(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 730 076**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **95 01314**

(51) Int Cl⁶ : G 06 F 12/14, 17/60, G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 31.01.95.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 02.08.96 Bulletin 96/31.

(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) :** *SOREP SA SOCIETE ANONYME* — FR.

(72) **Inventeur(s) :** ANDRE DOMINIQUE, BENTEO BRUNO, EVENAT PHILIPPE et RAYON STEPHANE.

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

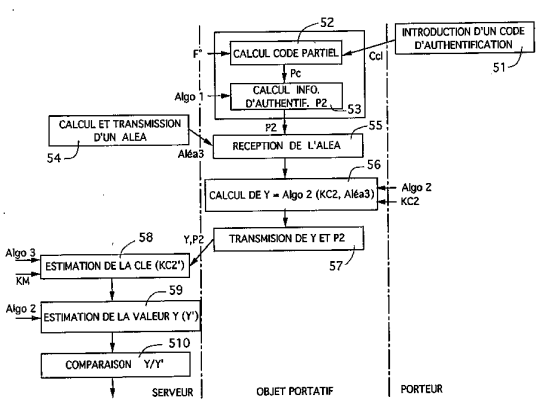
(74) **Mandataire :** CABINET PATRICE VIDON.

(54) PROCEDE D'AUTHENTIFICATION PAR UN SERVEUR DU PORTEUR D'UN OBJET PORTATIF A MICROPROCESSEUR, SERVEUR ET OBJET PORTATIF CORRESPONDANTS.

(57) L'invention concerne un procédé d'authentification d'un utilisateur par un serveur, à l'aide d'un objet portatif à microprocesseur, selon lequel ledit serveur tient compte d'une information d'authentification (P2) produite par ledit objet portatif, correspondant au résultat d'un algorithme spécifique (52, 53) appliqué à un premier code d'authentification (Ccl) fourni par ledit utilisateur, pour fournir un résultat positif ou négatif d'authentification. Ainsi, la connaissance du contenu de l'objet portatif (tel qu'une carte à microprocesseur) ne suffit pas pour accéder audit serveur.

Avantageusement, on effectue simultanément une authentification du porteur par l'objet portatif et/ou une authentification de l'objet portatif par le serveur.

L'invention s'applique dans tous les domaines où une authentification efficace est souhaitable ou nécessaire (contrôle d'accès à des lieux, des objets et/ou des données, distributeurs automatiques,...).



FR 2 730 076 - A1

Procédé d'authentification par un serveur du porteur d'un objet portatif à microprocesseur, serveur et objet portatif correspondants.

Le domaine de l'invention est celui de l'accès sécurisé à des données, des objets et/ou des lieux à l'aide de dispositifs électroniques. Plus précisément, l'invention concerne le contrôle d'accès à l'aide d'objets portatifs à microprocesseur, tels que classiquement des cartes à microprocesseur.

L'invention peut être mise en oeuvre dans de nombreux domaines, dès lors qu'il est nécessaire d'authentifier un utilisateur, porteur d'un objet portatif permettant un dialogue avec un dispositif gérant l'accès à des données (par exemple pour les procédures bancaires et les retraits d'argent assurées par un appareil automatique), à des objets (par exemple pour l'utilisation d'un ordinateur, d'un téléphone...) ou à des lieux (par exemple pour l'accès à des pièces ou des immeubles). Par la suite, un tel dispositif sera appelé de façon générique serveur, sans que cela ne soit limitatif ni de sa forme, ni de sa fonction.

De nombreuses solutions de contrôle d'accès sont déjà connues. D'une façon générale, le dialogue entre l'utilisateur et le serveur n'est possible qu'après une phase d'authentification. Lorsque le résultat de l'authentification est positif, le dialogue est autorisé. Il s'agit par exemple d'une autorisation d'utilisation ou d'accès, ou d'un échange de données, avantageusement sous une forme cryptée.

Classiquement, l'authentification comprend deux étapes : une première étape d'authentification du porteur par l'objet portatif et une seconde étape d'authentification de l'objet portatif par le serveur.

L'authentification du porteur par l'objet portatif est réalisé par cet objet portatif, par comparaison d'un code d'authentification introduit par le porteur avec une donnée de référence stockée dans ledit objet portatif. Classiquement, l'objet portatif calcule une réplique de la donnée de référence, à l'aide d'un algorithme prédéterminé appliqué au code d'authentification. Si l'estimation est égale à la donnée de référence, le porteur est authentifié.

Il est à noter que pour cette première phase, aucun échange n'a lieu entre le serveur et l'objet portatif. La seule information échangée est le code d'authentification fourni par le porteur.

L'authentification de l'objet portatif par le serveur est effectuée assurée par le serveur, à partir d'une clé secrète stockée dans ledit objet portatif, mais sans que cette clé soit transmise au serveur, de façon qu'il ne soit pas possible de la lire lors de son transfert. La clé secrète est recalculée par le serveur à partir d'une clé maître que ce dernier connaît. L'authentification est effectuée par comparaison de deux valeurs calculées selon un algorithme spécifique, connu du serveur et de l'objet portatif, en tenant compte de la clé secrète et d'une valeur aléatoire fournie par le serveur. Si le résultat de la comparaison est positif, l'authentification de l'objet portatif est concluante.

Cette technique présente un niveau de sécurité relativement élevé, sans qu'il soit nécessaire de stocker des informations spécifiques au porteur et à l'objet portatif dans le serveur. Celui-ci ne connaît que la clé maître, qui est commune à une pluralité d'objets portatifs.

Les informations nécessaires au protocole sécuritaire sont réparties de la façon suivante :

- porteur : code d'authentification ;
- objet portatif : donnée de référence du code d'authentification, clé secrète propre à la carte et algorithme de cryptage pour l'authentification par le serveur ;
- serveur : aucune information sur les utilisateurs et les objets portatifs. Il ne connaît que la clé maître et l'algorithme de cryptage.

L'authentification permet de vérifier que l'objet portatif est valide, et que le porteur est habilité. De prime abord, elle paraît particulièrement sûre. D'une part, toute personne non habilitée (ne connaissant pas le code d'authentification) ne peut pas se faire reconnaître par l'objet portatif. D'autre part, il n'est pas possible d'accéder au serveur sans détenir l'objet portatif, qui contient la clé secrète.

Toutefois, une analyse plus poussée permet de constater que la connaissance des informations contenues dans l'objet portatif sont suffisantes pour accéder au serveur. En d'autres termes, il est suffisant à une personne mal intentionnée de connaître la clé secrète et l'algorithme de cryptage pour être authentifiée par le serveur, bien qu'elle ne connaisse pas le code d'authentification.

L'homme du métier considère que cette situation ne pose pas de problème, car la clé secrète est inscrite dans le micro-processeur selon des techniques qui garantiraient l'impossibilité de la relecture de celle-ci. D'ailleurs, ces méthodes d'authentification sont mises en oeuvre depuis longtemps, et il semble que, jusqu'à aujourd'hui l'inviolabilité de ces techniques n'a pas été discutée.

Il est exact que l'accès à cette clé secrète n'est pas possible par des méthodes informatiques et logicielles, qui tenteraient de relire la clé. En revanche, les inventeurs ont vérifié qu'il est possible d'accéder à l'information telle qu'elle est inscrite dans le silicium, par des techniques mettant à jour le micro-processeur puis l'analysant, au niveau des transistors tracés sur le microprocesseur. Ces techniques nécessitent bien sûr des matériels importants, mais représentent cependant un risque non négligeable, du fait des enjeux parfois très importants associés à la détention d'un objet portatif (dans le domaine bancaire par exemple). Par ailleurs, on peut penser que ces matériels, aujourd'hui complexes et coûteux, sont appelés à se banaliser (l'analyse des micro-processeurs étant utiles pour de nombreuses applications). En conséquence, ils seront plus abordables pour des personnes mal intentionnées.

Les techniques actuelles d'authentification s'avèrent donc insuffisantes, du fait qu'elles ne permettent pas de garantir de façon certaine que le porteur est habilité à utiliser l'objet portatif qu'il détient. Il est en effet possible que cet objet portatif soit utilisé par un "pirate" qui a réussi à lire la clé secrète.

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

Ainsi, un objectif de l'invention est de fournir un procédé d'authentification par un serveur dans lequel la connaissance totale des informations stockées dans un objet portatif n'est pas suffisante pour que l'authentification soit concluante.

En d'autres termes, un objectif de l'invention est de fournir un tel procédé d'authentification, permettant de garantir que le porteur de l'objet portatif considéré est habilité à détenir et à utiliser cet objet portatif.

Un autre objectif de l'invention est de fournir un tel procédé, ne nécessitant aucune modification de la structure et de la fabrication des serveurs et des objets portatifs.

Notamment, un objectif de l'invention est de ne pas nécessiter la mise en oeuvre de techniques nouvelles pour la fabrication d'objets tels que les cartes à microprocesseurs.

Encore un autre objectif de l'invention est de fournir un tel procédé, ne nécessitant pas de modification des habitudes des utilisateurs d'objets portatifs. En particulier, selon une approche de l'invention, un objectif de l'invention est de fournir un tel procédé n'imposant pas de mémoriser de nouveaux codes d'authentification.

L'invention a également pour objectif de fournir un tel procédé d'authentification, qui puisse remplacer des procédés déjà mis en oeuvre dans des serveurs actuels, sans qu'aucune modification ne soit sensible pour l'utilisateur (à l'exception de l'octroi d'un nouvel objet portatif.

Un autre objectif de l'invention est de fournir un tel procédé, dont les coûts d'installation et d'exploitation soient identiques à ceux des procédés d'authentification actuellement mis en oeuvre.

Ces objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un procédé d'authentification d'un utilisateur (ou porteur) par un serveur, à l'aide d'un objet portatif à microprocesseur, dans lequel ledit serveur tient compte d'une information d'authentification (P2) produite par ledit objet portatif, correspondant au résultat d'un algorithme spécifique appliqué à un premier code d'authentification (Ccl) fourni par ledit utilisateur, pour fournir un résultat positif ou négatif d'authentification.

Ainsi, selon l'invention, l'authentification n'est possible que si le porteur apporte le code d'authentification qui lui est attribué (ou qu'il a choisi). Il n'est pas possible de déduire ce code des données stockées dans l'objet portatif. En conséquence, l'authentification par le serveur ne sera positive que si le porteur possède le bon code d'authentification. Toute tentative de fraude basée sur l'analyse du seul contenu de l'objet portatif est inopérante.

Comme cela apparaîtra par la suite, la procédure d'authentification peut être proche de celles classiquement mises en oeuvre, pour authentifier l'objet portatif dans le serveur. L'invention ne repose d'ailleurs pas principalement sur cette procédure, mais sur une approche tout à fait nouvelle de l'authentification, nécessitée par la mise à jour d'un

problème nouveau dans le domaine de la sécurité des échanges impliquant des objets portatifs.

En effet, l'homme du métier a toujours considéré qu'il était impossible de lire le contenu d'un objet portatif (classiquement une carte "à puce") dès lors qu'il était inscrit de façon adéquate. En conséquence, les techniques connues offraient un degré de sécurité qui apparaissait tout à fait suffisant, et il ne semblait pas nécessaire de chercher à les modifier.

Toutefois, les inventeurs ont vérifié que l'accès aux informations secrètes d'un microprocesseur était, contre toute attente, accessible. Ce constat introduit un problème nouveau : comment s'assurer que l'objet portatif n'est pas "piraté", et que son porteur a réellement le droit de l'utiliser.

L'invention apporte une solution inventive à ce problème, consistant à authentifier directement dans le serveur le porteur, et non plus seulement l'objet portatif. Ainsi, selon l'invention, l'objet portatif sert notamment de liaison entre l'utilisateur et le serveur. Il est nécessaire à la transaction, mais n'est plus suffisant.

De façon avantageuse, ledit algorithme spécifique comprend les opérations suivantes :

- production d'un code d'authentification partiel (Pc), déduit dudit premier code d'authentification (Ccl) ;
- application d'un premier algorithme de cryptage non réversible sur ledit code d'authentification partiel (Pc), produisant ladite information d'authentification (P2).

Le fait de ne tenir compte que d'une partie du code d'authentification est un gage supplémentaire de sécurité : l'information d'authentification qui circule entre le serveur et l'objet portatif n'est pas fonction de l'ensemble du code d'authentification. Il est donc complètement impossible de reconstruire ce dernier.

Selon un mode de réalisation préférentiel de l'invention, ledit serveur possède une clé maître (KM) commune à une pluralité d'utilisateurs, ledit objet portatif possède au moins une première clé secrète (KC2) fonction, de façon non réversible, de ladite clé maître (KM) et ledit utilisateur connaît au moins ledit premier code d'authentification

(Ccl). Le procédé comprend alors une phase d'authentification simultanée par ledit serveur dudit objet portatif et dudit utilisateur à partir de deux informations délivrées par ledit objet portatif :

- une première valeur (Y) résultat d'un second algorithme de cryptage non réversible tenant compte de ladite première clé secrète (KC2) et d'un premier aléa (Aléa3) transmis par ledit serveur ; et
- une information d'authentification (P2) dudit utilisateur obtenue à partir dudit premier code d'authentification donné par ledit utilisateur,

ledit serveur calculant une estimation de ladite première valeur (Y') à l'aide dudit second algorithme de cryptage, en tenant compte dudit premier aléa (Aléa3) et d'une estimation (KC2') de ladite première clé secrète, obtenue à partir de ladite clé maître (KM) et de ladite information d'authentification (P2), et comparant ladite première valeur (Y) et ladite estimation de ladite première valeur (Y') pour fournir ledit résultat positif ou négatif d'authentification.

L'authentification dudit utilisateur par ledit serveur peut notamment comprendre les étapes suivantes :

- introduction par ledit utilisateur dudit premier code d'authentification (Ccl), transmis audit objet portatif ;
- calcul par ledit objet portatif de ladite information d'authentification (P2), à partir dudit premier code d'authentification (Ccl) ;
- réception dans ledit objet portatif de ladite première valeur aléatoire (Aléa3) transmise par ledit serveur ;
- calcul par ledit objet portatif de ladite première valeur (Y), à l'aide dudit second algorithme de cryptage non réversible, à partir de ladite première clé secrète (KC2) stocké dans ledit objet portatif et de ladite première valeur aléatoire (Aléa3) ;
- transmission audit serveur, par ledit objet portatif, de ladite première information (Y) et de ladite information d'authentification (P2) ;
- calcul par ledit serveur de ladite estimation de la première clé secrète (KC2'), à l'aide d'un troisième algorithme de cryptage non réversible, à

partir de ladite clé maître (KM) stocké dans ledit serveur et de ladite information d'authentification (P2) ;

- calcul par ledit serveur de ladite estimation de la première valeur (Y'), à l'aide dudit second algorithme de cryptage non réversible, à partir de ladite estimation de la première clé secrète (KC2') et de ladite première valeur aléatoire (Aléa3) ;
- comparaison par ledit serveur de ladite première valeur (Y) et de ladite estimation de la première valeur (Y'), et authentification dudit utilisateur par ledit serveur si le résultat de la comparaison est favorable.

Préférentiellement, l'authentification directe de l'invention est précédée d'au moins une des phases classiques d'authentification utilisateur/objet portatif et objet portatif/serveur, ce qui permet de renforcer encore la sécurité.

Dans ce cas, le procédé comprend avantageusement une première phase préalable d'authentification dudit utilisateur par ledit objet portatif, comprenant les étapes suivantes :

- introduction par ledit utilisateur d'un second code d'authentification (Ccl), transmis audit objet portatif ;
- calcul par ledit objet portatif d'une empreinte (Cco) dudit second code d'authentification (Ccl), à l'aide d'un quatrième algorithme de cryptage ;
- comparaison de ladite empreinte (Cco) avec une donnée de référence (Cco') stockée dans ledit objet portatif, produisant une première information d'authentification partielle.

Il peut également comprendre une seconde phase préalable d'authentification dudit objet portatif par ledit serveur, comprenant les étapes suivantes :

- réception dans ledit objet portatif d'une seconde valeur aléatoire (Aléa1) transmise par ledit serveur ;
- calcul par ledit objet portatif d'une seconde valeur (X), à l'aide d'un cinquième algorithme de cryptage non réversible, à partir d'une seconde clé secrète (KC) stocké dans ledit objet portatif et de ladite seconde valeur aléatoire (Aléa1) ;

- transmission audit centre serveur, par ledit objet portatif, de ladite seconde information (X) et d'une donnée spécifique (Ns) stockée dans ledit objet portatif ;
- calcul par ledit serveur d'une estimation de ladite seconde clé secrète (KC'), à l'aide d'un sixième algorithme de cryptage non réversible, à partir de ladite clé maître (KM) et de ladite donnée spécifique (Ns) ;
- calcul par ledit centre serveur d'une estimation de ladite seconde information (X'), à l'aide dudit cinquième algorithme de cryptage non réversible, à partir de ladite estimation de la seconde clé secrète (KC') et de ladite seconde valeur aléatoire (Aléa1) ;
- comparaison par ledit centre serveur de ladite seconde information (X) et de ladite estimation de la seconde information (X'), produisant une seconde information d'authentification partielle.

Dans ce cas, deux clés secrètes sont exploitées, ce qui renforce clairement la sécurité du procédé.

De façon avantageuse, au moins certains desdits algorithmes de cryptage non réversible sont identiques.

Ainsi, la complexité du serveur et de l'objet portatif est peu augmentée, par rapport aux techniques actuelles, puisqu'aucune procédure complexe de calcul n'est ajoutée (à l'exception de l'étape simple d'extraction du code d'authentification partiel).

Par ailleurs, il est avantageux, pour que l'utilisateur n'ait pas plus d'informations à mémoriser que précédemment, que lesdits premier et second codes d'authentification correspondent à un même et unique code (Ccl), ou forment deux parties d'un code unique fourni par ledit utilisateur.

Selon un mode de réalisation particulier, le procédé comprend ensuite une étape de calcul d'une clé de session (S) effectuée simultanément par ledit serveur et par ledit objet portatif, à partir d'une troisième valeur aléatoire (Aléa2) délivrée par ledit objet portatif, ladite étape de calcul d'une clé de session n'étant mise en oeuvre que si le ledit résultat d'authentification est positif.

Dans ce cas, préférentiellement, ladite clé de session (S) tient compte de ladite

information d'authentification (P2).

L'invention concerne également les serveurs à accès contrôlé mettant en oeuvre ce procédé, et comprenant des moyens de communication avec un objet portatif à microprocesseur et des moyens d'authentification d'un utilisateur dudit objet portatif, lesdits moyens d'authentification tenant compte d'une information d'authentification (P2) produite par ledit objet portatif, correspondant au résultat d'un algorithme spécifique appliqué à un premier code d'authentification (Ccl) fourni par ledit utilisateur, pour délivrer un résultat positif ou négatif d'authentification.

L'invention concerne encore les objets portatifs à microprocesseur correspondants, comprenant des moyens de calcul d'une information d'authentification (P2), correspondant au résultat d'un algorithme spécifique appliqué à un premier code d'authentification (Ccl) fourni par un utilisateur.

Un tel objet portatif comprend avantageusement des moyens de stockage sécurisé d'au moins deux clés secrètes, une première clé secrète (KC2) étant destinée à l'authentification dudit utilisateur par ledit serveur, et une seconde clé secrète (KC) étant destinée à l'authentification dudit objet portatif par ledit serveur.

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

- la figure 1 est un schéma illustrant le principe général de l'invention, consistant notamment à authentifier le porteur d'un objet portatif à microprocesseur directement par le serveur ;
- la figure 2 est un synoptique présentant les grandes lignes d'une authentification selon l'invention, dans le cas où trois niveaux d'authentification sont prévus ;
- la figure 3 est un synoptique illustrant plus précisément l'authentification du porteur par l'objet portatif prévue dans la figure 3 ;
- la figure 4 est un synoptique illustrant plus précisément l'authentification de l'objet portatif par le serveur prévue dans la figure 3 ;
- la figure 5 présente un synoptique illustrant l'authentification directe du

porteur par le serveur selon l'invention.

Comme illustré en figure 1, l'invention s'applique aux systèmes d'accès à un serveur 11 à l'aide d'un objet portatif 12 (classiquement une carte) à microprocesseur 13 détenue par un utilisateur, ou porteur 14.

Le serveur 11 comprend un lecteur 15 capable de lire des données inscrites ou calculées sur le microprocesseur 13, et un clavier 16 permettant au porteur 14 de transmettre des données au serveur 11 et à l'objet 12. Le serveur 11 peut notamment assurer des fonctions de contrôle physique de l'accès à un lieu, de délivrance contrôlée de monnaie ou de tout type d'objet, de contrôle de l'utilisation d'un appareil ou de l'accès à des données. Dans certains cas, il peut être partiellement délocalisé (par exemple, dans le cas de l'accès à une base de données, seuls le lecteur 15 et le clavier 16 sont nécessaires sur place).

L'objet portatif 12 a pour but d'assurer la sécurité de la transaction. Pour cela, une procédure d'authentification est mise en oeuvre. De façon connue, l'authentification comprend une authentification 18 du porteur 14 par l'objet 12 par l'intermédiaire d'un code secret et une authentification 17 de l'objet portatif 12 par le serveur 11. Selon l'approche nouvelle de l'invention, l'authentification met en oeuvre une reconnaissance 19 du porteur 14 par le serveur 11.

Pour augmenter la sécurité, la double authentification 17, 18 peut être maintenue, préalablement à l'authentification 19 selon l'invention, mais cela n'est pas obligatoire.

La figure 2 illustre globalement le procédé mis en oeuvre, dans le cas de l'authentification complète (à trois niveaux).

Le procédé a pour but de permettre une session 21, qui est soit un simple accès (à un lieu, un objet, une fonction), soit un échange de données. Cette session 21 est précédée de l'authentification 22, qui comprend trois étapes successives :

- authentification 221 du porteur par l'objet portatif ;
- authentification 222 de l'objet par le serveur ;
- authentification 223 du porteur par le serveur.

Chacune de ces étapes 221 à 223 est décrite de façon plus détaillée, en relation respectivement avec les figures 3 à 5.

Comme déjà indiqué précédemment, les étapes 221 et 222 ne sont pas nouvelles en elles-mêmes. elles correspondent en effet à la technique actuellement mise en oeuvre. Il est à noter qu'elles ne sont pas obligatoires pour mettre en oeuvre l'invention. Plus précisément, l'invention concerne tout procédé mettant en oeuvre l'étape 223 (précisée en figure 5), qu'elle soit mise en oeuvre seule ou simultanément avec d'autres techniques.

On décrit maintenant plus précisément chaque étape. Le tableau suivant résume les différentes données calculées et échangées.

SERVEUR	CARTE	PORTEUR
	authentification porteur Cco = algo4(Ccl) Cco'∈ carte Cco' = Cco =>ok P2 = algo1 (Pc⊂Ccl)	<= Code clair : Ccl
authentification carte Aléa 1 KC' = algo 6 (KM, n° série) KM ∈ serveur X' = algo 5 (KC', Aléa 1) X' = X => ok	=> X= algo5(KC2, Aléa 1) KC ∈ carte <= X, n° série, (Aléa 2)	
authentification porteur/carte Aléa 3 KC2'= algo3 (KM,P2) Y'=algo2 (KC2', Aléa3) Y'=Y =>ok	=> Y=algo2 (KC2, Aléa3) KC2 ∈ carte <= Y, P2	
calcul clé session S = algo7(KC, X.Aléa2) (P2 peut être utilisé)	calcul clé session S = algo7 (KC, X, Aléa2)	

L'authentification du porteur par l'objet portatif est illustré par le synoptique de la figure 3. Le porteur introduit un code secret d'authentification Ccl à l'aide du clavier (numérique ou alphanumérique) associé au serveur.

L'objet portatif reçoit (31) ce code Ccl, et calcule (32) une empreinte Cco de

ce code secret, à l'aide d'un algorithme de cryptage (algo4) 33 stocké en mémoire. Cette empreinte Cco est comparée (34) à une référence Cco' 35 également stockée en mémoire. Si le résultat de la comparaison est positif, le porteur est authentifié par l'objet portatif.

La figure 4 illustre l'authentification, également connue en elle-même, de l'objet portatif par le serveur.

Le serveur calcule et transmet (41) à l'objet portatif une valeur aléatoire, ou aléa (aléa1). L'objet portatif reçoit (42) l'aléa, et l'utilise pour calculer (43) une valeur X, résultat d'un algorithme de cryptage (algo5) non réversible appliqué à une clé secrète KC stockée de façon sécurisée (bien que lisible par des moyens adéquats) et à l'aléa aléa1.

Cette valeur X est transmise (44) au serveur, en même temps qu'une donnée spécifique à l'objet portatif, telle qu'un numéro de série Ns, inscrite dans l'objet portatif.

Le serveur calcule (45) tout d'abord une estimation KC' de la clé secrète, à l'aide d'un algorithme de cryptage algo6, tenant compte d'une clé maître stockée KM et du numéro de série Ns transmis.

Ensuite, il calcule (46), à l'aide de l'algorithme algo5 (utilisé pour calculer X) une estimation X' de X, en fonction de KC' et de aléa 1. Les valeurs X et X' sont comparées (47) et, si elles sont identiques, l'objet portatif est authentifié par le serveur.

On peut noter que cette technique présente l'avantage qu'aucune information secrète ne circule entre le serveur et l'objet portatif. Par ailleurs, on vérifie que cette authentification est indépendante du porteur, et que la connaissance du contenue de l'objet permettrait à tout tiers non habilité d'accéder au serveur.

L'invention pallie cet inconvénient, en mettant en oeuvre une méthode d'authentification illustrée par la figure 5.

Cette étape prend en compte un code d'authentification Ccl introduit (51) par le porteur. Ce code peut être identique ou distinct de celui utilisé précédemment (figure 3).

A partir de ce code Ccl, l'objet portatif extrait (52) un code partiel Pc, à l'aide d'une fonction adaptée, prenant par exemple en compte un nombre d'éléments donné parmi ceux introduits par l'utilisateur. Toute combinaison est possible, par exemple pour mêler les deux codes fournis par le porteur. Cette extraction d'un code partiel n'est pas obligatoire, mais est préférable d'un point de vue sécuritaire.

Il est à noter que, lorsque l'authentification du porteur par l'objet portatif ne tient compte que d'une partie des éléments fournis par le porteur, il n'est pas obligatoire que la référence (Cco') stockée dans l'objet soit cryptée. Elle peut éventuellemen être stockée en clair, puisque l'identification ne prend en compte qu'une partie des éléments délivrés par le porteur.

A partir du code partiel Pc, l'objet portatif calcule (53) une information d'authentification P2, obtenue à l'aide d'un algorithme non réversible algo1.

Parallèlement, le serveur calcule et transmet (54) une valeur aléatoire Aléa3. L'objet portatif reçoit (55) la valeur Aléa3, puis calcule (56) une valeur Y, à partir d'un algorithme de cryptage algo2, appliqué à une clé secrète KC2 (différente de la clé KC) et de la valeur Aléa3.

La valeur Y et l'information d'authentification P2 sont ensuite transmises (57) au serveur. Celui-ci calcule (58) une estimation KC2' de la clé secrète KC2, à l'aide de l'algorithme algo3, à partir de la clé maître KM et de P2.

Ensuite, le serveur calcule (59) une estimation Y' de la valeur Y, à l'aide de l'algorithme de cryptage algo2, et à partir de la clé estimée KC2' et de la valeur aléa3. Celle-ci est comparée (510) à la valeur Y. Si le résultat est positif, le serveur authentifie le porteur.

Ainsi, selon l'invention, il est impossible que le serveur délivre une autorisation d'accès sans que le porteur fournisse un code d'authentification exact. La connaissance du contenu de l'objet portatif n'est donc plus suffisante.

Il est à noter que les différents algorithmes de cryptage mentionnés ne sont pas forcément différents. Par exemple, les calculs de X et de Y, ou ceux de KC' et de KC2' peuvent être les mêmes.

En résumé, selon l'invention, la répartition des données est modifiée par

rapport à l'état de la technique. En effet, il manque dans la carte une information majeure.

Pour cela, on prévoit une procédure d'authentification qui peut être considérée comme une authentification du porteur par le serveur, la carte servant de relais pour la répartition des informations. Cela implique la création d'une clé secrète spécifique.

Cette clé est fabriquée au moyen de KM la clé maître du serveur et de P2 une partie du code en clair du porteur que l'on crypte (l'algorithme de cryptage peut être celui qui est déjà présent sur la carte et le serveur). Le code utilisateur de référence doit être écrit crypté dans la carte (algorithme de cryptage non réversible sans la clé de chiffrement/déchiffrement), ce qui va dans le sens d'une amélioration de la sécurité.

Cette clé est implantée sur la carte de la même façon que la clé classique. Elle est utilisée pour fabriquer au travers de l'algorithme une information à partir d'un aléa envoyé par le serveur. Cette information est envoyée au serveur. Parallèlement, cette information doit être recalculée dans le serveur pour pouvoir la comparer avec ce que lui a envoyé la carte. Pour cela, le serveur doit recalculer la seconde clé. Il le fait au moyen de P2 le résultat de cryptage d'une partie du code en clair du porteur que lui envoie la carte. P2 n'est pas disponible dans la carte et est pourtant indispensable au serveur pour que l'information calculée soit identique à celle reçue de la carte.

Il manque donc dans la carte une information majeure permettant une authentification carte/porteur par le serveur.

La connaissance du contenu de la carte ne suffit plus pour contourner les systèmes de sécurité.

REVENDICATIONS

1. Procédé d'authentification d'un utilisateur (14) par un serveur (11), à l'aide d'un objet portatif (12) à microprocesseur (13),

caractérisé en ce que ledit serveur (11) tient compte d'une information d'authentification (P2) produite par ledit objet portatif (12), correspondant au résultat d'un algorithme spécifique (223 ; 52, 53) appliqué à un premier code d'authentification (Ccl) fourni par ledit utilisateur (14), pour fournir un résultat positif ou négatif d'authentification.

2. Procédé selon la revendication 1, caractérisé en ce que ledit algorithme spécifique comprend les opérations suivantes :

- production (52) d'un code d'authentification partiel (Pc), déduit dudit premier code d'authentification (Ccl) ;
- application (53) d'un premier algorithme de cryptage non réversible (algo1) sur ledit code d'authentification partiel (Pc), produisant ladite information d'authentification (P2).

3. Procédé selon l'une quelconque des revendications 1 et 2, dans lequel ledit serveur (11) possède une clé maître (KM) commune à une pluralité d'utilisateurs, ledit objet portatif (12) possède au moins une première clé secrète (KC2) fonction, de façon non réversible, de ladite clé maître (KM) et ledit utilisateur (14) connaît au moins ledit premier code d'authentification (Ccl),

caractérisé en ce qu'il comprend une phase d'authentification simultanée par ledit serveur (11) dudit objet portatif (12) et dudit utilisateur (14) à partir de deux informations délivrées par ledit objet portatif (11) :

- une première valeur (Y) résultat d'un second algorithme de cryptage non réversible (algo2) tenant compte de ladite première clé secrète (KC2) et d'un premier aléa (Aléa3) transmis par ledit serveur (11) ; et
- une information d'authentification (P2) dudit utilisateur (14) obtenue à partir dudit premier code d'authentification (Ccl) donné par ledit utilisateur (14),

ledit serveur (11) calculant une estimation de ladite première valeur (Y') à l'aide dudit

second algorithme de cryptage (algo2), en tenant compte dudit premier aléa (Aléa3) et d'une estimation (KC2') de ladite première clé secrète, obtenue à partir de ladite clé maître (KM) et de ladite inforamtion d'authentification (P2), et comparant ladite première valeur (Y) et ladite estimation de ladite première valeur (Y') pour fournir ledit résultat positif ou négatif d'authentification.

4. Procédé selon la revendication 3, caractérisé en ce que l'authentification dudit utilisateur (14) par ledit serveur (11) comprend les étapes suivantes :

- introduction par ledit utilisateur dudit premier code d'authentification (Ccl), transmis audit objet portatif ;
- calcul par ledit objet portatif de ladite information d'authentification (P2), à partir dudit premier code d'authentification (Ccl) ;
- réception dans ledit objet portatif de ladite première valeur aléatoire (Aléa3) transmise par ledit serveur ;
- calcul par ledit objet portatif de ladite première valeur (Y), à l'aide dudit second algorithme de cryptage non réversible (algo2), à partir de ladite première clé secrète (KC2) stocké dans ledit objet portatif et de ladite première valeur aléatoire (Aléa3) ;
- transmission audit serveur, par ledit objet portatif, de ladite première information (Y) et de ladite information d'authentification (P2) ;
- calcul par ledit serveur de ladite estimation de la première clé secrète (KC2'), à l'aide d'un troisième algorithme de cryptage non réversible (algo3), à partir de ladite clé maître (KM) stocké dans ledit serveur et de ladite information d'authentification (P2) ;
- calcul par ledit serveur de ladite estimation de la première valeur (Y'), à l'aide dudit second algorithme de cryptage non réversible (algo2), à partir de ladite estimation de la première clé secrète (KC2') et de ladite première valeur aléatoire (Aléa3) ;
- comparaison par ledit serveur de ladite première valeur (Y) et de ladite estimation de la première valeur (Y'), et authentification dudit utilisateur par ledit serveur si le résultat de la comparaison est

favorable.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comprend une première phase préalable d'authentification (221) dudit utilisateur (14) par ledit objet portatif (12), comprenant les étapes suivantes :

- introduction (31) par ledit utilisateur d'un second code d'authentification (Ccl), transmis audit objet portatif ;
- calcul (32) par ledit objet portatif d'une empreinte (Cco) dudit second code d'authentification (Ccl), à l'aide d'un quatrième algorithme de cryptage non réversible (algo4) ;
- comparaison (35) de ladite empreinte (Cco) avec une donnée de référence (Cco') stockée dans ledit objet portatif, produisant une première information d'authentification partielle.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comprend une seconde phase préalable d'authentification (222) dudit objet portatif (12) par ledit serveur (11), comprenant les étapes suivantes :

- réception (42) dans ledit objet portatif d'une seconde valeur aléatoire (Aléa1) transmise par ledit serveur ;
- calcul (43) par ledit objet portatif d'une seconde valeur (X), à l'aide d'un cinquième algorithme de cryptage non réversible (algo5), à partir d'une seconde clé secrète (KC) stocké dans ledit objet portatif et de ladite seconde valeur aléatoire (Aléa1) ;
- transmission (44) audit centre serveur, par ledit objet portatif, de ladite seconde information (X) et d'une donnée spécifique (Ns) stockée dans ledit objet portatif ;
- calcul (45) par ledit serveur d'une estimation de ladite seconde clé secrète (KC'), à l'aide d'un sixième algorithme de cryptage non réversible (algo6), à partir de ladite clé maître (KM) et de ladite donnée spécifique (Ns) ;
- calcul (46) par ledit centre serveur d'une estimation de ladite seconde information (X'), à l'aide dudit cinquième algorithme de cryptage non

réversible, à partir de ladite estimation de la seconde clé secrète (KC') et de ladite seconde valeur aléatoire (Aléa1) ;

- comparaison (47) par ledit centre serveur de ladite seconde information (X) et de ladite estimation de la seconde information (X'), produisant une seconde information d'authentification partielle.

7. Procédé selon l'une quelconque des revendications 5 et 6, caractérisé en ce qu'au moins certains desdits algorithmes de cryptage non réversible (algo1 à algo6) sont identiques.

8. Procédé selon l'une quelconque des revendications 5 à 7, caractérisé en ce que lesdits premier et second codes d'authentification correspondent à un même et unique code (Cc1), ou forment deux parties d'un code unique fourni par ledit utilisateur (11).

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'il comprend une étape de calcul d'une clé de session (S) effectuée simultanément par ledit serveur et par ledit objet portatif, à partir d'une troisième valeur aléatoire (Aléa2) délivrée par ledit objet portatif, ladite étape de calcul d'une clé de session n'étant mise en oeuvre que si le ledit résultat d'authentification est positif.

10. Procédé selon la revendication 9, caractérisé en ce que ladite clé de session (S) tient compte de ladite information d'authentification (P2).

11. Serveur (11) à accès contrôlé, comprenant des moyens de communication avec un objet portatif (12) à microprocesseur et des moyens d'authentification d'un utilisateur (14) dudit objet portatif,

caractérisé en ce que lesdits moyens d'authentification tiennent compte d'une information d'authentification (P2) produite par ledit objet portatif, correspondant au résultat d'un algorithme spécifique (223 ; 52, 53) appliqué à un premier code d'authentification (Cc1) fourni par ledit utilisateur (14), pour délivrer un résultat positif ou négatif d'authentification.

12. Objet portatif (12) à microprocesseur (13) destiné à dialoguer avec un serveur (11), caractérisé en ce qu'il comprend des moyens de calcul d'une information d'authentification (P2), correspondant au résultat d'un algorithme spécifique (223 ;

52, 53) appliqué à un premier code d'authentification (Ccl) fourni par un utilisateur (14) dudit objet portatif.

13. Objet portatif selon la revendication 12, caractérisé en ce qu'il comprend des moyens de stockage sécurisé d'au moins deux clés secrètes, une première clé secrète (KC2) étant destinée à l'authentification dudit utilisateur (14) par ledit serveur (11), et une seconde clé secrète (KC) étant destinée à l'authentification dudit objet portatif (12) par ledit serveur (11).

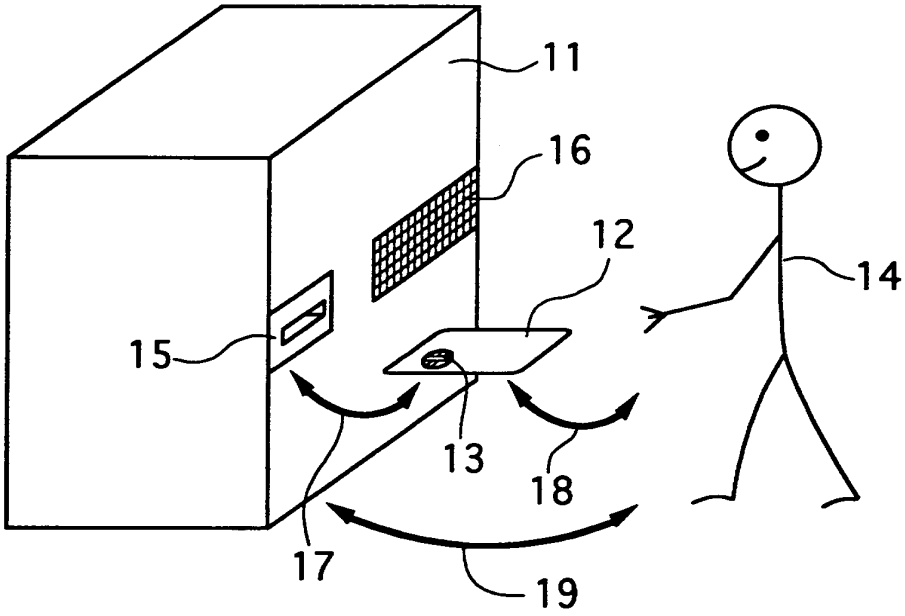

11
16
12
14
15
13
18
17
19

Fig. 1

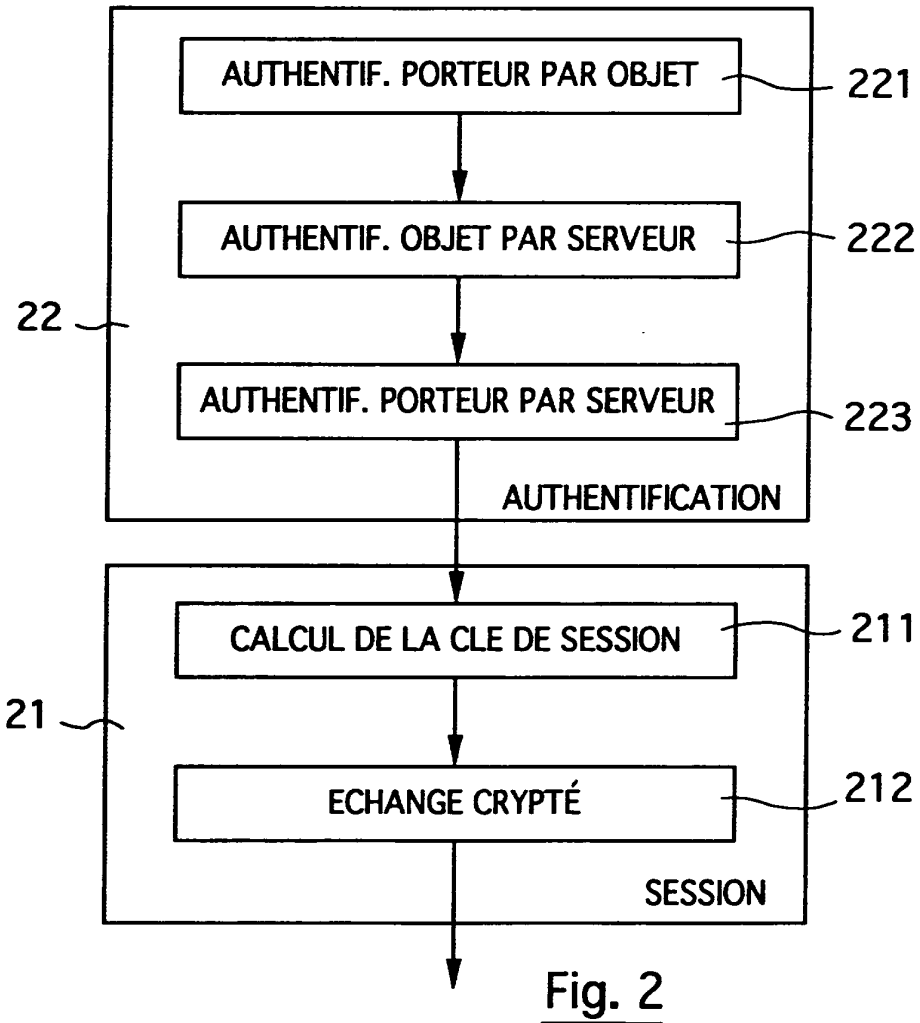

AUTHENTIF. PORTEUR PAR OBJET
221
AUTHENTIF. OBJET PAR SERVEUR
222
22
AUTHENTIF. PORTEUR PAR SERVEUR
223
AUTHENTIFICATION
CALCUL DE LA CLE DE SESSION
211
21
ECHANGE CRYPTÉ
212
SESSION

Fig. 2

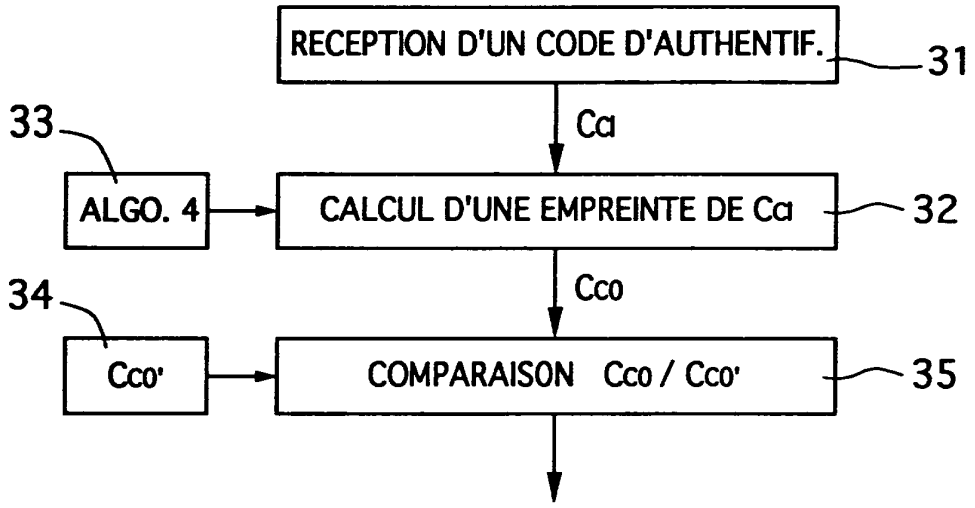

RECEPTION D'UN CODE D'AUTHENTIF.
31
Cα
33
ALGO. 4
CALCUL D'UNE EMPREINTE DE Cα
32
Cco
34
Cco'
COMPARAISON Cco / Cco'
35

Fig. 3

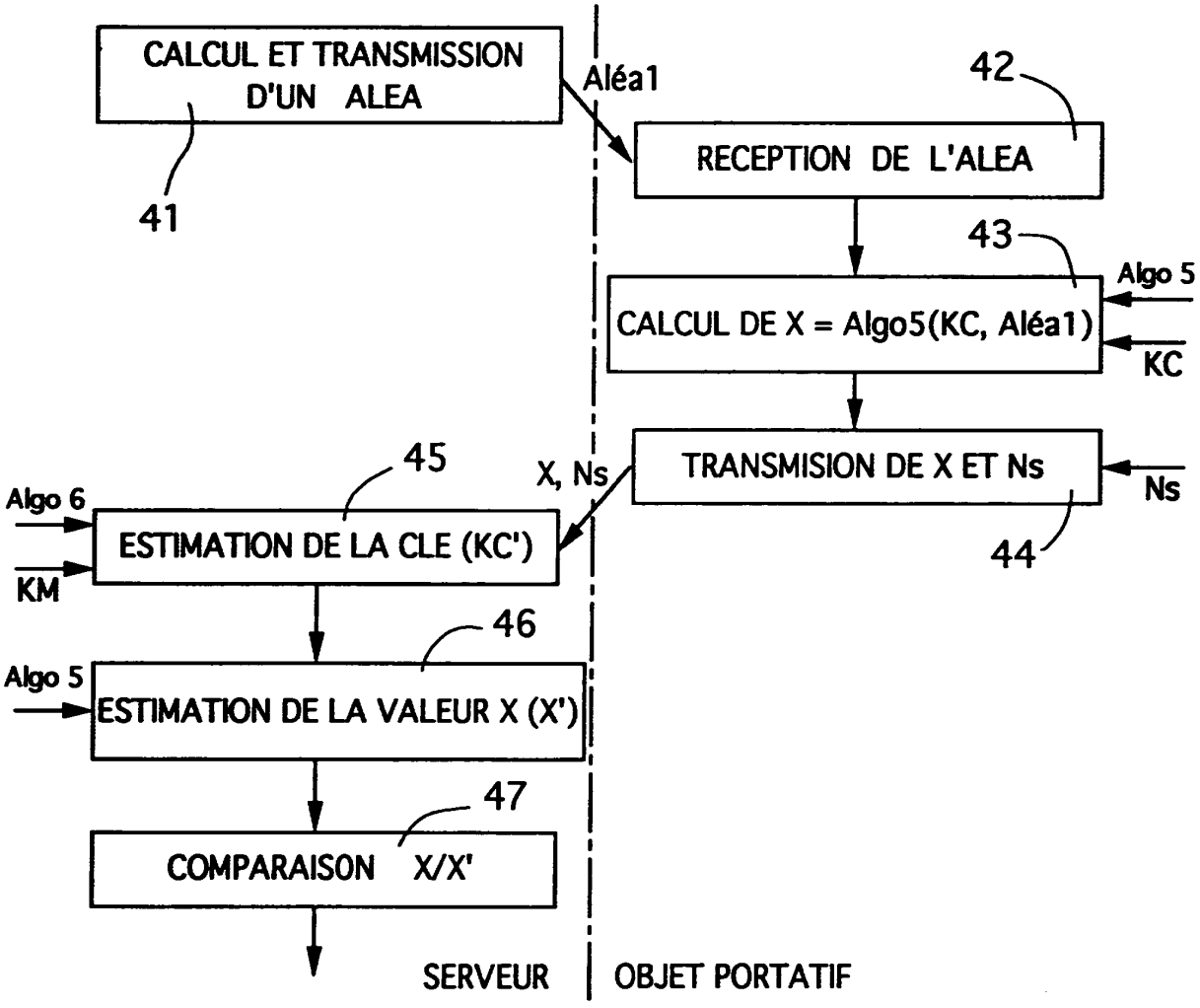

CALCUL ET TRANSMISSION D'UN ALEA
41
Aléa1
42
RECEPTION DE L'ALEA
43
Algo 5
CALCUL DE X = Algo5(KC, Aléa1)
KC
TRANSMISION DE X ET Ns
Ns
44
X, Ns
45
Algo 6
ESTIMATION DE LA CLE (KC')
KM
46
Algo 5
ESTIMATION DE LA VALEUR X (X')
47
COMPARAISON X/X'
SERVEUR
OBJET PORTATIF

Fig. 4

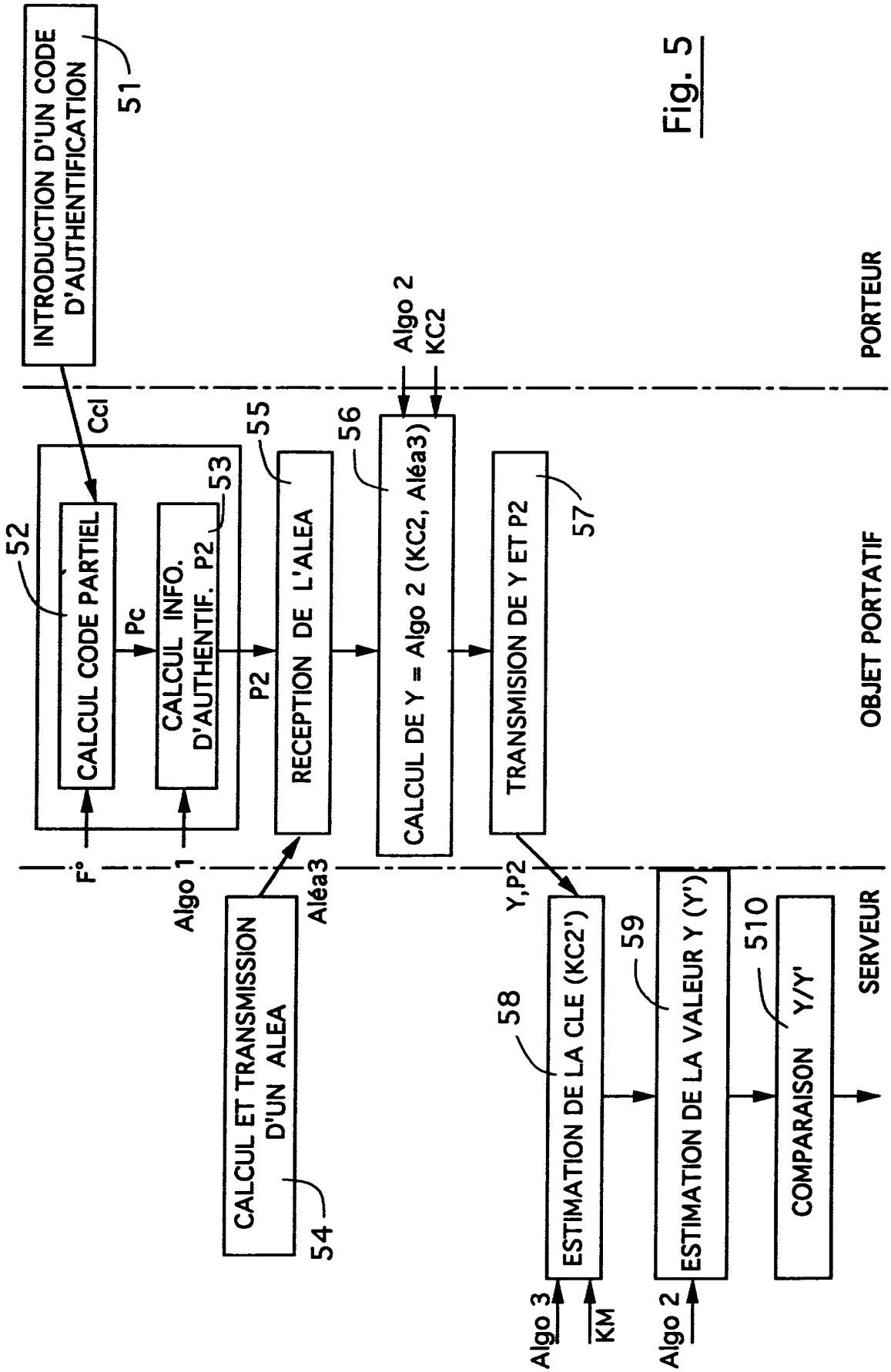

INTRODUCTION D'UN CODE D'AUTHENTIFICATION
51
PORTEUR
Algo 2
KC2
Ccl
55
56
52
CALCUL CODE PARTIEL
Pc
CALCUL INFO. D'AUTHENTIF. P2
53
P2
RECEPTION DE L'ALEA
CALCUL DE Y = Algo 2 (KC2, Aléa3)
TRANSMISION DE Y ET P2
57
OBJET PORTATIF
F°
Algo 1
Aléa3
Y,P2
CALCUL ET TRANSMISSION D'UN ALEA
54
58
ESTIMATION DE LA CLE (KC2')
59
ESTIMATION DE LA VALEUR Y (Y')
510
COMPARAISON Y/Y'
SERVEUR
Algo 3
KM
Algo 2

Fig. 5

REPUBLIQUE FRANÇAISE

2730076

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

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

N° d'enregistrement national

FA 514855
FR 9501314

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X Y A	EP-A-0 566 512 (INNOVATRON TERMINAUX) * colonne 9, ligne 25 - colonne 12, ligne 49; revendications 1,6 * ---	1-4 5,6 11,12
Y A	EP-A-0 547 975 (BULLCP8) * abrégé; revendication 2 * ---	5,6 1-4,11, 12
A	EP-A-0 628 935 (BULL CP8) * abrégé * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G07F

Date d'achèvement de la recherche: 29 Septembre 1995

Examinateur: Taccoen, J-F

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)