;

la figure 3 représente, de façon très schématique et sous forme de blocs, un système exploitant une étiquette électronique selon un mode de réalisation du deuxième aspect de l'invention ;

la figure 4 est un organigramme partiel illustrant un mode de mise en oeuvre de l'invention selon son deuxième aspect ; et

la figure 5 représente, de façon très schématique et sous forme de blocs, un mode de réalisation d'un système selon l'invention pour la mise en oeuvre d'une fonction préférée d'authentification.

Les mêmes éléments du système et étape du procédé ont été désignés par les mêmes références aux différentes figures. Pour des raisons de clarté, seuls les étapes de procédé et les

constituants du système qui sont nécessaires à la compréhension de l'invention ont été représentés aux figures et seront décrits par la suite. En particulier, les moyens utilisés pour effectuer les transmissions proprement dites entre le circuit intégré de l'étiquette et son lecteur et entre le lecteur et le serveur n'ont pas été détaillés et ne font pas l'objet de la présente invention. Celle-ci s'applique quel que soit le protocole de transmission utilisé pour véhiculer les données et informations mises en oeuvre par l'invention.

La figure 1 représente, de façon très schématique et sous forme de blocs, un système du type auquel s'applique la présente invention selon ce premier aspect. Une étiquette électronique 1 (TAG) appartenant par exemple à la famille des transpondeurs électromagnétiques est portée par un produit (non représenté) que l'on souhaite authentifier. Dans le cas d'une étiquette de type transpondeur électromagnétique, celle-ci peut communiquer sans contact et sans fil (liaison radiofréquence 2) avec un lecteur 3 (READER) ou coupleur radiofréquence dont une fonction classique est de servir d'interface électrique entre l'étiquette électronique 1 et un serveur 4 (HOST) chargé d'exécuter l'application une fois l'étiquette électronique authentifiée. Le lecteur ou coupleur 3 communique avec le serveur 4, par exemple, par une liaison filaire 5.

Dans un exemple d'application aux cartouches d'encre pour imprimante, l'étiquette 1 est constituée d'une puce de circuit intégré fixée (par exemple, collée) ou incluse dans le boîtier de la cartouche d'encre. Le lecteur 3 est constitué d'un coupleur radiofréquence dont est équipée l'imprimante et qui communique avec un microcontrôleur constitué par le serveur 4. Le serveur 4 est, par exemple, inclus dans les circuits de commande de l'imprimante ou déporté dans un ordinateur auquel celle-ci est connectée.

L'authentification de la cartouche sert notamment à empêcher un piratage de la liaison 5 qui aurait pour conséquence de faire accepter par l'imprimante n'importe quelle cartouche.

Selon l'invention, on prévoit une phase d'authentification entre l'étiquette 1 et lecteur 3, puis une transmission de cette authentification vers le serveur 4.

Selon l'invention, la transmission de l'authentification du lecteur 3 au serveur 4 s'effectue selon une procédure sécurisée qui sera décrite ci-après en relation avec la figure 2.

Pour la mise en oeuvre de l'invention selon son premier aspect illustré par les figures 1 et 2, l'étiquette électronique 1 et le lecteur 3 comportent ou intègrent une clé secrète KS connue des deux. Selon ce premier aspect, le lecteur 3 est dédié à un type d'étiquette 1 (par exemple, un type de cartouche d'imprimante).

Comme l'illustre la figure 1, l'étiquette 1 et le lecteur 3 possèdent également une fonction f commune de chiffrement, comme on le verra par la suite en relation avec la figure 2.

Le lecteur 3 et le microcontrôleur 4 possèdent ou intègrent chacun une clé commune K1 ainsi qu'une fonction g de chiffrement. Selon ce mode de réalisation, le lecteur 3 contient également une fonction h pour coder une absence d'authentification.

Une caractéristique de l'invention est de différencier, dans la transmission entre le lecteur 3 et le serveur 4, la fonction de codage ou de chiffrement mise en oeuvre selon que l'authentification opérée par le lecteur 3 est positive ou non. Ainsi, on ne se contente pas de transmettre au serveur 4 qu'on est en présence d'une authentification correcte et ne rien transmettre en l'absence d'authentification. On transmet toujours quelque chose, mais le serveur 4 ne l'interprète que s'il s'agit d'une authentification positive.

Ce qui est illustré en figure 1 par une différenciation de fonction (g et h) doit s'entendre soit d'une différenciation de la fonction codant une même donnée résultat comme cela sera exposé par la suite en relation avec la figure 2, soit

d'un même fonction codant deux données différentes selon le résultat de l'authentification.

Cette transmission entre le lecteur 3 et le serveur 4 est indépendante de la transmission entre l'étiquette 1 et le lecteur 3, en ce sens que le serveur 4 ignore à la fois la clé KS partagée entre le lecteur et l'étiquette, et la fonction f de chiffrement mise en oeuvre dans la transmission entre ces deux éléments.

La figure 2 illustre, sous forme d'organigramme, un mode de mise en oeuvre de l'invention selon son premier aspect. En figure 2, les étapes du procédé illustré par l'organigramme ont été réparties dans trois colonnes TAG, READER et HOST selon qu'elles sont effectuées par l'étiquette électronique, par le lecteur ou par le serveur.

La première étape (bloc 10, GEN(DATA)) du procédé d'authentification de l'invention consiste en la génération, par l'étiquette électronique (TAG), d'un message de données DATA à transmettre pour authentification. Ce message DATA contient, par exemple, un identifiant du produit portant l'étiquette électronique (par exemple, le numéro de série et/ou le type de cartouche d'encre). La génération de cet identifiant par l'étiquette électronique est, par exemple et de façon classique, provoquée par l'alimentation de cette étiquette lorsqu'elle entre dans le champ du lecteur 3. Le fonctionnement d'une étiquette de type transporteur électromagnétique est parfaitement connu et ne fait pas l'objet de l'invention. Brièvement, l'alimentation du circuit intégré de l'étiquette (ou une commande spécifique reçue du lecteur) provoque l'émission, par rétromodulation de la porteuse de téléalimentation, du message DATA.

Lorsqu'il reçoit les données, le lecteur (READER) qui possède un démodulateur adapté au type de transpondeur, mémorise (bloc 11, MEM(DATA)) le message transmis. Par ailleurs, le lecteur communique les données DATA au serveur 4 qui lui-même les mémorise (bloc 12, MEM(DATA)).

La transmission exposée ci-dessus ne constitue pas proprement dit une authentification. C'est simplement la transmission d'un identifiant de l'étiquette électronique au serveur (HOST). Avant d'autoriser la poursuite de l'application, le serveur doit s'assurer que l'étiquette appartient à un produit authentique. Il initie donc la procédure d'authentification proprement dite.

Selon l'invention, le serveur génère (bloc 13, GEN(ALEA)) un nombre aléatoire ou pseudoaléatoire ALEA qu'il mémorise et communique au lecteur 3. Le lecteur 3 mémorise (bloc 14, MEM(ALEA)) le nombre ALEA et le transmet à l'étiquette électronique 1.

Le circuit intégré de l'étiquette 1 calcule alors (bloc 15, St=f(ALEA, DATA, KS)) une première signature St en utilisant la fonction algorithmique f et comme opérandes les grandeurs ALEA, DATA et KS. En d'autres termes, l'étiquette électronique calcule sa signature St qu'elle transmet au lecteur 3.

En parallèle (ou après avoir reçu la signature St de l'étiquette 1), le lecteur 3 calcule (bloc 16, Sr=f(ALEA, DATA, KS)) une grandeur Sr en appliquant la même fonction algorithmique f aux données ALEA, DATA et KS qu'il contient. On voit ici apparaître le rôle de la clé KS et de la fonction f communes à l'étiquette 1 et au lecteur 3 qui est de permettre une authentification chiffrée de l'étiquette par le lecteur.

Le lecteur 3 effectue ensuite un test de cohérence (bloc 17, St=Sr?) entre la grandeur Sr qu'il a calculé et la signature St transmise par l'étiquette électronique.

A ce stade du procédé d'authentification, l'invention prévoit, de façon caractéristique, de ne pas transmettre le résultat (Y ou N) de l'authentification en clair (c'est-à-dire de façon visible) au serveur. Selon l'invention, on chiffre l'authentification qu'elle soit positive ou négative.

Dans l'exemple représenté, le lecteur calcule une deuxième signature SIGN qui est différente selon le résultat du test 17. Si le test 17 a validé (Y) l'authentification de

l'étiquette 1, on calcule (bloc 18, SIGN=g(ALEA, DATA, K1)) la signature SIGN en appliquant la fonction algorithmique g aux grandeurs ALEA, DATA et K1. En cas d'authentification négative, le lecteur 3 calcule (bloc 19, SIGN=h(ALEA, DATA, K1)) la signature SIGN en appliquant la fonction h aux mêmes grandeurs.

La signature SIGN ainsi calculée est alors transmise au serveur exploitant l'authentification. Le serveur calcule (bloc 20, VAL=g(ALEA, DATA, K1)) au préalable ou après réception de la signature SIGN, une grandeur de validation VAL correspondant à l'application de la fonction g aux grandeurs ALEA, DATA et K1 qu'il connaît. On voit apparaître ici le rôle de la clé secrète K1, connue du lecteur et du microcontrôleur et de la fonction g qu'ils partagent.

Le serveur compare (bloc 21, SIGN=VAL?) la signature SIGN reçue du lecteur a la valeur de validation VAL qu'il a calculé. Le résultat Y ou N de ce test authentifie ou non l'étiquette électronique 1.

Ce résultat est alors exploité (bloc 22, AUTHENT) par les procédures classiques qui suivent une authentification, qui ne font pas en elles-mêmes l'objet de l'invention.

Un avantage de la présente invention est qu'en codant aussi bien l'authentification positive que l'authentification négative côté lecteur 3, on empêche un pirate de tirer profit d'un espionnage des communications sur la liaison 5 (figure 1). En effet, celui-ci observera dans tous les cas un message que l'authentification soit ou non positive.

Un autre avantage de l'invention est que l'authentification mise en oeuvre entre le lecteur et l'étiquette électronique est indépendante du serveur, plus précisément du microcontrôleur 4, exploitant les résultats de l'authentification et contrôlant le déroulement de l'application.

Les données DATA transmises peuvent être quelconques pourvu qu'elles permettent la mise en oeuvre du procédé d'authentification décrit. Par exemple, le mot de données DATA est composé d'une partie de données fixes liées à l'étiquette et

d'une partie de données variables. La partie de donnée fixe est, par exemple, un numéro unique propre à chaque étiquette. La partie variable correspond, par exemple, au résultat d'un compteur décrémentiel totalisant le nombre d'authentifications effectuées. Un tel mode de réalisation garantit qu'en utilisation normale il ne puisse pas y avoir plusieurs authentifications avec la même donnée, ce qui améliore la fiabilité du système.

Le nombre aléatoire ALEA généré par le serveur pourra être un nombre pseudoaléatoire utilisant une donnée comme graine. Par exemple, ce nombre pseudoaléatoire pourra utiliser une partie de la donnée DATA comme graine. Par exemple, on peut sauvegarder la valeur de l'état courant en sortie du générateur pseudo-aléatoire, lors de l'extinction du système, pour utiliser cette valeur comme graine à l'utilisation suivante. Toutefois, idéalement, la graine est issue d'une grandeur "analogique", par exemple, un bruit thermique dans une résistance.

La figure 3 représente, de façon très schématique et sous forme de blocs, un système à étiquette électronique, lecteur et serveur selon le deuxième aspect de l'invention. Cette figure est à rapprocher de la figure 1 et seules les différences par rapport à cette figure 1 seront exposées.

Selon ce deuxième aspect de l'invention, on cherche à pouvoir individualiser les clés KS contenues dans chacune des étiquettes électroniques, donc dans chacun des produits à authentifier. Une telle individualisation requiert que ces clés soient écrites dans les étiquettes électroniques, par exemple et de façon préférentielle, lors de la première utilisation du produit qui les porte.

Ainsi, dans le mode de réalisation illustré par la figure 3, l'étiquette électronique 1 et le lecteur 3 partagent la clé KS et la fonction f comme dans le mode de réalisation précédent. Une différence par rapport à ce mode de réalisation précédent est que le lecteur 3 et le serveur 4 ne partagent que la fonction g. De plus, l'étiquette 1 et le serveur 4 partagent

quant à eux une deuxième clé K2 qui est inscrite dans l'étiquette électronique lors de sa première utilisation associée au serveur 4.

Dans l'exemple d'application aux cartouches d'imprimante, cela revient à dire que, lors de la mise en place d'une nouvelle cartouche dans une imprimante donnée, le microcontrôleur associé à cette imprimante fournira à l'étiquette électronique de la cartouche une clé K2 générée, de préférence de façon aléatoire, et stockée dans l'étiquette électronique.

Lors de l'authentification de cette étiquette électronique, par exemple à chaque utilisation, le procédé débute comme le procédé exposé en relation avec la figure 2 jusqu'à l'étape 15 de calcul d'une signature intermédiaire St côté étiquette électronique.

La figure 4 représente la suite du procédé d'authentification selon un mode de mise en oeuvre de ce deuxième aspect de l'invention. Côté étiquette 1 (TAG), la donnée de départ est donc la signature intermédiaire St (St=f(ALEA, DATA, KS)). Côté lecteur 3 (READER), celui-ci a calculé une grandeur intermédiaire correspondante Sr (Sr=f(ALEA, DATA, KS)).

Selon ce deuxième mode de mise en oeuvre, l'étiquette électronique calcule (bloc 30, Stt=St+K2) la première signature Stt comme correspondant à une combinaison de type OU-Exclusif (XOR) de la signature intermédiaire St avec la clé K2. Cette signature Stt, chiffrée par la clé K2, est transmise au lecteur 3. De son côté, ce lecteur 3 calcule (bloc 31, Srt=Stt+Sr) une combinaison Srt de type OU-Exclusif de la première signature Stt avec la grandeur intermédiaire Sr qu'il a calculé précédemment. Si l'étiquette est authentique (c'est-à-dire contient les bonnes clés KS et K2 et la bonne fonction f), la combinaison Srt est égale à la clé K2 (Sr=St). Cette combinaison Srt sert au lecteur 3 pour calculer (bloc 32, SIGN=g(ALEA, DATA, Srt)) la deuxième signature SIGN en appliquant la fonction g aux opérandes ALEA, DATA et Srt. Cette signature SIGN est alors transmise au serveur 4 (HOST).

On notera ici une autre différence par rapport au premier mode de mise en oeuvre qui est que le lecteur ne possède pas à proprement parlé de fonction d'authentification négative (fonction h, figures 1 et 2). La différenciation entre une authentification et une absence d'authentification provient ici de la prise en compte de la grandeur Srt dans l'application de la fonction g. Cette variante, qui est nécessaire dans le mode de réalisation de la figure 4, pourra être mise en oeuvre de façon alternative dans le mode de réalisation de la figure 2 en utilisant comme opérande à la fonction g, le résultat positif ou négatif du test du bloc 17.

En revenant au mode de réalisation de la figure 4, le serveur vérifie l'authenticité de l'étiquette électronique 1 en comparant (bloc 31, SIGN=VAL?) la signature SIGN reçue du lecteur 3 à une grandeur de validation VAL calculée (bloc 33, VAL=g(ALEA, DATA, K2)) en appliquant la fonction g aux grandeurs ALEA, DATA et K2. Si les grandeurs SIGN et VAL sont identiques, cela signifie que l'étiquette électronique possède bien, non seulement la fonction f du lecteur 3, mais également la clé K2 inscrite par le serveur 4 dans l'étiquette 1 lors de sa première utilisation. Dans le cas contraire, le serveur 4 peut mettre en oeuvre les procédures d'absence d'authentification.

Un avantage de ce mode de mise en oeuvre est qu'il ne nécessite pas, côté étiquette électronique 1, de stocker la clé K2 dès la fabrication. Cela permet d'individualiser les produits à authentifier au moment de leur première utilisation par un appareil donné.

Un autre avantage de ce mode de réalisation est que si la fonction g parvient à être cassée, c'est-à-dire découverte par un pirate, malgré les précautions prises, le produit portant l'étiquette électronique 1 ne pourra cependant pas être utilisé sur un autre appareil (plus précisément avec un autre microcontrôleur 4), dans la mesure où la clé K2 sera alors inconnue de cet autre appareil.

La contrainte à respecter pour la mise en oeuvre de l'invention selon son deuxième aspect est l'emploi d'une fonction de type OU-Exclusif dans les fonctions de combinaison (blocs 30 et 31).

Bien entendu, les modes de réalisation des figures 1, 2 et 3, 4 peuvent être combinés. Dans ce cas, les grandeurs SIGN (bloc 32, figure 4) et VAL (bloc 33, figure 4) sont fonction également de la clé K1, connue seulement du lecteur et du serveur, considérée alors comme une troisième clé.

La figure 5 illustre un mode de réalisation préféré d'une fonction de codage ou chiffrement (g) entre lecteur et serveur selon la présente invention. La figure 5 est à rapprocher des figures 1 et 3 en ce qu'elle représente, de façon schématique et sous forme de blocs, une étiquette électronique 1, un lecteur 3 et un serveur 4.

Selon ce mode de réalisation, le lecteur 3 et le serveur 4 comportent chacun un générateur pseudoaléatoire (PSEUDO RAND GEN) 40, respectivement 40', correspondant à la fonction g. Les deux générateurs 40 et 40' sont identiques en ce sens que, pour une même graine donnée, ils fournissent une même valeur en sortie. En d'autres termes, les fonctions de génération pseudoaléatoire des deux blocs 40 et 40' sont les mêmes.

Selon l'invention, les générateurs 40 et 40' fournissent respectivement, côté lecteur 3 et côté serveur 4, les grandeurs SIGN et VAL, c'est-à-dire les grandeurs permettant au serveur de valider l'authentification réalisée par le lecteur.

Dans chaque générateur pseudoaléatoire, on utilise une graine (B, bloc 41 et 41') fonction de différentes grandeurs utilisées dans le processus d'authentification.

Selon l'invention, côté lecteur 3, la graine B prend en compte les grandeurs DATA, ALEA et Srt (en variante la grandeur Sr dans la mise en oeuvre de la figure 2). Côté serveur 4, la graine B' prend en compte les grandeurs DATA, ALEA et K2 (en variante, la grandeur K1 dans la mise en oeuvre de la figure 2). Les graines B et B' sont, par exemple, obtenues par concaté-

nation des grandeurs prises en compte ou par une fonction plus complexe.

Selon l'invention, les deux générateurs pseudoaléatoires 40 et 40' sont donc initialisés avec une même graine si l'authentification est correcte.

Dans le mode de réalisation de la figure 4, la valeur Srt sera, en cas d'authentification négative, différente de la clé K2.

Dans le mode de réalisation de la figure 2, si l'authentification faite par le lecteur 3 (test 17) est incorrecte, le générateur 40 est initialisé avec une grandeur différente que celle initialisant le générateur 40'. Pour cela, le résultat binaire (valeur 0 ou 1) du test 17 participe à la graine B. Côté serveur, la valeur (par exemple, 1) choisie arbitrairement pour indiquer une authentification correcte participe à la graine B'. On notera qu'ici la fonction g du lecteur 3 sera la même que l'authentification soit positive ou négative.

Dans tous les cas, cela permet bien de masquer l'authentification en transmettant à la fois une authentification positive et une authentification négative entre le lecteur et le serveur.

Un avantage du mode de réalisation de la figure 5 est que sa mise en oeuvre est particulièrement peu coûteuse et simple, tout en offrant une sécurité optimale contre les éventuels piratages.

La fréquence des authentifications dépend de l'application. Par exemple, pour une imprimante, une authentification pourra être déclenchée à chaque utilisation (à chaque impression), à chaque mise en service (allumage), à chaque détection de changement de cartouche et/ou périodiquement. Pour une machine à boissons, l'authentification pourra être mise en oeuvre après chaque intervention de remplacement d'une recharge en produit, détectée de façon classique.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, le choix des fonctions de génération pseudoaléatoires ou plus généralement des fonctions algorithmiques mises en oeuvre dans les différents échanges est à la portée de l'homme du métier à partir des indications fonctionnelles données ci-dessus, de l'application, et des fonctions algorithmiques et de génération pseudoaléatoire classiques dont il dispose. Par ailleurs, les tailles (nombre de bits) des grandeurs numériques utilisées seront choisies, de façon classique, notamment en fonction de la sécurité souhaitée.

De plus, l'exploitation des résultats de l'authentification ne fait pas l'objet de la présente invention et pourra donc être quelconque selon l'application.

En outre, les processus d'authentification peuvent être mis en oeuvre, côté lecteur 3 et côté serveur 4, soit de façon logicielle au moyen d'un microcontrôleur, soit en logique câblée. Toutefois, côté étiquette électronique 1, on notera que l'invention, sans exclure une mise en oeuvre logicielle par un microcontrôleur, s'applique préférentiellement à une réalisation en logique câblée, c'est-à-dire d'une étiquette peu coûteuse.

Enfin, l'étiquette électronique comprenant un circuit intégré pour la mise en oeuvre de l'invention pourra être un élément rapporté sur le produit (par exemple, recharge) à authentifier, ou inclus dans celui-ci (par exemple, inclus dans le boîtier du produit).

REVENDICATIONS

1. Procédé d'authentification d'une étiquette électronique (1) par un serveur (4) communiquant avec cette étiquette par l'intermédiaire d'un lecteur (3), caractérisé en ce qu'il consiste :

à calculer, côté étiquette (1), une première signature numérique (St, Stt) à l'aide d'au moins une première fonction (f) partagée par l'étiquette et le lecteur, en prenant en compte au moins une première clé secrète (KS) connue seulement de l'étiquette électronique et du lecteur ;

à transmettre la première signature au lecteur ;

à calculer, côté lecteur (3), une deuxième signature numérique (SIGN) à l'aide d'au moins une deuxième fonction (g), différente de la première fonction et partagée par le lecteur et le serveur, en tenant compte de la première signature ;

à transmettre la deuxième signature (SIGN) au serveur ; et

à vérifier, côté serveur (4), la cohérence entre la deuxième signature et une grandeur de validation (VAL) calculée à partir de ladite deuxième fonction (g) et d'une deuxième clé secrète (K1, K2) connue du serveur et d'un seul élément choisi parmi l'étiquette et le lecteur.

2. Procédé selon la revendication 1, caractérisé en ce que la deuxième clé secrète (K1) est connue seulement du lecteur (3) et du serveur (4), cette deuxième clé étant prise en compte dans le calcul, par le lecteur, de la deuxième signature (SIGN) transmise au serveur.

3. Procédé selon la revendication 1, caractérisé en ce que la deuxième clé secrète (K2) est connue seulement de l'étiquette électronique (1) et du serveur (4) et est mémorisée dans l'étiquette lors d'une première utilisation associée au serveur.

4. Procédé selon la revendication 3, caractérisé en ce qu'il consiste à utiliser, pour les calculs de la deuxième signature (SIGN) et de la grandeur de validation (VAL), une

troisième clé (K1) connue seulement du lecteur (3) et du serveur (4).

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comprend les étapes successives suivantes :

extraire de l'étiquette électronique (1) des données (DATA) à transmettre au serveur (4) ;

transmettre ces données au serveur (4) par l'intermédiaire du lecteur (3), en mémorisant ces données côté serveur et côté lecteur ;

générer, côté serveur (4), un nombre aléatoire ou pseudoaléatoire (ALEA), et le transmettre à l'étiquette (1) par l'intermédiaire du lecteur, en mémorisant ce nombre (ALEA) côté serveur, côté lecteur et côté étiquette ;

calculer, côté étiquette électronique (1), une signature intermédiaire (St) par application de ladite première fonction (f) avec comme opérandes ledit nombre (ALEA), lesdites données (DATA) et ladite première clé secrète (KS) ; et

côté lecteur (3), calculer une grandeur intermédiaire (Sr) par application de la première fonction (f) avec comme opérandes ledit nombre (ALEA), lesdites données (DATA) et ladite première clé secrète (KS).

6. Procédé selon la revendication 5 dans son rattachement à la revendication 2, ladite grandeur intermédiaire constituant ladite première signature (St), caractérisé en ce qu'il comporte, côté lecteur (3), les étapes suivantes :

comparer ladite première signature (St) à ladite grandeur intermédiaire (Sr) calculée par le lecteur ; et

calculer ladite deuxième signature (SIGN) en prenant en compte ledit nombre (ALEA), lesdites données (DATA), ladite deuxième clé secrète (K1) et le résultat de la comparaison précédente.

7. Procédé selon la revendication 6, caractérisé en ce que le calcul de la deuxième signature (SIGN) consiste à

utiliser la deuxième fonction (g) ou une troisième fonction (h) selon le résultat de ladite comparaison.

8. Procédé selon la revendication 6, caractérisé en ce que le calcul de la deuxième signature (SIGN) consiste à utiliser la deuxième fonction (g) avec comme opérandes ledit nombre (ALEA), lesdites données (DATA), ladite deuxième clé secrète (K1) et le résultat de ladite comparaison.

9. Procédé selon la revendication 5 dans son rattachement à la revendication 3, caractérisé en ce qu'il comporte les étapes suivantes :

côté étiquette électronique (1), calculer (31) une première combinaison de type OU-Exclusif de ladite signature intermédiaire (St) avec ladite deuxième clé secrète (K2), pour obtenir ladite première signature (Stt) à transmettre au lecteur (3) ; et

côté lecteur (3) :

calculer (31) une deuxième combinaison (Srt) de type OU-Exclusif de la première signature reçue (Stt) avec ladite grandeur intermédiaire (Sr) ; et

calculer ladite deuxième signature (SIGN) par application de ladite deuxième fonction (g) avec comme opérandes le résultat de la deuxième combinaison, ledit nombre (ALEA) et desdites données (DATA).

10. Procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce que ladite deuxième fonction (g) est une fonction de génération d'un nombre pseudoaléatoire, commune au lecteur (3) et au serveur (4).

11. Procédé selon la revendication 10 dans son rattachement à la revendication 9, caractérisé en ce que ladite fonction de génération pseudoaléatoire utilise comme graines (B, B') lesdites données (DATA), ledit nombre (ALEA) et, respectivement côté lecteur et côté serveur, ladite deuxième combinaison de type OU-Exclusif (Srt) et ladite deuxième clé secrète (K2).

12. Procédé selon l'une quelconque des revendications 1 à 11, caractérisé en ce que ladite étiquette électronique (1) est un transpondeur électromagnétique.

13. Etiquette électronique (1), caractérisée en ce qu'elle comporte un circuit intégré et des moyens de mémorisation d'une première clé secrète (KS) et d'exécution d'une première fonction algorithmique (f) pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 12.

14. Lecteur (3) d'étiquette électronique (1), caractérisé en ce qu'il comporte des moyens pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 12.

15. Lecteur selon la revendication 14 dans son rattachement aux revendications 10 ou 11, caractérisé en ce qu'il comporte un générateur pseudoaléatoire (40) propre à fournir ladite deuxième signature (SIGN).

16. Microcontrôleur (4) d'authentification d'une étiquette électronique (1), caractérisé en ce qu'il comporte des moyens propres à la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 12.

17. Microcontrôleur selon la revendication 16 dans son rattachement aux revendications 10 ou 11, caractérisé en ce qu'il comporte un générateur pseudoaléatoire (40') propre à fournir ladite grandeur de validation (VAL).

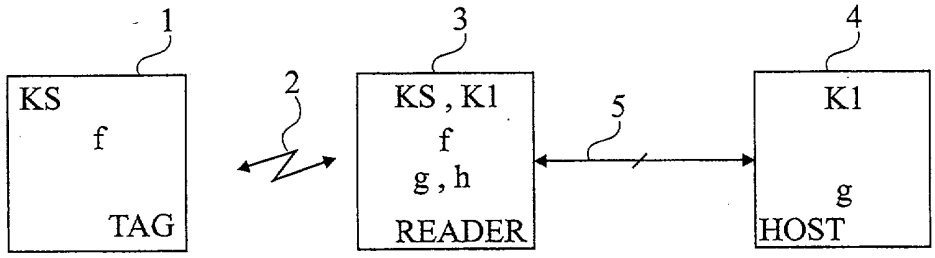

1
KS
f
TAG
2
3
KS , K1
f
g , h
READER
5
4
K1
g
HOST

Fig 1

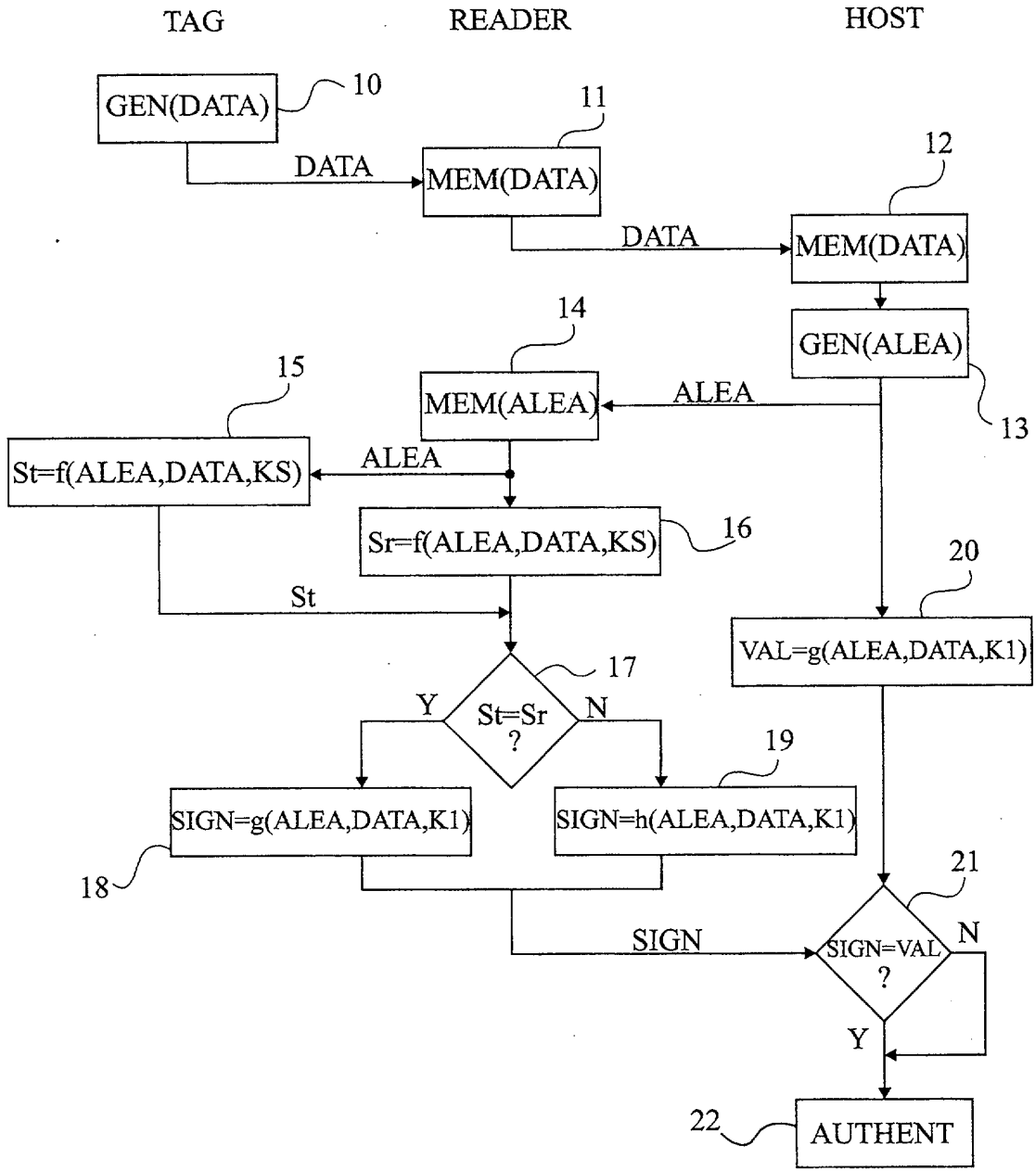

TAG
READER
HOST
GEN(DATA)
10
DATA
MEM(DATA)
11
DATA
MEM(DATA)
12
GEN(ALEA)
13
MEM(ALEA)
14
ALEA
St=f(ALEA,DATA,KS)
15
ALEA
Sr=f(ALEA,DATA,KS)
16
St
VAL=g(ALEA,DATA,K1)
20
St=Sr ?
17
Y
N
SIGN=g(ALEA,DATA,K1)
18
SIGN=h(ALEA,DATA,K1)
19
SIGN
SIGN=VAL ?
21
N
Y
AUTHENT
22

Fig 2

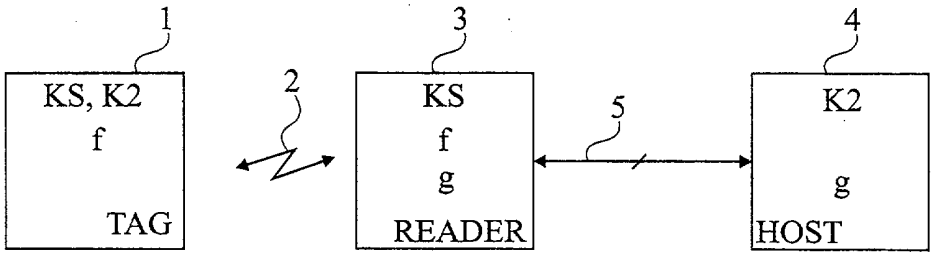


Fig 3

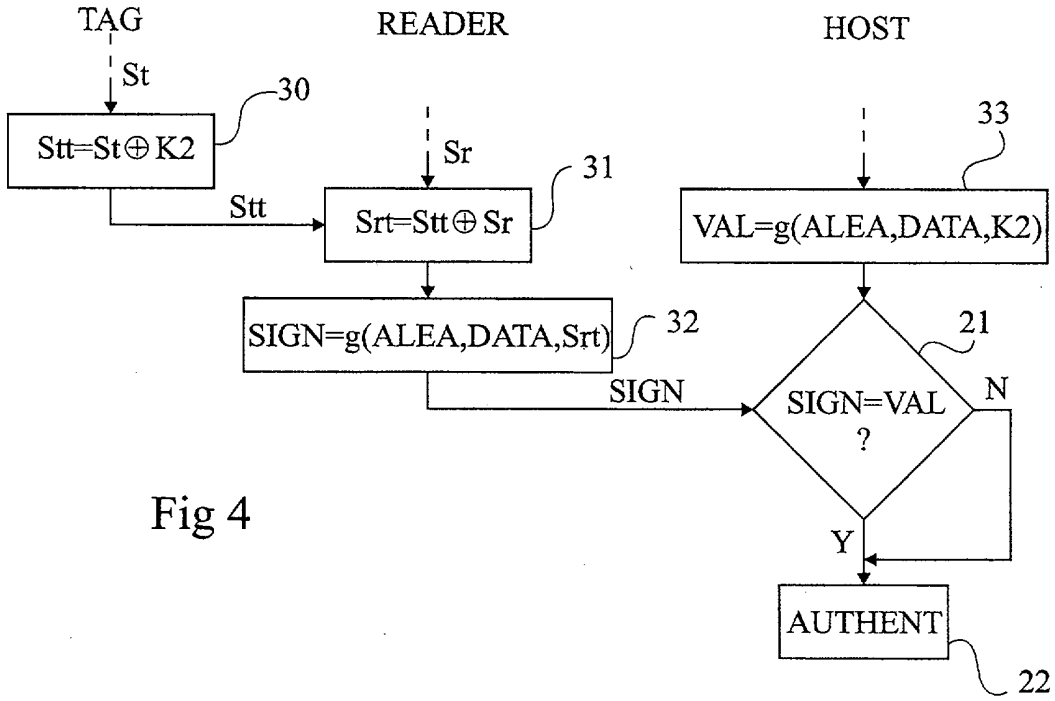


Fig 4

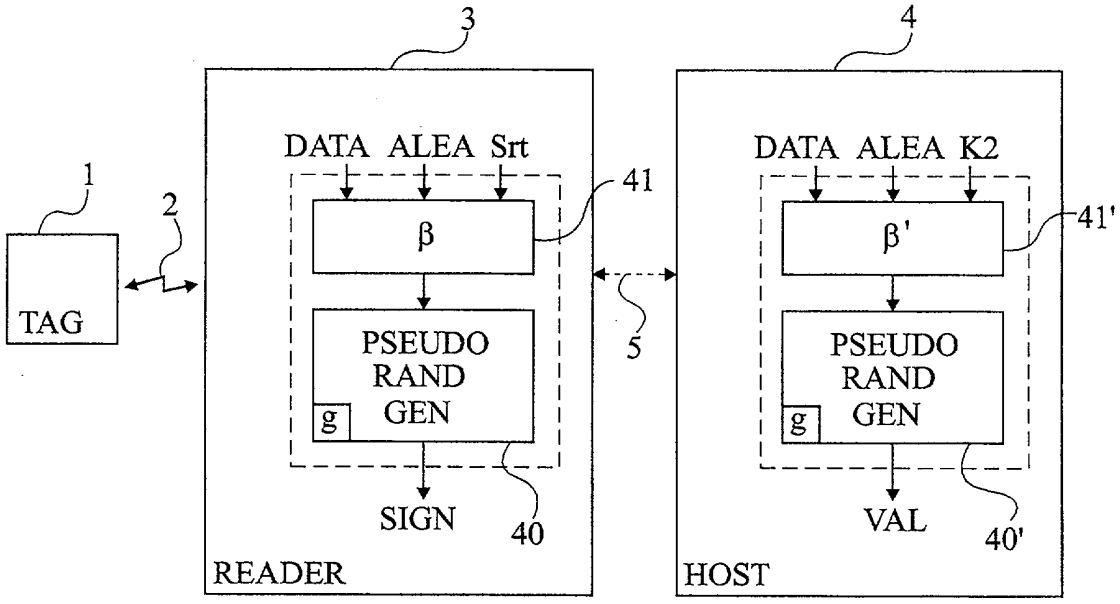


Fig 5

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2841020

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 621208
FR 0207298

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 0 032 193 A (INTERNATIONAL BUSINESS MACHINES) 22 juillet 1981 (1981-07-22) * le document en entier * ---	1-3,5,6, 9,13,14, 16	G06K7/08 H04L9/28
A	WO 97 42610 A (FRANCE TELECOM) 13 novembre 1997 (1997-11-13) * abrégé; revendications; figures 6,7 * ---	1,5,9, 13,14,16	
A	FR 2 796 788 A (FRANCE TELECOM) 26 janvier 2001 (2001-01-26) -----		

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G07F
G06F
H04L

Date d'achèvement de la recherche	Examinateur
9 avril 2003	David, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
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 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0207298 FA 621208

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 09-04-2003
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0032193	A	22-07-1981	US	4302810 A	24-11-1981
			AU	533865 B2	15-12-1983
			AU	6410080 A	20-08-1981
			BR	8008516 A	21-07-1981
			CA	1147863 A1	07-06-1983
			DE	3065401 D1	24-11-1983
			EP	0032193 A1	22-07-1981
			ES	8202168 A1	01-04-1982
			JP	1275574 C	31-07-1985
			JP	56123589 A	28-09-1981
			JP	60001628 B	16-01-1985
WO 9742610	A	13-11-1997	FR	2748591 A1	14-11-1997
			EP	0909433 A1	21-04-1999
			WO	9742610 A1	13-11-1997
			JP	2000510254 T	08-08-2000
			US	6105862 A	22-08-2000
FR 2796788	A	26-01-2001	FR	2796788 A1	26-01-2001
			AU	6577900 A	05-02-2001
			EP	1195020 A1	10-04-2002
			WO	0106702 A1	25-01-2001
			JP	2003505927 T	12-02-2003

EPO FORM P0465