(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 048 631 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
15.04.2009 Bulletin 2009/16

(51) Int Cl.:
G07F 7/10 *(2006.01)* *G06K 19/073* *(2006.01)*

(21) Numéro de dépôt: **08166402.1**

(22) Date de dépôt: **10.10.2008**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Etats d'extension désignés:
AL BA MK RS

(30) Priorité: **12.10.2007 FR 0758292**

(71) Demandeur: **Compagnie Industrielle et Financiere d'Ingenierie "Ingenico"**
92200 Neuilly sur Seine (FR)

(72) Inventeur: **Naccache, David**
75018, Paris (FR)

(74) Mandataire: **Bioret, Ludovic**
Cabinet Vidon
Technopôle Atalante
16 B, rue de Jouanet
35703 Rennes Cedex 07 (FR)

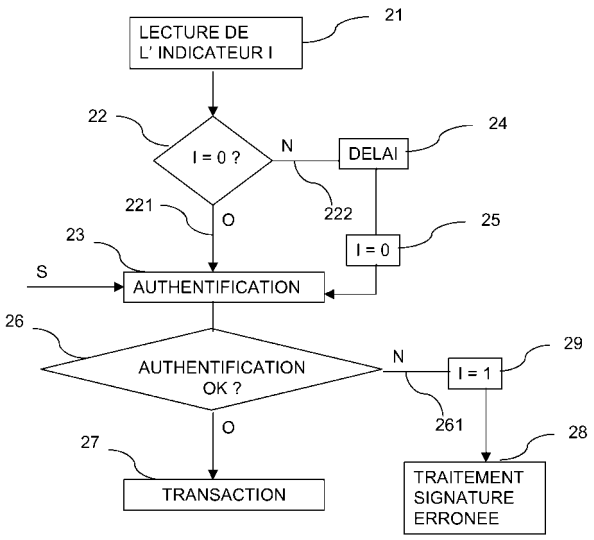
(54) Procédé d'authentification, objet portatif et programme d'ordinateur correspondants

(57) L'invention concerne un procédé d'authentification d'un porteur d'un objet portatif comprenant des moyens de mémorisation d'au moins une information secrète, comprenant les étapes suivantes :
- traitement d'authentification d'une signature délivrée par ledit porteur, tenant compte de ladite information secrète ;
- délivrance d'une information de décision d'authentification, positive ou négative,

le procédé mettant en oeuvre, dans une mémoire non volatile dudit objet portatif, un indicateur de signature erronée pouvant prendre une valeur indiquant une situation normale et au moins une valeur indiquant une situation anormale, et comprenant :
- après ladite étape de délivrance, une étape d'écriture, dans ledit indicateur de signature erronée, d'une valeur indiquant une situation anormale, si ladite décision d'authentification est négative ; et
- avant ladite étape d'authentification, et si ledit indicateur de signature erronée contient une valeur indiquant une situation anormale, une étape de génération d'un retard.

Selon l'invention, ladite étape d'écriture comprend également une opération de mémorisation d'au moins une information relative au contexte, tels que la date et l'heure et/ou un identifiant du terminal utilisé.

Figure 2



EP 2 048 631 A1

Description

1. Domaine de l'invention

[0001] Le domaine de l'invention est celui des objets portatifs sécurisés, tels que des cartes à microprocesseur, ou cartes à puce. Plus précisément, l'invention concerne l'authentification des porteurs, ou utilisateurs, de tels objets portatifs, et la lutte contre les tentatives de fraude, par des personnes mal intentionnées tentant d'utiliser un objet portatif sécurisé dont elles ne sont pas titulaires.

2. Art antérieur

[0002] Par la suite, on décrit l'utilisation de cartes à puce comme cartes de paiement. D'autres applications, telles que l'accès à un site ou à un service, sont bien sûr également connues, et traitées de la même façon. De même, on comprend que la notion de « carte à puce » peut être généralisée à d'autres types d'objets portatifs équipés d'un microprocesseur sécurisé.

[0003] Les cartes à puce sont connues et sont actuellement utilisées largement. Lorsqu'une carte à puce est utilisée comme carte de paiement, l'utilisateur autorisé (le titulaire) de la carte à puce peut l'utiliser par exemple pour régler des achats chez un commerçant ou pour effectuer un retrait de billets à un distributeur automatique de billets.

[0004] Lorsque la carte à puce est utilisée pour effectuer une telle opération, il est généralement nécessaire que l'utilisateur autorisé glisse sa carte à puce dans un terminal de paiement et entre son code confidentiel à l'aide d'un clavier du terminal de paiement.

[0005] Ce code confidentiel est également appelé signature, numéro d'identification personnel (NIP) du titulaire de la carte, que l'on appelle aussi PIN (en anglais Personal Identification Number) ou code secret. Le code confidentiel associé à une carte à puce de paiement est généralement composé d'une suite d'au moins quatre chiffres.

[0006] Une information secrète est par ailleurs stockée (mémorisée) dans une mémoire de la carte à puce. Une vérification (traitement mathématique) est réalisée dans la carte à puce, tenant compte (au moins) de cette information secrète et du code confidentiel. Ainsi, quand le code saisi au clavier (signature) concorde avec l'information secrète mémorisée dans la carte à puce, la carte délivre un résultat d'authentification positif et autorise, par exemple, des transactions électroniques sécurisées.

[0007] Un problème est qu'une carte à puce est vulnérable aux attaques d'un tiers malintentionné (un fraudeur) qui pourrait, par exemple après avoir volé la carte à puce, tenter de saisir au clavier un grand nombre de combinaisons successives de code pour retrouver le code confidentiel de la carte.

[0008] Différentes solutions à ce problème ont été proposées. La plus connue est sans doute celle qui utilise un compteur contenu dans une mémoire de la carte à puce qui mémorise le nombre de tentatives incorrectes d'entrée du code confidentiel pendant un laps de temps prédéterminé. Ainsi, l'utilisation de la carte à puce est bloquée lorsque le nombre de tentatives incorrectes successives pendant ce laps de temps prédéterminé atteint une valeur seuil prédéterminée.

[0009] Un inconvénient avec cette solution est qu'un fraudeur peut interrompre l'alimentation de la carte à puce afin de provoquer une remise à zéro du compteur et alimenter de nouveau la carte à puce afin d'effectuer de nouvelles tentatives pour retrouver le code confidentiel, et ainsi de suite.

[0010] Une solution complémentaire ou alternative à la précédente consiste à imposer un délai de temporisation prédéterminé entre deux tentatives de saisie d'un code, lorsque la première tentative est incorrecte, afin de ralentir le fraudeur dans sa recherche du code confidentiel par essais successifs et donc de diminuer la probabilité que le code confidentiel ne soit découvert par un fraudeur. Il est envisageable cependant que le fraudeur accélère l'horloge externe qui pilote la carte à puce afin de réduire le temps d'attente entre deux tentatives successives de saisie d'un code.

[0011] Dans le cas où le temps de mise sous tension de la carte à puce est inférieur au délai de temporisation entre deux tentatives successives de saisie d'un code (lorsque la première tentative est incorrecte), le fraudeur peut également interrompre temporairement l'alimentation de la carte à puce suite à la première tentative et ainsi réduire le temps d'attente entre deux tentatives successives de saisie d'un code.

3. Objectifs de l'invention

[0012] L'invention a notamment pour objectif de pallier ces inconvénients de l'art antérieur.

[0013] Plus précisément, un objectif de l'invention est de fournir une technique de lutte contre les tentatives d'usage frauduleux d'une carte à puce, ou d'un objet portatif similaire.

[0014] Un autre objectif de l'invention est de diminuer la probabilité qu'un éventuel fraudeur découvre le code confidentiel de la carte à puce par essais successifs dans un laps de temps relativement court, quels que soient les moyens techniques mis en oeuvre.

[0015] L'invention a également pour objectif de fournir une telle technique qui soit relativement peu coûteuse, fiable et simple à mettre en oeuvre.

4. Exposé de l'invention

[0016] L'invention propose une solution nouvelle qui ne présente pas l'ensemble de ces inconvénients de l'art antérieur, sous la forme d'un procédé d'authentification d'un porteur d'un objet portatif selon la revendication 1.

[0017] Ainsi, l'invention permet de ralentir les tentatives d'un éventuel fraudeur qui aurait l'intention d'entrer

successivement une série de signatures, afin de trouver la signature correcte, permettant d'authentifier un porteur. En effet, même si le fraudeur coupe l'alimentation de l'objet portatif, ce dernier a mémorisé l'existence d'une tentative possible de fraude, et imposera systématiquement un délai, ou retard, avant de permettre une nouvelle tentative.

[0018] Le délai peut être fonction d'informations relatives au contexte, tels que la date et l'heure et/ou un identifiant du terminal utilisé, qui sont mémorisés dans l'objet portatif.

[0019] En d'autres termes, l'invention permet de retarder l'authentification d'un porteur d'un objet portatif quand la signature délivrée précédemment ne correspond pas à l'information secrète associée à l'objet portatif, et diminue ainsi la probabilité qu'un éventuel fraudeur découvre, par essais successifs, l'information secrète stockée dans l'objet portatif, en augmentant le temps entre deux essais, sans possibilité de contourner ou éviter ce délai.

[0020] Selon un aspect particulier de la présente invention, le procédé comprend, après ladite étape de génération d'un retard ou après ladite étape de délivrance, une étape d'écriture, dans ledit indicateur de signature erronée, de ladite valeur indiquant une situation normale.

[0021] Ainsi, l'invention permet de dissuader les fraudeurs, sans introduire une gêne trop importante pour l'utilisateur autorisé, qui aurait simplement fait une erreur de saisie.

[0022] Selon un mode de réalisation particulier de l'invention, ledit indicateur de signature erronée est un élément binaire.

[0023] Selon un autre mode de réalisation particulier de l'invention, ledit indicateur de signature erronée est un compteur, remis à zéro en présence d'une décision d'authentification positive et incrémenté en présence d'une décision d'authentification négative.

[0024] Ainsi, l'indicateur de signature erronée qui est alloué dans une mémoire non volatile de l'objet portatif peut être soit un élément binaire, soit un compteur, ce qui permet une mise en oeuvre simple, relativement peu coûteuse et fiable de l'invention.

[0025] En particulier, ledit retard peut être proportionnel à la valeur dudit compteur.

[0026] Ainsi, le délai appliqué par l'objet portatif peut être augmenté progressivement, de façon à augmenter la difficulté pour le fraudeur.

[0027] L'invention concerne également un produit programme d'ordinateur stocké sur un objet portatif et/ou exécutable par un microprocesseur, comprenant des instructions de code de programme pour l'exécution des étapes du procédé d'authentification décrit précédemment.

[0028] Finalement, l'invention concerne un objet portatif sécurisé adapté à la mise en oeuvre du procédé décrit ci-dessus selon la revendication 7

[0029] Selon un aspect particulier de l'invention, ledit objet portatif comprend :

- des moyens d'écriture, dans ledit indicateur de signature erronée, d'une valeur indiquant une situation anormale, si ladite décision d'authentification est négative ; et
- des moyens de génération d'un retard, si ledit indicateur de signature erronée contient une valeur indiquant une situation anormale.

[0030] Selon encore un autre aspect particulier de l'invention, ladite mémoire non volatile de l'objet portatif est une mémoire de type EEPROM ou Flash.

5. Liste des figures

[0031] D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante de deux modes de réalisation particuliers, donnés à titre de simples exemples illustratifs et non limitatifs, et des dessins annexés, parmi lesquels :

- la figure 1 illustre un exemple de système mettant en oeuvre l'invention selon un mode de réalisation particulier de l'invention ;
- la figure 2 présente les étapes principales du procédé d'authentification selon un premier mode de réalisation ;
- la figure 3 présente les étapes principales du procédé d'authentification selon un second mode de réalisation.

6. Description de modes de réalisation de l'invention

6.1 Principe général

[0032] Le principe général de l'invention repose sur l'utilisation d'un indicateur de signature erronée mémorisé dans une mémoire non volatile d'un objet portatif, qui ne peut donc pas être modifiée par une interruption d'alimentation. La valeur de l'indicateur commande selon l'invention la durée du procédé d'authentification d'un porteur de l'objet portatif, en imposant un délai, ou un retard, systématique si la précédente tentative d'authentification avait délivré un résultat erroné.

6.2 Exemple de système mettant en oeuvre l'invention

[0033] On se place dans la suite dans le cadre d'un mode de réalisation particulier de l'invention, en relation avec la figure 1, selon lequel l'objet portatif est une carte à puce 7, qui est une carte de paiement émise par une banque, communiquant avec un terminal de paiement 2 (terminal lecteur de cartes à puce).

[0034] Le porteur de la carte à puce 7, qui peut être soit l'utilisateur autorisé de la carte à puce 7 soit un fraudeur, souhaite accéder à un service bancaire nécessitant qu'il s'authentifie au préalable par l'intermédiaire du terminal de paiement 2. Par exemple, ce service peut être le paiement d'un produit ou d'un service par le porteur à

un commerçant au moyen de la carte à puce 7 par l'intermédiaire du terminal de paiement 2.

[0035] Le terminal de paiement 2 peut être connecté à un serveur 1 distant, qui est par exemple situé dans une banque, via un réseau de communication 9 qui permet donc l'échange d'informations entre le terminal de paiement 2 et le serveur 1. Le serveur 1 distant appartenant à la banque autorise des transactions électroniques sécurisées et peut être connecté à plusieurs terminaux de paiement.

[0036] De façon classique, le terminal de paiement 2 est alimenté électriquement par un réseau de distribution électrique et/ou par une ou plusieurs piles ou batteries intégrées au terminal de paiement 2. Le terminal de paiement 2 comprend généralement un écran d'affichage 5, un clavier numérique ou alphanumérique 3, un lecteur de carte 4, une unité centrale de traitement (CPU) et une imprimante (non représentés).

[0037] La carte à puce 7 comprend un support de type plastique 6 et au moins un circuit intégré (puce) 8 qui est généralement situé dans le corps de la carte 7. Le circuit intégré 8 de la carte à puce 7 comprend une interface 12, qui se présente généralement sous la forme de contacts électriques en cuivre, permettant une alimentation électrique du terminal de paiement 2 et l'échange d'informations, sous forme de signaux électriques, lorsque la carte est insérée dans le lecteur de carte 4 du terminal de paiement 2.

[0038] Pour que le porteur de la carte à puce 7 puisse obtenir une autorisation par la banque émettrice de la carte à puce 7 pour effectuer un paiement, il lui est nécessaire de s'authentifier comme étant le titulaire de la carte à puce 7 ou l'utilisateur autorisé.

[0039] Pour ce faire, le porteur insère la carte à puce 7 dans le lecteur de carte 4 du terminal de paiement 2 fourni par le commerçant et saisit son code confidentiel (signature) par le biais du clavier 3 du terminal de paiement 2.

[0040] Le microprocesseur de la carte à puce 7 exécute un traitement de comparaison, ou d'authentification, selon un algorithme de contrôle connu de l'homme du métier, tenant compte du code délivré par le porteur par le biais du clavier 3 et de l'information secrète dérivée du code confidentiel contenu dans une mémoire ROM de la carte à puce 7, et le cas échéant d'une donnée aléatoire fournie par le terminal de paiement 2. Le microprocesseur de la carte à puce 7 délivre ensuite au terminal de paiement 2 une information de décision d'authentification, selon que la signature délivrée est correcte ou erronée.

[0041] Quand l'information secrète mémorisée dans la carte à puce 7 concorde avec la signature délivrée par le porteur, les transactions électroniques sécurisées (ou tout autre opération) sont autorisées, sous le contrôle du terminal 2 et/ou du serveur 1 distant.

[0042] La carte à puce comprend classiquement un microprocesseur et différentes mémoires RAM et ROM. Elle comprend également, selon l'invention, une mémoire modifiable non volatile, par exemple une EEPROM 14.

[0043] L'invention propose donc d'utiliser un indicateur de signature erronée (I), qui peut être un élément binaire, tel qu'un bit de mémoire. L'élément binaire est mémorisé dans la mémoire EEPROM 14 de la carte à puce 7. L'élément binaire peut également être stocké dans une mémoire de type Flash ou tout autre type de mémoire non volatile.

6.3 Premier exemple de mise en oeuvre

[0044] On présente ci-dessous, en relation avec la figure 2, les étapes principales d'un procédé d'authentification d'un porteur d'un objet portatif selon un premier mode de réalisation particulier de l'invention. On se place donc dans la suite dans une configuration où la carte à puce 7 est insérée dans le lecteur de carte 4 du terminal de paiement 2.

[0045] Comme illustré en figure 2, le procédé d'authentification selon l'invention débute par une étape nouvelle, n'existant pas dans les techniques de l'art antérieur, à savoir la lecture (21) de l'indicateur de signature erronée, appelée par la suite I, dans l'emplacement de la mémoire EEPROM 14 qui lui est alloué. En fonction de la valeur de cet indicateur I (test 22), la carte à puce 7 décide d'elle-même (c'est-à-dire sans l'intervention ni le contrôle du terminal de paiement 2) d'appliquer ou non un délai, ou retard, avant d'effectuer le traitement classique d'authentification.

[0046] Ainsi, dans l'hypothèse où une valeur 0 de l'indicateur I signale une situation correcte, et la valeur 1 une situation anormale, la sortie "oui" (221) du test « I = 0 » (22) permet un passage direct, sans délai, à l'étape d'authentification classique (23), qui va comparer la signature S délivrée par l'utilisateur à l'aide d'une interface adaptée (par exemple un clavier) aux données présentes dans la carte à puce 7. Ce traitement, connu en soi et appliqué dans toutes les cartes à puce, n'est pas décrit plus en détail ici. L'homme du métier saura, selon les circonstances, mettre en oeuvre l'algorithme d'authentification adapté.

[0047] En revanche, dans le cas où l'indicateur I vaut 1, la sortie « Non » (222) du test (22) conduit à la génération d'un délai (24) qui peut par exemple être compris entre 10 et 60 secondes. À l'issue de ce délai (24), la valeur de l'indicateur I est repositionnée à 0 (étape 25), puis l'on reprend le traitement d'authentification classique (23).

[0048] Ce traitement d'authentification (23) délivre une information représentative du résultat de l'authentification. Si l'authentification est validée (test 26), la transaction (27) peut s'effectuer, de façon classique. Cette transaction peut être un paiement, une autorisation d'accès à des données ou à un site, ... Si l'authentification n'est pas correcte (261), le terminal de paiement 2 met en oeuvre un traitement adapté (28), qui n'est pas l'objet de la présente invention. Il peut par exemple compter le nombre d'erreurs d'authentification, et empêcher de réa-

liser, par exemple, plus de trois tentatives. Cependant, ce traitement étant effectué par le terminal de paiement 2, il peut aisément être détourné ou annulé par un fraudeur qui aurait adapté son terminal pour pouvoir entrer, sans limitation, un nombre très élevé de signatures, par exemple de façon aléatoire, dans l'espoir de trouver la bonne dans un laps de temps raisonnable.

[0049] C'est pour cette raison que, selon l'invention, on effectue préalablement à ce traitement (28) l'écriture (29) de la valeur 1 dans l'indicateur I de la carte à puce 7.

[0050] Ainsi, même dans le cas où le fraudeur a adapté son terminal de paiement 2, ou dans le cas où il dispose de plusieurs terminaux qu'il prévoit d'utiliser successivement, il sera confronté à un délai d'attente, généré par la carte à puce 7 elle-même, empêchant la réalisation d'une série automatisée d'essais de signatures dans un temps raisonnable.

[0051] Le délai, ou retard, appliqué est choisi de façon qu'il soit suffisamment long pour dissuader les fraudeurs, sans introduire une gêne trop importante pour l'utilisateur autorisé, qui aurait simplement fait une erreur de saisie.

6.4 Deuxième exemple d'implémentation

[0052] Selon une variante du procédé décrit ci-dessus, on peut prévoir que l'indicateur I n'est pas un simple élément binaire, indiquant si la précédente signature était erronée ou valide, mais un compteur, comptabilisant le nombre de signatures erronées successives. Ceci peut permettre d'augmenter progressivement le délai appliqué par la carte à puce 7, de façon à limiter la nuisance pour l'utilisateur autorisé, et augmenter la difficulté pour le fraudeur. Ce compteur peut également permettre, le cas échéant, lorsqu'il a atteint un seuil, d'entraîner un blocage définitif de la carte à puce 7 (à nouveau, gérée par elle-même, et non pas par les terminaux).

[0053] Cette approche est illustrée par la figure 3. Le procédé débute, de la même manière que dans le premier mode de réalisation, par la lecture (21) de l'indicateur I. Un test (31) est effectué sur la valeur de ce dernier. Si celle-ci vaut 0, on effectue le traitement d'authentification (23), de la même façon que dans le premier mode de réalisation. Si le résultat du test (31) indique (312) que la valeur de I est différente de 0, la carte à puce 7 génère un délai (32), pendant lequel elle ne fera aucun traitement. Ce délai n'est plus fixe, mais fonction de la valeur de I. On peut prévoir par exemple, une fonction linéaire, une fonction par paliers, ou une fonction exponentielle.

[0054] Une fois le délai (32) écoulé, on passe à l'étape d'authentification (23), puis l'on fait le test (26) sur le résultat de l'authentification. Si le résultat de ce test (26) est correct, c'est-à-dire que la signature fournie est authentifiée, on repositionne (34) la valeur de l'indicateur à 0, puis on effectue la transaction (27).

[0055] En revanche, si le résultat de l'authentification (26) est négatif (261), on incrémente (33) la valeur de I, avant de réaliser le traitement de signature erronée (28) dans le terminal.

6.5 Variantes

[0056] Si l'authentification n'est pas correcte (261), l'écriture (29, 33) dans l'indicateur I de la carte à puce 7 peut également comprendre une opération de mémorisation dans une mémoire non volatile (l'EEPROM 14 par exemple) de la carte à puce 7 d'au moins une information relative au contexte, tels que la date et l'heure et/ou un identifiant du terminal de paiement utilisé. L'étape 21 de lecture de l'indicateur I peut comprendre une étape de lecture des informations relatives au contexte qui sont éventuellement mémorisées dans la carte à puce 7 et le délai (24, 32) peut être fonction de ces informations.

[0057] Dans d'autres modes de réalisation, l'objet portatif peut être une clé USB et le terminal électronique peut être un ordinateur portable ou un ordinateur personnel par exemple.

[0058] La saisie de la signature peut être effectuée par d'autres moyens qu'un clavier (écran tactile, commande vocale,...).

[0059] La liaison entre le terminal et l'objet portatif peut être effectuée par contact ou à distance (RFID par exemple).

[0060] La présente invention peut s'appliquer également à toute situation nécessitant une restriction de l'accès à un lieu ou un local protégé, à un véhicule appartenant à une ou plusieurs personnes, un site internet ou une base de données, par exemple.

Revendications

1. Procédé d'authentification d'un porteur d'un objet portatif comprenant des moyens de mémorisation d'au moins une information secrète, comprenant les étapes suivantes :

   - traitement d'authentification d'une signature délivrée par ledit porteur, tenant compte de ladite information secrète ;
   - délivrance d'une information de décision d'authentification, positive ou négative,

   le procédé mettant en oeuvre met en oeuvre, dans une mémoire non volatile dudit objet portatif, un indicateur de signature erronée pouvant prendre une valeur indiquant une situation normale et au moins une valeur indiquant une situation anormale, et comprenant :

   - après ladite étape de délivrance, une étape d'écriture, dans ledit indicateur de signature erronée, d'une valeur indiquant une situation anormale, si ladite décision d'authentification est négative ; et
   - avant ladite étape d'authentification, et si ledit indicateur de signature erronée contient une valeur indiquant une situation anormale, une étape

de génération d'un retard,

caractérisé en ce que ladite étape d'écriture comprend également une opération de mémorisation d'au moins une information relative au contexte, tels que la date et l'heure et/ou un identifiant du terminal utilisé.

2. Procédé d'authentification selon la revendication 1, **caractérisé en ce qu'**il comprend, après ladite étape de génération d'un retard ou après ladite étape de délivrance :

- une étape d'écriture, dans ledit indicateur de signature erronée, de ladite valeur indiquant une situation normale

3. Procédé d'authentification selon l'une quelconque des revendications 1 et 2 **caractérisé en ce que** ledit indicateur de signature erronée est un élément binaire.

4. Procédé d'authentification selon l'une quelconque des revendications 1 et 2
caractérisé en ce que ledit indicateur de signature erronée est un compteur, remis à zéro en présence d'une décision d'authentification positive et incrémenté en présence d'une décision d'authentification négative.

5. Procédé d'authentification selon la revendication 4, **caractérisé en ce que** ledit retard est proportionnel à la valeur dudit compteur.

6. Produit programme d'ordinateur stocké sur un objet portatif et/ou exécutable par un microprocesseur, **caractérisé en ce qu'**il comprend des instructions de code de programme pour l'exécution des étapes du procédé d'authentification selon l'une quelconque des revendications 1 à 5.

7. Objet portatif sécurisé comprenant :

- des moyens de mémorisation d'au moins une information secrète ;
- des moyens d'authentification d'une signature délivrée par ledit porteur, tenant compte de ladite information secrète ;
- des moyens de délivrance d'une information de décision d'authentification, positive ou négative,
- des moyens de mémorisation non volatile d'un indicateur de signature erronée pouvant prendre une valeur indiquant une situation normale et au moins une valeur indiquant une situation anormale,

caractérisé en qu'il comprend des moyens de mémorisation d'au moins une information relative au contexte, tels que la date et l'heure et/ou un identifiant du terminal utilisé.

8. Objet portatif selon la revendication 7, **caractérisé en qu'**il comprend :

- des moyens d'écriture, dans ledit indicateur de signature erronée, d'une valeur indiquant une situation anormale, si ladite décision d'authentification est négative ; et
- des moyens de génération d'un retard, si ledit indicateur de signature erronée contient une valeur indiquant une situation anormale.

9. Objet portatif selon l'une quelconque des revendications 7 et 8, **caractérisé en ce que** ladite mémoire non volatile est une mémoire de type EEPROM ou Flash.

Figure 1

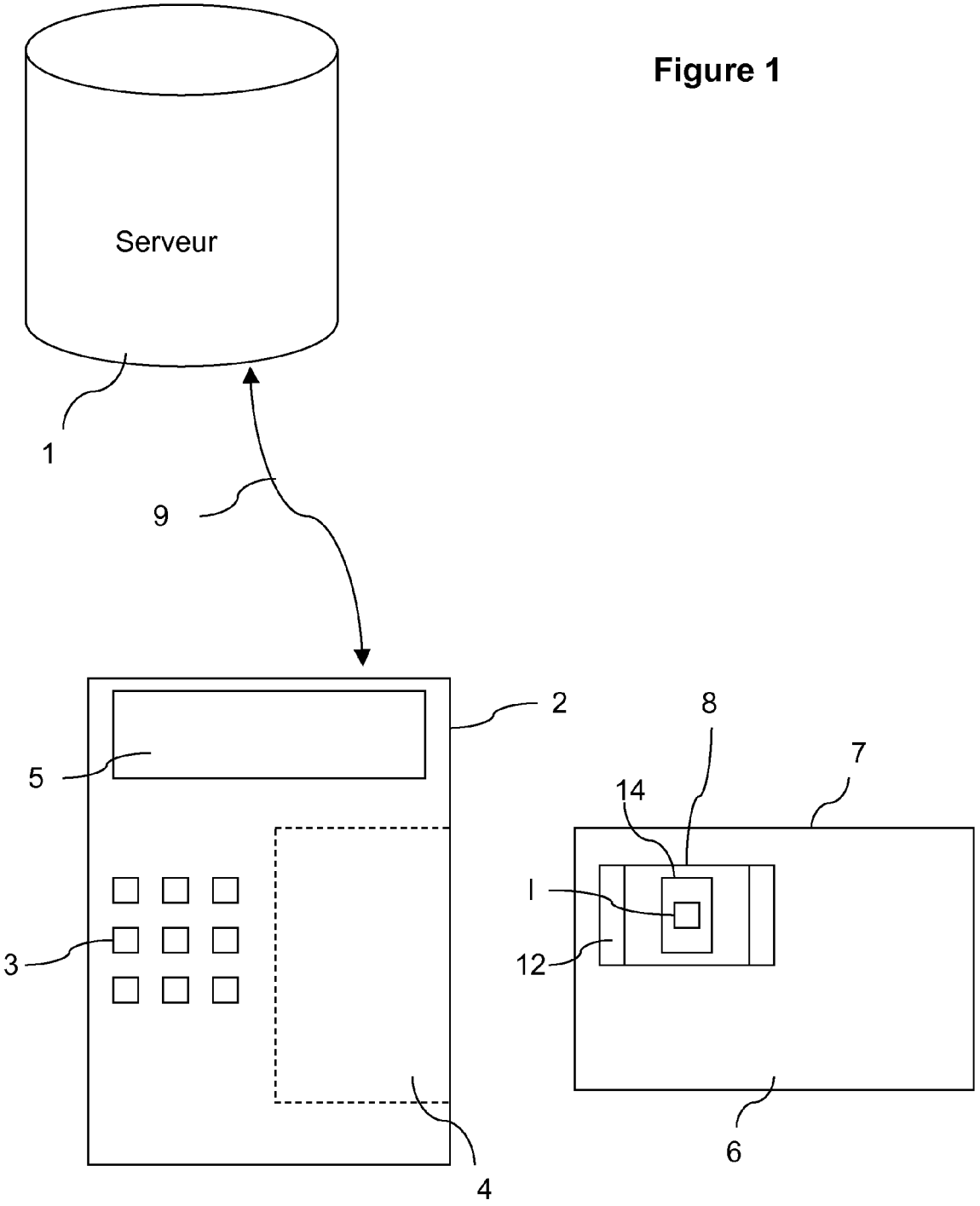


Figure 2

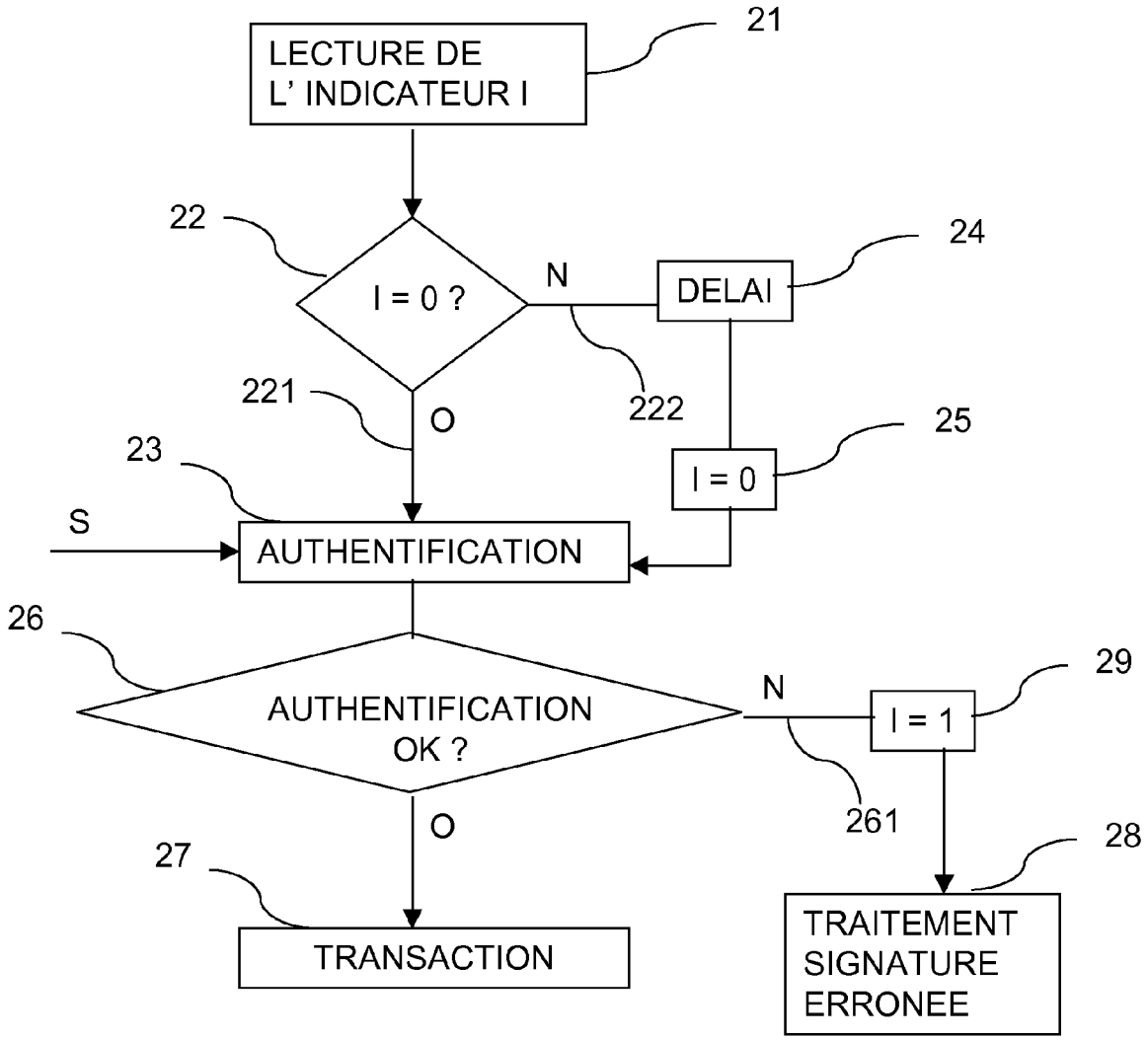
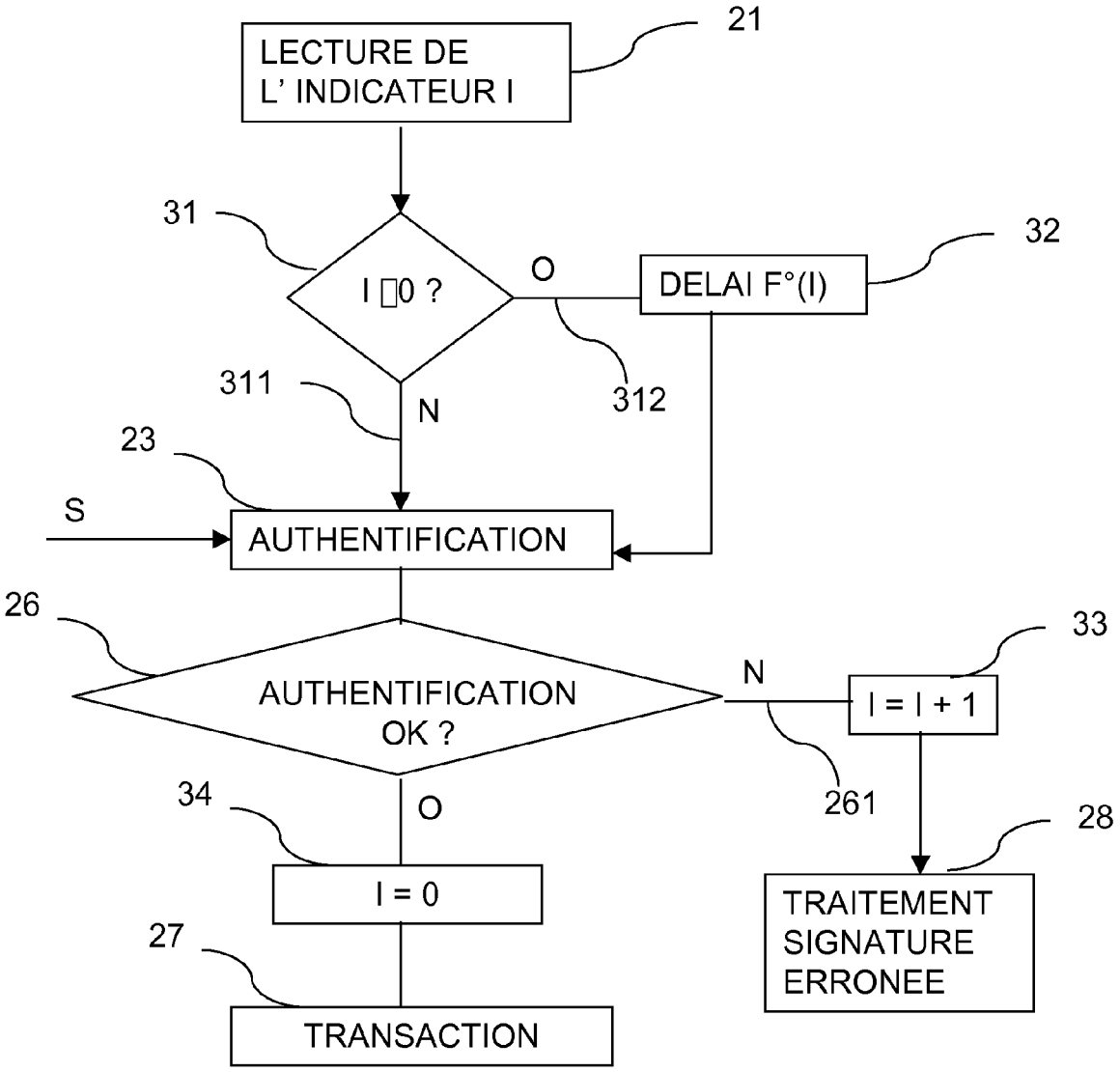

LECTURE DE L' INDICATEUR I
21
22
I = 0 ?
N
DELAI
24
221
O
222
25
I = 0
23
S
AUTHENTIFICATION
26
AUTHENTIFICATION OK ?
N
I = 1
29
261
O
27
28
TRANSACTION
TRAITEMENT SIGNATURE ERRONEE

Figure 3


LECTURE DE L' INDICATEUR I
21
31
I □0 ?
O
DELAI F°(I)
32
312
311
N
23
S
AUTHENTIFICATION
26
AUTHENTIFICATION OK ?
N
33
I = I + 1
261
34
O
I = 0
28
TRAITEMENT SIGNATURE ERRONEE
27
TRANSACTION

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 08 16 6402

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X	EP 1 413 980 A1 (SCHLUMBERGER SYSTEMS & SERVICE [FR]) 28 avril 2004 (2004-04-28) * alinéa [0006] - alinéa [0018] * * alinéa [0022] - alinéa [0035] * * figure 2 * -----	1-9	INV. G07F7/10 ADD. G06K19/073
X	FR 2 493 564 A1 (GAO GES AUTOMATION ORG [DE]) 7 mai 1982 (1982-05-07) * le document en entier * -----	1-9	
A	US 5 594 227 A (DEO VINAY [US]) 14 janvier 1997 (1997-01-14) * le document en entier * -----	1-9	
A	US 4 092 524 A (MORENO ROLAND) 30 mai 1978 (1978-05-30) * colonne 2, ligne 62 - colonne 4, ligne 58 * -----	1-9	DOMAINES TECHNIQUES RECHERCHES (IPC) G07F G06K

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	2 décembre 2008	Reino, Bernardo

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1 EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 08 16 6402

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

02-12-2008

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1413980 A1	28-04-2004	AU 2003269365 A1	13-05-2004
		WO 2004038652 A1	06-05-2004
		JP 2006512690 T	13-04-2006
		US 2006015938 A1	19-01-2006
FR 2493564 A1	07-05-1982	BE 890950 A1	15-02-1982
		CH 656014 A5	30-05-1986
		DE 3041109 A1	09-06-1982
		GB 2088605 A	09-06-1982
		IT 1145571 B	05-11-1986
		JP 1747224 C	25-03-1993
		JP 57120183 A	27-07-1982
		JP 63043791 B	01-09-1988
		JP 1727825 C	19-01-1993
		JP 2288993 A	28-11-1990
		JP 4013753 B	10-03-1992
		NL 8104842 A	17-05-1982
		SE 462876 B	10-09-1990
		SE 8106354 A	01-05-1982
		SE 506491 C2	22-12-1997
		SE 9001035 A	23-09-1991
		US 4484067 A	20-11-1984
US 5594227 A	14-01-1997	AUCUN	
US 4092524 A	30-05-1978	DE 2621271 A1	25-11-1976
		FR 2311360 A1	10-12-1976
		GB 1543602 A	04-04-1979
		JP 1490000 C	07-04-1989
		JP 52007649 A	20-01-1977
		JP 60001666 B	16-01-1985
		NL 7605119 A	16-11-1976

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82