

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
18 décembre 2003 (18.12.2003)

PCT

(10) Numéro de publication internationale
WO 03/105096 A2

(51) Classification internationale des brevets⁷ : **G07F 7/10**

(21) Numéro de la demande internationale :
PCT/IB03/02470

(22) Date de dépôt international : 3 juin 2003 (03.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0951/02 5 juin 2002 (05.06.2002) CH

(71) Déposant (pour tous les États désignés sauf US) : **NA-GRACARD SA** [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **JOLY, Stéphane** [CH/CH]; Port Roulant 10, CH-2000 Neuchâtel

(CH). **MOERI, Nicolas** [CH/CH]; Chemin des Golliettes 13, CH-1032 Romanel sur Lausanne (CH). **LUGEON, Blaise** [CH/CH]; Chemin des Grands-Champs 9, CH-1033 Cheseaux sur Lausanne (CH).

(74) Mandataire : **LEMAN CONSULTING SA**; Route de Clémenty 62, CH-1260 Nyon (CH).

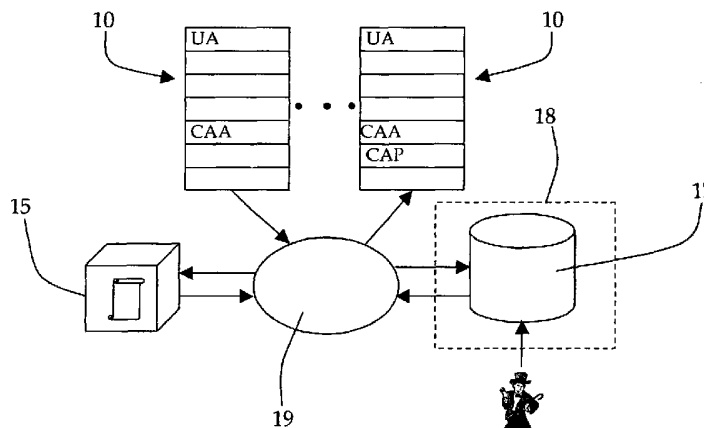
(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: METHOD FOR UPDATING DATA ON A CHIP, IN PARTICULAR OF A SMART CARD

(54) Titre : PROCEDE DE MISE A JOUR DE DONNEES SUR UNE PUCE, NOTAMMENT D'UNE CARTE A PUCE



(57) Abstract: The invention concerns a method for secure communication between a security module and a remote server. The invention also concerns a security module. The security module contains a unique identification number (UA). The inventive method is characterized in that it consists in: inserting into said security module (10), an anonymous authentication certificate (CAA); inserting in parallel data concerning the holder of the security module (10) in a database (17) of a management center (18), said data being associated with the unique identification number (UA). When setting up a first communication, the latter is made secure by using the anonymous authentication certificate (CAA). It consists in: transmitting the unique identification number (UA) in encrypted form to the management center (18), associating said unique identification number (UA) with the data concerning the holder of the security module and generating at least one customized authentication certificate (CAP), containing data concerning the holder of said security module derived from said database (17); then transmitting said customized authentication certificate (CAP) in encrypted form to the security module. Subsequent communications between the security module and the remote server use the customized authentication certificate (CAP).

[Suite sur la page suivante]

WO 03/105096 A2



européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Publiée :

- *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

(57) Abrégé : La présente invention concerne un procédé pour communiquer de façon sécurisée entre un module de sécurité et un serveur distant. Elle concerne également un module de sécurité. Le module de sécurité contient un numéro d'identification unique (UA). Le procédé selon l'invention est caractérisé en ce que l'on introduit dans ce module de sécurité (10), un certificat d'authentification anonyme (CAA). Parallèlement, on introduit des données relatives au titulaire du module de sécurité (10) dans une base de données (17) d'un centre de gestion (18), ces données étant liées au numéro d'identification unique (UA). Lorsque l'on établit une première communication, celle-ci est sécurisée en utilisant le certificat d'authentification anonyme (CAA). On transmet le numéro d'identification unique (UA) sous forme chiffrée au centre de gestion (18), on associe ce numéro d'identification unique (UA) aux données relatives au titulaire du module de sécurité et on génère au moins un certificat d'authentification personnalisé (CAP), contenant des informations relatives au titulaire dudit module de sécurité provenant de ladite base de données (17). On transmet ensuite ce certificat d'authentification personnalisé (CAP) de façon chiffrée au module de sécurité. Les communications ultérieures entre le module de sécurité et le serveur distant utilisent ce certificat d'authentification personnalisé (CAP).

PROCÉDÉ DE MISE À JOUR DE DONNÉES SUR UNE PUCE, NOTAMMENT D'UNE CARTE À PUCE.

La présente invention concerne un procédé pour communiquer de façon
5 sécurisée entre un module de sécurité, tel que notamment une carte à
puce, et un serveur distant, le module de sécurité contenant au moins
un numéro d'identification unique.

Elle concerne également un module de sécurité tel que notamment une
carte à puce ou un support analogue contenant une puce, comportant
10 un numéro d'identification unique.

Actuellement, lorsque des données doivent être mises à jour sur une
puce d'une carte à puce ou d'un support analogue, il n'est pas
souhaitable d'effectuer une telle mise à jour par un réseau public
d'ordinateurs tel qu'Internet, sans prendre des précautions relatives à la
15 confidentialité des échanges d'informations. En effet, un tel réseau
présente des problèmes de sécurité qui rendent cette mise à jour sans
précaution risquée pour l'utilisateur.

Pour pallier à ce problème, il existe des protocoles de communication
sécurisés tels que par exemple un protocole connu sous la
20 dénomination « Secure Socket Layer » (SSL). Selon ce protocole,
lorsque l'on veut établir une communication, il est nécessaire de
disposer d'un certificat d'authentification et d'une clé de chiffrement, en
particulier d'une clé de chiffrement dite privée, associée à ce certificat.
Sans un tel certificat, établi par une autorité de certification, la
25 communication ne peut matériellement pas être établie.

Pour des raisons de sécurité, on ne souhaite pas conserver dans un
ordinateur non sécurisé, un tel certificat et sa clé privée. En outre, si le
certificat et la clé sont stockées dans un ordinateur, la connexion à un

serveur distant ne peut se faire qu'à partir de cet ordinateur, ce qui empêche toute mobilité.

Avec les modules de sécurité actuels permettant une communication sécurisée, la puce contient un certificat d'authentification avec des informations relatives à son titulaire. Selon une première forme de réalisation, le certificat d'authentification personnalisé est introduit dans la puce lors de la fabrication de la carte ou du module, au moment où le futur titulaire de ce module est connu. Cela signifie que le module doit impérativement être fabriqué et réalisé « sur mesure », pour chaque titulaire, puisqu'il est personnalisé à la fabrication. Cela implique que la production de la carte à puce ne peut être entreprise qu'au moment où les informations relatives au titulaire sont connues et qu'il n'est pas possible de produire les cartes par avance. Ceci rend la gestion de la production peu pratique et complexe. Bien entendu, ceci a également une influence négative sur les coûts de production.

Selon une deuxième forme de réalisation, le module de sécurité ne contient pas de certificat au moment de sa fabrication. Celui-ci est introduit ultérieurement par une autorité de certification. Pour ceci, le titulaire d'un tel module doit se présenter personnellement auprès de l'autorité de certification, muni de son module et doit faire établir le certificat et le faire enregistrer dans le module. Ceci crée une contrainte pour le titulaire puisqu'il est obligé de se rendre en un lieu donné. Cela crée également une contrainte pour l'autorité de certification puisque cela l'oblige à se mettre au service des titulaires de module de sécurité.

La présente invention se propose de pallier ces inconvénients en réalisant un module de sécurité qui puisse être produit sans connaître les informations relatives à son futur titulaire. Ce module permet toutefois d'établir une communication sécurisée, par l'intermédiaire d'un protocole de communication sécurisé, entre ledit module et un serveur

distant, en utilisant par exemple un réseau public d'ordinateurs tels qu'Internet.

Ce but est atteint par un procédé tel que défini en préambule et caractérisé en ce que l'on introduit dans ledit module de sécurité, un
5 certificat d'authentification anonyme, en ce que l'on introduit des données relatives au titulaire dudit module de sécurité dans une base de données d'un centre de gestion, ces données étant liées audit numéro d'identification unique, en ce que l'on établit une première communication sécurisée au moyen d'un protocole de communication
10 sécurisé en utilisant ledit certificat d'authentification anonyme, en ce que l'on transmet ledit numéro d'identification unique sous forme chiffrée audit centre de gestion, en ce que l'on associe ledit numéro d'identification unique audites données relatives au titulaire du module de sécurité, en ce que l'on génère au moins un certificat
15 d'authentification personnalisé, contenant des informations relatives au titulaire dudit module de sécurité provenant de ladite base de données, en ce que l'on transmet ledit certificat d'authentification personnalisé de façon chiffrée au module de sécurité, et en ce que l'on établit des communications sécurisées ultérieures entre ledit module de sécurité et
20 ledit serveur distant en utilisant ledit certificat d'authentification personnalisé.

Ce but est également atteint par un module de sécurité tel que défini en préambule et caractérisée en ce qu'il comporte en outre un certificat d'authentification anonyme ne contenant pas de données définies par
25 l'identité du titulaire de la puce.

La présente invention et ses avantages seront mieux compris en référence à la description d'un mode de réalisation particulier de l'invention et aux dessins annexés dans lesquels :

- la figure 1 représente de façon schématique, un module de sécurité selon la présente invention, ainsi que son contenu au moment de la production de ce module;
- la figure 2 illustre le procédé de communication selon la présente invention ; et
- la figure 3 représente de façon schématique, un module de sécurité selon la présente invention, ainsi que son contenu après sa première utilisation.

En référence aux figures, le module de sécurité 10 est illustré comme ayant la forme d'une carte à puce 11. Il est clair que d'autres formes de réalisation sont également couvertes par l'invention. En particulier, le module de sécurité et la puce qu'il contient pourrait avoir la forme d'une étiquette électronique ou tag, ou être intégré dans un support quelconque tel qu'un badge, une montre, un bracelet ou tout support analogue.

En référence à la figure 1, un module de sécurité 10 tel qu'une carte à puce 11 est tout d'abord produit de façon conventionnelle, en introduisant la partie « technique », à savoir une puce électronique 12 d'une part, et une partie « visuelle », par exemple sous la forme de champs 13 non remplis dans lesquelles seront imprimées ultérieurement des informations relatives au titulaire de la carte.

Comme cela est également illustré par la figure 1, la partie électronique est identifiée de façon unique. Pour ceci, on introduit dans la puce, un numéro d'identification unique (UA) qui permettra de distinguer ce module de sécurité de tous les autres modules produits.

Une paire de clés de chiffrement 14 est ensuite introduite dans la puce du module de sécurité au moment de sa production. Cette paire de clés est liée à un certificat d'authentification unique délivré par une autorité de

certification 15. Contrairement aux modules de sécurité de l'art antérieur, le certificat ne contient aucune données relatives au titulaire de la carte. Il en résulte que même si celui-ci n'est pas encore connu, le certificat d'authentification, dénommé certificat d'authentification anonyme CAA dans la suite du texte, peut être introduit au moment de la production de la carte. Ce certificat d'authentification anonyme permet d'authentifier la carte de façon univoque. De plus, grâce à la présence de ce certificat, il est possible d'établir une connexion en utilisant un protocole qui requiert un tel certificat, comme c'est le cas pour le protocole SSL. En outre, grâce à la paire de clés 14 contenues dans la puce, le transfert d'informations peut être chiffré et la communication est donc sécurisée.

Simultanément à l'introduction de la première paire de clés dans la puce du module de sécurité, une deuxième paire de clés 16, dite clés utilisateur, est introduite dans la puce. Cette deuxième paire de clés n'est toutefois pas active à ce stade.

La figure 2 illustre le procédé de communication selon la présente invention. Plus précisément, il illustre l'initialisation de la première communication établie au moyen du module de sécurité 10 tel que décrit ci-dessus, en référence à la figure 1.

Avant la première utilisation du module de sécurité ou au plus tard, lors de cette première utilisation, des données personnelles relatives au titulaire du module sont introduites dans une base de données 17 d'un centre de gestion 18 de ces modules. Certaines de ces informations peuvent par exemple être rendues visibles sur la carte, en les imprimant dans les champs 13 prévus à cet effet. D'autres informations sont uniquement contenues dans la base de données 17, sans qu'elles soient contenues dans le module de sécurité. Ces données personnelles sont associées, dans la base de données, au numéro

d'identification unique (UA) du module de sécurité, de sorte qu'un lien univoque est établi entre une carte et une personne.

Lorsque les données relatives au titulaire du module de sécurité sont connues, il est possible de générer un certificat d'authentification
5 personnalisé (CAP). Celui-ci peut être stocké dans le centre de gestion 18 ou auprès de l'autorité de certification 15, ou de façon plus générale, dans tout endroit pouvant être connecté à la base de données 17 du centre de gestion.

Lors de la première utilisation du module de sécurité, une
10 communication est établie entre le module de sécurité, par exemple au moyen d'un lecteur de carte à puce, le centre de gestion 18 et l'autorité de certification 15. Cette communication se fait par exemple par le biais d'un réseau d'ordinateurs 19 tel qu'Internet. Cette communication utilise un protocole sécurisé tel que le protocole SSL. Les clés publiques et
15 privées sont utilisées pour authentifier le module de sécurité 10 qui est utilisé et pour initialiser la connexion selon ce protocole sécurisé. Dans cette première communication, le numéro d'identification unique (UA) est transmis de façon chiffrée au centre de gestion 18. Celui-ci détermine le titulaire au moyen de ce numéro d'identification et des
20 données relatives au titulaire contenues dans la base de données, associées à ce numéro d'identification. Le dispositif utilisé par le titulaire du module de sécurité pour établir la connexion vérifie tout d'abord s'il existe un certificat autre que le certificat d'authentification anonyme (CAA) sur la carte. Dans le cas d'une première connexion, le certificat
25 anonyme est le seul existant. Le certificat d'authentification anonyme est également utilisé pour vérifier que le titulaire est autorisé à accéder à un service donné. Pour ceci, le centre de gestion contient dans une base de données, les droits d'accès liés à chaque certificat anonyme ou à chaque groupe de certificat.

Dans une première forme de réalisation, le centre de gestion vérifie, en utilisant les données stockées dans la base de données, s'il y a adéquation entre le numéro d'identification unique (UA) du module de sécurité, les données personnelles du titulaire et le certificat d'authentification anonyme (CAA). Cette vérification implique bien entendu qu'il existe un lien dans la base de données 17 qui permette de tester cette adéquation. A titre d'exemple, la base de données peut contenir le numéro d'identification unique lié aux données personnelles du titulaire d'une part et au certificat d'identification anonyme d'autre part. Lorsque la carte est utilisée pour la première fois, le numéro d'identification est lu sur le module de sécurité. Le nom du titulaire peut être demandé. Le centre de gestion vérifie si le numéro d'identification unique enregistré dans la base de données correspond au nom introduit par le titulaire et au certificat d'authentification anonyme enregistré dans le module. Si tel est le cas, le centre de gestion envoie un message (dénommé « Entitlement management message » ou « EMM ») qui contient un nouveau certificat d'authentification personnalisé (CAP) qui contient lui-même les données personnelles du titulaire du module de sécurité. Ce nouveau certificat est enregistré dans le module de sécurité. Il est à noter que, pour gagner du temps lors de la première communication et comme la génération d'un certificat d'authentification complet est relativement longue, il est possible d'utiliser un certificat d'authentification pré-existant qui est simplement transmis au module de sécurité au moment de cette première communication. Cela signifie que le certificat personnalisé est généré par exemple au moment où le titulaire du module a transmis toutes les données qui le concerne à la base de données.

Dans une deuxième forme de réalisation, généralement utilisée en pratique, le centre de gestion 18 ne vérifie pas l'adéquation entre le numéro d'identification unique (UA) du module de sécurité, les données

personnelles du titulaire et le certificat d'authentification anonyme (CAA). Les autres étapes décrites ci-dessus se déroulent de la même façon pour les deux modes de réalisation.

5 A ce stade, la paire de clés utilisateur 16 est rendue disponible tandis que la paire de clés 14 liée au certificat d'authentification anonyme est rendue indisponible, comme cela est représenté par la figure 3.

10 Le module de sécurité contient alors les données schématisées par la figure 3, à savoir son numéro d'identification unique UA, un certificat d'authentification personnalisé CAP et une paire de clés 16 qui y est associé. Des informations visuelles sont également imprimées sur la carte.

15 Lors des connexions ultérieures, il est tout d'abord vérifié si le module de sécurité 10 contient plus d'un certificat d'authentification. Si tel est le cas, le certificat d'authentification personnalisé CAP, ou l'un d'eux s'il en contient plusieurs, est utilisé pour établir une communication sécurisée. Dans ce cas, la paire de clé utilisateur 16 est employée pour chiffrer et déchiffrer des messages. Le certificat d'authentification anonyme et/ou personnalisé est également utilisé pour vérifier si le module de sécurité et son titulaire sont autorisés à accéder au centre de gestion 18 d'une
20 part et au serveur distant d'autre part. Il est en effet possible d'utiliser un module de sécurité pour un seul serveur distant, par exemple celui d'un établissement bancaire déterminé et par conséquent, uniquement au centre de gestion qui gère les données des seuls utilisateurs. Il est également possible d'utiliser une carte contenant des droits d'accès à
25 différents services variables par utilisateur ou groupe d'utilisateurs.

Le module de sécurité selon l'invention ainsi que le procédé de communication utilisant ce module présentent de nombreux avantages par rapport à l'art antérieur. En effet, il est possible de fabriquer le module ou un grand nombre de modules sans avoir aucune information

relative à son futur titulaire. Ceci simplifie considérablement la gestion de la production et diminue le coût. La mise à jour des données visuelles ne nécessite pas d'équipement complexe et coûteux. La mise à jour des données « techniques » peut se faire de façon totalement sécurisée, en utilisant un réseau public d'ordinateurs, malgré le fait qu'un tel réseau n'est pas fiable d'un point de vue de la sécurité des informations qui y circulent. Cela signifie que ces communications peuvent se faire depuis n'importe quel point de connexion, sans qu'il soit nécessaire de se rendre en un lieu donné. Ceci facilite bien entendu l'utilisation du module de sécurité.

Cela signifie également qu'il est possible de mettre à jour des données contenues sur la carte, et en particulier le certificat d'authentification personnalisé, à distance, sans contrainte pour l'utilisateur. Ainsi, sans aucune contrainte pour l'utilisateur, il est possible de changer le certificat personnalisé, par exemple tous les ans.

L'utilisation du module de sécurité par une personne autre que le titulaire peut être empêchée de façon classique, par exemple au moyen d'un code alphanumérique tel qu'un PIN code ou un nom d'utilisateur et/ou un mot de passe.

Le fait de disposer d'un certificat d'authentification anonyme permet également de recycler le module de sécurité, en supprimant le certificat personnalisé et en recommençant la procédure décrite ci-dessus, relative à une première connexion.

Revendications

1. Procédé pour communiquer de façon sécurisée entre un module de sécurité, tel que notamment une carte à puce, et un serveur distant, le module de sécurité contenant au moins un numéro d'identification unique (UA), caractérisé en ce que :
 - l'on introduit dans ledit module de sécurité (10), un certificat d'authentification anonyme (CAA),
 - l'on introduit des données relatives au titulaire dudit module de sécurité (10) dans une base de données (17) d'un centre de gestion (18), ces données étant liées audit numéro d'identification unique (UA),
 - l'on établit une première communication sécurisée au moyen d'un protocole de communication sécurisé en utilisant ledit certificat d'authentification anonyme (CAA),
 - l'on transmet ledit numéro d'identification unique (UA) sous forme chiffrée audit centre de gestion (18),
 - l'on associe ledit numéro d'identification unique (UA) audites données relatives au titulaire du module de sécurité,
 - l'on génère au moins un certificat d'authentification personnalisé (CAP), contenant des informations relatives au titulaire dudit module de sécurité provenant de ladite base de données (17),
 - l'on transmet ledit certificat d'authentification personnalisé (CAP) de façon chiffrée au module de sécurité,
 - et l'on établit des communications sécurisées ultérieures entre ledit module de sécurité et ledit serveur distant en utilisant ledit certificat d'authentification personnalisé (CAP).

2. Procédé selon la revendication 1, caractérisé en ce que, pour établir une connexion, l'utilisateur introduit un code alphanumérique, et en ce que l'on compare ledit code alphanumérique introduit par l'utilisateur à un code alphanumérique enregistré dans la base de données (17) du centre de gestion (18).
3. Procédé selon la revendication 1, caractérisé en ce qu'au moment d'une première connexion, on vérifie qu'il existe une adéquation entre le certificat d'authentification anonyme (CAA), le numéro d'identification unique (UA) et les données personnelles relatives au titulaire du module de sécurité (10).
4. Procédé selon la revendication 1, caractérisé en ce qu'au moins lors de la première connexion, on vérifie que le certificat d'authentification anonyme (CAA) donne droit d'accéder à la base de données (17) du centre de gestion (18).
5. Procédé selon la revendication 1, caractérisé en ce que le certificat d'authentification personnalisé (CAP) est remplacé après une certaine durée d'utilisation.
6. Module de sécurité tel que notamment carte à puce ou support analogue contenant une puce, comportant un numéro d'identification unique, caractérisé en ce qu'il comporte en outre un certificat d'authentification anonyme (CAA) ne contenant pas de données définies par l'identité du titulaire de la puce.
7. Module de sécurité selon la revendication 6, caractérisé en ce qu'il est utilisé pour établir une communication sécurisée avec un serveur distant, en utilisant le procédé selon l'une quelconque des revendications 1 à 5

