PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 :		(11) Numéro de publication internationale:
H04L 9/32	A1	WO 98/28878
		(43) Date de publication internationale: 2 juillet 1998 (02.07.98)

(21) Numéro de la demande internationale: PCT/FR97/02409

(22) Date de dépôt international: 23 décembre 1997 (23.12.97)

(30) Données relatives à la priorité:
96/15942 24 décembre 1996 (24.12.96) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F–75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CAMPANA, Mireille [FR/FR]; 7, villa Jeanne d'Arc, F–92140 Clamart (FR). ARDITTI, David [FR/FR]; 46 ter, rue Paul Vaillant Couturier, F–92140 Clamart (FR). GILBERT, Henri [FR/FR]; 2, allée des Peupliers, F–91440 Bures–sur–Yvette (FR). LECLERCQ, Thierry [FR/FR]; 22, avenue de Choisy, F–75013 Paris (FR). BONTRON, Nicolas [FR/FR]; 5, rue de Braque, F–75003 Paris (FR).

(74) Mandataire: SOCIETE DE PROTECTION DES INVENTIONS; 25, rue de Ponthieu, F–75008 Paris (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: AUTHENTICATING METHOD FOR AN ACCESS AND/OR PAYMENT CONTROL SYSTEM

(54) Titre: PROCEDE D'AUTHENTIFICATION AUPRES D'UN SYSTEME DE CONTROLE D'ACCES ET/OU DE PAIEMENT

(57) Abstract

The invention concerns an authenticating method for an access and/or payment control system ensuring anonymity with respect to third parties, which consists in emitting, according to a one–way authentication protocol, an authenticating sequence which varies entirely with each transaction and does not enable a third party to determine the identity of the client, or even to determine which transactions are from the same client.

(57) Abrégé

La présente invention concerne un procédé d'authentification auprès d'un système de contrôle d'accès et/ou paiement assurant l'anonymat vis–à–vis d'un tiers, dans lequel on émet, selon un protocole d'authentification monodirectionnel, une séquence d'authentification qui varie entièrement à chaque transaction et ne permet pas à un tiers de déterminer l'identité du client, ni même de déterminer quelles transactions sont issues d'un même client.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE D'AUTHENTIFICATION AUPRES D'UN SYSTEME DE CONTROLE D'ACCES ET/OU DE PAIEMENT

DESCRIPTION

Domaine technique

La présente invention concerne un procédé d'authentification auprès d'un système de contrôle d'accès et/ou paiement de services vocaux ou télématiques offerts par un fournisseur de service, qui peut être ou non un opérateur de télécommunications.

La configuration de référence, illustrée sur la figure, montre un dispositif classique relatif :

1°) aux équipements d'un client (terminal téléphonique ou télématique) ;

2°) aux équipements d'un fournisseur de service (par exemple : point de commande de services du réseau d'un opérateur, serveur vocal, serveur Internet appartenant à un fournisseur de services, etc.) ;

3°) à un serveur de contrôle d'accès et/ou de paiement.

Cette configuration de référence s'applique aux échanges considérés dans la suite de la description. Les fonctions 2°) et 3°) peuvent relever ou non du même opérateur/fournisseur de service.

Dans un tel dispositif, le déroulement d'une transaction donnant lieu à contrôle d'accès et/ou paiement est le suivant :

(I) Etablissement d'une communication entre le client et le fournisseur de service.

(II) Vérification par le fournisseur de service auprès du serveur de contrôle d'accès et/ou de paiement des droits d'accès du client et/ou de l'existence d'un compte solvable (compte client à facturer ou compte prépayé) ; obtention éventuelle de données complémentaires telles que le crédit maximum pour le compte du considéré.

(III) Fourniture de la prestation.

(IV) Envoi éventuel de données de taxation, du fournisseur de service vers le serveur de contrôle d'accès et/ou de paiement.

Dans une telle transaction les besoins de sécurité identifiés sont les suivants :

• Anonymat du client vis-à-vis du tiers

Par tiers, on entend ici :

1°) toute personne susceptible d'avoir accès aux échanges entre client et fournisseur de service. Il ne doit pas être possible d'utiliser les données d'identification et d'authentification transmises lors de ces échanges pour retrouver l'identité du client, ou même déceler quelles communications sont relatives à un même client.

2°) Le fournisseur de service lui-même, dans le cas où celui-ci n'assure pas la fonction de contrôle d'accès et/ou de facturation. Dans le cas où ces fonctions sont séparées, on peut ne pas souhaiter que le fournisseur de service puisse établir l'identité des clients, ni même établir des statistiques basées sur le regroupement des transactions relatives à un

même client. L'identité du client (ou du compte utilisé), indispensable pour le contrôle d'accès et/ou de paiement du service, ne doit donc alors être communiquée au fournisseur de service, ni en clair ni sous forme d'un pseudonyme statique.

- Authentification de l'identité du client lors de la phase (II)

Cette authentification permet de s'assurer que le client, dont le numéro de client ou le numéro de compte est indiqué dans les données d'identification qui parviennent (via le fournisseur de service) au système de contrôle, a bien établi une communication avec le fournisseur de service. Une authentification active est indispensable afin de prévenir des fraudes par rejeu de données anciennes.

En outre, un service de sécurité additionnel peut être offert optionnellement :

- Authentification de données du client

Cette fonction peut permettre, par exemple au serveur de contrôle d'accès et/ou de paiement, de s'assurer de l'acceptation par un client du montant d'une prestation dans le cas où les données, sur lesquelles portent le calcul d'authentification, représentent ce montant.

Etat de la technique antérieure

A l'heure actuelle, la plupart des dispositifs à clé secrète assurant une authentification utilisent un schéma du type « identification-

authentification » (typiquement nom + mot de passe) et n'assurent en conséquence aucun anonymat.

Les dispositifs garantissant l'anonymat en même temps que l'accès légal à une ressource sont rares et systématiquement basés sur l'utilisation d'une clé publique, comme décrit dans l'article référencé [1] en fin de description, mais cela implique des échanges assez lourds (au moins 512 bits). Or, le client peut ne disposer que d'un téléphone et aboutir, chez le fournisseur de service, sur un opérateur humain, ou un serveur, vocal ou non. Le client peut aussi disposer d'un micro-ordinateur sans modem. Il n'est alors pas possible de lui demander de taper sur son clavier, ou d'énoncer oralement, une trop longue séquence de caractères.

Dans le procédé de l'invention, du fait des fortes contraintes sur la longueur du message d'identification-authentification, le recours à une méthode d'authentification à clé publique (qui conduirait à des messages de plus de 100 digits) n'est pas envisageable. De plus, on ne peut pas recourir à la technique classique d'authentification d'un nombre aléatoire émis par le réseau, qui nécessite un échange bidirectionnel.

L'invention a pour objet un procédé d'authentification qui permette de résoudre les problèmes énoncés ci-dessus.

Exposé de l'invention

La présente invention concerne un procédé d'authentification auprès d'un système de contrôle d'accès et/ou de paiement assurant l'anonymat vis-à-vis d'un tiers, caractérisé en ce qu'on émet, selon un protocole d'authentification monodirectionnel, une

séquence d'authentification qui varie entièrement à chaque transaction et ne permet pas à un tiers de déterminer l'identité du client, ni même de déterminer quelles transactions sont issues d'un même client.

Avantageusement on utilise un compteur incrémenté de une unité dans l'authentifieur du client à chaque tentative d'authentification, les données d'authentification transmises lors de chaque accès étant la valeur courante C du compteur du client et un code d'authentification CA de d digits, calculé à partir de la clé secrète d'authentification du client, K_{client}, et du compteur C, à l'aide d'un algorithme d'authentification A, le code CA étant donné par la relation :

$$CA = A(K_{client} , C)$$

Dans le cas où le client souhaite « signer » des données M, on fait également intervenir le paramètre M dans le calcul d'authentification, le code d'authentification CA étant donné par la relation :

$$CA = A(K_{client} , C||M).$$

Dans le serveur de contrôle d'accès et/ou de paiement, la valeur de compteur correspondant à la dernière authentification réussie, C', est conservée pour chaque client.

Le serveur de contrôle d'accès et/ou de paiement est capable de reconstituer la clé secrète d'authentification K_{client} de chaque client.

Avantageusement, cette clé peut être reconstituée à partir d'une clé maîtresse d'authentification KA commune à tout le système et de

l'identité du client, à l'aide d'un algorithme dit de diversification et noté D, avec :

$$K_{client} = D(KA, ID[client]).$$

Avantageusement une tentative d'authentification n'est acceptée que si pour le client considéré la valeur de compteur C est supérieure à C' de une à quelques dizaines d'unités et si la valeur d'authentification CA qui l'accompagne est égale à la valeur d'authentification recalculée par le serveur à partir de C et de la clé K_{client}.

Avantageusement afin d'assurer l'anonymat de l'identité du client vis-à-vis du fournisseur de service, on chiffre cette identité à l'aide d'une clé partagée entre l'authentifieur du client et le serveur de contrôle d'accès et/ou paiement.

On peut optionnellement répartir les clients en groupes et utiliser une clé de chiffrement distincte pour chaque groupe.

Dans une première variante de l'invention, non basée sur l'utilisation de numéros de groupe, le client transmet, lors de chaque accès :

- son numéro d'identification individuel NI chiffré avec la clé K de chiffrement du système en utilisant la valeur d'authentification CA comme vecteur d'initialisation ;
- les données d'authentification CA et une représentation abrégée de la valeur du compteur C (qui peut par exemple être constituée des deux digits de poids faible de C) notée c. Avantageusement, c peut être chiffré à l'aide de la clé K, en utilisant la valeur d'authentification CA comme vecteur d'initialisation.

Dans une seconde variante, basée sur l'utilisation de numéros de groupe, le client transmet, lors de chaque accès :

- le numéro du groupe auquel il appartient, NG, en clair ;
- son numéro d'identification individuel à l'intérieur du groupe, NI, chiffré avec la clé K_{NG} de chiffrement du groupe NG en utilisant la valeur d'authentification CA comme vecteur d'initialisation. L'identité complète d'un client est donnée par le couple (NG, NI) ;
- les données d'authentification CA et une représentation abrégée de la valeur du compteur C (qui peut par exemple être constituée des deux digits de poids faible de C) notée c. Avantageusement, c peut être chiffré à l'aide de la clé K_{NG}, en utilisant la valeur de CA comme vecteur d'initialisation.

Dans une troisième variante, on chiffre en outre le numéro de groupe NG à l'aide d'une clé de chiffrement K commune à tout le système.

Pour faciliter la gestion des clés de groupe dans le serveur de contrôle d'accès et/ou paiement, toutes les clés de groupe K_{NG} peuvent dépendre d'une même clé maîtresse KE, à travers un algorithme de diversification :

$$K_{NG} = D(KE, NG)$$

L'algorithme de chiffrement de NI et de C à l'aide de la clé K_{NG} étant noté E, l'algorithme de chiffrement de NG à l'aide de la clé K étant noté E', la concaténation de deux chaînes décimales (ou binaires ou hexadécimales, etc..) A et B étant notée A||B, le

message d'identification-authentification est constitué de la concaténation des éléments suivants :

- le chiffré $E'_{K,CA}$ (NG) du numéro de groupe ;
- le code d'authentification CA ;
- le chiffré $E_{KNG,CA}(c||NI)$, où c est une représentation abrégée de la valeur du compteur C (c est par exemple constitué des deux digits de poids faible du compteur C) ;

la séquence d'identification-authentification est donnée par la chaîne :

$$E'_{K,CA}\ (NG)||E_{KNG,CA}(c||NI)||CA.$$

Brève description des dessins

La figure illustre un dispositif classique relatif à des équipements d'un client, d'un fournisseur de service et d'un serveur de contrôle d'accès et/ou de paiement.

Exposé détaillé de modes de réalisation

Dans le dispositif illustré sur la figure, pour que les échanges clients-réseaux véhiculant les données d'identification et d'authentification, réalisés lors de la phase (I) définie précédemment soient réalisables depuis tous types de terminaux, et en particulier depuis un combiné téléphonique, le système de contrôle d'accès et/ou paiement est tel que :

- sur le tronçon client-fournisseur l'échange d'identification-authentification est monodirectionnel et se résume à l'envoi d'un message unique émis par le client ;

- le message d'identification-authentification est avantageusement codé en décimal (afin de pouvoir être, par exemple, transmis en DTMF (multiplication de fréquence à partir de deux sons) ou dicté en vocal depuis un combiné téléphonique), sa longueur n'excédant pas une quinzaine de chiffres, pour des raisons d'ergonomie.

Les calculs cryptographiques d'authentification et de chiffrement sont effectués dans des dispositifs sécurisés offrant une protection suffisante des clés utilisées. Pour le serveur de contrôle d'accès et/ou paiement, on a avantageusement recours à un module de sécurité physiquement protégé. Trois options d'implantation du dispositif de sécurité d'un client, appelé ici authentifieur, sont possibles :

- distribution au client d'un authentifieur personnel, assez semblable à une calculette de poche, le fonctionnement de l'authentifieur étant conditionné par le contrôle, en local, d'un code personnel ;

- logiciel implanté sur un micro-ordinateur, les clés étant alors stockées chiffrées en-dehors du logiciel ;

- serveur télématique, fournissant à un client ses séquences d'authentification.

Selon le procédé de l'invention, afin de faire varier la séquence d'authentification envoyée par le client (ou son authentifieur), on applique un algorithme d'authentification à un nombre, dont le serveur de contrôle d'accès et/ou paiement vérifie simplement qu'il varie à chaque transaction.

On peut utiliser un compteur incrémenté de une unité dans l'authentifieur du client, à chaque tentative d'authentification. Les données

d'authentification transmises, lors de chaque accès, sont la valeur courante C du compteur du client et un code d'authentification CA de d digits, calculé à partir de la clé secrète d'authentification du client, K_{client}, et du compteur C, à l'aide d'un algorithme d'authentification A.

Dans le cas où le client ne souhaite pas seulement établir son identité auprès du serveur de contrôle d'accès et/ou paiement, mais également « signer » des données M, on fait également intervenir le paramètre M dans le calcul d'authentification.

On a ainsi :

- dans le cas d'une pure authentification, le code CA donné par la relation :

$$CA = A(K_{client}, C) \ ;$$

- dans le cas où le client doit également authentifier des données, le code d'authentification CA donné par la relation :

$$CA = A(K_{client}, C||M).$$

Si l'algorithme d'authentification A est bien conçu, un fraudeur ayant observé les échanges d'un client ne sait pas prédire le code d'authentification correspondant à une nouvelle valeur de C (ou à un nouveau couple (C,M)) avec une probabilité supérieure à 10^{-d}.

Dans le serveur de contrôle d'accès et/ou de paiement, la valeur de compteur correspondant à la dernière authentification réussie, C', est conservée pour chaque client. Par ailleurs, si la méthode de diversification mentionnée plus haut est mise en oeuvre, le serveur de contrôle d'accès et/ou de paiement est capable de reconstituer la clé secrète

d'authentification K_{client} de chaque client, à partir d'une clé maîtresse d'authentification KA commune à tout le système et de l'identité du client, à l'aide d'un algorithme dit de « diversification », noté D :

$$K_{client} = D(KA, ID[client]).$$

Une tentative d'authentification n'est acceptée que si pour le client considéré la valeur de compteur C est supérieure à C' de une à quelques dizaines d'unités et si la valeur d'authentification CA qui l'accompagne est égale à la valeur d'authentification recalculée par le serveur à partir de C et de la clé K_{client}.

Dans le cas d'un authentifieur multi-utilisateur, il peut être difficile de garantir que les utilisateurs emploient leurs tickets de connexion dans l'ordre exact où ceux-ci ont été délivrés. On peut alors aménager une procédure de vérification des données d'authentification pour que de légers déséquencements de la valeur de C soient admissibles.

Afin d'assurer l'anonymat de l'identité du client vis-à-vis du fournisseur de service, on chiffre cette identité à l'aide d'une clé partagée entre l'authentifieur du client et le serveur de contrôle d'accès et/ou paiement (chiffrement à clé secrète).

Cette clé ne peut pas être propre à chaque client : le serveur de contrôle d'accès et/ou paiement aurait besoin, pour la retrouver et la déchiffrer, de recevoir l'identité ou un pseudonyme du client en clair, ce que l'on cherche précisément à éviter. Mais à l'inverse, l'utilisation d'une clé de chiffrement unique pour tout le système, implantée dans les modules de sécurité de tous les utilisateurs, serait peu sûre.

On peut alors répartir les clients en groupes et utiliser une clé de chiffrement distincte pour chaque groupe. La taille d'un groupe doit être suffisamment grande pour que la connaissance du groupe, auquel appartient un client, ne constitue qu'un faible indice pour l'identifier, et le nombre de groupes doit être suffisant pour que la compromission de la clé de chiffrement commune au groupe ait des conséquences limitées (perte d'anonymat pour un groupe).

Dans une première variante de l'invention, non basée sur l'utilisation de numéros de groupe, le client transmet, lors de chaque accès :

- son numéro d'identification individuel NI chiffré avec la clé K de chiffrement du système en utilisant la valeur d'authentification CA comme vecteur d'initialisation ;
- les données d'authentification CA et une représentation abrégée de la valeur du compteur C (qui peut par exemple être constituée des deux digits de poids faible de C) notée c. Avantageusement, c peut être chiffré à l'aide de la clé K, en utilisant la valeur d'authentification CA comme vecteur d'initialisation.

Dans une seconde variante, basée sur l'utilisation de numéros de groupe, le client transmet, lors de chaque accès :

- le numéro du groupe auquel il appartient (NG) en clair ;
- son numéro d'identification individuel à l'intérieur du groupe (NI, trois digits) chiffré avec la clé K_{NG} de chiffrement du groupe NG en utilisant la valeur d'authentification CA comme vecteur d'initialisation. L'identité complète d'un client est donnée par le couple (NG, NI) ;

- les données d'authentification (CA et C) : on choisit ici de ne pas chiffrer CA ; par contre, C est chiffré à l'aide de la clé K_{NG}.

On peut légèrement perfectionner la solution ci-dessus en chiffrant en outre le numéro de groupe NG à l'aide d'une clé de chiffrement K commune à tout le système, au lieu de la transmettre en clair. On obtient ainsi une troisième variante.

Pour faciliter la gestion des clés de groupe dans le serveur de contrôle d'accès et/ou paiement, on peut faire dépendre toute les clés de groupe K_{NG} d'une même clé maîtresse KE, à travers un algorithme de diversification :

$$K_{NG} = D(KE, NG).$$

L'algorithme de chiffrement de NI et de C à l'aide de la clé K_{NG} est noté E, et l'algorithme de chiffrement de NG à l'aide de la clé K est noté E'.

La concaténation de deux chaînes décimales (ou binaires, ou hexadécimales) A et B étant notée A||B, le message d'identification-authentification est constitué de la concaténation des éléments suivants :

- le chiffre $E'_{K,CA}$ (NG) du numéro de groupe (longueur variable, supérieure ou égale à 1) ;
- le code d'authentification CA, en clair ;
- le chiffré $E_{KNG,CA}(c||NI)$, où c est une représentation abrégée de la valeur du compteur C (c est par exemple constitué des deux digits de poids faible du compteur C).

La séquence d'identification-authentification est ainsi donnée par une chaîne :

$$E'_{K,CA}(NG)||E_{KNG,CA}(C||NI)||CA.$$

REFERENCES

[1] Article de D. Chaum intitulé « Untraceable Electronic Cash, Advances In Cryptology » (Crypto 88, Springer Verlag 1990, pages 319-327)

REVENDICATIONS

1. Procédé d'authentification auprès d'un système de contrôle d'accès et/ou paiement de services vocaux ou télématiques offerts à un client par un fournisseur de service, permettant d'assurer l'anonymat du client vis-à-vis des tiers, caractérisé en ce que le client émet, selon un protocole d'authentification monodirectionnel, une séquence d'authentification formée en appliquant un algorithme cryptographique faisant intervenir un nombre qui varie à chaque transaction ; de manière à ce qu'un tiers ne puisse déterminer ni l'identité de ce client, ni même quelles transactions sont issues de celui-ci.

2. Procédé selon la revendication 1, caractérisé en ce qu'on utilise un compteur incrémenté de une unité dans l'authentifieur du client à chaque tentative d'authentification.

3. Procédé selon la revendication 2, caractérisé en ce que les données d'authentification transmises lors de chaque accès sont une représentation abrégée de la valeur C du compteur du client et un code d'authentification CA, calculé à partir de la clé secrète K_{client} d'authentification du client, et de la valeur courant du compteur C, à l'aide d'un algorithme d'authentification A, le code d'authentification CA étant donné par la relation :

$$CA = A(K_{client}, C).$$

4. Procédé selon la revendication 3, caractérisé en ce que, dans le cas où le client souhaite signer des données M, le code d'authentification CA est donné par la relation :

$$CA = A(K_{client}, C||M).$$

5. Procédé selon la revendication 1, caractérisé en ce que, dans le serveur de contrôle

d'accès et/ou de paiement, la valeur de compteur C', correspondant à la dernière authentification réussie, est conservée pour chaque client, et en ce que le serveur de contrôle d'accès et/ou de paiement reconstitue la clé secrète authentification K_{client} de chaque client à partir d'une clé maîtresse d'authentification KA commune et de l'identité du client, à l'aide d'un algorithme noté D, avec :

$$K_{client} = D(KA, ID[client]).$$

6. Procédé selon la revendication 5, caractérisé en ce qu'une tentative d'authentification n'est acceptée que si, pour le client considéré, la valeur de compteur C est supérieure à C' d'au moins une unité et si la valeur d'authentification CA, qui l'accompagne, est égale à la valeur d'authentification recalculée par le serveur à partir de la valeur du compteur C et de la clé K_{client}.

7. Procédé selon la revendication 1, caractérisé en ce qu'on chiffre l'identité du client à l'aide d'une clé partagée entre l'authentifieur du client et le serveur de contrôle d'accès et/ou paiement, en faisant intervenir la valeur d'authentification CA à titre de vecteur d'initialisation de l'algorithme de chiffrement.

8. Procédé selon la revendication 7, caractérisé en ce qu'on répartit les clients en groupes et on utilise une clé de chiffrement distincte pour chaque groupe.

9. Procédé selon la revendication 1, caractérisé en ce que le client transmet, lors de chaque accès :

- son numéro d'identification individuel (NI) chiffré avec la clé (K) de chiffrement du système en utilisant la valeur du code d'authentification (CA) comme vecteur d'initialisation ;

- les données d'authentification (CA) et une représentation abrégée (c) de la valeur du compteur (C).

10. Procédé selon la revendication 9, caractérisé en ce que la représentation abrégée (c) est chiffrée à l'aide de la clé K, en utilisant la valeur du compte d'authentification (CA) comme vecteur d'initialisation.

11. Procédé selon la revendication 1, caractérisé en ce que le client transmet, lors de chaque accès :

- le numéro (NG) du groupe auquel il appartient en clair ;

- son numéro d'identification individuel (NI) à l'intérieur du groupe, chiffré avec la clé, (K_{NG}) de chiffrement du groupe (NG), en utilisant la valeur du compte d'authentification (CA) comme vecteur d'initialisation ;

- les données d'authentification (CA) et la valeur abrégée (c) du compteur (C).

12. Procédé selon la revendication 10, caractérisé en ce que la valeur abrégée (c) est chiffrée à l'aide de la clé de chiffrement du groupe (K_{NG}) en utilisant la valeur du compte d'authentification (CA) comme vecteur d'initialisation.

13. Procédé selon la revendication 11, caractérisé en ce qu'on chiffre le numéro de groupe (NG) à l'aide d'une clé de chiffrement (K) commune, en utilisant la valeur du compte d'authentification (CA) comme vecteur d'initialisation.

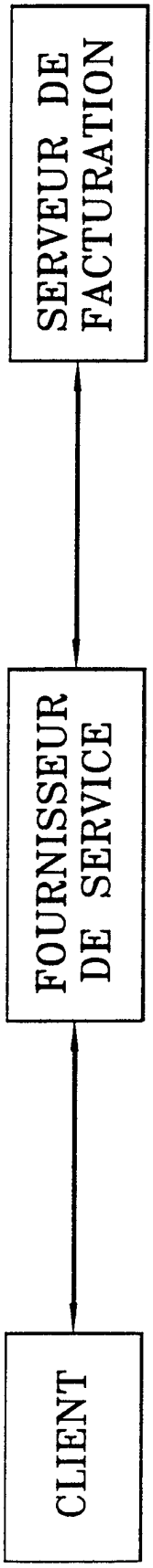
14. Procédé selon la revendication 13, caractérisé en ce que toutes les clés de groupe (K_{NG}) dépendent d'une même clé maîtresse (KE), à travers un algorithme D tel que :

$$K_{NG} = D(KE, NG).$$

15. Procédé selon la revendication 11, caractérisé en ce que l'algorithme de chiffrement du numéro d'identification individuel (NI) et de la représentation abrégé (c) de la valeur du compteur à l'aide de la clé K_{NG} étant noté E, l'algorithme de chiffrement du numéro de groupe (NG) à l'aide de la clé K étant noté E', la concaténation de deux chaînes A et B étant notée A||B, la séquence d'identification-authentification est donnée par la chaîne :

$$E'_{K,CA}(NG)||E_{KNG,CA}(c||NI)||CA.$$

FIG. 1



INTERNATIONAL SEARCH REPORT

Inte .onal Application No
PCT/FR 97/02409

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 13920 A (IBM ;TSUDIK GENE (CH)) 9 May 1996	1
A	see abstract see page 4, line 1 - line 8 see page 6, line 15 - line 22 see page 7, line 6 - line 12 see page 10, line 1 - line 16 see page 13, line 18 - line 21 see page 18, line 13 - line 22 --- -/--	2

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
21 April 1998	28/04/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/FR 97/02409

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	JANSON P ET AL: "Security in open networks and distributed systems" COMPUTER NETWORKS AND ISDN SYSTEMS, 21 OCT. 1991, NETHERLANDS, vol. 22, no. 5, ISSN 0169-7552, pages 323-346, XP000228961	1
A	see page 334, right-hand column, line 32 - line 45 see page 335, left-hand column, line 10 - line 24 see page 335, right-hand column, line 22 - line 30	2,3,6
A	EP 0 414 314 A (TRT TELECOM RADIO ELECTR ;PHILIPS NV (NL)) 27 February 1991 see page 4, line 1 - line 28 see page 6, line 2 - line 38 see page 7, line 22 - line 45	1,2,5
A	GB 2 294 795 A (PATERSON WILLIAM MUNRO GROVES ;BICC PLC (GB)) 8 May 1996 see page 4, line 15 - page 5, line 2 see page 9, line 3 - line 9	1,7
A	EP 0 613 073 A (INTERNATIONAL COMPUTERS) 31 August 1994 see column 4, line 43 - line 52	1,2
P,X	FR 2 745 965 A (INSIDE TECHNOLOGIES) 12 September 1997 see page 1, line 11 - line 15	1,2
A	see page 4, line 31 - page 5, line 37 see page 10, line 21 - line 25 see page 11, line 3 - line 11	4,6,7

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ɔnal Application No
PCT/FR 97/02409

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9613920 A	09-05-96	EP 0788688 A	13-08-97
		JP 9511888 T	25-11-97
		PL 319786 A	18-08-97
EP 0414314 A	27-02-91	FR 2651347 A	01-03-91
		DE 69031889 D	12-02-98
		JP 3237483 A	23-10-91
		US 5068894 A	26-11-91
GB 2294795 A	08-05-96	NONE	
EP 613073 A	31-08-94	AU 667155 B	07-03-96
		AU 5522894 A	01-09-94
		ZA 9306234 A	21-03-94
FR 2745965 A	12-09-97	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Dem. Internationale No
PCT/FR 97/02409

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04L

Documentation consultée autre que la documentationminimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 96 13920 A (IBM ;TSUDIK GENE (CH)) 9 mai 1996 voir abrégé voir page 4, ligne 1 - ligne 8 voir page 6, ligne 15 - ligne 22	1
A	voir page 7, ligne 6 - ligne 12 voir page 10, ligne 1 - ligne 16 voir page 13, ligne 18 - ligne 21 voir page 18, ligne 13 - ligne 22	2

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

1

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
21 avril 1998	28/04/1998

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 97/02409

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	JANSON P ET AL: "Security in open networks and distributed systems" COMPUTER NETWORKS AND ISDN SYSTEMS, 21 OCT. 1991, NETHERLANDS, vol. 22, no. 5, ISSN 0169-7552, pages 323-346, XP000228961	1
A	voir page 334, colonne de droite, ligne 32 - ligne 45 voir page 335, colonne de gauche, ligne 10 - ligne 24 voir page 335, colonne de droite, ligne 22 - ligne 30	2,3,6
A	EP 0 414 314 A (TRT TELECOM RADIO ELECTR ;PHILIPS NV (NL)) 27 février 1991 voir page 4, ligne 1 - ligne 28 voir page 6, ligne 2 - ligne 38 voir page 7, ligne 22 - ligne 45	1,2,5
A	GB 2 294 795 A (PATERSON WILLIAM MUNRO GROVES ;BICC PLC (GB)) 8 mai 1996 voir page 4, ligne 15 - page 5, ligne 2 voir page 9, ligne 3 - ligne 9	1,7
A	EP 0 613 073 A (INTERNATIONAL COMPUTERS) 31 août 1994 voir colonne 4, ligne 43 - ligne 52	1,2
P,X	FR 2 745 965 A (INSIDE TECHNOLOGIES) 12 septembre 1997 voir page 1, ligne 11 - ligne 15	1,2
A	voir page 4, ligne 31 - page 5, ligne 37 voir page 10, ligne 21 - ligne 25 voir page 11, ligne 3 - ligne 11	4,6,7

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Den e internationale No
PCT/FR 97/02409

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9613920 A	09-05-96	EP 0788688 A	13-08-97
		JP 9511888 T	25-11-97
		PL 319786 A	18-08-97
EP 0414314 A	27-02-91	FR 2651347 A	01-03-91
		DE 69031889 D	12-02-98
		JP 3237483 A	23-10-91
		US 5068894 A	26-11-91
GB 2294795 A	08-05-96	AUCUN	
EP 613073 A	31-08-94	AU 667155 B	07-03-96
		AU 5522894 A	01-09-94
		ZA 9306234 A	21-03-94
FR 2745965 A	12-09-97	AUCUN	