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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
2 mars 2006 (02.03.2006)

(10) Numéro de publication internationale
WO 2006/021661 A2

(51) Classification internationale des brevets[7] : H04L 9/28, G06F 17/60

(21) Numéro de la demande internationale : PCT/FR2005/002034

(22) Date de dépôt international : 5 août 2005 (05.08.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0408797 10 août 2004 (10.08.2004) FR

(71) Déposant et
(72) Inventeur : LELEU, Jean-Luc [FR/FR]; 8, place de la porte de Champerret, F-75017 Paris (FR).

(74) Mandataires : PICHAT, Thierry etc.; Novagraaf Technologies, 122, rue Edouard Vaillant, F-92593 Levallois Perret Cedex (FR).

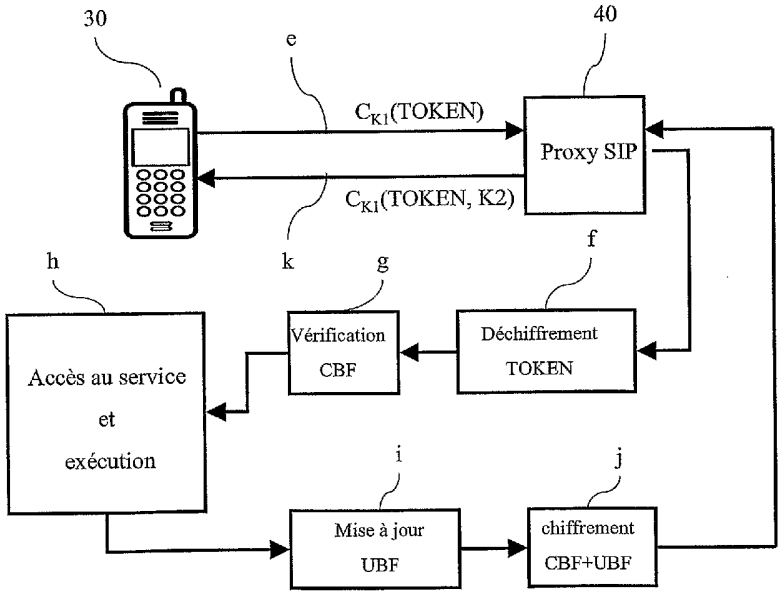
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK,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

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) Title: SECURED AUTHENTICATION METHOD FOR PROVIDING SERVICES ON A DATA TRANSMISSION NETWORK

(54) Titre : PROCEDE D'AUTHENTIFICATION SECURISEE POUR LA MISE EN ŒUVRE DE SERVICES SUR UN RESEAU DE TRANSMISSION DE DONNEES



F TOKEN DECIPHERING
G CBF VERIFICATION
H ACCESS TO A SERVICE AND PERFORMANCE
I UFB UPDATING
J CBF+UFB CIPHERING

(57) Abstract: The invention relates to a method for accessing to a network service by means of a user's terminal (30) involving an application phase which consists in generating a container (TOKEN) containing a first authentication data set (XO, Xl, X2, X3) for accessing to a service and a second useful data set related to access rights for said service (RBF, UBF, TBF), in securely transmitting (d) said container to said terminal and an access phase which consists in securely transmitting (e) the container from said terminal to a managing server (40) which is connected to the network while an access request, after deciphering (f) data of said container, in verifying (g) the validity of the first data set by the server and, following the successful verification, in authorising (h) the access to the service for performing it according to said access rights.

[Suite sur la page suivante]

WO 2006/021661 A2

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

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

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.

(57) Abrégé : L'invention concerne un procédé d'accès à un service sur un réseau, par un terminal utilisateur (30) , comprenant une phase de souscription où : un container (TOKEN) est généré, comprenant un premier ensemble de données d'authentification (XO, Xl, X2 , X3) de l'accès au service et un second ensemble de données utiles relatives à des droits d'accès audit service (RBF, UBF, TBF) , lesdits premier et second ensembles de données étant chiffrés ; ledit container est transmis (d) de façon sécurisée sur ledit terminal ; et une phase d'accès où : ledit container est transmis (e) de façon sécurisée dudit terminal vers un serveur de gestion (40) connecté au réseau lors d'une requête d'accès ; le serveur vérifie (g), après déchiffrement (f) des données dudit container, la validité dudit premier ensemble de données et, en cas de succès de la vérification, autorise (h) l'accès au service pour son exécution selon lesdits droits d'accès .

PROCEDE D'AUTHENTIFICATION SECURISEE POUR LA MISE EN ŒUVRE DE SERVICES SUR UN RESEAU DE TRANSMISSION DE DONNEES

La présente invention concerne de manière générale le domaine de l'authentification sur un réseau de transmission de données et concerne, en particulier, un procédé d'accès à un service sur un réseau de transmission de données, par l'intermédiaire d'un terminal utilisateur connecté au réseau.

Au sens de la présente invention, un service peut désigner tout échange d'informations, via un réseau de transmission de données numérique ou de télécommunication soit entre deux ou plusieurs utilisateurs, soit entre un utilisateur et un fournisseur de services.

Les services mis en œuvre sur les réseaux de transmission de données numériques, tels que le réseau Internet, connaissent un développement considérable. En particulier, ceux se rapportant à des services de voix sur IP, où les données constituant la voix numérisée sont donc transportées sous forme de paquets d'information selon le protocole IP, voient leur potentiel de développement encore renforcé par le déploiement des réseaux locaux sans fil, tels que les réseaux utilisant la technologie de transmission sans fil basée sur la norme de réseau radioélectrique 802.11 et ses évolutions, regroupées sous l'appellation Wifi (pour « Wireless Fidelity »).

L'arrivée sur le marché de terminaux mobiles équipés de moyens pour établir une connexion sans fil

avec l'Internet, via un réseau d'accès Wifi par exemple, rend d'autant plus prégnante l'émergence de services de voix sur IP.

Cependant, l'un des freins qui limite actuellement la mise en œuvre de tels services sur ce type de réseau, réside dans la forte exigence de sécurité devant être associée aux transactions mises en oeuvre, en particulier pour l'authentification des utilisateurs abonnés au service et l'intégrité des données.

Les mécanismes de sécurité à employer conduisent à une gestion lourde et complexe des autorisations permettant de donner ou non la permission d'accéder au service, en l'occurrence effectuer un appel dans le cadre d'un service de téléphonie sur IP souscrit auprès d'un l'opérateur.

La présente invention a pour but de proposer un système d'authentification robuste, très souple à mettre en place, et pouvant être implémenté sur des terminaux utilisateurs bon marchés disposant de ressources de calcul limitées, pour l'accès à des services, notamment des services de type voix sur IP, sur un réseau de transmission de données.

Avec cet objectif en vue, l'invention a pour objet un procédé d'accès à un service sur un réseau de transmission de données, par l'intermédiaire d'un terminal utilisateur connecté audit réseau, caractérisée en ce qu'il comprend une phase de souscription audit service où:

- un container d'informations associé à l'utilisateur est généré, comprenant un premier ensemble de données d'authentification de l'accès au

service et un second ensemble de données utiles relatives audit utilisateur et à des droits d'accès audit service, lesdits premier et second ensembles de données étant chiffrés, et où

- ledit container est transmis de façon sécurisée sur ledit terminal utilisateur,

et une phase d'accès audit service où :

- ledit container est transmis de façon sécurisée dudit terminal utilisateur vers au moins un serveur de gestion connecté au réseau lors d'une requête d'accès audit service, et où

- le serveur vérifie, après déchiffrement des données constitutives dudit container, la validité dudit premier ensemble de données d'authentification et, en cas de succès de la vérification, autorise l'accès au service pour son exécution en fonction desdits droits d'accès du second ensemble de données.

De préférence, la phase de souscription au service comprend le paiement dudit service par l'utilisateur auprès d'un serveur de paiement.

Dans un mode de réalisation, la phase de souscription comprend en outre la fourniture d'un mot de passe à usage unique par le serveur de paiement à l'utilisateur, la transmission dudit mot de passe du terminal utilisateur vers le serveur de gestion, déclenchant la transmission sécurisée du container dudit serveur vers ledit terminal.

Avantageusement, après l'exécution du service, une étape de mise à jour des données utiles du container relatives aux droits d'accès au service est mise en

œuvre côté serveur, lesdites données mises à jour étant sauvegardées côté serveur de gestion.

Selon une caractéristique, suite à la mise à jour, les premier et second ensembles de données du container sont chiffrés côté serveur, puis ledit container mis à jour est transmis de façon sécurisée du serveur de gestion vers le terminal utilisateur pour une phase d'accès au service ultérieure.

De préférence, la transmission sécurisée du container consiste à transmettre sous forme cryptée les données constitutives dudit container par application d'un algorithme de chiffrement symétrique utilisant une clé secrète partagée par le terminal utilisateur et par le serveur.

De préférence, la clé secrète mise en œuvre est renouvelée par période paramétrable.

Selon un mode de réalisation, le renouvellement de la clé secrète consiste à transmettre une nouvelle clé en même temps que le container lors de sa transmission sécurisée du serveur vers le terminal utilisateur pour une phase d'accès au service ultérieure.

De préférence, l'algorithme de chiffrement symétrique mis en œuvre côté terminal et côté serveur est de type RC4.

De préférence, le chiffrement des premier et deuxième ensembles de données constitutives du container avant leur transmission sécurisée est obtenue par application aux dites données d'un algorithme de chiffrement à clé publique, la clé privée correspondante étant mémorisée uniquement côté serveur.

Selon un mode de réalisation, le premier ensemble de données d'authentification est représenté par des collisions de fonction de hashing.

Selon ce mode de réalisation, l'étape de vérification côté serveur consiste à contrôler que les données d'authentification forment effectivement des collisions de fonction de hashing.

Selon un autre mode de réalisation, l'étape de vérification, consiste à vérifier la correspondance des données d'authentification issue du container avec des données d'authentification référencées dans une base de données utilisateurs pour cet utilisateur.

De préférence, un élément de facturation du coût du service est généré au niveau du serveur après exécution dudit service, à partir des données utiles du container relatives aux droits d'accès au service pour l'utilisateur, les données d'authentification étant associées audit élément de facturation généré en tant que preuve que l'accès audit service a été autorisé.

Avantageusement, l'élément de facturation est mémorisé en vue d'être utilisé pour compensation financière ultérieure.

Selon un mode de réalisation, le service accédé est un service de voix sur IP.

Avantageusement, la transmission du container du terminal utilisateur vers le serveur ou du serveur vers le terminal utilisateur pour l'accès au service, est intégrée dans un protocole permettant des transmissions de voix sur IP, par exemple le protocole SIP.

Selon une variante, la transmission du container du terminal utilisateur vers le serveur de gestion lors

d'une phase d'accès à un service est réalisée par l'intermédiaire d'une passerelle intermédiaire du réseau, ladite passerelle mettant en œuvre une étape de vérification préliminaire de la validité du container avant de router celui-ci vers ledit serveur.

Selon cette variante, l'étape de vérification préliminaire de la validité du container consiste à vérifier la validité d'un troisième ensemble de données d'authentification dudit container.

L'invention concerne encore un serveur connecté à un réseau de transmission de données, pour l'accès à un service par l'intermédiaire d'un terminal utilisateur connecté audit réseau, caractérisé en ce qu'il comprend des moyens de mise en œuvre des étapes du procédé telles qu'elles viennent d'être décrites.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante donnée à titre d'exemple illustratif et non limitatif et faite en référence aux figures annexées dans lesquelles :

-la figure 1 illustre schématiquement un exemple d'architecture de réseau dans laquelle peut être décrite l'invention ;

-la figure 2 illustre, selon un exemple de réalisation préféré, les étapes mises en œuvre lors de l'enregistrement d'un utilisateur auprès d'un service sur un réseau de transmission de données ;

-la figure 3 illustre un modèle possible pour la structure d'un container sécurisé portant les informations nécessaires à l'accès et l'exécution du service sur le réseau ;

-la figure 4 illustre des étapes d'obtention du container sécurisé par le terminal suite à la souscription au service pour l'accès à celui-ci ;

-la figure 5 est un schéma fonctionnel illustrant une suite d'étapes mises en œuvre côté serveur lors de l'accès au service.

L'invention concerne donc un procédé d'accès à un service sur un réseau de transmission de données. L'accès au service est effectué de préférence par l'intermédiaire d'un terminal utilisateur 30 connecté à un réseau d'accès RA couplé par une passerelle PA au réseau de transmission de données, typiquement le réseau Internet et de manière générale avec ses couplages vers d'autres réseaux autonomes, tels que le réseau téléphonique commuté public RTCP.

Le réseau d'accès peut être soit un réseau local sans fil, par exemple un réseau Wifi, un réseau public ou privé fonctionnant avec le protocole IP ou avec un autre protocole que IP, un réseau téléphonique commuté public ou privé.

En référence à la figure 2, sont illustrées les étapes permettant à un utilisateur 10 de souscrire à un service sur le réseau de transmission de données. Par exemple, le service souscrit par l'utilisateur peut être un service de téléphonie sur IP, de visiophonie ou encore un service de téléchargement de fichiers numériques, par exemple des fichiers musicaux de type MP3. D'autres types de services multimédia sur le réseau de transmission de données peuvent encore être envisagés et proposés à l'utilisateur, lequel, pour pouvoir y accéder doit préalablement y souscrire.

La figure 2 illustre précisément cette phase de souscription de l'utilisateur au service, qui est plus particulièrement matérialisée par un acte de paiement (a) de la part de l'utilisateur auprès d'un serveur de paiement 20. Pour souscrire ainsi au service souhaité, l'utilisateur peut de préférence effectuer la transaction par l'intermédiaire de sa carte de crédit sur un site Web prévu à cet effet.

L'utilisateur obtient en retour (b) un numéro d'activation du service souscrit. Ce numéro d'activation comprend un mot de passe à usage unique OTP, ainsi qu'une clé secrète K_0, dont l'usage sera explicité plus loin.

La transaction entre l'utilisateur et le serveur de paiement est de préférence mise en œuvre selon un protocole permettant la transmission sécurisée d'informations, tel que le protocole SSL par exemple.

Toutefois, il convient de noter que le numéro d'activation pourrait être transmis à l'utilisateur par tout autre moyen adéquat, par exemple par courrier, par un appel à un système de réponse vocal interactif ou encore par l'intermédiaire d'une carte à gratter.

Considérons maintenant la notion de container sécurisé introduite ici dans le contexte de la présente invention. Un container sécurisé est une valeur numérique chiffrée représentative d'informations variées associées à un utilisateur abonné à un service et, notamment, aux droits d'accès à ce service. Il permet à ces informations de transiter entre différents nœuds du réseau d'une manière sécurisée sans qu'il y ait nécessité de prévoir la mise en œuvre d'un canal

chiffré. Le container permet en outre à son propriétaire, en l'occurrence un terminal utilisateur, d'être autorisé à accéder à un service sur le réseau en fonction des droits d'accès à ce service tels qu'ils ont été définis lors de la souscription au service et qui sont stockés sous forme numérique dans le container sécurisé.

La figure 3 illustre un exemple de structure d'un container sécurisé TOKEN, qui est généré sur un serveur de gestion du réseau lors de la phase de souscription au service par l'utilisateur. Il comprend un premier ensemble de données CBF formant le cœur du container, comprenant essentiellement des données d'authentification de l'accès au service X0, X1, X2 et X3, qui forment la preuve que l'accès au service peut être autorisé pour son exécution. Selon un principe de l'invention, la valeur et la provenance de ce premier ensemble de données d'authentification doivent être authentifiables et vérifiables facilement par l'entité autorisant l'accès et ce, de façon sûre.

Un champ TPID peut ainsi être inséré dans ce premier ensemble de données, représentatif de l'entité productrice du container.

Egalement, selon un mode de réalisation de l'invention, les données d'authentification de l'accès au service, notées X0, X1, X2 et X3 dans l'exemple de la figure 3, sont fabriquées selon une méthode décrite dans l'article intitulé « PayWord and Micromint - Two Simple Micropayment Schemes » par R.L. RIVEST et A. SHAMIR et présenté le 26 janvier 1996 lors de la conférence RSA de 1996. Cet article décrit un système

de fabrication de pièces de monnaie électroniques, représentées par des chaînes de bits dont la validité peut être vérifiée par n'importe qui, mais qui sont très difficiles à produire. Dans ce système, les pièces sont représentées par des collisions de fonction de hashing.

Ainsi, en reprenant ce principe, les données d'authentification de l'accès au service contenues dans le container sont elles-même représentées par des chaînes de bits obtenues par des collisions de fonction de hashing h, et il est possible de vérifier très facilement la validité de ces données en contrôlant que : $h(X0) = h(X1) = h(X2) = h(X3)$.

Le container comprend également un second ensemble de données utiles PBF, comprenant des données relatives à l'utilisateur du service et à des droits d'accès à ce service qui ont été définis au moment de la souscription au service par l'utilisateur.

Ainsi, si l'on prend l'exemple d'un service souscrit de téléphonie sur IP, un champ RBF du container comprend des données définissant les conditions d'accès au services, par exemple indiquant si l'utilisateur peut passer des appels locaux et/ou nationaux et/ou internationaux. Un champ UBF comprend des données de valeur associées au service permettant d'établir une facturation, par exemple un nombre d'unités représentative du montant du paiement acquitté par l'utilisateur lors de sa souscription au service. Un champ TCBF comprend des données temporelles, par exemple des données représentatives d'un temps de communication. D'autres informations critiques

pourraient encore être insérées dans le second ensemble de données utiles PBF, telles que par exemple une date d'expiration de la validité du container.

Le second ensemble de données utiles peut également comprendre un champ SID/PN comprenant des données relatives à l'utilisateur, telles qu'un numéro d'identifiant d'abonné et/ou son numéro de téléphone.

Il convient de noter que la définition des champs du container se rapportant aux données utiles du container permettant d'utiliser le service pour lequel le container a été créé, ne confère aucun caractère restrictif pour la présente invention.

Le premier ensemble de données d'authentification fournit donc des fonctions de sécurité et d'intégrité du second ensemble de données utiles et peut être assimilé à une clé unique non forgeable permettant d'authentifier l'accès à un service donné.

Le container peut ainsi garantir par l'intermédiaire d'une vérification du premier ensemble de données d'authentification que l'accès à un service donné peut être autorisé, en fonction de droits d'accès définis dans le container, et que celui-ci a déjà été payé ou que l'utilisateur peut être facturé pour ce service.

Une fois le premier ensemble de données CBF et le second ensemble de données PBF du container générés, ces premier et second ensembles de données sont chiffrés par application d'un algorithme de chiffrement à clé publique E_{PK}, par exemple un algorithme de type RSA. On obtient de cette manière le container sécurisé TOKEN.

Ce container ainsi sécurisé est prévu pour être stocké côté terminal utilisateur, afin de permettre la mise en oeuvre, à partir de ce terminal, d'une phase d'accès au service, qui sera mise en œuvre au niveau d'une passerelle PA du réseau de transmission de données, typiquement le serveur de gestion. La clé privée correspondante à la clé publique mise en œuvre dans le cadre de l'algorithme RSA pour le chiffrement des données constitutives du container étant mémorisée uniquement côté serveur.

De cette manière, les champs du container ne peuvent être modifiés que côté serveur de gestion et le terminal utilisateur ne pourra pas avoir accès aux données constitutives du container en clair.

Le réseau de transmission de données doit comprendre, au niveau de chaque serveur de gestion intervenant dans une phase d'accès au service par le terminal utilisateur, un système de traitement de données programmé de manière à réaliser les différentes étapes du procédé de l'invention. Ce système de traitement de données peut être individualisé en tant que système séparé du système informatique gérant le serveur, ou être intégré au système informatique par l'adjonction de logiciels intégrés.

Ainsi, pour pouvoir mettre en œuvre une phase d'accès au service, le container sécurisé doit d'abord être stocké côté terminal utilisateur. Cette étape est décrite en référence à la figure 4 illustrant un échange sécurisé du container TOKEN, entre un terminal utilisateur 30 et un serveur de gestion 40 du réseau de transmission de données, lequel est prévu pour assurer

la distribution des containers sur les terminaux, la vérification de ces containers et leur validation pour autoriser l'accès à un service donné et son exécution. La mise en œuvre de ces étapes sera décrite plus en détail par la suite.

Toujours selon l'exemple où le service souscrit par l'utilisateur est un service de téléphonie sur IP, le serveur 40 est un serveur placé dans le réseau devant une infrastructure de voix sur IP VoIP et qui transmettra tous les paquets de signalisation de l'appel vers le prochain dispositif VoIP de cette infrastructure, une fois que l'information d'un container TOKEN reçu d'un terminal ou, selon une variante, d'un autre nœud du réseau, dans le cadre d'une requête d'accès au service VoIP aura été récupérée et vérifiée, comme expliqué plus loin. Le serveur 40 est par exemple un serveur de type proxy SIP (« Session Initiation Protocol »).

Ainsi, selon la variante introduite ci-dessus, le container et son utilisation dans un réseau de transmission de données comme décrit dans la présente description pour authentifier l'accès à un service donné, peuvent également être mis en œuvre dans le cadre d'un protocole de communication entre deux nœuds du réseau intervenant dans l'accès au service, par exemple entre deux serveurs de type proxy SIP.

Préalablement à la phase d'accès au service par l'intermédiaire du terminal utilisateur 30, une étape c de transmission du mot de passe OPT du terminal utilisateur 30 vers le serveur de gestion 40 est mise en oeuvre, déclenchant la transmission sécurisée à

l'étape d, du container TOKEN, lui-même déjà sécurisé par le chiffrement lourd de type RSA, du serveur 40 vers le terminal 30.

Avantageusement, la transmission sécurisée du container TOKEN sur le réseau est assurée par l'application d'un algorithme de chiffrement symétrique C_{K0}, par exemple de type RC4, avec la clé secrète K_0, fournie préalablement à l'utilisateur et partagée par le serveur de gestion.

Deux types de chiffrement sont donc appliqués sur le container. D'une part, le premier ensemble de données du container CBF est lié de façon sécurisé au second ensemble de données PBF par un chiffrement lourd de type RSA, géré côté serveur. D'autre part, le container bénéficie d'un second niveau de chiffrement, plus léger, de type RC4 pour sa transmission sécurisée à travers le réseau. Comme il apparaîtra plus loin, ce dernier type de chiffrement est prévu pour être mis en œuvre à la fois côté serveur et côté terminal, de sorte à assurer des propriétés anti-rejeu au container sécurisé.

Les clés secrètes utilisés dans les transmissions sécurisées du container sur le réseau sont changées très souvent de manière à renforcer davantage la sécurité compte-tenu de l'algorithme de chiffrement léger employé.

Les clés secrètes mises en œuvre sont donc renouvelées par période paramétrable. Ainsi, le renouvellement de la clé secrète K_0 est réalisée en transmettant une nouvelle clé K1 en même temps que le container TOKEN lors de sa transmission sécurisée du

serveur 40 vers le terminal utilisateur 30. Le serveur 40 envoie donc C_{K0}(TOKEN, K1) à destination du terminal 30.

A la réception, le terminal 30 déchiffre la valeur reçue à l'aide de la clé secrète K_0 dont il dispose déjà, et récupère ainsi la valeur de container TOKEN, toujours chiffrée RSA, et la clé secrète K1.

En référence à la figure 5, pour mettre en œuvre une phase d'accès au service souscrit, une requête d'accès au service envoyée par le terminal 30, consiste à transmettre en (e) le container de façon sécurisé C_{K1}(TOKEN) vers le serveur 40, par application côté terminal de l'algorithme RC4 avec la clé secrète K1 sur le container.

Compte-tenu du schéma de chiffrement léger, type RC4 choisi pour la transmission sécurisé du container, les étapes du procédé peuvent avantageusement être mises en œuvre sur des terminaux utilisateurs disposant de peu de ressources CPU disponibles. En outre, les opérations lourdes de sécurité du container étant gérées principalement côté serveur de gestion, notamment le chiffrement RSA des données constitutives du container, l'implémentation côté client sur le terminal utilisateur ne requiert qu'une application simple pouvant assurer un stockage sécurisé du container sur le terminal et la mise en œuvre du chiffrement RC4, servant à la transmission sécurisée du container.

A la réception du container chiffré RC4 C_{K1}(TOKEN) côté serveur de gestion 40, la série d'étapes f à k est mise en œuvre.

A l'étape f, le serveur réalise une opération de déchiffrement des données reçues du terminal. Il déchiffre tout d'abord C_{K1}(TOKEN) avec la clé secrète K1 de manière à récupérer le container TOKEN, dont les données sont chiffrées avec RSA. Puis dans un second temps, il récupère le premier ensemble de données d'authentification CBF et le second ensemble de données utiles UBF du container par l'opération de déchiffrement RSA avec la clé privée correspondante dont il est le seul à disposer.

Une fois les données en clair du container récupérées, une étape de vérification de la validité du premier ensemble de données d'authentification X0, X1, X2, X3 est mise en œuvre. Cette étape peut simplement consister à contrôler que les données d'authentification X0, X1, X2, X3 forment effectivement des collisions de fonction de hashing.

En cas de succès de la vérification, le serveur 40 autorise l'accès au service pour son exécution en fonction des droits d'accès à ce service référencés dans le second ensemble de données utiles du container. Par exemple, le service accédé peut être un appel SIP vers un numéro international, autorisé en vertu des valeurs RBF/UBF/TCBF, les paquets de signalisation de cet appel étant alors transmis par le serveur vers l'infrastructure VoIP.

Les propriétés du container mis en œuvre apporte ainsi une grande souplesse dans la gestion d'accès au service de téléphonie sur IP. Notamment en ce qui concerne la problématique de « roaming ». Grâce au container, on n'est pas obligé de remonter vers une

base de donnée centralisée pour identifier l'utilisateur. Les droits d'accès de l'utilisateur pour accéder au service peuvent en effet être vérifiés directement à partir du container sans avoir à remonter vers un compte utilisateur définissant ces droits.

Lors de l'étape g, le serveur 40 peut toutefois faire appel à une base de données utilisateur. La vérification peut ainsi consister à vérifier la correspondance des données d'authentification de la transaction issue du container avec des données d'authentification référencées dans une base de données utilisateurs pour cet utilisateur. Les données d'authentification de l'accès au service peuvent en effet être constituées dans une variante par une empreinte digitale numérisée de l'utilisateur, présentant les mêmes garanties de sécurité que l'utilisation des collisions de fonction de hashing.

Le serveur peut également vérifier dans la base de données utilisateur que les données utiles RBF, UBF et TCBF issues du container correspondent effectivement aux données utiles courantes pour l'accès au service mémorisées pour cet utilisateur dans la base.

Après l'exécution du service, une étape i de mise à jour des données utiles du container relatives aux droits d'accès au service, est mise en œuvre, en particulier, une étape de mise à jour des données RBF, UBF et TCBF. Par exemple, si une durée prépayée de 500 minutes avait été souscrite par l'utilisateur, à la fin d'une session d'appel de 7 minutes, la valeur initiale 500 du champ TCBF des données utiles du container est diminuée de 7. Les données utiles mises à jour sont

alors sauvegardées côté serveur de gestion dans la base de données utilisateur.

Au cours de cette étape, un élément de facturation du coût du service peut éventuellement être généré et stocké au niveau du serveur 40, dont le contenu est déterminé à partir des données utiles du container relatives aux droits d'accès au service pour l'utilisateur. Par exemple, pour chaque accès au service VoIP, les variations des données TCBF, donnant le temps de communication, et UBF pour le coût d'une unité de communication, peuvent être mémorisées pour former l'élément de facturation. Les données d'authentification sont également associées à l'élément de facturation généré en tant que preuve que l'accès au service a bien été autorisé. L'élément de facturation ainsi mémorisé côté serveur 40 peut alors être utilisé ultérieurement auprès d'un organisme tiers afin d'obtenir une compensation financière sur la base des données accumulées.

Suite à l'étape de mise à jour des donnée utiles du container, une étape de chiffrement RSA du premier ensemble de données d'authentification CBF et du second ensemble de données utiles PBF avec les données mises à jour, est mise en œuvre. On obtient de cette manière le container sécurisé mis à jour.

Enfin, le container sécurisé mis à jour est transmis à l'étape k de manière sécurisé vers le terminal utilisateur 30 pour une phase d'accès au service ultérieure, la transmission sécurisé étant assurée comme expliqué précédemment par l'application de l'algorithme RC4 avec K1. Eventuellement, le

renouvellement de la clé secrète K1 est réalisée lors de cette étape, en transmettant une nouvelle clé K2 qui servira lors de la phase d'accès au service ultérieur. La nouvelle clé secrète K2 est transmise en même temps que le container mis à jour TOKEN, lors de la transmission sécurisée du serveur 40 vers le terminal utilisateur 30. Le serveur 40 envoie donc C_{K1}(TOKEN, K2) à destination du terminal 30.

La transmission sécurisée du container TOKEN, dont les données sont déjà chiffrées, du terminal utilisateur 30 vers le serveur de gestion 40, ou du serveur vers le terminal utilisateur, ou encore entre deux serveurs du réseau, pour la mise en œuvre de l'accès au service et son exécution, est prévue pour être intégrée dans un protocole permettant des transmissions de voix sur IP, par exemple le protocole SIP, selon l'exemple de réalisation décrit en référence à un service VoIP souscrit. Afin d'insérer le container dans un paquet de données selon le protocole choisi, il est nécessaire de définir une en-tête afin de permettre le traitement adéquat selon l'invention des paquets porteurs de containers. Cette en-tête pourra par exemple être constituée de plusieurs champs tels que la taille des données, un numéro de contrôle, un identifiant de session ou d'autres informations de contrôle.

Selon une variante, le container d'informations TOKEN peut comprendre un troisième ensemble de données d'authentification, dont le rôle va être décrit ci-après.

Ainsi, selon cette variante, une passerelle intermédiaire du réseau est mise en œuvre pour réaliser la transmission du container du terminal utilisateur vers le serveur de gestion lors d'une phase d'accès à un service sur le réseau. La passerelle intermédiaire est alors prévue pour réaliser une vérification préliminaire de la validité du container avant de router celui-ci vers le serveur de gestion, consistant à vérifier la validité du troisième ensemble de données d'authentification du container.

Le troisième ensemble de données d'authentification peut être représentées par des chaînes de bits obtenues par des collisions de fonction de hashing, de la même façon que pour le premier ensemble de données du container.

Le troisième ensemble de données du container peut également être chiffré en utilisant un algorithme de chiffrement à clés symétriques, type RC4.

REVENDICATIONS

1. Procédé d'accès à un service sur un réseau de transmission de données, par l'intermédiaire d'un terminal utilisateur (30) connecté audit réseau, caractérisée en ce qu'il comprend une phase de souscription audit service où:

- un container d'informations (TOKEN) associé à l'utilisateur est généré, comprenant un premier ensemble de données d'authentification (X0, X1, X2, X3) de l'accès au service et un second ensemble de données utiles relatives audit utilisateur (SID/PN) et à des droits d'accès audit service (RBF, UBF, TBF), lesdits premier et second ensembles de données étant chiffrés, et où

- ledit container est transmis (d) de façon sécurisée sur ledit terminal utilisateur (30),

et une phase d'accès audit service où :

- ledit container est transmis (e) de façon sécurisée dudit terminal utilisateur (30) vers au moins un serveur de gestion (40) connecté au réseau lors d'une requête d'accès audit service, et où

- le serveur (40) vérifie (g), après déchiffrement (f) des données constitutives dudit container, la validité dudit premier ensemble de données d'authentification et, en cas de succès de la vérification, autorise (h) l'accès au service pour son exécution en fonction desdits droits d'accès du second ensemble de données.

2. Procédé selon la revendication 1, caractérisé en ce que la phase de souscription au service comprend le paiement (a) dudit service par l'utilisateur (10) auprès d'un serveur de paiement (20).

3. Procédé selon la revendication 2, caractérisé en ce que la phase de souscription comprend en outre la fourniture (b) d'un mot de passe à usage unique (OTP) par le serveur de paiement (20) à l'utilisateur (10), la transmission (c) dudit mot de passe du terminal utilisateur (30) vers le serveur (40) de gestion, déclenchant la transmission sécurisée (d) du container (TOKEN) dudit serveur (40) vers ledit terminal (30).

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que, après l'exécution du service, une étape de mise à jour (i) des données utiles du container (TOKEN) relatives aux droits d'accès au service est mise en œuvre côté serveur (40), lesdites données mises à jour étant sauvegardées côté serveur de gestion (40).

5. Procédé selon la revendication 4, caractérisé en ce que, suite à la mise à jour, les premier et second ensembles de données du container sont chiffrés (j) côté serveur (40), puis ledit container mis à jour est transmis (k) de façon sécurisée du serveur de gestion(40) vers le terminal utilisateur (30) pour une phase d'accès au service ultérieure.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la transmission sécurisée (d) du container consiste à transmettre sous forme cryptée les données constitutives dudit container par application d'un algorithme de chiffrement symétrique utilisant une clé secrète (K_0, K1, K2) partagée par le terminal utilisateur (30) et par le serveur (40).

7. Procédé selon la revendication 6, caractérisé en ce que la clé secrète mise en œuvre est renouvelée par période paramétrable.

8. Procédé selon les revendications 5 et 7, caractérisé en ce que le renouvellement de la clé secrète consiste à transmettre une nouvelle clé en même temps que le container lors de sa transmission sécurisée du serveur (40) vers le terminal utilisateur (30) pour une phase d'accès au service ultérieure.

9. Procédé selon l'une quelconque des revendication 6 à 8, caractérisé en ce que l'algorithme de chiffrement symétrique mis en œuvre côté terminal (30) et côté serveur (40) est de type RC4.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le chiffrement des données constitutives du container avant leur transmission sécurisée est obtenue par application aux dites données d'un algorithme de chiffrement à clé publique, la clé privée

correspondante étant mémorisée uniquement côté serveur (40).

11. Procédé selon la revendication 10, caractérisé en ce que l'algorithme de chiffrement est un algorithme de type RSA.

12. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le premier ensemble de données d'authentification (X0, X1, X2, X3) est représenté par des collisions de fonction de hashing.

13. Procédé selon la revendication 12, caractérisé en ce que l'étape de vérification côté serveur (40) consiste à contrôler que les données d'authentification (X0, X1, X2, X3) forment effectivement des collisions de fonction de hashing.

14. Procédé selon l'une quelconque des revendications 1 à 11, caractérisé en ce que l'étape de vérification, consiste à vérifier la correspondance des données d'authentification (X0, X1, X2, X3) issue du container avec des données d'authentification référencées dans une base de données utilisateurs pour cet utilisateur.

15. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que un élément de facturation du coût du service est généré au niveau du serveur (40) après exécution dudit service, à

partir des données utiles du container relatives aux droits d'accès au service pour l'utilisateur, les données d'authentification étant associées audit élément de facturation généré en tant que preuve que l'accès audit service a été autorisé.

16. Procédé selon la revendication 15, caractérisé en ce que l'élément de facturation est mémorisé en vue d'être utilisé pour compensation financière ultérieure.

17. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le service accédé est un service de voix sur IP.

18. Procédé selon la revendication 17, caractérisé en ce que la transmission du container du terminal (30) utilisateur vers le serveur (40) ou du serveur vers le terminal utilisateur pour l'accès au service, est intégrée dans un protocole permettant des transmissions de voix sur IP.

19. Procédé selon la revendication 18, caractérisé en ce que le protocole est un protocole SIP.

20. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la transmission du container (TOKEN) du terminal (30) utilisateur vers le serveur de gestion (40) est réalisée par l'intermédiaire d'une passerelle intermédiaire du réseau, ladite passerelle mettant en œuvre une étape de vérification préliminaire de la

validité du container avant de router celui-ci vers ledit serveur.

21. procédé selon la revendication 20, caractérisé en ce que l'étape de vérification préliminaire de la validité du container (TOKEN) consiste à vérifier la validité d'un troisième ensemble de données d'authentification dudit container.

22. Serveur (40) connecté à un réseau de transmission de données, pour l'accès à un service par l'intermédiaire d'un terminal utilisateur (30) connecté audit réseau, caractérisé en ce qu'il comprend des moyens de mise en œuvre des étapes du procédé selon l'une quelconque des revendications 1 à 21.

23. Serveur selon la revendication 22, caractérisé en ce qu'il est de type proxy SIP.

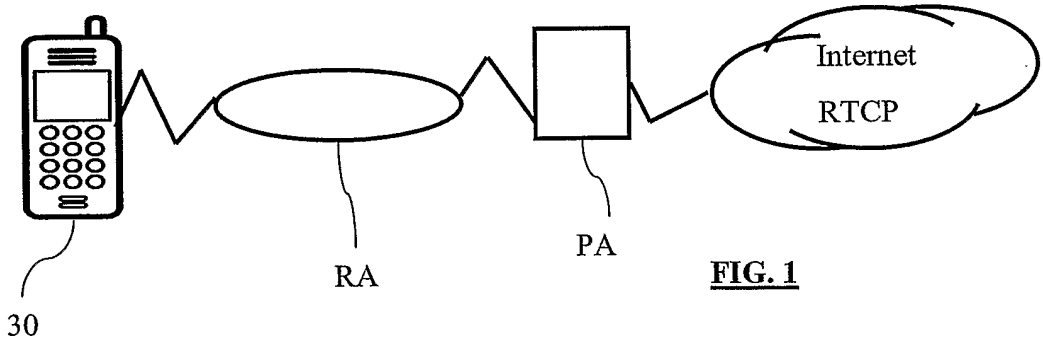


FIG. 1

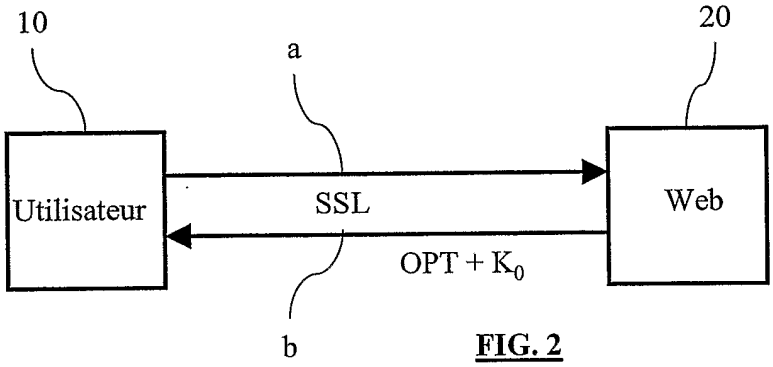


FIG. 2

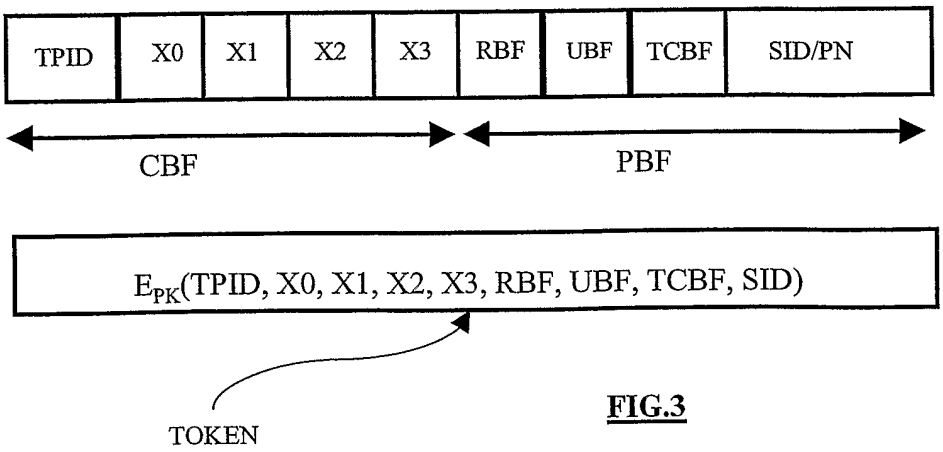


FIG.3

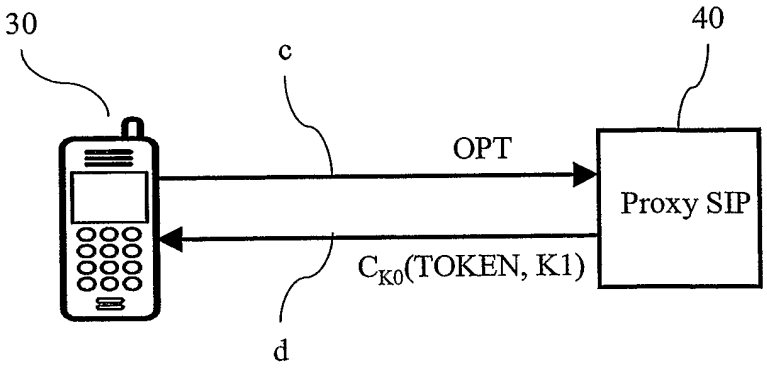

30
40
c
OPT
Proxy SIP
C_{K0}(TOKEN, K1)
d

FIG. 4

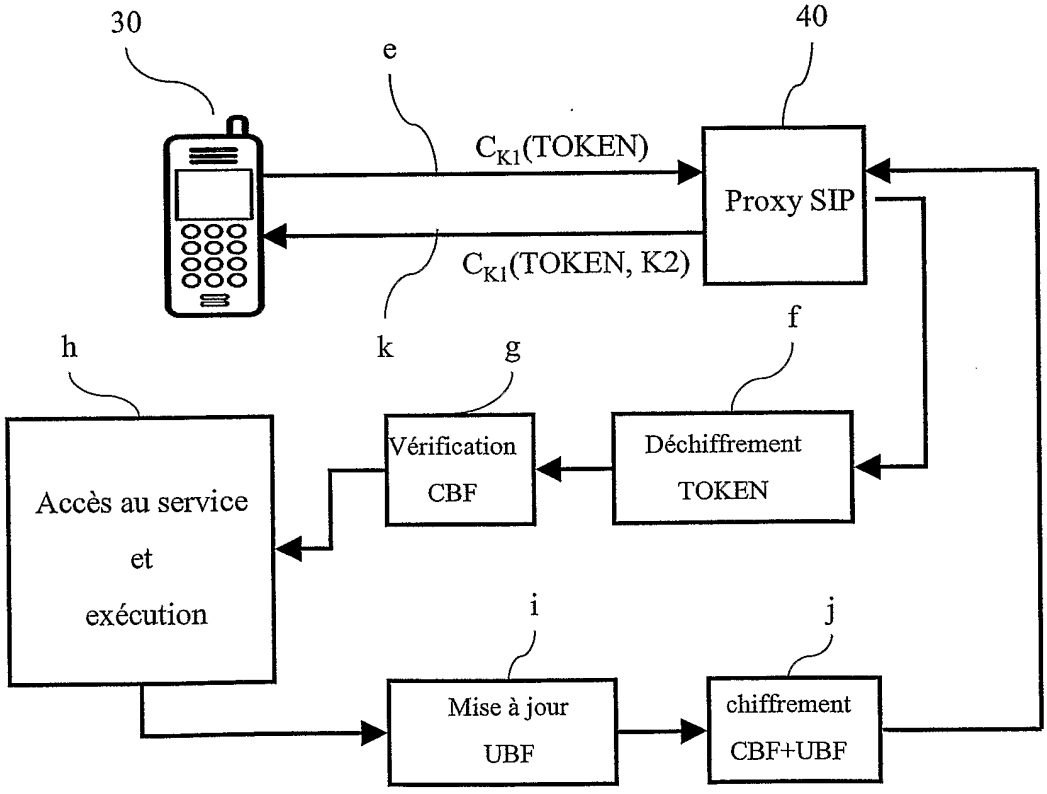

30
40
e
C_{K1}(TOKEN)
Proxy SIP
C_{K1}(TOKEN, K2)
k
g
f
h
Vérification CBF
Déchiffrement TOKEN
Accès au service et exécution
i
j
Mise à jour UBF
chiffrement CBF+UBF

FIG. 5