



(43) Date de la publication internationale
6 septembre 2013 (06.09.2013)

WIPO | PCT

(10) Numéro de publication internationale
WO 2013/128091 A1

- (51) Classification internationale des brevets :
H04L 9/32 (2006.01)
- (21) Numéro de la demande internationale :
PCT/FR2013/050197
- (22) Date de dépôt international :
31 janvier 2013 (31.01.2013)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
12 51753 27 février 2012 (27.02.2012) FR
- (71) Déposant : MORPHO [FR/FR]; 11, boulevard Gallieni,
F-92130 Issy-les-Moulineaux (FR).
- (72) Inventeurs : BERTEAU, Guillaume; c/o Morpho, 11,
boulevard Gallieni, F-92130 Issy-les-Moulineaux (FR).
BENTEO, Bruno; c/o Morpho, 11, boulevard Gallieni, F-
92130 Issy-les-Moulineaux (FR).
- (74) Mandataires : LOISEL, Bertrand et al.; Cabinet Plasse-
raud, 52, rue de la Victoire, F-75440 Paris Cedex 09 (FR).
- (81) États désignés (sauf indication contraire, pour tout titre
de protection nationale disponible) : AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ,
TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ,
TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : METHOD FOR VERIFYING THE IDENTITY OF A USER OF A COMMUNICATING TERMINAL AND ASSOCIATED SYSTEM

(54) Titre : PROCÉDE DE VERIFICATION D'IDENTITE D'UN UTILISATEUR D'UN TERMINAL COMMUNIQUE ET SYSTEME ASSOCIE

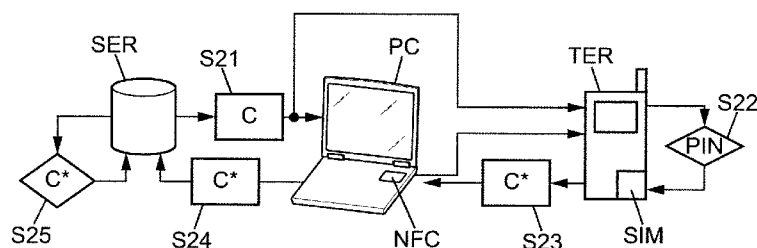


FIG. 2

(57) Abstract : The invention relates to a method for verifying the identity of a user of a communicating terminal (TER), comprising: * a prior step comprising: - communicating a first piece of identity data of a user to at least one server (SER), - generating a second piece of identity data of the user from the server, the second piece of data defining a derived identity of the user, and - storing the second piece of identity data in a secure memory of the terminal, * a current step for identity verification comprising: - transmitting a token (C) for encryption from the server to the terminal, - using the second piece of data at the terminal at least to generate an encryption of the token, the encrypted token (C*) being transmitted to the server and verified by the server, and in case of positive verification of the encrypted token by the server, the server validates the identity verification of the user of the terminal.

(57) Abrégé : L'invention concerne un procédé de vérification d'identité d'un utilisateur d'un terminal communicant (TER), comportant : * une étape préalable comprenant : - une communication à au moins un serveur (SER) d'une première

[Suite sur la page suivante]



donnée d'identité de l'utilisateur, - une génération auprès du serveur d'une deuxième donnée d'identité de l'utilisateur, la deuxième donnée définissant une identité dérivée de l'utilisateur, et - un stockage de la deuxième donnée d'identité dans une mémoire sécurisée du terminal, * une étape courante de vérification d'identité comprenant : - une transmission du serveur au terminal d'un jeton (C) à chiffrer, - une utilisation auprès du terminal de la deuxième donnée au moins pour générer un chiffrement du jeton, le jeton chiffré (C*) étant transmis au serveur et vérifié auprès du serveur, et en cas de vérification positive du jeton chiffré auprès du serveur, le serveur valide la vérification d'identité de l'utilisateur du terminal.

**Procédé de vérification d'identité d'un utilisateur d'un terminal communiquant
et système associé**

5 La présente invention concerne le conditionnement d'accès et/ou la souscription à un service par vérification d'identité d'un utilisateur, à partir d'un terminal communicant (notamment un terminal mobile) de l'utilisateur.

10 La notion d'identité devient omniprésente et quotidienne dans l'environnement dit « mobile ». Cette identité numérique doit être cependant protégée contre toute forme d'usurpation en restant ergonomique dans son utilisation par son porteur.

15 Les solutions connues (à mot de passe unique ou « OTP » pour « One Time Password », ou à signature unique OTS ou SSO (pour Single Sign On), ou par SMS (Short Message Service), ou normalisées « Open ID », ou autres), toutes basées sur des processus de type « login/mot de passe » ou identifiants réseau (numéro de téléphone par exemple) associés à une gestion d'attributs de l'utilisateur, ne sont pas pleinement satisfaisantes.

20 L'invention propose une solution. L'invention propose notamment un procédé de vérification d'identité d'un utilisateur d'un terminal communicant, comportant :

* une étape préalable comprenant :

- une communication à au moins un serveur d'une première donnée d'identité de l'utilisateur,
- une génération auprès du serveur d'une deuxième donnée d'identité de l'utilisateur, la deuxième donnée définissant une identité dérivée de l'utilisateur, et
- un stockage de la deuxième donnée d'identité dans une mémoire sécurisée du terminal,

* une étape courante de vérification d'identité comprenant :

- une transmission du serveur au terminal d'un jeton à chiffrer,
- une utilisation auprès du terminal de la deuxième donnée au moins pour générer un chiffrement du jeton, le jeton chiffré étant transmis au serveur et vérifié auprès du serveur, et

- en cas de vérification positive du jeton chiffré auprès du serveur, le serveur valide la vérification d'identité de l'utilisateur du terminal.

5 Un terminal communicant (téléphone, tablette, smartphone) devient ainsi, s'il est associé à une identité dérivée issue d'un titre authentique, un support connecté facilitant la validation des droits (par authentification forte notamment) et le partage de données de sécurité avec les acteurs locaux ou distants d'une transaction.

10 Selon les modes de réalisation, le procédé de l'invention peut présenter une ou plusieurs des caractéristiques suivantes :

- le chiffrement utilise une infrastructure à clé publique, la donnée d'identité dérivée au moins étant utilisée pour générer une clé de chiffrement ;
- la donnée d'identité dérivée est un certificat numérique certifiant le chiffrement par le terminal ;
- 15 - en cas de vérification positive, le jeton chiffré est lié à un certificat numérique d'identification de l'utilisateur ;
- la communication au serveur de la première donnée d'identité de l'utilisateur est autorisée après vérification d'une donnée biométrique de l'utilisateur du terminal ;
- 20 - l'étape courante comporte une vérification d'une donnée propre à l'utilisateur avant d'initier sur le terminal l'utilisation de la deuxième donnée pour le chiffrement du jeton ;
- on prévoit une pluralité d'étapes préalables avec une pluralité de communications à une pluralité de serveurs de la première donnée d'identité de l'utilisateur, chaque serveur générant des deuxièmes données respectives d'identité de l'utilisateur, chaque deuxième donnée définissant une identité dérivée de l'utilisateur, chaque identité dérivée étant propre à un service dont l'accès est conditionné par une vérification de jeton chiffré auprès d'un serveur dédié audit service ;
- 25 - la communication au serveur de la première donnée d'identité est effectuée via un lecteur comportant un module de communication de courte portée ou filaire, et, le terminal comportant un module homologue de communication de courte portée ou filaire, la deuxième donnée est transmise du serveur au
- 30

lecteur, puis du lecteur au terminal par communication en courte portée ou filaire ;

- 5 - la transmission du jeton à chiffrer et/ou du jeton chiffré, entre le serveur et le terminal, est effectuée via un équipement sollicitant un accès à un service auquel le serveur est associé, l'accès au service étant conditionné par une vérification de l'identité de l'utilisateur à partir du terminal de l'utilisateur à ladite étape courante ;
- 10 - la transmission du jeton à chiffrer et/ou du jeton chiffré, entre le terminal et l'équipement, est effectuée par une communication de courte portée ou filaire, le terminal comportant un module de communication de courte portée ou filaire et l'équipement comportant un module homologue de communication de courte portée ou filaire ;
- 15 - la transmission du jeton à chiffrer du serveur au terminal est effectuée par un réseau mobile, et la transmission du jeton chiffré du terminal au serveur est effectuée via un équipement sollicitant un accès à un service auquel le serveur est associé, l'accès au service étant conditionné par une vérification de l'identité de l'utilisateur à partir du terminal de l'utilisateur à ladite étape courante ;
- 20 - la transmission du jeton à chiffrer du serveur au terminal est effectuée via un équipement sollicitant un accès à un service auquel le serveur est associé, et la transmission du jeton chiffré du terminal au serveur est effectuée par un réseau mobile, l'accès au service étant conditionné par une vérification de l'identité de l'utilisateur à partir du terminal de l'utilisateur à ladite étape courante.
- 25 L'invention concerne aussi un système de vérification d'identité d'un utilisateur, comportant au moins un terminal et un serveur pour la mise en œuvre du procédé selon l'invention.

30 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-après présentant des exemples possibles de réalisation, et à l'examen des dessins annexés sur lesquels :

- la figure 1 illustre les principales opérations mises en œuvre par un système au sens de l'invention, pendant l'étape préalable de déclaration du terminal ; et

- la figure 2 illustre les principales opérations mises en œuvre par un système au sens de la présente invention, pendant une étape courante de vérification d'identité, basée sur le terminal.

5 En référence à la figure 1, un utilisateur présente un support physique tel que, par exemple, une carte nationale d'identité CNI, une carte de fidélité, une carte d'étudiant, ou autre, pour lecture par un lecteur LEC. Pour vérifier que ce support CNI est bien porté par son détenteur (« MR X »), l'utilisateur présente une donnée biométrique, par exemple une empreinte digitale, dans un lecteur BIO relié au lecteur LEC de la carte

10 CNI. Dans un exemple de réalisation possible, le lecteur lit (par exemple par scan) les données de la carte CNI et les communique, avec les données biométriques, par exemple à un serveur distant. Ce serveur distant vérifie une coïncidence entre les données de la carte CNI et les données biométriques relevées (validation du test S13) et le cas échéant le procédé peut se poursuivre. Dans un autre exemple de réalisation

15 possible, les données biométriques peuvent servir à protéger certaines données embarquées sur le support physique ; les données biométriques sont alors transmises au support qui effectue une vérification locale (par exemple via du « Match On Card ») et autorise l'exploitation desdites données protégées.

20 Suite à cette première opération, le lecteur peut communiquer à l'étape S10 une première donnée d'identité de l'utilisateur Id1 vers un serveur distant SER. Cette identité Id1 peut être par exemple une identité régalienne de l'individu, ou encore une identité bancaire (dans le cas où la carte CNI est une carte bancaire), ou autres. La première donnée d'identité Id1 peut également être un certificat numérique transmis

25 au serveur distant SER qui vérifie la validité de ce certificat (chaîne de certification, état de révocation, date de validité, ...).

Dans un mode de réalisation, le serveur distant SER détermine, à partir de la première donnée d'identité Id1, une identité dérivée Id2, à l'étape S11 (par exemple

30 par application d'une fonction de hachage à la donnée Id1), et communique une deuxième donnée de cette identité dérivée Id2 au lecteur LEC dans l'exemple représenté. Dans une forme de réalisation, le lecteur LEC peut comporter des moyens de communication de courte portée (par exemple un module NFC, pour

« Near Field Communication », ou encore une communication Wifi, Bluetooth, ou filaire (par câble USB par exemple)), pour transmettre la deuxième donnée d'identité dérivée Id2 à un terminal communiquant TER du choix de l'utilisateur, à l'étape S12, ce terminal TER étant bien entendu équipé aussi d'un module de communication de courte portée. En variante, l'identité dérivée Id2 peut être transmise directement du serveur SER au terminal TER par un réseau mobile.

Dans un autre mode de réalisation, l'identité dérivée Id2 peut être un certificat numérique. Un élément sécurisé du terminal communiquant TER génère localement une bi-clé (i.e. un couple clé publique – clé privée), la clé privée étant un secret inextractible de l'élément sécurisé du terminal. La clé publique est alors communiquée au serveur distant SER avec une demande de certification de la bi-clé. Le serveur distant SER génère un certificat lié au titre authentique, i.e. lié à la première donnée d'identité de l'utilisateur Id1. Ce certificat est ensuite renvoyé au terminal communiquant TER à côté de la bi-clé.

Plus particulièrement, le terminal TER de l'utilisateur stocke l'identité dérivée Id2 dans une mémoire sécurisée (par exemple dans la carte SIM, pour « Subscriber Identity Module », ou plus généralement dans un module UICC pour « Universal Integrated Circuit Card », ou encore dans un élément de sécurité quelconque du terminal). A cet effet, une application peut être transmise depuis le serveur et via le lecteur LEC, vers le terminal, comme par exemple une « cardlet » qui s'installe sur le terminal TER pour stocker l'identité dérivée Id2, par exemple selon un procédé de type OTA, pour « Over The Air ».

Selon un mode de réalisation, le terminal TER peut générer une clé ou une bi-clé à partir de la donnée de l'identité dérivée Id2, permettant un chiffrement symétrique (ou respectivement asymétrique, pour une cryptographie asymétrique) intervenant ultérieurement dans la vérification de l'identité de l'utilisateur, à partir de son terminal TER, comme on le verra ci-après en référence à la figure 2.

Selon un autre mode de réalisation, lorsque l'identité dérivée Id2 est un certificat numérique comme décrit plus haut, la bi-clé associé au certificat du titre authentique

sera utilisée pour le chiffrement intervenant ultérieurement dans la vérification de l'identité de l'utilisateur à partir de son terminal TER comme décrit en référence à la figure 2.

5 Dans un exemple de réalisation, illustré à la figure 2, un équipement quelconque, par exemple un ordinateur PC, une borne de service automatique ou autre, communique avec une plateforme de service via un réseau de type Internet. Avant de fournir un service sécurisé, le serveur SER associé à ce service doit vérifier l'identité de l'utilisateur. Ainsi, il est fait recours ici à l'étape précitée de vérification de l'identité de l'utilisateur, à partir de son terminal TER. A cet effet, en référence à la figure 2, le serveur SER envoie, à l'étape S21, un jeton C (i.e. un « challenge » qui peut par exemple correspondre à un aléa ou un « hash » d'un document) par exemple à destination de l'équipement PC. Par communication en champ proche NFC (l'équipement PC étant équipé d'un module NFC), le jeton est communiqué au terminal TER, lequel exploite les données stockées en mémoire sécurisée (par exemple dans sa carte SIM) et ses ressources cryptographiques pour signer ce jeton à l'étape S23. Avantageusement, il peut être mis en œuvre auprès du terminal TER une procédure systématique consistant en une vérification d'une donnée propre à l'utilisateur, dès lors qu'il s'agit d'utiliser la ou les clé(s) de chiffrement stockée(s) dans le terminal pour générer une signature. Par exemple, il peut être proposé via une interface homme-machine à l'utilisateur de saisir un code personnel à l'étape S22, ou encore de saisir une donnée biométrique prédéterminée (empreinte digitale, iris, ou autres). Ainsi, en cas de détention frauduleuse du terminal TER par un tiers malveillant, aucune signature ne peut être générée à l'étape S23 et bien entendu aucun service ne pourra être fourni ultérieurement à l'ordinateur PC ou à la borne de service.

Le jeton signé C* est retournée à l'étape S24 au serveur SER, par exemple via l'ordinateur PC par une communication en champ proche, via le module NFC notamment. A l'étape S25, le serveur SER vérifie cette signature à l'aide de sa ou ses propre(s) clé(s) et, bien entendu, à l'aide du jeton C qu'il a lui-même initié. La validité de la signature peut comprendre une vérification standard de validité de certificat (chaîne de certification, état de révocation, date de validité, ...). Par ailleurs,

connaissant le jeton envoyé à l'étape S21, la « réponse » (i.e. le jeton signé par la clé privée du terminal TER) retournée à l'étape S24 ainsi que la clé publique présente dans le certificat, un serveur de validation est capable de contrôler la validité de la signature.

5

On comprendra alors que cette signature correspond à un certificat numérique identifiant l'utilisateur par rapport au service précité.

10 L'étape de vérification de l'identité de l'utilisateur décrite en référence à la figure 2 peut être bi-canal, c'est-à-dire par exemple que le jeton C à signer (« challenge » ou « hash » d'un document) peut-être envoyé par le réseau mobile du serveur SER directement sur le terminal communiquant TER, signé par le terminal communiquant, puis le jeton signé C* est renvoyé au serveur via une interface NFC de l'équipement (ordinateur PC ou borne de service automatique). Il est entendu que la
15 communication bi-canal peut également comprendre une communication du jeton C à signer du serveur SER au terminal communiquant TER via une interface NFC de l'équipement (ordinateur PC ou borne de service automatique) et une communication du jeton signé C* renvoyé directement du terminal TER au serveur SER par le réseau mobile.

20

Dans une réalisation particulière, l'identité dérivée Id2 précitée est calculée par exemple à partir d'une fonction de hachage appliquée à la première donnée d'identité Id1 issue de la lecture de la carte CNI. Ensuite, au moins une clé (ou un couple de clés publique et privée), stockée dans la mémoire sécurisée du terminal TER, peut
25 être calculée à partir de cette identité dérivée Id2 (par exemple la clé privée, dans le cas d'un chiffrement asymétrique). Par ailleurs, une fois que l'identité de l'utilisateur est vérifiée grâce à son terminal, une session peut être établie pour un service sécurisé. Par exemple, une clé diversifiée peut être utilisée ensuite pour les échanges entre l'équipement PC et une plateforme de service reliée au serveur SER.

30

Bien entendu, la présente invention ne se limite pas à la forme de réalisation décrite ci-avant à titre d'exemple. Elle s'étend à d'autres variantes.

Par exemple, on a décrit ci-avant une interaction avec un lecteur par communication en champ proche. Dans une variante, une communication peut être établie directement entre le terminal TER et le serveur SER, par exemple via un réseau cellulaire, tant pour l'étape préalable de déclaration du terminal que pour l'étape ultérieure de vérification d'identité.

Par ailleurs, on a décrit ci-avant en référence à la figure 2 l'utilisation d'un équipement PC (ou encore d'un lecteur LEC, tel qu'une borne communicante). Dans une variante plus simple, il peut être utilisé directement le terminal TER pour accéder au service (ou pour l'enrôlement initial du terminal) et la vérification de la signature du challenge (ou l'enrôlement) s'effectue directement par une communication entre le serveur et le terminal, sans équipement intermédiaire. Toutefois, l'utilisation d'un appareil communicant (une borne de lecture LEC, un ordinateur PC, une tablette ou encore une télévision) offre avantageusement une interface améliorant l'ergonomie d'utilisation.

Par ailleurs, on a décrit ci-avant une interaction avec un serveur d'application SER. En variante, il peut être prévu de façon équivalente une interaction avec un équipement de type CMS (pour « Card Management System ») ou TSM (pour « Trusted Service Management »).

Ainsi, l'invention propose d'utiliser un (ou plusieurs) élément(s) de sécurité embarqué(s) dans un objet communicant pour embarquer une identité dérivée dont l'évolution (vol, perte, répudiation, etc.) peut être gérée déjà par l'émetteur initial du support CNI et qui permet une validation simple, rapide, sécurisée et anonyme des droits associés.

A cet effet, on prévoit un calcul, suivi d'un transfert de l'identité dérivée via des interfaces (souvent standardisées) des objets communicants, par exemple par des échanges locaux (en champ proche ou NFC pour « Near Field Communication »), ou en variante via Internet (par une liaison WiFi, ou autres), ou encore possiblement via des interfaces utilisateurs de réseaux sociaux (Facebook, LinkedIn, voire iTunes ®), ou encore par communication par un réseau cellulaire (3G, LTE ou autres). L'identité

dérivée peut ne pas être stockée seule dans la mémoire sécurisée. On peut prévoir une mémorisation dans l'objet communicant d'une application de gestion des relais de requêtes externes transmises selon les mêmes interfaces que pour l'implémentation de l'étape préalable de déclaration du terminal. Avantageusement, une authentification locale des données du porteur peut être prévue (par exemple par saisie de données de biométrie), avant la déclaration du terminal mobile. L'invention permet ensuite une personnalisation des opérations cryptographiques en fonction des demandes ou des services en ligne concernés, avec des créations de signatures numériques spécifiques à chaque service. L'invention permet en outre d'éviter le partage d'informations significatives avec les parties concernées par la transaction pendant le service.

Avantageusement, la validation de l'appairage du terminal, du titre authentique et du porteur peut se baser sur 2 ou 3 facteurs (les données du titre authentique – ce que j'ai, un code PIN – ce que je sais, une donnée biométrie – ce que je suis). Après validation des données d'authentification sur 2 ou 3 facteurs du porteur authentique, un enrôlement initial du terminal peut être effectué par utilisation d'un titre authentique CNI, carte de fidélité, carte d'étudiant ou autre. Ainsi, l'introduction de la biométrie/cryptographie dans la génération d'une signature digitale est une réalisation optionnelle mais avantageuse. L'invention permet alors un partage de données non significatives avec une vérification auprès de serveurs distants, sans partage d'identité. Elle permet en outre une génération et une communication de certificat et/ou de signature numérique en offrant donc une option d'audit *a posteriori*, et ce, dans des conditions de personnalisation après émission d'applications signées sans besoin d'environnements spécifiques.

Il est assuré ainsi une personnalisation d'applications à forte sensibilité sur la base de l'identification du porteur initial, du fait de la création d'un lien unique entre le porteur authentique et une donnée calculée sur la base d'une information du support initial CNI qui d'ailleurs peut être un produit de sécurité (carte ou système à processeur de sécurité). Ensuite, la création de conditions de génération d'algorithme diversifié sur la base de données produites par le porteur (et non disponibles dans les objets) est aussi un avantage.

REVENDICATIONS

1. Procédé de vérification d'identité d'un utilisateur d'un terminal communicant (TER), comportant :
- 5 * une étape préalable comprenant :
- une communication à au moins un serveur (SER) d'une première donnée d'identité (Id1) de l'utilisateur (S10),
 - une génération auprès du serveur d'une deuxième donnée d'identité (Id2) de l'utilisateur (S11), la deuxième donnée définissant une identité dérivée de l'utilisateur, et
 - 10 - un stockage de la deuxième donnée d'identité (Id2) dans une mémoire sécurisée (SIM) du terminal (S12),
- * une étape courante de vérification d'identité comprenant :
- une transmission du serveur au terminal d'un jeton (C) à chiffrer (S21),
 - 15 - une utilisation auprès du terminal de la deuxième donnée au moins pour générer un chiffrement du jeton (S23), le jeton chiffré (C*) étant transmis au serveur et vérifié auprès du serveur (S25), et
 - en cas de vérification positive du jeton chiffré auprès du serveur, le serveur valide la vérification d'identité de l'utilisateur du terminal.
- 20
2. Procédé selon la revendication 1, dans lequel le chiffrement utilise une infrastructure à clé publique, la donnée d'identité dérivée (Id2) au moins étant utilisée pour générer une clé de chiffrement.
- 25
3. Procédé selon la revendication 1, dans lequel la donnée d'identité dérivée (Id2) est un certificat numérique certifiant le chiffrement par le terminal.
4. Procédé selon l'une des revendications précédentes, dans lequel, en cas de vérification positive, le jeton chiffré est lié à un certificat numérique d'identification de l'utilisateur.
- 30
5. Procédé selon l'une des revendications précédentes, dans lequel ladite communication au serveur de la première donnée d'identité (Id1) de l'utilisateur est

autorisée après vérification d'une donnée biométrique de l'utilisateur du terminal (S13).

5 6. Procédé selon l'une des revendications précédentes, dans lequel l'étape courante comporte une vérification d'une donnée propre à l'utilisateur (S22) avant d'initier sur le terminal l'utilisation de la deuxième donnée pour le chiffrement du jeton.

10 7. Procédé selon l'une des revendications précédentes, dans lequel on prévoit une pluralité d'étapes préalables avec une pluralité de communications à une pluralité de serveurs de la première donnée d'identité de l'utilisateur, chaque serveur générant des deuxièmes données respectives d'identité de l'utilisateur, chaque deuxième donnée définissant une identité dérivée de l'utilisateur, chaque identité dérivée étant propre à un service dont l'accès est conditionné par une vérification de jeton chiffré auprès d'un serveur dédié audit service.

15 8. Procédé selon l'une des revendications précédentes, dans lequel la communication au serveur (SER) de la première donnée d'identité (Id1) est effectuée via un lecteur (LEC) comportant un module de communication de courte portée (NFC) ou filaire, et, le terminal comportant un module homologue de communication de courte portée
20 ou filaire, la deuxième donnée (Id2) est transmise du serveur au lecteur, puis du lecteur au terminal par communication en courte portée ou filaire.

25 9. Procédé selon l'une des revendications 1 à 8, dans lequel la transmission du jeton (C) à chiffrer et/ou du jeton chiffré (C*), entre le serveur et le terminal, est effectuée via un équipement (PC) sollicitant un accès à un service auquel le serveur (SER) est associé, l'accès au service étant conditionné par une vérification de l'identité de l'utilisateur à partir du terminal de l'utilisateur à ladite étape courante.

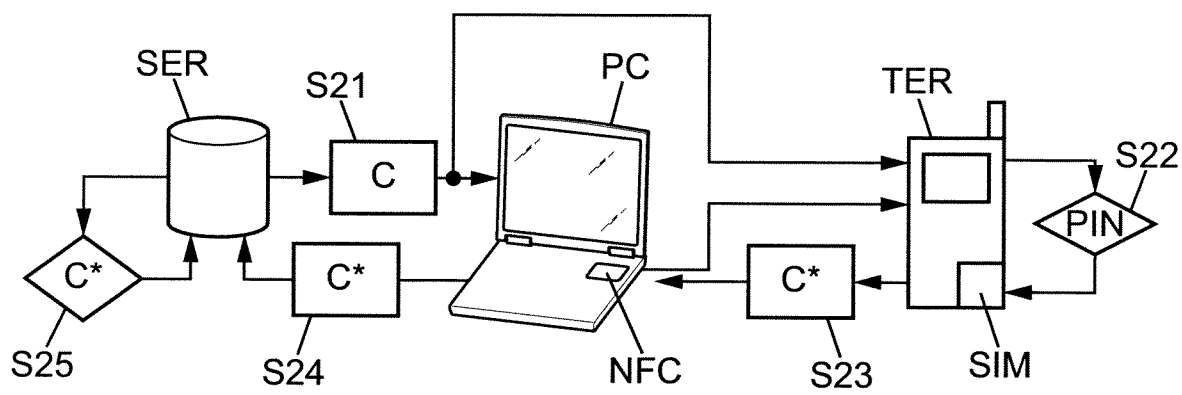
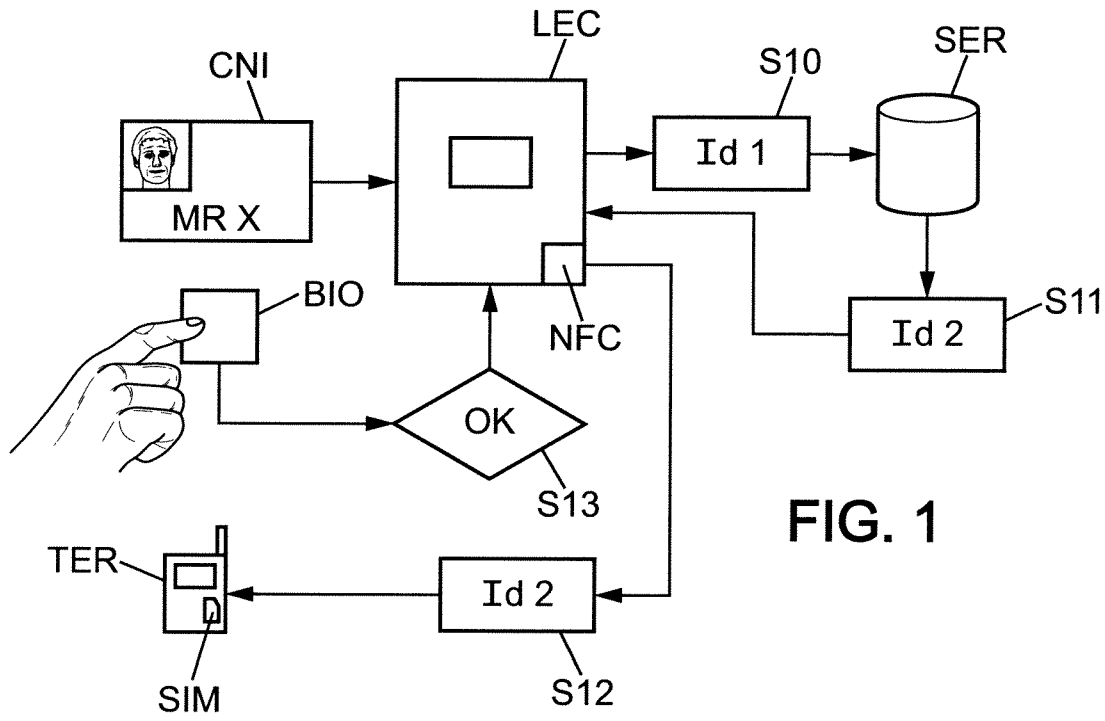
30 10. Procédé selon la revendication 9, dans lequel la transmission du jeton (C) à chiffrer et/ou du jeton chiffré (C*), entre le terminal (TER) et l'équipement (PC), est effectuée par une communication de courte portée (NFC) ou filaire,

le terminal (TER) comportant un module de communication de courte portée (NFC) ou filaire et l'équipement (PC) comportant un module homologue de communication de courte portée ou filaire.

5 11. Procédé selon l'une des revendications 1 à 8, dans lequel la transmission du jeton (C) à chiffrer du serveur (SER) au terminal (TER) est effectuée par un réseau mobile, et la transmission du jeton chiffré (C*) du terminal au serveur est effectuée via un équipement (PC) sollicitant un accès à un service auquel le serveur (SER) est associé, l'accès au service étant conditionné par une vérification de l'identité de
10 l'utilisateur à partir du terminal de l'utilisateur à ladite étape courante.

12. Procédé selon l'une des revendications 1 à 8, dans lequel la transmission du jeton (C) à chiffrer du serveur (SER) au terminal (TER) est effectuée via un équipement (PC) sollicitant un accès à un service auquel le serveur (SER) est associé, et la
15 transmission du jeton chiffré (C*) du terminal au serveur est effectuée par un réseau mobile, l'accès au service étant conditionné par une vérification de l'identité de l'utilisateur à partir du terminal de l'utilisateur à ladite étape courante.

13. Système de vérification d'identité d'un utilisateur, comportant au moins un terminal (TER) et un serveur (SER) pour la mise en œuvre du procédé selon l'une des
20 revendications précédentes.



INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2013/050197

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/32

ADD.

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)

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 practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 2 323 308 A1 (SAGEM ORGA GMBH [DE]) 18 May 2011 (2011-05-18) abstract; claims 1,8,14; figures 1,2 paragraphs [0006], [0007], [0012], [0017], [0027], [0028], [0030], [0034], [0036] - [0038], [0042], [0045] ----- -/--	1-13



Further documents are listed in the continuation of Box C.



See patent family 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 application or patent 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

Date of the actual completion of the international search

21 March 2013

Date of mailing of the international search report

02/04/2013

Name and mailing address of the ISA/

 European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Wolters, Robert

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2013/050197

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"Chapter 10: Identification and Entity Authentication ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 385 - 424 1 October 1996 (1996-10-01), XP001525010, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL: http://www.cacr.math.uwaterloo.ca/hac/ Sections 10.3	1-13
Y	----- DOMINIKUS S ET AL: "mCoupons: An Application for Near Field Communication (NFC)", ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS, 2007, AINAW '07. 21ST INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 21 May 2007 (2007-05-21), pages 421-428, XP031334719, ISBN: 978-0-7695-2847-2 abstract Sections 5.5 et 5.6	1-13
A	----- MIHIR BELLARE ET AL: "Security Proofs for Identity-Based Identification and Signature Schemes", JOURNAL OF CRYPTOLOGY, SPRINGER-VERLAG, NE, vol. 22, no. 1, 22 August 2008 (2008-08-22), pages 1-61, XP019699801, ISSN: 1432-1378 abstract Section 1: Introduction -----	1-13

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2013/050197

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2323308	A1	18-05-2011	AU 2010318058 A1 03-05-2012
			CA 2780717 A1 19-05-2011
			CN 102640450 A 15-08-2012
			EP 2323308 A1 18-05-2011
			US 2012303966 A1 29-11-2012
			WO 2011057983 A1 19-05-2011

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2013/050197

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04L9/32 ADD.		
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) H04L		
Documentation consultée autre que la documentation minimale 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) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 2 323 308 A1 (SAGEM ORGA GMBH [DE]) 18 mai 2011 (2011-05-18) abrégé; revendications 1,8,14; figures 1,2 alinéas [0006], [0007], [0012], [0017], [0027], [0028], [0030], [0034], [0036] - [0038], [0042], [0045] ----- -/-	1-13
☒ Voir la suite du cadre C pour la fin de la liste des documents ☒ 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		
Date à laquelle la recherche internationale a été effectivement achevée		Date d'expédition du présent rapport de recherche internationale
21 mars 2013		02/04/2013
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, Fax: (+31-70) 340-3016		Wolters, Robert

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	"Chapter 10: Identification and Entity Authentication ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 385 - 424 1^{er} octobre 1996 (1996-10-01), XP001525010, ISBN: 978-0-8493-8523-0 Extrait de l'Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/ Sections 10.3	1-13
Y	----- DOMINIKUS S ET AL: "mCoupons: An Application for Near Field Communication (NFC)", ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS, 2007, AINAW '07. 21ST INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 21 mai 2007 (2007-05-21), pages 421-428, XP031334719, ISBN: 978-0-7695-2847-2 abrégé Sections 5.5 et 5.6 -----	1-13
A	MIHIR BELLARE ET AL: "Security Proofs for Identity-Based Identification and Signature Schemes", JOURNAL OF CRYPTOLOGY, SPRINGER-VERLAG, NE, vol. 22, no. 1, 22 août 2008 (2008-08-22), pages 1-61, XP019699801, ISSN: 1432-1378 abrégé Section 1: Introduction -----	1-13

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2013/050197

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 2323308	A1	18-05-2011	AU 2010318058 A1	03-05-2012
			CA 2780717 A1	19-05-2011
			CN 102640450 A	15-08-2012
			EP 2323308 A1	18-05-2011
			US 2012303966 A1	29-11-2012
			WO 2011057983 A1	19-05-2011
