(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
22 août 2013 (22.08.2013)

WIPO | PCT

(10) Numéro de publication internationale
WO 2013/121127 A1

(51) Classification internationale des brevets :
G06Q 20/32 (2012.01) *G06Q 20/40* (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2013/050218

(22) Date de dépôt international :
1 février 2013 (01.02.2013)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1251438 16 février 2012 (16.02.2012) FR
1259235 28 septembre 2012 (28.09.2012) FR

(71) Déposants : **ORANGE** [FR/FR]; 78 Rue Olivier de Serres, F-75015 Paris (FR). **MORPHO** [FR/FR]; 11 Bld Galliéni, F-92130 Issy-les-Moulineaux (FR).

(72) Inventeurs : **GENESTIER, Philippe**; Le Sabot, F-38570 Hurtieres (FR). **MOREAU, Jérôme**; 32, rue des Peupliers, F-75013 Paris (FR). **GONCALVES, Louis-Philippe**; c/o MORPHO, 27, rue Leblanc, F-75015 Paris (FR). **BENTEO, Bruno**; c/o MORPHO, 27, rue Leblanc, F-75015 Paris (FR).

(74) Mandataires : **HASSINE, Albert** et al.; Cabinet Plasseraud, 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.

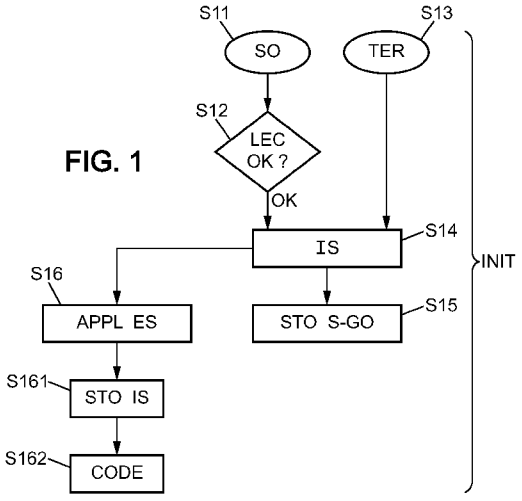
(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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).

[Suite sur la page suivante]

(54) Title : SECURING A DATA TRANSMISSION

(54) Titre : SECURISATION D'UNE TRANSMISSION DE DONNEES

FIG. 1



(57) Abstract : The invention relates to a securing of data transmission by verification of an identity of a user, comprising: a prior step (INIT) of enrolling a terminal of the user, comprising: an association between an authentic identity datum of the user and a datum of a terminal available to the user and communicating via a network, the association being stored with data regarding contact of the terminal via the network, and a determination of an identity derived at least from said information, stored in the memory of the terminal, in correspondence with a datum specific to the user, with a view to a subsequent strong authentication based both on the datum specific to the user and on the derived identity, as well as a current step (VERIF) of verifying the user's identity, comprising: on the basis of the data regarding contact of the terminal, a contact of the terminal via the network so as to launch at the terminal interrogation of a user so as to ask the user to enter the datum specific to the user, as well as a verification of this datum at the terminal, the verification of the user datum being positive, a verification of the derived identity, and, in the case of successful verification of the derived identity, a validation of the verification of identity of the user.

(57) Abrégé :

[Suite sur la page suivante]

WO 2013/121127 A1

Publiée :

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

L'invention concerne une sécurisation de transmission de données par vérification d'une identité d'un utilisateur, comportant: une étape préalable (INIT) d'enrôlement d'un terminal de l'utilisateur, comprenant : une association entre une donnée d'identité authentique de l'utilisateur et une donnée d'un terminal à disposition de l'utilisateur et communiquant via un réseau, l'association étant mémorisée avec des données de contact du terminal via le réseau, et une détermination d'une identité dérivée au moins de ladite information, stockée en mémoire du terminal, en correspondance d'une donnée propre à l'utilisateur, en vue d'une authentification forte, ultérieure, basée à la fois sur la donnée propre à l'utilisateur et sur l'identité dérivée, ainsi qu'une étape courante (VERIF) de vérification d'identité de l'utilisateur, comprenant : à partir des données de contact du terminal, un contact du terminal via le réseau pour lancer auprès du terminal une interrogation de l'utilisateur pour demander à l'utilisateur de saisir la donnée propre à l'utilisateur, ainsi qu'une vérification de cette donnée auprès du terminal, la vérification de la donnée d'utilisateur étant positive, une vérification de l'identité dérivée, et, en cas de succès de vérification de l'identité dérivée, une validation de la vérification d'identité de l'utilisateur.

Sécurisation d'une transmission de données

La présente invention concerne une sécurisation d'une transmission de données, par vérification d'identité d'un utilisateur, notamment pour l'accès à un service.

Le service précité peut viser par exemple l'accès à des données bancaires, ou à des données d'un dossier médical, ou autre. Généralement, l'accès est autorisé après vérification d'un support comprenant par exemple un processeur de sécurité, tel une carte à puce (comme une carte bancaire par exemple). Néanmoins, la vérification du support nécessite un lecteur du support à chaque demande d'accès au service. Par exemple, la carte SESAM-Vitale (définissant des droits pour l'assurance maladie en France) nécessite un lecteur (par exemple sous la forme d'une borne de lecture reliée à un central) pour qu'un utilisateur puisse consulter ses droits d'accès aux soins, ou mettre à jour le dossier médical du porteur de la carte.

Malgré les efforts réalisés pour déployer ces bornes de lecture, elles ne sont pas toujours facilement accessibles, notamment en cas d'urgence ou en situation de mobilité.

Il convient de noter aussi un déploiement de lecteurs auprès des professionnels de santé pour consulter le dossier médical d'un patient pendant une consultation. De même, les professionnels de santé ont eux-mêmes une autre carte professionnelle en France (dite CPS pour « Carte de Professionnel de Santé ») dont la lecture nécessite l'utilisation d'un autre lecteur.

De fait, une telle organisation duplique les lecteurs de cartes dont doivent disposer les intervenants de santé dans leur environnement de travail. De plus, elle ne permet pas les usages en situation de mobilité ou l'utilisation de terminaux ne disposant pas d'interface de lecture de cartes.

La présente invention vient améliorer la situation.

Elle propose à cet effet un procédé pour vérifier une identité d'un utilisateur, comportant :

- une étape préalable d'enrôlement d'un terminal de l'utilisateur, comprenant un stockage d'une identité dérivée d'au moins une donnée d'identité authentique de l'utilisateur, dans des moyens de stockage du terminal, en correspondance avec une donnée propre à l'utilisateur, et
- une étape courante de vérification auprès du terminal de l'identité de l'utilisateur, comprenant une authentification forte basée sur l'identité dérivée stockée et sur la donnée propre à l'utilisateur stockée.

On entend par « donnée d'identité authentique de l'utilisateur », un élément d'information sur l'identité de l'utilisateur portée par un support d'identité. Elle peut être par exemple issue d'une carte personnelle portant un processeur de sécurité (par exemple une carte bancaire, ou plus généralement une carte à puce donnant accès à des droits telle que par exemple une carte SESAM-Vitale ouvrant, en France, droit à des soins de santé). En variante, il peut s'agir d'une pièce d'identité (passeport, éventuellement biométrique, ou autre). L'identité authentique de l'utilisateur peut être une identité régalienne de l'utilisateur. Comme on le verra dans un exemple de réalisation décrit plus loin, il est préférable (mais optionnel) qu'un lecteur de cette carte à puce ou de cette pièce d'identité (borne ou terminal de lecture) relève, vérifie et communique l'information de l'identité de l'utilisateur que comporte la carte ou la pièce d'identité.

Une authentification forte, du type précité, garantit, comme on le verra plus loin, la robustesse dans la vérification d'identité de l'utilisateur.

Dans une réalisation, l'étape préalable d'enrôlement comporte une détermination de l'identité dérivée par combinaison entre :

- la donnée d'identité authentique de l'utilisateur, et
- une donnée de terminal.

En particulier, cette association peut être, dans une réalisation, mémorisée avec des données de contact du terminal via un réseau auquel est connecté le terminal.

L'étape courante de vérification comprend, dans une réalisation :

- une vérification de concordance entre la donnée propre à l'utilisateur stockée et une donnée propre à l'utilisateur saisie par l'utilisateur au moyen du terminal, et
- une transmission de l'identité dérivée stockée dans le terminal à une entité distante de vérification.

Dans un exemple de réalisation, elle peut s'appuyer sur une vérification basée sur une comparaison d'une donnée saisie par l'utilisateur avec la donnée propre à l'utilisateur, puis, en cas de succès dans cette vérification, sur une vérification de l'identité dérivée grâce à l'enrôlement préalable du terminal.

Ainsi, dans une telle réalisation, l'étape courante de vérification d'identité de l'utilisateur, comprend par exemple :

* à partir des données de contact du terminal via un réseau auquel le terminal est connecté, un contact du terminal via ce réseau pour déclencher auprès du terminal une interrogation de l'utilisateur pour demander à l'utilisateur de saisir une donnée propre à l'utilisateur,
* une vérification par le terminal de la donnée saisie,

* et, la vérification de la donnée propre à l'utilisateur saisie étant positive, une vérification de l'identité dérivée,
* et, la vérification de l'identité dérivée étant positive, une validation de la vérification d'identité de l'utilisateur.

On entend par « donnée de terminal » tout type de donnée permettant d'identifier le terminal. Par exemple, dans le cas où le terminal est équipé d'un élément de sécurité tel que par exemple une carte SIM (pour « Subscriber Identity Module »), cette donnée peut être un identifiant de la carte SIM.

Par ailleurs, on entend par « données de contact du terminal » des données permettant de joindre le terminal via le réseau précité. Il peut tout simplement s'agir du numéro de téléphone (MSISDN, Mobile Station International Subscriber Directory Number, notamment) attribué au terminal dans le cas où ce dernier est un terminal téléphonique (terminal téléphonique mobile, smartphone, tablette ou autre). Il peut toutefois s'agir, en variante, d'une adresse IP par exemple pour un équipement connecté via un réseau IP (Internet Protocol), ou encore une adresse de courriel (« email »).

On relèvera que, dans le cas où les données de contact n'ont pas vocation à changer, par exemple dans le cas d'un numéro de téléphone du terminal, les « données de contact » peuvent désigner le terminal et peuvent correspondre simplement à la « donnée de terminal » précitée.

On entend par identité « dérivée » une donnée d'identité résultant de toute transformation de l'information d'identité portée par le support initialement utilisé pour produire l'identité de l'utilisateur (par exemple son identité régalienne), par exemple une transformation par une fonction de hachage (par exemple non interprétable par des tiers), ou autre.

On entend par « donnée propre à l'utilisateur » par exemple un code personnel d'identification (ou code « PIN »), ou encore une donnée d'identification biométrique (reconnaissance vocale ou d'empreinte digitale, ou d'iris, etc.), ou toute autre information permettant une identification de l'utilisateur par une interface homme/machine du terminal.

Ainsi, une mise en œuvre possible de la présente invention, à titre de mode de réalisation, peut consister en un procédé pour vérifier une identité d'un utilisateur, comportant une étape préalable d'enrôlement d'un terminal de l'utilisateur, comprenant :

* une association entre :
  - une donnée d'information authentique de l'identité de l'utilisateur, et

- une donnée de terminal, ce terminal étant à disposition de l'utilisateur et communiquant via un réseau,

cette association étant mémorisée avec des données de contact du terminal via le réseau,

* une détermination d'une identité dérivée au moins de ladite information, et un stockage de ladite identité dérivée dans des moyens de stockage du terminal, en correspondance avec une donnée propre à l'utilisateur, en vue d'une authentification forte, ultérieure, basée à la fois sur la donnée propre à l'utilisateur et sur l'identité dérivée.

Par exemple, dans une forme de réalisation simple, la donnée précitée de terminal peut correspondre directement aux données de contact précitées du terminal.

Le procédé peut alors comporter ensuite une étape courante de vérification d'identité de l'utilisateur, comprenant :

* à partir des données de contact du terminal, un contact du terminal via le réseau pour déclencher auprès du terminal une interrogation de l'utilisateur pour demander à l'utilisateur de saisir ladite donnée propre à l'utilisateur, ainsi qu'une vérification de ladite donnée propre à l'utilisateur auprès du terminal,

* la vérification de la donnée propre à l'utilisateur étant positive, une vérification de l'identité dérivée,

* et, la vérification de l'identité dérivée étant positive, une validation de la vérification d'identité de l'utilisateur.

De manière générale, la présente invention permet avantageusement de déporter la fonction d'authentification de l'identité de l'utilisateur (habituellement à partir d'une carte bancaire, d'une carte SESAM-Vitale ou autre) vers son terminal, et ce grâce au stockage de l'identité dérivée auprès du terminal et d'une authentification forte basée à la fois sur la vérification du code de l'utilisateur et sur la vérification de cette identité dérivée. La mise en œuvre de la présente invention rend possible alors l'utilisation d'un simple terminal communicant (téléphone mobile, Smartphone, tablette, ou autre) pour accéder à un ou plusieurs services distincts nécessitant une sécurisation de transmission de données (données de dossier médical, données bancaires, ou autres).

Par exemple, la validité de la vérification de l'identité de l'utilisateur à l'issue de l'étape courante précitée, peut conditionner la délivrance d'une clé de session ou de chiffrement pour une transmission sécurisée ultérieure de données, dans le cadre d'un service notamment. Par exemple, il peut s'agir d'une clé diversifiée à chaque autorisation d'accès au service, après vérification de l'identité de l'utilisateur au sens de l'étape courante précitée.

Dans un mode de réalisation, l'identité dérivée est stockée dans des moyens de stockage dont l'accès est sécurisé, typiquement dans des moyens de stockage d'un élément de sécurité du terminal, comme par exemple des moyens de stockage de la carte SIM.

La mémorisation d'association peut être mise en œuvre auprès d'un module d'association, distant du terminal (par exemple sur un serveur distant d'une plateforme de service). Ainsi, dans une telle réalisation, ce module d'association peut déterminer l'identité dérivée (par exemple en calculant un hachage de l'information d'identité d'origine) et communiquer cette identité dérivée au terminal.

Dans une réalisation, l'identité dérivée peut être transmise au terminal par une technique de type « OTA » pour « Over-The-Air » conjointement avec des données d'une application s'exécutant auprès du terminal au moins pour commander le stockage de l'identité dérivée. Ainsi, l'application qui s'installe sur le terminal peut, lorsqu'elle est exécutée, conduire :

- au stockage de l'identité dérivée auprès du terminal,
- à l'animation d'une interface homme/machine pour demander à l'utilisateur de saisir une donnée de l'utilisateur, qui lui est propre, pour une authentification forte future,
- ultérieurement, pendant une étape courante, demander à l'utilisateur de saisir sa donnée propre, vérifier cette donnée auprès du terminal, et par exemple transmettre l'identité dérivée à un module distant (pour vérification auprès de ce module distant), si la donnée saisie est valide.

Ainsi, pendant l'étape courante précitée, l'identité dérivée peut être transmise du terminal vers une entité de vérification, distante du terminal, la vérification de l'identité dérivée étant validée auprès de ladite entité distante si en outre la donnée propre à l'utilisateur a été vérifiée avec succès auprès du terminal. Ainsi, la vérification auprès de cette entité se base sur une authentification forte, à la fois sur la donnée d'utilisateur et sur l'identité dérivée.

Avantageusement, cette entité distante peut comporter au moins un module d'authentification, coopérant avec au moins ledit module d'association pour contrôler l'identité dérivée reçue du terminal pendant l'étape courante.

Pendant l'étape préalable d'enrôlement du terminal, l'identité dérivée peut être déterminée auprès du module d'association, puis transmise au terminal via par exemple la plateforme d'un opérateur du réseau précité.

Initialement, la donnée d'identité authentique de l'utilisateur peut être fournie par lecture d'un composant de sécurité (de type processeur de sécurité par exemple) d'un support à disposition de

l'utilisateur (une carte à puce, comme une carte bancaire, une carte SESAM-Vitale, ou autres). Ainsi, la validité de l'information d'identité que porte la carte peut être assurée par le lecteur et éventuellement par un serveur de vérification distant, avant de procéder à son association avec une donnée de terminal.

Comme indiqué précédemment, dans une réalisation à titre d'exemple, le terminal peut être un terminal de télécommunication et les données de contact du terminal comportent alors un numéro d'appel du terminal via le réseau précité.

Ainsi, dans une réalisation particulière,

- pendant ladite étape préalable :
  * le terminal transmet à un module d'association, distant du terminal, une donnée de terminal avec la donnée d'identité authentique de l'utilisateur,
  * le module d'association détermine une identité dérivée, et communique ladite identité dérivée au terminal,
  * sur réception de l'identité dérivée, le terminal exécute une application :
    . d'enregistrement de l'identité dérivée et
    . de présentation d'une interface à l'utilisateur, pour l'enregistrement d'une donnée propre à l'utilisateur,
- pendant ladite étape courante :
  * sur un équipement connecté pour une transmission sécurisée de données, l'équipement demande à l'utilisateur une donnée de contact du terminal via une interface homme/machine de l'équipement connecté, et l'équipement transmet ladite donnée de contact à une entité de vérification, distante du terminal,
  * l'entité de vérification distante contacte le terminal pour lancer une application auprès du terminal, déclenchant les opérations :
    . demander à l'utilisateur de saisir la donnée propre à l'utilisateur via une interface homme/machine du terminal, et
    . la vérification de la donnée propre à l'utilisateur étant positive, transmettre l'identité dérivée depuis le terminal vers l'entité de vérification,
  * en cas de succès dans une vérification de l'identité dérivée auprès de l'entité de vérification, l'entité de vérification valide la vérification d'identité de l'utilisateur pour autoriser une transmission de données via l'équipement connecté.

La présentation précitée d'une interface à l'utilisateur, pour la saisie de la donnée propre à l'utilisateur, peut consister par exemple à présenter un code que doit retenir l'utilisateur, ou consister à demander à l'utilisateur d'entrer un code personnel, ou encore faire saisir un paramètre biométrique.

L'équipement connecté peut par exemple être un ordinateur, une tablette, ou autre, relié à une plateforme de service via un réseau étendu et sollicitant l'accès au service, ou peut être le terminal lui-même. Ainsi, dans l'évolution de l'interaction entre l'équipement et une plateforme de service, il est demandé à l'utilisateur, à une étape, d'entrer le numéro de téléphone de son terminal. La plateforme de service contacte alors le terminal pour lancer l'authentification forte (vérification par exemple du code auprès du terminal, puis de l'identité dérivée).

Préalablement, pour vérifier l'information initiale d'identité de l'utilisateur, il peut être prévu, pendant l'étape préalable précitée, que :

* le module d'association vérifie ladite information d'identité auprès d'un module de gestion d'identité (par exemple un serveur de gestion des cartes SESAM-Vitale),
* et en cas de vérification positive, le module d'association détermine une identité dérivée, et communique ladite identité dérivée au terminal.

Dans une réalisation, un identifiant est transmis avec une donnée de contact du terminal via un réseau à une plateforme de service. Ainsi, si la vérification d'identité est positive à l'étape courante, l'utilisateur est autorisé à accéder à des données d'informations, fonction dudit identifiant.

Il peut être avantageux, notamment dans une application détaillée ci-après, de prévoir que le terminal reçoive, par interaction avec un objet communiquant, une donnée d'accès à un service encodant cet identifiant.

Cet objet communiquant peut être un deuxième terminal à disposition d'un deuxième utilisateur, et apte à communiquer avec le premier terminal enrôlé au cours de l'étape préalable.

Par ailleurs, les données d'informations peuvent comportent au moins des données propres à un utilisateur de l'objet communiquant précité.

Dans une réalisation, l'identifiant peut être transmis à une plateforme de service et cette plateforme de service vérifie l'identifiant et autorise un accès aux données d'informations si la vérification de l'identifiant est positive.

Une telle réalisation trouve une application avantageuse notamment dans l'assistance à une personne nécessitant des soins d'urgence, auquel cas l'objet communiquant peut être un deuxième terminal à disposition d'une deuxième personne (nécessitant des soins d'urgence), et apte à

communiquer avec le premier terminal enrôlé au cours de ladite étape préalable (à disposition par exemple d'un urgentiste).

Dans cette réalisation, le premier terminal peut recevoir la donnée de service du deuxième terminal par communication en champ proche, le deuxième terminal appartenant à une personne nécessitant des soins d'urgence (et n'étant par exemple pas en mesure de s'identifier avec son téléphone ou plus généralement d'utiliser son téléphone pour communiquer la donnée de service précitée), et le premier terminal appartenant à un urgentiste.

Dans une telle application, les données d'informations fonctions de l'identifiant de service peuvent comporter au moins des données médicales de la personne nécessitant des soins d'urgence. Ainsi, l'identifiant relatif à un service peut alors être transmis à une plateforme de service. Cette plateforme de service vérifie l'identifiant et n'autorise un envoi des données d'informations que si la vérification de l'identifiant de service est positive.

La présente invention vise aussi un procédé de sécurisation d'une transmission de données, entre un équipement et une plateforme de service, comportant une vérification d'identité d'un utilisateur de l'équipement selon l'étape courante du procédé ci-avant, le procédé de sécurisation comportant :

- une transmission des données de contact du terminal à la plateforme de service,
- la mise en œuvre de l'étape courante de vérification d'identité à partir du terminal de l'utilisateur, et
- la vérification d'identité étant positive, une étape pour autoriser une transmission de données entre l'équipement et la plateforme de service.

L'équipement peut être le terminal lui-même. Il peut s'agir par exemple d'un ordinateur connecté à un réseau étendu tel l'Internet. Par exemple dans ce cas, l'adresse IP de l'ordinateur peut former des données de contact du terminal.

Par ailleurs, la transmission de données entre l'équipement et la plateforme de service peut être chiffrée, assortie de l'allocation d'une clé de session ou de chiffrement dans la communication entre l'équipement et la plateforme.

La présente invention vise aussi un programme informatique comportant des instructions pour la mise en œuvre du procédé ci-avant, lorsque ce programme est exécuté par un processeur. A ce titre, la figure 1 commentée ci-après peut représenter l'organigramme de l'algorithme général d'un exemple de réalisation de ce programme.

La présente invention vise aussi un terminal pour la mise en œuvre d'un procédé de vérification d'une identité d'un utilisateur, comportant :

- des moyens de stockage pour stocker une identité dérivée d'au moins une donnée d'identité authentique de l'utilisateur en correspondance avec une donnée propre à l'utilisateur et
- des instructions de programme informatique pour, lorsque lesdites instructions sont exécutées par un processeur du terminal, sur sollicitation par une entité distante de vérification de ladite identité dérivée:
  - animer une interface homme/machine pour demander à l'utilisateur de saisir ladite donnée propre à l'utilisateur, puis vérifier une concordance de la donnée propre saisie avec la donnée propre stockée,
  - transmettre l'identité dérivée stockée à l'entité distante pour vérification.

La présente invention vise aussi une entité de vérification pour la mise en œuvre au moins de l'étape courante du procédé ci-avant, comportant des moyens :

- de contact du terminal, via le réseau précité pour déclencher auprès du terminal une interrogation de l'utilisateur,
- de réception et de vérification de l'identité dérivée, reçue du terminal, et
- les vérifications de l'identité dérivée et de la donnée propre à l'utilisateur étant positives, de validation de vérification d'identité de l'utilisateur.

Bien entendu, la présente invention vise aussi un système comportant au moins le terminal et l'entité de vérification (distante du terminal par exemple), et optionnellement le module d'association précité.

On indique en effet que l'entité de vérification et le module d'association peuvent être deux entités séparées (par exemple deux serveurs distants l'un de l'autre), ou qu'en variante le module d'association peut être intégré à l'entité de vérification.

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

- la figure 1 illustre schématiquement les principales étapes du procédé au sens de l'invention,
- la figure 2 illustre un système pour la mise en œuvre de l'étape préalable d'enrôlement du terminal, et
- la figure 3 illustre un système pour la mise en œuvre de l'étape courante de vérification d'identité,

- la figure 4 illustre un mode de réalisation dans lequel un identifiant relatif à un service est transmis par le terminal, dans un exemple de réalisation, pour recevoir des données relatives au service.

On a représenté sur la figure 1 un exemple de réalisation de la succession des étapes d'un procédé au sens de l'invention comportant une phase initiale INIT, d'enrôlement préalable d'un terminal, et une étape courante de vérification VERIF d'identité de l'utilisateur.

Dans cet exemple de réalisation, pendant la phase préalable INIT, à l'étape S13, l'utilisateur d'un terminal TER (représenté sur les figures 2 et 3) transmet à un module d'association S-As, distant du terminal, une donnée de terminal, par exemple un numéro d'appel du terminal, avec, à l'étape S11, une information d'identité de l'utilisateur par exemple contenue dans un support d'origine SO. A cet effet, l'utilisateur peut mettre en œuvre une borne de lecture du support d'origine. A l'étape S12, le module d'association (par exemple un serveur d'association S-As représenté sur la figure 2) peut vérifier l'information d'identité de l'utilisateur reçue de la borne de lecture auprès d'un module de gestion d'identité (par exemple un serveur S-GO de gestion des supports SO). En cas de vérification positive (flèche OK en sortie du test S12), le module d'association détermine une identité dérivée IS, à l'étape S14, et communique cette identité dérivée au terminal à l'étape S16, pour démarrer une application auprès du terminal (par exemple une application de type « cardlet » sur la carte SIM du terminal), notamment pour enregistrer à l'étape S161 l'identité dérivée dans une mémoire de l'élément de sécurité du terminal (par exemple sa carte SIM). Les données de cette application peuvent être transmises par une technique de type OTA (pour « Over-the-Air »), ou par téléchargement à partir d'un lien URL, ou autre. L'exécution de cette application sur le terminal peut en outre consister à présenter à l'étape S161 une interface homme/machine à l'utilisateur, pour l'enregistrement d'une donnée propre à l'utilisateur, par exemple sous forme de code propre à l'utilisateur. En outre, à l'étape S15, l'information d'association entre l'identité dérivée IS et l'identité d'origine peut être transmise à une plateforme pour y être mémorisée, cette plateforme pouvant être gérée par exemple par le module de gestion du support d'origine S-GO.

On décrit maintenant des exemples de réalisation plus détaillés, en référence à la figure 2 représentant différentes entités intervenant dans la première phase d'initialisation INIT, ces différentes entités étant reliées par un réseau étendu RE (par exemple l'internet).

La première phase INIT est mise en œuvre pour la génération d'une identité secondaire IS :

- dérivée d'une identité d'origine IO, portée par exemple par un support d'origine SO, et,

- destinée à être mise en place dans un élément de sécurité ES du terminal TER (par exemple stockée dans une mémoire d'un composant de sécurité du terminal mobile communiquant, tel qu'une carte SIM (pour « Subscriber Identity Module »)).

L'association des identités s'effectue en présence des deux supports :

- le support d'identité d'origine SO, et
- l'élément de sécurité ES du terminal, à associer.

A titre d'exemple, le support d'origine SO peut être avantageusement, dans le cadre de la transmission sécurisée d'informations médicales, une carte de type SESAM-VITALE ou carte CPS (pour « Carte de Professionnel de Santé »). Plus généralement toutefois, le support d'origine peut être un document d'identité, un document de gestion de droits d'usage ou un élément de sécurité portant des informations vérifiables concernant son porteur. Typiquement, la carte SESAM-VITALE ou la carte CPS disposent de plusieurs éléments liés à l'identité du porteur et à des droits associés.

L'association des deux supports se déroule comme suit, dans un exemple de réalisation possible.

A l'étape S11 précitée, l'utilisateur U se connecte à un service d'association (par exemple une application web hébergée), auprès d'un serveur d'association S-As sur lequel il s'identifie/authentifie à l'aide du support d'identité d'origine SO.

A cet effet, l'utilisateur U peut utiliser un lecteur LEC du support d'origine SO (soit intégré à un équipement EQ de type ordinateur, soit relié à cet équipement EQ via un port USB), ou encore une borne de lecture de carte santé, un lecteur de carte bancaire, ou autre. Cependant, il doit disposer aussi du terminal communicant TER (téléphone, Smartphone, tablette, ou autre) disposant d'un élément de sécurité ES (carte SIM ou autre), lequel est identifié par la suite comme destinataire futur des données d'identité secondaire IS.

Le serveur d'association S-As lit ou obtient d'un lecteur les données du support d'origine, incluant les données relatives à l'identité d'origine IO du porteur du support d'origine SO, prévues pour le transfert et la génération ultérieurs d'une identité dérivée IS. Il convient toutefois d'indiquer ici qu'une variante de réalisation consiste à préinstaller une application sur le terminal TER, capable de générer elle-même les données d'identité secondaire IS, par exemple à la suite d'une lecture en champ proche (ou « NFC ») de la carte SO par le terminal. En effet, il peut être prévu un transfert en proximité (via un lecteur, une borne, ou un objet) activant une transaction de type sans contact ISO14443 ou NFC (en « champ proche ») par exemple.

A l'étape S12 précitée, le serveur d'association S-As peut avantageusement interroger un serveur de gestion S-GO du support d'origine SO pour vérifier notamment sa validité. Par exemple, les données issues du support d'origine peuvent être transmises par le lecteur précité LEC, par exemple sur requête du serveur d'association S-As, vers le serveur de gestion S-GO pour validation des données et des droits (avantageusement en vue d'une lutte contre la fraude et pour une vérification d'intégrité des données).

Une fois cette vérification effectuée, à l'étape S13, le serveur d'association S-As demande, via une interface du lecteur LEC, la saisie d'une donnée de terminal (par exemple le numéro de téléphone, l'identifiant de la carte SIM, ou autre) permettant une identification ultérieure du terminal TER et son association au support d'origine SO.

Si le lecteur LEC ne dispose pas d'interface de saisie, l'interface de saisie de l'équipement EQ peut être utilisée. Il peut être prévu au cours de cette même opération la saisie et le stockage dans une mémoire du terminal TER de données spécifiques de l'utilisateur U, lequel peut alors disposer de plusieurs moyens d'auto-identification notamment auprès de son terminal personnel TER.

Dans une réalisation possible, afin de vérifier en outre qu'aucune erreur n'a été effectuée dans la saisie du numéro de terminal TER, un message sécurisé peut être communiqué vers le numéro de téléphone qu'a saisi l'utilisateur, ce message contenant par exemple une demande de vérification par l'utilisateur et de renvoi d'un accusé de réception (par exemple le clic d'un choix « ok » dans une fenêtre « pop-up », effectué par l'utilisateur via l'interface homme/machine du terminal TER).

Ensuite, à l'étape S14, à partir des deux informations reçues suivantes :

- la donnée de terminal (carte SIM, numéro de téléphone du terminal TER, ou autre),
- et les données issues du support d'origine SO, incluant l'identité d'origine IO,

le serveur d'association S-As génère au moins une identité dérivée IS (et la stocke en mémoire). Cette identité dérivée IS peut être une transformation et/ou combinaison des deux informations précédentes, ou simplement une transformation de l'identité d'origine IO issue du support SO (par exemple par une fonction de hachage, par chiffrement ou cryptage, ou autre).

Cette identité dérivée IS peut se présenter sous la forme d'un code alphanumérique sans signification particulière afin de garantir un anonymat et optimiser l'entropie de la solution de sécurité.

Dans une forme de réalisation, le serveur d'association S-As génère en outre une donnée propre à l'utilisateur, sous forme de code personnel, propre à l'utilisateur (qui peut par exemple être redéfini

ultérieurement par une saisie personnelle de l'utilisateur). Dans une variante de réalisation, la donnée propre à l'utilisateur est définie, choisie et saisie par l'utilisateur.

Cette identité dérivée et cette donnée propre à l'utilisateur sont stockés ultérieurement (à l'étape S16 détaillée ci-après) dans le terminal TER en référence à une application de type « cardlet » personnalisée (« applet » java exécutée depuis une carte), installée dans le terminal. A ce titre, la présente invention vise aussi un terminal comportant une mémoire MEM stockant notamment des instructions pour exécuter une telle application. Cette application prend en charge ensuite les échanges du terminal TER avec une entité distante de vérification d'identité, pour des services ultérieurs, comme décrit plus loin.

A l'étape S15, l'identité dérivée est également envoyée au serveur de gestion du support d'origine S-GO qui stocke alors en mémoire en association l'identité dérivée et l'identité authentique de l'utilisateur, afin de pouvoir retrouver l'identité d'origine à partir de l'identité dérivée.

L'étape S16 vise, suite à l'installation de l'application « cardlet » précitée dans le terminal TER, à enregistrer l'identité dérivée de cette application dans une mémoire sécurisée de l'élément de sécurité ES. Dans une réalisation, l'identité dérivée est envoyée du serveur d'association S-As vers par exemple une plateforme d'opérateur PF-OP du réseau de télécommunication qu'utilise le terminal, cette plateforme PF-OP qui elle-même est en charge de leur envoi ensuite vers le terminal TER de l'utilisateur. Par exemple, cette plateforme PF-OP envoie un message sécurisé au terminal de l'utilisateur, lequel contient par exemple un lien hypertexte vers l'application et l'identité dérivée, à télécharger dans l'élément de sécurité ES. Lorsque l'utilisateur clique sur ce lien, le téléchargement et l'installation de l'application « cardlet » par exemple dans la carte SIM du terminal peuvent commencer. Il se déroule ensuite les étapes de stockage de l'identité dérivée IS dans une mémoire de l'élément de sécurité ES du terminal et de présentation d'une interface à l'utilisateur par exemple pour visualiser un code défini par la plateforme d'association et qu'il peut modifier pour le personnaliser.

En référence à nouveau à la figure 1, on décrit maintenant un exemple de réalisation des principales étapes de la phase courante VERIF d'identification de l'utilisateur par son terminal.

Sur un équipement EQ connecté pour une transmission sécurisée de données, l'équipement EQ demande à l'utilisateur le numéro d'appel du terminal via une interface homme/machine de l'équipement connecté, et l'équipement transmet ce numéro d'appel à une entité de vérification distante, à l'étape S21.

Cette entité distante contacte le terminal pour lancer une application, à l'étape S22, auprès du terminal, déclenchant les opérations :

- demander à l'utilisateur d'entrer le code personnel via une interface homme/machine du terminal,
- et, en cas de succès dans une vérification du code à l'étape S23 par vérification de concordance entre le code personnel saisi et le code personnel stocké dans les moyens de stockage du terminal ou de l'élément de sécurité de ce terminal, transmettre l'identité dérivée depuis le terminal vers l'entité de vérification.

Comme on le verra dans un exemple de réalisation décrit plus loin en référence à la figure 3, l'entité de vérification peut comporter plusieurs modules ou serveurs distants les uns des autres (incluant dans un mode de réalisation le module d'association S-As de la figure 2).

En cas de succès dans une vérification de l'identité dérivée auprès de l'entité de vérification à l'étape S24, l'entité de vérification valide la vérification d'identité de l'utilisateur pour autoriser une suite dans l'échange de données entre l'équipement EQ et la plateforme de service PF-S. Par exemple, la plateforme de service PF-S peut recevoir de l'entité de vérification une donnée d'état de validation de l'identité vérifiée (étape S25) et générer sur réception de cette donnée d'état une clé de session allouée à la communication avec l'équipement EQ. En complément ou en variante, pour sécuriser davantage les échanges de données entre l'équipement EQ et la plateforme PF-S, cette dernière peut générer une clé de chiffrement des données (par exemple une clé diversifiée associée au service). En effet, les données échangées après l'étape de vérification peuvent être confidentielles, et concerner par exemple des données médicales concernant l'utilisateur. On indique qu'en variante encore, la clé de chiffrement peut être générée par le serveur de gestion du support d'origine S-GO.

Ainsi, après la phase d'enrôlement d'un terminal TER sur la base d'un support d'origine SO, il est proposé l'identification/authentification d'un utilisateur U à partir de ce terminal TER pour l'accès à un service en ligne par exemple (ou à un applicatif quelconque) demandant une identification forte. On utilise préférentiellement une couche de contrôle d'accès liée à l'applicatif ou au service, et dont le rôle est d'assurer une protection des accès à l'applicatif ou au service, ainsi qu'une gestion des relations entre les différents moyens d'authentification.

En référence à la figure 3, à l'étape S21 précitée, l'utilisateur choisit l'un des terminaux dont il dispose (téléphone, tablette, ordinateur, etc.) pour communiquer avec une plateforme de service distante PF-S, ces terminaux ayant bien entendu été enrôlés lors d'une phase d'initialisation comme décrit ci-avant en référence aux figures 1 et 2.

Le terminal TER, disposant d'un élément de sécurité ES, est ici le vecteur de données d'identification/authentification, ce qui permet ainsi de ne pas transmettre d'informations sensibles via l'équipement EQ pouvant être l'objet ou directement le porteur d'un moyen d'attaque.

La plateforme de service PF-S transmet par une couche logicielle appropriée une demande de validation à un serveur d'authentification S-Aut.

Le serveur d'authentification S-Aut contacte le terminal TER pour exécuter, à l'étape S22, un applicatif protégé sur le terminal TER, cet applicatif proposant à l'utilisateur une interface de communication et de saisie de données. Plus particulièrement, le serveur d'authentification S-Aut envoie une sollicitation (message sécurisé) à l'élément de sécurité du terminal TER. Ce message est traité par l'application « cardlet » dans l'élément de sécurité ES du terminal, installée lors de la phase d'initialisation. Il est alors demandé à l'utilisateur de fournir, à l'étape S23, un vecteur d'auto-identification (par exemple le code personnel de l'utilisateur), dont la validité est vérifiée localement sur le terminal.

L'utilisateur répond via l'interface du terminal TER en fournissant l'un des vecteurs d'auto-identification (par exemple le code personnel précité) pour poursuivre les opérations d'authentification.

Si le bon vecteur a été produit par l'utilisateur U à l'étape S23, l'application dans l'élément de sécurité ES renvoie au serveur d'authentification S-Aut un compte-rendu de succès, accompagné de l'identité dérivée IS associée au service.

Le serveur d'authentification S-Aut communique ensuite l'identité dérivée au serveur d'association S-As, qui la vérifie et, en cas de validité de l'identité dérivée, coopère ensuite avec le serveur S-GO de gestion de l'identité d'origine, pour vérifier en outre, à l'étape S24, la non-répudiation de l'identité de l'utilisateur et la validité des droits qui lui sont associés. Le cas échéant, le serveur S-GO retourne la confirmation de la qualité de l'identité d'origine associée à l'utilisateur.

Cette information de validation de l'identité est ensuite remontée par le serveur d'authentification S-Aut vers la plateforme de service PF-S, préférentiellement via une couche logicielle de contrôle d'accès.

Dans le cas où l'identité initiale portée sur le support d'origine doit être partagée avec une plateforme de service, cette dernière dispose préférentiellement, sur la base des informations

reçues, de l'accord de l'utilisateur et d'un moyen de récupérer cette information auprès du serveur de gestion d'identité S-GO.

Sur la base des données de validation, toutes les transactions associées à cet acte peuvent ensuite être signées par exemple par une clé diversifiée (étape S25). Chaque acte peut alors être identifié, permettant ainsi une solution d'audit et de gestion de répudiation basée sur des éléments issus de l'ensemble des parties du système.

Cette clé de signature peut être générée par la plateforme de service PF-S, ou, en variante, par le serveur de gestion du support d'origine S-GO (disposant d'outils techniques à cet effet).

Bien entendu, il est possible pour un utilisateur de se désinscrire du service et configurer son terminal à cet effet, ou encore simplement de changer de terminal et conserver l'accès au service via son nouveau terminal.

Pour une désinscription à l'initiative du gestionnaire du service d'association d'identité, l'opérateur peut arrêter les fonctionnalités d'identification du terminal ou directement les fonctionnalités opérées pendant le service. Il est préférable que l'identité dérivée et éventuellement d'autres informations de personnalisation mémorisées par le terminal soient effacées lors de cette opération.

En outre, le gestionnaire des droits peut invalider les services sans modification nécessaire des informations et applications enregistrées dans le terminal. Sur tentative de vérification d'accès par un utilisateur, les services s'avèrent alors non accessibles.

L'utilisateur peut se désinscrire lui-même d'un service ou invalider une association de son identité à un service. Dans ce cas, il peut lancer une application de désinstallation sur son terminal qui peut par exemple se dérouler comme suit :

- identification de l'utilisateur,
- vérification de la possibilité de gérer ce droit de désinscription auprès d'une plateforme,
- une fois les vérifications effectuées, désinstallation de l'application de vérification d'identité sur le terminal et effacement des références à l'utilisateur sur le ou les serveur(s) distant(s).

Le service ne dispose alors plus d'aucun lien avec l'utilisateur, les identifiants utilisés perdant leur droit d'accès au service. Si l'utilisateur souhaite réutiliser ce service, il peut bien entendu relancer l'étape d'enrôlement initiale.

L'utilisateur peut changer de support matériel. Il peut changer son support d'identité d'origine SO ou changer de terminal portant son identité mobile. Dans les deux cas, l'utilisateur peut se désinscrire par exemple du service, puis recommencer l'étape d'enrôlement de son terminal (le cas échéant son nouveau terminal et/ou, le cas échéant, avec le nouveau support d'origine).

Ainsi, la présente invention permet avantageusement de s'affranchir d'un support tel qu'une carte à puce. Elle permet, pour des applications courantes, de n'utiliser finalement qu'un terminal, notamment un terminal mobile communiquant. L'invention trouve une application avantageuse notamment pour un patient devant fournir une autorisation de transmission de données de son dossier médical à un professionnel de santé donné. Par exemple, le professionnel de santé peut indiquer via un équipement connecté EQ qu'il souhaite récupérer des données concernant Monsieur X. Un message s'affiche par exemple sur le terminal communiquant de Monsieur X en lui demandant s'il autorise une communication de ses données au Docteur Y. S'il répond « oui », il peut lui être demandé d'entrer son code personnel et en cas de succès le terminal envoie l'identité dérivée conformément à l'étape VERIF ci-avant.

Toutefois, dans certaines situations d'urgence, la vérification du code de l'utilisateur peut ne pas être nécessaire, par exemple pour télécharger sur le terminal d'un utilisateur des premières données telles que par exemple son groupe sanguin, ses principales allergies, etc.

Bien entendu, dans certains cas, un terminal peut comporter plusieurs identités dérivées, pour accéder à des services différents ou pour, par exemple, les membres d'une même famille accédant à un service (par exemple pour l'accès au soin, des enfants pouvant être « identifiés » sur le terminal d'un parent).

On décrit ci-après une réalisation avantageuse notamment dans le cadre de services d'urgence, en référence maintenant à la figure 4. Dans une telle réalisation, le terminal TER représenté sur la figure 4 exécute les mêmes étapes que celles décrites ci-avant, une authentification forte étant mise encore en œuvre pour s'assurer que l'utilisateur U du terminal TER est bien titulaire préenregistré du terminal. Dans l'application décrite ci-après à titre illustratif, l'utilisateur U est un urgentiste, par exemple un professionnel de santé, et doit intervenir auprès d'une personne nécessitant des soins d'urgence. Dans l'exemple décrit, la personne nécessitant des soins d'urgence possède un deuxième terminal TERP. A titre illustratif, la personne nécessitant des soins n'est pas en mesure d'utiliser de façon autonome son terminal. L'urgentiste U utilise alors son terminal TER pour :

- obtenir un identifiant ID propre à la personne P, en utilisant le deuxième terminal TERP dans l'exemple représenté sur la figure 4,

- s'identifier ensuite auprès d'une plateforme de service PF-S, en utilisant le terminal TER, et
- transmettre l'identifiant ID propre à la personne P et obtenir en retour des données de la personne P, par exemple des données confidentielles et/ou propres à la personne, en l'occurrence des données d'informations médicales, habituellement confidentielles, de la personne P nécessitant des soins et à laquelle est associé l'identifiant ID.

A cet effet, la personne P pouvant nécessiter des soins est préenregistrée pour un service du type décrit ci-avant. Les données de la personne P précitées peuvent être stockées par exemple auprès d'un espace personnel en ligne ou directement sur un élément de sécurité tel que la carte SIM du terminal TERP (auquel cas néanmoins une plateforme de service intervient encore pour vérifier l'habilitation, à obtenir les données propres à la personne P, identifiée par l'identifiant ID, du porteur du terminal TER ayant sollicité ce service d'urgence). Ainsi, l'urgentiste U est aussi enregistré pour un service de sécurisation d'accès à de telles données. Chaque terminal TER et TERP des personnes U et P comporte une application installée par exemple sur carte SIM pour traiter les opérations décrites ci-après à titre d'exemple.

Dans le cas précité où l'urgentiste U doit accéder à des données propres à la personne P, le terminal TER de l'urgentiste U obtient une donnée d'accès à un service ID-TR, cette donnée d'accès étant propre à la personne P. Cette donnée d'accès est obtenue, dans l'exemple de la figure 4, par interaction et/ou communication avec le terminal TERP de la personne P, par exemple par communication en champ proche (NFC) entre le terminal TERP et le terminal TER. Bien entendu, d'autres réalisations sont possibles. Il peut s'agir d'une lecture de code optique (par exemple un « flash code ») sur un casque de motard ou un véhicule appartenant à la personne P. Il peut s'agir aussi d'une lecture d'étiquette NFC ou RFID prévue pour cette application.

A partir de la donnée d'accès ID-TR obtenue auprès du terminal TER, le terminal TER obtient :

- optionnellement, une adresse d'une plateforme de service d'urgence PF-S auquel l'urgentiste U peut se connecter ensuite avec son terminal TER, et
- un identifiant ID propre à la personne P, par exemple un identifiant de son terminal TERP (identifiant MSISDN par exemple) ou son numéro d'abonné, ou encore un identifiant propre au service d'urgence, via lequel la personne P est enregistrée auprès de la plateforme de service comme ayant requis le service d'urgence permettant la fourniture de données de la personne requérante.

L'identifiant et/ou l'adresse de la plateforme de service sont :

- soit encodées dans la donnée d'accès ID-TR, et dans ce cas obtenues par le terminal TER par décodage de cette donnée d'accès ID-TR ; cet encodage / décodage peut impliquer un chiffrement / déchiffrement;
- soit obtenues par le terminal TER par envoi d'une requête d'interrogation de la plateforme de service d'urgence contenant cette donnée d'accès ID-TR et obtention en retour de l'identifiant ID et/ou l'adresse de la plateforme de service.

Le traitement de la donnée d'accès ID-TR par le terminal TER permet alors au terminal TER de l'urgentiste de se connecter à la plateforme de service avec l'adresse obtenue pour :

- transmettre à la plateforme l'identifiant ID propre à la personne P, pour une vérification par la plateforme que la personne P a bien requis au préalable un tel service d'urgence et/ou est abonnée à un tel service,
- déclencher l'exécution par le terminal TER d'une vérification d'identité de l'urgentiste U par authentification forte, selon le procédé décrit plus haut,
- et, si la vérification est positive, recevoir de la plateforme des données de la personne P, par exemple informations confidentielles sur la personne P, en l'occurrence des données médicales de la personne P, à destination de l'urgentiste qui en a besoin pour de premiers secours (par exemple, dans cette application, des données médicales telles que le groupe sanguin, des allergies à certains anesthésiants, des contrindications avec d'autres traitements médicaux en cours, ou autres).

En outre, il est supposé dans cette application que la personne P nécessitant des soins n'est pas en mesure d'utiliser son terminal TERP, ni d'entrer par exemple un code d'accès pour mettre en service le terminal TERP (code PIN) et passer un appel. Toutefois, typiquement si le code PIN n'est pas entré, il est possible néanmoins de passer des appels vers des numéros d'urgence (souvent à deux ou trois chiffres), dans de nombreux terminaux. Ainsi, l'urgentiste peut saisir un numéro d'urgence sur le terminal TERP de la personne P et communiquer avec une plateforme de service d'urgence pour renseigner notamment un identifiant personnel de l'urgentiste U. La plateforme vérifie dans une base de données que la personne P est bien requérante / abonnée du service d'urgence, par exemple en fonction du numéro d'appelant du terminal TERP. La plateforme retrouve le numéro d'abonné de l'urgentiste U, à partir de son identifiant personnel et contacte l'urgentiste sur son terminal TER pour vérifier son identité par la mise en œuvre de l'étape précitée d'authentification forte de l'urgentiste via son terminal TER. Si cette vérification d'identité est positive, alors la plateforme transmet les données médicales de la personne P à l'urgentiste.

On comprendra de ces différentes variantes que la plateforme de service, sur réception:

- d'une donnée de contact du terminal de l'urgentiste U (par exemple un numéro d'appel sur son terminal TER), et
- d'un identifiant ID propre à la personne P (par exemple un identifiant ID servant à vérifier si la personne est bien enregistrée auprès de la plateforme de service comme ayant requis ce service),

. procède à une vérification d'identité par authentification forte de l'urgentiste U via son terminal TER (préalablement enrôlé), et

. si la vérification est positive, transmet les données de la personne P au terminal de l'urgentiste (ou à tout autre objet communiquant EQ, comme indiqué précédemment).

Le principe de l'invention est généralisable à l'utilisation d'un identifiant ID, relatif à un service, mais non nécessairement propre à une personne. Cet identifiant ID est transmis avec une donnée de contact du terminal TER via le réseau auquel est connecté le terminal (typiquement à la plateforme de service PF-S), et, si la vérification d'identité de l'utilisateur U est validée ultérieurement sur le terminal TER, l'utilisateur peut recevoir alors au moins des données d'informations, fonction de l'identifiant de service ID transmis (par exemple des données médicales de la personne P sur son terminal TER, lorsque l'identifiant ID relatif au service est aussi propre à la personne). L'identifiant ID est ainsi représentatif d'un ensemble de données d'informations à transmettre et il permet donc à la plateforme de service de sélectionner, identifier, obtenir les données d'informations à transmettre au terminal TER. En outre, à une même personne P, peut être associé un ou plusieurs identifiants ID, identifiant chacun un jeu de données d'informations différent : par exemple, un jeu de données médicales, un jeu de données bancaire, etc. Ainsi différentes applications de l'invention sont envisageables selon le contenu du jeu de données d'informations transmis.

Dans une réalisation particulière, le terminal TER peut alors :

- lire l'identifiant ID par interaction avec un objet communiquant (le terminal TERP de la personne P, ou encore une étiquette RFID ou encore un flash code considéré dans ces termes génériques comme un objet communiquant), et
- transmettre l'identifiant ID, pour recevoir, suite à cette transmission et à la validation de vérification d'identité, les données d'informations précitées, fonction de l'identifiant ID.

Toutefois, comme décrit précédemment, l'identifiant ID peut être transmis directement depuis le terminal TERP de la personne P, avec par exemple une donnée d'accès à un service encodant en outre un lien vers une plateforme de service.

Ainsi, dans une réalisation particulière, le terminal TER reçoit une donnée d'accès à un service encodant l'identifiant ID, par interaction avec un objet (étiquette flash code par exemple), cet objet

pouvant être un objet communiquant (tag RFID, ou terminal mobile par interaction NFC). Dans cette réalisation particulière, la donnée d'accès à un service ID-TR permet au terminal TER d'obtenir l'adresse de la plateforme de service et l'identifiant ID.

Le terminal TER transmet alors l'identifiant de service ID à la plateforme de service, pour recevoir, suite à cette transmission et en cas de vérification positive à l'étape courante de vérification d'identité, les données d'informations, fonction de l'identifiant ID transmis.

Dans l'exemple de réalisation de la figure 4, l'objet communiquant précité est un deuxième terminal TERP, apte à communiquer avec le premier terminal TER enrôlé au cours de l'étape préalable d'enrôlement. Par exemple, le premier terminal TER reçoit l'identifiant ID du deuxième terminal TERP par communication en champ proche avec le deuxième terminal, ce qui est avantageux notamment dans le cas où le deuxième terminal TERP appartient à une personne P nécessitant des soins d'urgence, n'étant pas en mesure d'utiliser son terminal TERP, et où le premier terminal TER appartient à un urgentiste U.

La lecture de la donnée d'accès à un service ID-TR sur le premier terminal TER déclenche la connexion du terminal TER de l'urgentiste à la plateforme de service, à laquelle le terminal TER transmet des données de contact du terminal TER (par exemple son numéro d'abonné) et l'identifiant ID (par exemple le numéro d'abonné du terminal TERP si les deux terminaux TER et TERP ont eu une interaction).

Lorsque l'identité de l'utilisateur du terminal TER a été vérifiée par la plateforme de service, la plateforme de service vérifie, par exemple par consultation d'un profil d'utilisateur associé à l'utilisateur authentifié (définissant une ou plusieurs catégories d'utilisateurs auxquelles l'utilisateur authentifié appartient, par exemple : professionnel de santé, sapeur-pompier, ou autres), si au moins une des catégorie d'utilisateurs définies dans le profil utilisateur est habilitée à accéder aux données d'informations identifiées par l'identifiant ID. Dans le cas où l'identifiant ID est propre à une personne P, la plateforme de service vérifie si l'utilisateur du terminal TER est habilité à accéder aux données de cette personne P.

La plateforme valide en outre dans un exemple de réalisation une non-répudiation du service par la personne P (vérification d'aucun signalement d'une perte ou d'un vol du terminal TERP, ou autre).

La plateforme de service sollicite en outre le service d'authentification pour une authentification forte de l'urgentiste U, via par exemple le serveur d'authentification S-Aut de la figure 4. A cet effet, l'urgentiste est sollicité au travers d'une demande de saisie d'informations personnelles sur

son terminal mobile. Comme décrit ci-avant, des plateformes de service de mémorisation d'association S-AS et/ou de gestion de l'identité d'origine S-GO peuvent être consultées optionnellement en tant que de besoin. Si l'urgentiste présumé s'authentifie, mais que l'identité dérivée remontée à la plateforme ne correspond pas à un type d'identité habilité à accéder aux données de la personne P, l'accès lui en est refusé.

Il peut être prévu en outre que le terminal TERP de la personne P soit enrôlé préalablement pour ce service d'urgence (via son élément de sécurité, par exemple sa carte SIM). Par exemple, si l'urgentiste a été authentifié avec succès et qu'il possède l'une des identités habilitées pour accéder aux données d'informations, fonction de l'identifiant ID, la plateforme de service peut transmettre par exemple un message sécurisé (par exemple un message SMS) au terminal TERP, pour activer l'élément de sécurité du terminal TERP. Il peut par exemple s'exécuter sur le terminal TERP une routine de vérification de l'enrôlement du terminal TERP, par exemple en vérifiant un identifiant (ou un secret cryptographique) stocké dans la carte SIM. Dans une telle réalisation, à l'issue de cette vérification, une présentation des données d'informations peut être effectuée par le terminal TERP.

Dans une variante, on peut prévoir l'envoi au terminal TER d'une clé pouvant être à usage unique et permettant à l'utilisateur U du terminal TER d'accéder aux données d'informations, via une plateforme de stockage. Par exemple, la plateforme de service peut transmettre une requête à la plateforme de stockage, pour autoriser un accès aux données d'informations qui sont ensuite présentées à l'utilisateur U du terminal TER dans un navigateur de son terminal TER par exemple.

On a décrit ci-avant une application d'une telle réalisation à la gestion d'une urgence, notamment médicale. Bien entendu, d'autres applications sont possibles. Par exemple, il peut être prévu une application dans laquelle l'identité d'un enfant et d'une personne l'accompagnant est vérifiée par une mise en œuvre de la réalisation décrite en référence à la figure 4. Dans une telle application, une plateforme de service vérifie l'identité de la personne accompagnant l'enfant par une authentification forte sur le terminal de cette personne. D'autres applications sont encore possibles : par exemple la lecture par le terminal TER d'un motif de type flash code, cette lecture pouvant donner droit à un service particulier (entrée dans un cinéma, un théâtre ou autre). Dans une telle application, la lecture du flash code permet de se connecter à une plateforme avec un identifiant de service et, suite à une validation de l'identité du porteur du terminal TER, le porteur peut accéder au service.

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 pluralité de serveurs et une plateforme pour mettre en œuvre l'étape courante de vérification. Dans une réalisation possible, ces différents éléments peuvent être regroupés auprès d'une même plateforme de service, par exemple.

En outre, on a décrit ci-avant la réception de l'identité dérivée auprès du terminal à l'issue de la phase initiale d'enrôlement. On indique toutefois qu'une variante peut consister à exécuter une application préexistante auprès du terminal pour générer l'identité dérivée et la stocker en relation avec un service donné, puis éventuellement la communiquer à un serveur d'association, lié au service.

REVENDICATIONS

1. Procédé pour vérifier une identité d'un utilisateur, comportant :

- une étape préalable (INIT) d'enrôlement d'un terminal de l'utilisateur, comprenant un stockage d'une identité dérivée d'au moins une donnée d'identité authentique de l'utilisateur, dans des moyens de stockage du terminal, en correspondance avec une donnée propre à l'utilisateur, et
- une étape courante (VERIF) de vérification auprès du terminal de l'identité de l'utilisateur, comprenant une authentification forte basée sur l'identité dérivée stockée et sur la donnée propre à l'utilisateur stockée.

2. Procédé selon la revendication 1, caractérisé en ce que l'étape préalable (INIT) d'enrôlement comporte une détermination de l'identité dérivée par combinaison entre :

- la donnée d'identité authentique de l'utilisateur, et
- une donnée de terminal.

3. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape préalable (INIT) d'enrôlement comporte une association entre :

- la donnée d'identité authentique de l'utilisateur, et
- une donnée de terminal,

ladite association étant mémorisée avec des données de contact du terminal via un réseau auquel est connecté le terminal.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape courante de vérification comprend :

- une vérification de concordance entre la donnée propre à l'utilisateur stockée et une donnée propre à l'utilisateur saisie par l'utilisateur au moyen du terminal, et
- une transmission de l'identité dérivée stockée dans le terminal à une entité distante de vérification.

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape courante (VERIF) de vérification d'identité de l'utilisateur, comprend :

* à partir des données de contact du terminal via un réseau auquel le terminal est connecté, un contact du terminal via ledit réseau pour déclencher auprès du terminal une interrogation de l'utilisateur pour demander à l'utilisateur de saisir ladite donnée propre à l'utilisateur,
* une vérification par le terminal de ladite donnée saisie, propre à l'utilisateur,
* la vérification de la donnée propre à l'utilisateur saisie étant positive, une vérification de l'identité dérivée stockée,

* et, la vérification de l'identité dérivée étant positive, une validation de la vérification d'identité de l'utilisateur.

6. Procédé selon l'une des revendications précédentes, dans lequel ladite identité dérivée est stockée dans des moyens de stockage d'un élément de sécurité (ES) du terminal.

7. Procédé selon la revendication 2, dans lequel la mémorisation d'association est mise en œuvre auprès d'un module d'association (S-As), distant du terminal.

8. Procédé selon l'une des revendications précédentes, dans lequel l'identité dérivée est transmise au terminal par une technique de type « Over-The-Air » conjointement avec des données d'une application s'exécutant auprès du terminal au moins pour commander le stockage de l'identité dérivée (IS).

9. Procédé selon la revendication 8, dans lequel la transmission de l'identité dérivée est effectuée via une plateforme (PF-OP) d'un opérateur de réseau de communication auquel est relié le terminal.

10. Procédé selon l'une des revendications précédentes, dans lequel la donnée d'identité authentique de l'utilisateur est fournie, à ladite étape préalable, par lecture (LEC) d'un composant de sécurité d'un support (SO) d'identité de l'utilisateur.

11. Procédé selon l'une des revendications précédentes, dans lequel, pendant ladite étape courante, l'identité dérivée est transmise du terminal vers une entité de vérification distante du terminal, et vérifiée par ladite entité (S24), la vérification de l'identité dérivée étant validée auprès de ladite entité si en outre la donnée propre à l'utilisateur a été vérifiée avec succès par le terminal (S23).

12. Procédé selon la revendication 11, prise en combinaison avec la revendication 7, dans lequel l'entité distante comporte un module d'authentification (S-Aut) coopérant avec au moins ledit module d'association (S-As) pour contrôler l'identité dérivée reçue du terminal pendant l'étape courante.

13. Procédé selon la revendication 12, dans lequel :

- pendant ladite étape préalable :
  * le terminal transmet à un module d'association (S-As), distant du terminal, une donnée de terminal avec la donnée d'identité authentique de l'utilisateur,

* le module d'association détermine une identité dérivée, et communique ladite identité dérivée au terminal,
* sur réception de l'identité dérivée, le terminal exécute une application :
  . d'enregistrement de l'identité dérivée et
  . de présentation d'une interface à l'utilisateur, pour l'enregistrement d'une donnée propre à l'utilisateur,

- pendant ladite étape courante :
  * sur un équipement connecté (EQ) pour une transmission sécurisée de données, l'équipement demande à l'utilisateur une donnée de contact du terminal via une interface homme/machine de l'équipement connecté, et l'équipement transmet ladite donnée de contact à une entité de vérification, distante du terminal,
  * l'entité de vérification distante contacte le terminal pour lancer une application auprès du terminal, déclenchant les opérations :
    . demander à l'utilisateur de saisir la donnée propre à l'utilisateur via une interface homme/machine du terminal (S23), et
    . la vérification de la donnée propre à l'utilisateur étant positive, transmettre l'identité dérivée depuis le terminal vers l'entité de vérification,
  * en cas de succès dans une vérification de l'identité dérivée auprès de l'entité de vérification (S24), l'entité de vérification valide la vérification d'identité de l'utilisateur pour autoriser une transmission de données via l'équipement connecté.

14. Procédé selon la revendication 13, dans lequel, pendant ladite étape préalable :
* le module d'association vérifie ladite information d'identité auprès d'un module de gestion d'identité (S-GO), et
* en cas de vérification positive, le module d'association détermine une identité dérivée, et communique ladite identité dérivée au terminal.

15. Procédé selon l'une des revendications précédentes, dans lequel un identifiant (ID) est transmis avec une donnée de contact du terminal (TER) via un réseau à une plateforme de service, et si la vérification d'identité est positive à l'étape courante, l'utilisateur est autorisé à accéder à des données d'informations, fonction dudit identifiant (ID).

16. Procédé selon la revendication 15, dans lequel le terminal (TER) reçoit, par interaction avec un objet communiquant, une donnée d'accès à un service (ID-TR) encodant ledit identifiant (ID).

17. Procédé selon la revendication 16, dans lequel l'objet communiquant est un deuxième terminal (TERP) à disposition d'un deuxième utilisateur (P), et apte à communiquer avec le premier terminal (TER) enrôlé au cours de ladite étape préalable.

18. Procédé selon l'une des revendications 15 à 17, dans lequel les données d'informations comportent au moins des données propres à un utilisateur (P) de l'objet communiquant.

19. Procédé selon l'une des revendications 15 à 18, dans lequel ledit identifiant (ID) est transmis à une plateforme de service (PF-S), ladite plateforme de service vérifie ledit identifiant (ID) et autorise un accès auxdites données d'informations si la vérification dudit identifiant (ID) est positive.

20. Procédé de sécurisation d'une transmission de données, entre un équipement (EQ) et une plateforme de service (PF-S), comportant une vérification d'identité d'un utilisateur de l'équipement selon ladite étape courante du procédé selon l'une des revendications précédentes, le procédé de sécurisation comportant :

- une transmission des données de contact du terminal à la plateforme de service,
- la mise en œuvre de l'étape courante de vérification d'identité à partir du terminal de l'utilisateur, et
- la vérification d'identité étant positive, une étape pour autoriser une transmission de données entre l'équipement et la plateforme de service.

21. Programme informatique comportant des instructions pour la mise en œuvre d'un procédé selon l'une des revendications précédentes, lorsque ce programme est exécuté par un processeur.

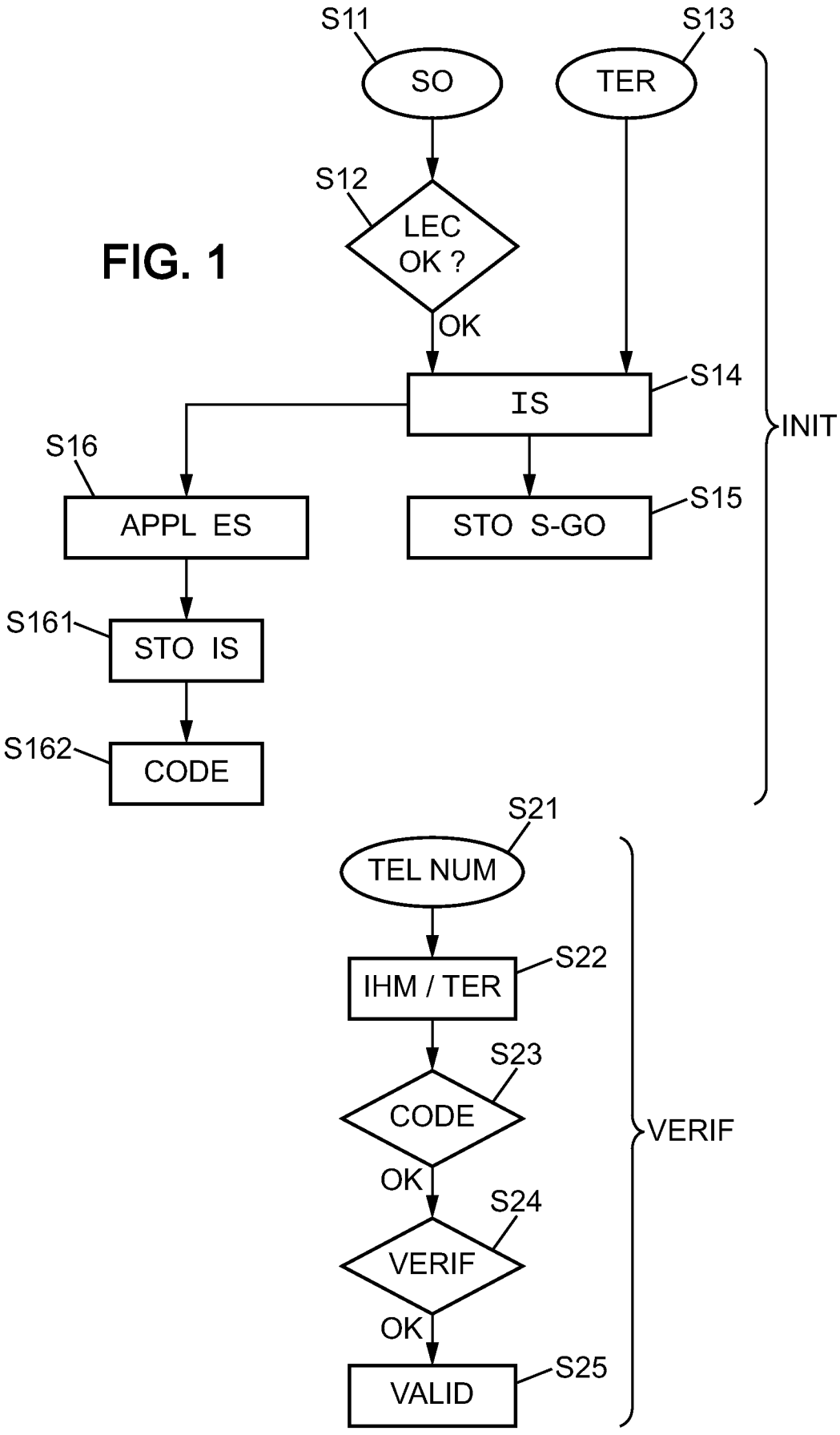
22. Terminal pour la mise en œuvre d'un procédé de vérification d'une identité d'un utilisateur, comportant

- des moyens de stockage (ES, MEM) pour stocker une identité dérivée d'au moins une donnée d'identité authentique de l'utilisateur en correspondance avec une donnée propre à l'utilisateur et
- des instructions de programme informatique pour, lorsque lesdites instructions sont exécutées par un processeur du terminal, sur sollicitation par une entité distante de vérification de ladite identité dérivée:
  - animer une interface homme/machine pour demander à l'utilisateur de saisir ladite donnée propre à l'utilisateur, puis vérifier une concordance de la donnée propre saisie avec la donnée propre stockée,
  - transmettre l'identité dérivée stockée à l'entité distante pour vérification.

23. Entité de vérification pour la mise en œuvre au moins de l'étape courante d'un procédé selon l'une des revendications 1 à 20, comportant des moyens :

- de contact du terminal, via le réseau (RE) précité pour déclencher auprès du terminal une interrogation de l'utilisateur,
- de réception et de vérification de l'identité dérivée (S-Aut, S-As), reçue du terminal, et
- les vérifications de l'identité dérivée et de la donnée propre à l'utilisateur étant positives, de validation de vérification d'identité de l'utilisateur.

FIG. 1


S11
SO
S13
TER
S12
LEC
OK ?
OK
S14
IS
INIT
S16
APPL ES
STO S-GO
S15
S161
STO IS
S162
CODE
S21
TEL NUM
S22
IHM / TER
S23
CODE
VERIF
OK
S24
VERIF
OK
S25
VALID

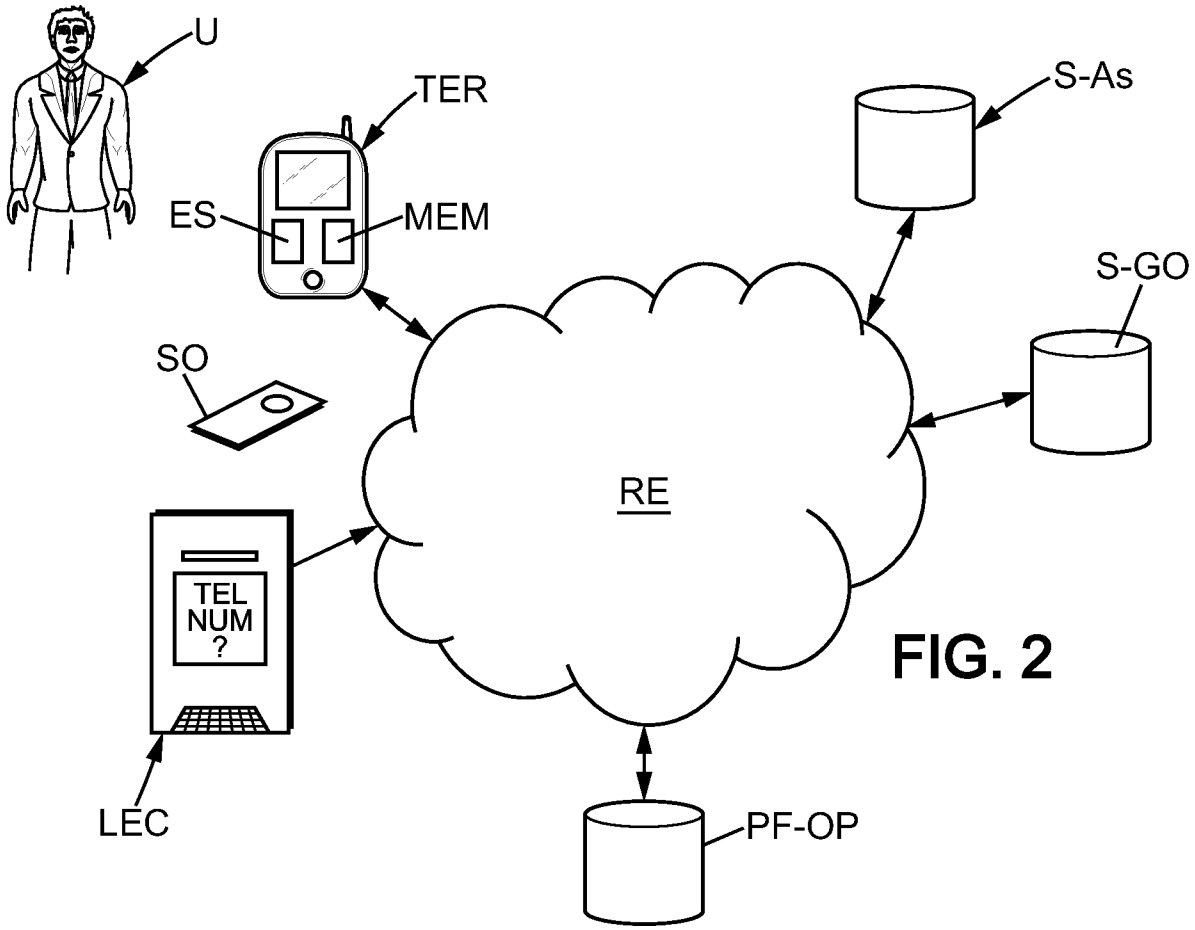

U
TER
S-As
ES
MEM
S-GO
SO
RE
TEL
NUM
?
LEC
PF-OP

FIG. 2

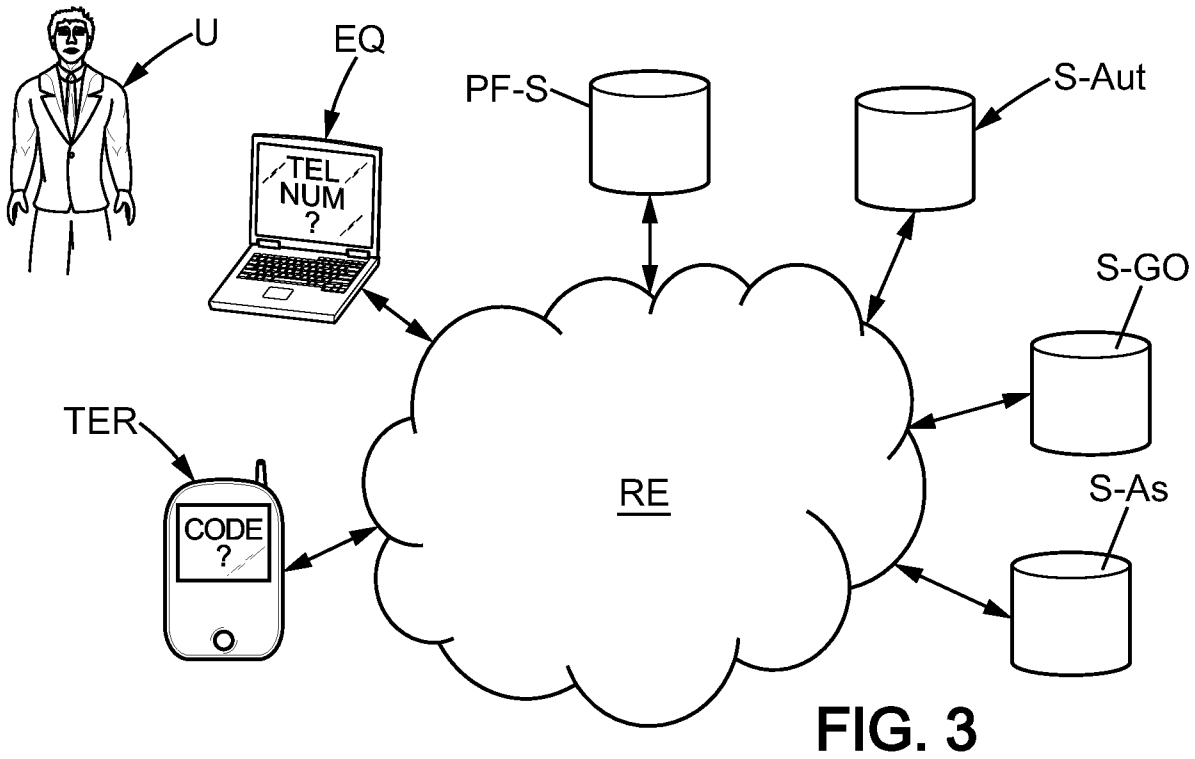

U
EQ
PF-S
S-Aut
TEL
NUM
?
S-GO
TER
RE
CODE
?
S-As

FIG. 3

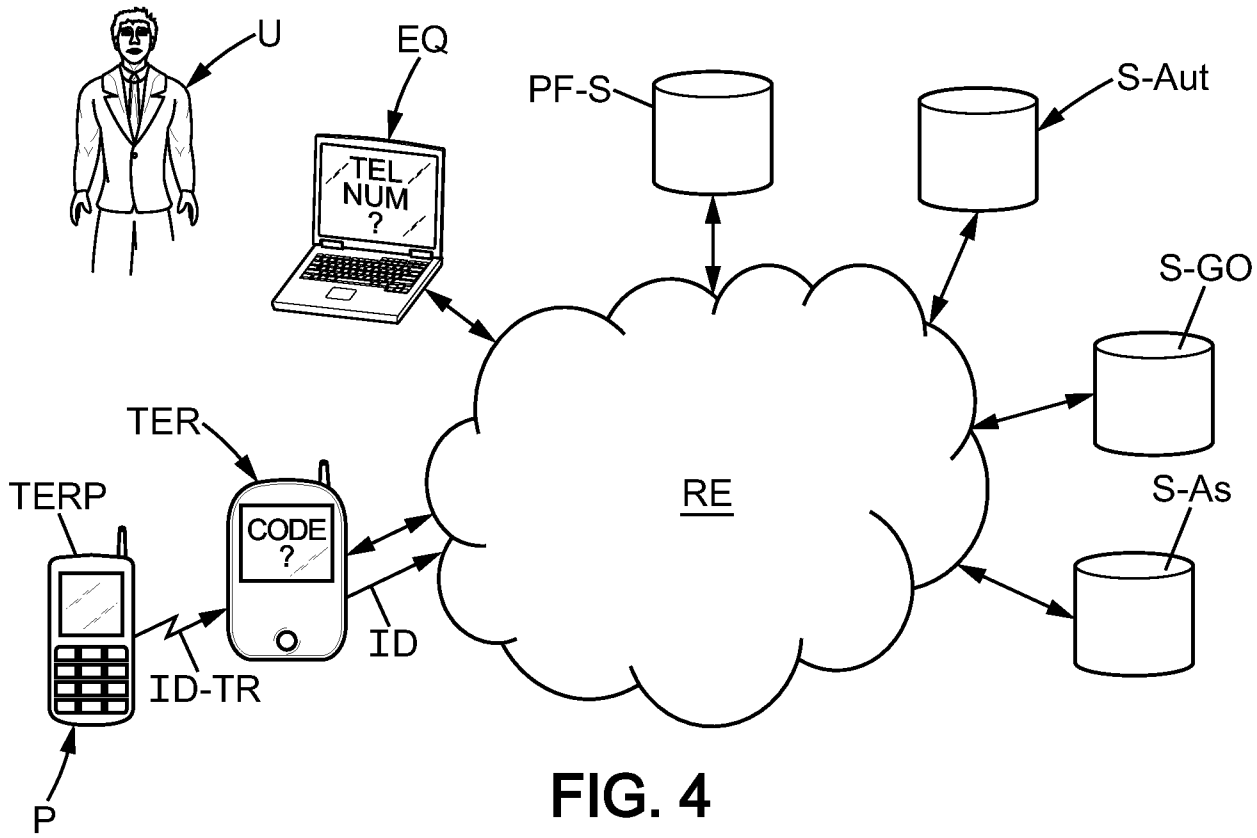


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2013/050218

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32 G06Q20/40
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)
G06Q

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Secure Authentication for Mobile Internet Services", , 31 December 2011 (2011-12-31), XP055043212, Retrieved from the Internet: URL:http://www.idc-informatique.fr/SecureAuthenticationFinal.pdf?PHPSESSID=03ef7d91d6629f98d30195f412fada93 [retrieved on 2012-11-06] abstract chapitres 2.3, 2.4 chapites 3.3, 3.4 chapitre 4.1; the whole document ----- -/--	1-23

[X] 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	Date of mailing of the international search report
25 March 2013	05/04/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dedek, Frédéric

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2013/050218

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KHACHTCHANSKI V I ET AL: "Universal SIM toolkit-based client for mobile authorization system", INTERNATIONAL CONFERENCE ON INFORMATION INTEGRATION AND WEB-BASED APPLICATIONS AND SERVICES, XX, XX, 10 September 2001 (2001-09-10), pages 337-344, XP002282125, abstract chapitres 2-4 -----	1-23

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2013/050218

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/32 G06Q20/40
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)
G06Q

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

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	"Secure Authentication for Mobile Internet Services", , 31 décembre 2011 (2011-12-31), XP055043212, Extrait de l'Internet: URL:http://www.idc-informatique.fr/SecureAuthenticationFinal.pdf?PHPSESSID=03ef7d91d6629f98d30195f412fada93 [extrait le 2012-11-06] abrégé chapitres 2.3, 2.4 chapites 3.3, 3.4 chapitre 4.1; le document en entier ----- -/--	1-23

[X] 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
25 mars 2013	05/04/2013

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	Dedek, Frédéric

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KHACHTCHANSKI V I ET AL: "Universal SIM toolkit-based client for mobile authorization system", INTERNATIONAL CONFERENCE ON INFORMATION INTEGRATION AND WEB-BASED APPLICATIONS AND SERVICES, XX, XX, 10 septembre 2001 (2001-09-10), pages 337-344, XP002282125, abrégé chapitres 2-4 -----	1-23