(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 987 199**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **12 51438**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2013.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.02.12.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 23.08.13 Bulletin 13/34.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *FRANCE TELECOM Société anonyme* — FR et *MORPHO Société anonyme* — FR.

(72) **Inventeur(s) :** GENESTIER PHILIPPE, MOREAU JEROME, GONCALVES LOUIS-PHILIPPE et BENTEO BRUNO.

(73) **Titulaire(s) :** FRANCE TELECOM Société anonyme, MORPHO Société anonyme.

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) SECURISATION D'UNE TRANSMISSION DE DONNEES.

(57) 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'information authentique de l'identité 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

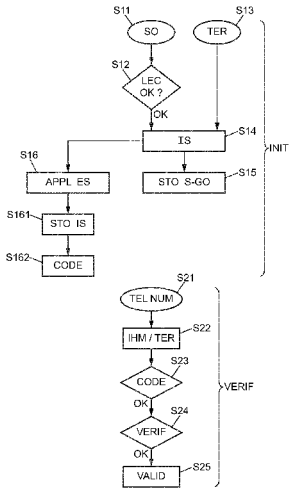
* une détermination d'une identité dérivée au moins de ladite information, stockée en mémoire du terminal, en correspondance d'une donnée propre à l'utilisateur, en vue d'une authentification forte, ultérieure, basée à la fois sur la donnée propre à l'utilisateur et sur l'identité dérivée,

- 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.



FR 2 987 199 - A1

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

- 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.

On entend par « donnée d'information 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.

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 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.

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, 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'information authentique de l'identité 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 les données propres au 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 :

* l'utilisateur transmet à un module d'association, distant du terminal, un numéro d'appel du terminal avec l'information d'identité 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 le numéro d'appel du terminal via une interface homme/machine de l'équipement connecté, et l'équipement transmet ledit numéro d'appel 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.

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, l'étape d'autorisation de la transmission de données entre l'équipement et la plateforme de service peut être 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 du procédé, comportant des moyens de stockage pour stocker l'identité dérivée et des instructions de programme informatique pour, lorsque ces instructions sont exécutées par un processeur du terminal :

- enregistrer une donnée propre à l'utilisateur dans le terminal, en correspondance de l'identité dérivée stockée, et
- sur sollicitation par une entité distante de ladite identité dérivée, animer une interface homme/machine pour demander à l'utilisateur de saisir la donnée propre à l'utilisateur, vérifier une concordance de la donnée saisie avec la donnée enregistrée, et, la vérification étant positive, transmettre l'identité dérivée à l'entité distante.

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.

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, 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'un 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, de type ordinateur (relié à un lecteur 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 les données relatives à l'identité 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 information permettant l'identification et l'association du terminal TER (par exemple le numéro de téléphone, l'identifiant de la carte SIM, ou autre).

Si le lecteur LEC ne dispose pas d'interface de saisie, le terminal TER peut être utilisé pour son interface de saisie. Il peut être prévu au cours de cette même opération la création et le stockage dans une mémoire du terminal TER de données spécifiques de l'utilisateur U, lequel peut alors disposer de plusieurs vecteurs 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 saisies suivantes :

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

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 combinaison des deux informations précédentes, ou simplement une transformation d'une donnée d'identité 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 un code personnel (qui peut par exemple être redéfini ultérieurement par une saisie personnelle de l'utilisateur).

Cette identité dérivée et ce code 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 les données d'association des identités.

L'étape S16 vise, suite à l'installation de l'application « cardlet » précitée dans le terminal TER, à enregistrer les données d'accompagnement de cette application dans une mémoire sécurisée de l'élément de sécurité ES. Dans une réalisation, ces données d'association sont envoyées 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 les données correspondantes, 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 via une interface homme/machine du terminal,
- et, en cas de succès dans une vérification du code à l'étape S23, 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 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).

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 :
  * une association entre :
    - une donnée d'information authentique de l'identité de l'utilisateur, et
    - une donnée de terminal, ledit terminal étant à disposition de l'utilisateur et communiquant via un réseau,

    ladite 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,
- 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 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.

2. Procédé selon la revendication 1, dans lequel ladite identité dérivée est stockée dans des moyens de stockage d'un élément de sécurité (ES) du terminal.

3. Procédé selon l'une des revendications précédentes, dans lequel la mémorisation d'association est mise en œuvre auprès d'un module d'association (S-As), distant du terminal.

4. 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).

5. Procédé selon la revendication 4, dans lequel la transmission de l'identité dérivée est effectuée via une plateforme (PF-OP) d'un opérateur du réseau de communication du terminal.

6. Procédé selon l'une des revendications précédentes, dans lequel la donnée d'information authentique de l'identité 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.

7. 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 auprès du terminal (S23).

8. Procédé selon la revendication 7, prise en combinaison avec la revendication 3, 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.

9. Procédé selon l'une des revendications précédentes, dans lequel le terminal est un terminal de télécommunication et les données de contact du terminal comportent un numéro d'appel du terminal.

10. Procédé selon la revendication 9, dans lequel :

- pendant ladite étape préalable :
  * l'utilisateur transmet à un module d'association (S-As), distant du terminal, un numéro d'appel du terminal avec l'information d'identité 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 le numéro d'appel du terminal via une interface homme/machine de l'équipement connecté, et l'équipement transmet ledit numéro d'appel 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.

11. Procédé selon la revendication 10, 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.

12. 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.

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

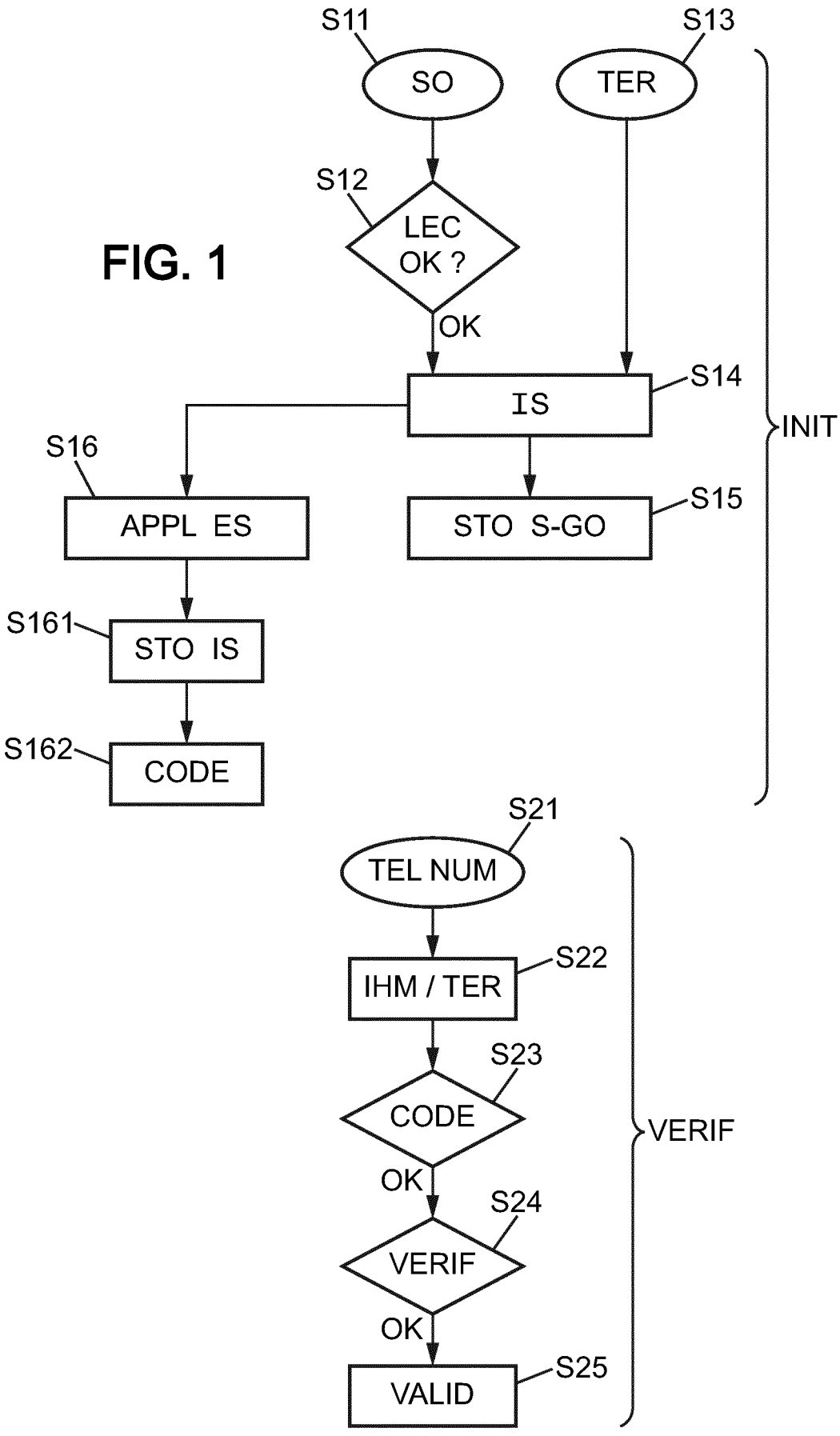
14. Terminal pour la mise en œuvre du procédé selon l'une des revendications 1 à 12, comportant des moyens de stockage (ES, MEM) pour stocker ladite identité dérivée et des instructions de programme informatique pour, lorsque lesdites instructions sont exécutées par un processeur du terminal :

- enregistrer une donnée propre à l'utilisateur dans le terminal, en correspondance de l'identité dérivée stockée, et
- sur sollicitation par une entité distante de ladite identité dérivée, animer une interface homme/machine pour demander à l'utilisateur de saisir ladite donnée propre à l'utilisateur, vérifier une concordance de la donnée saisie avec la donnée enregistrée, et, la vérification étant positive, transmettre l'identité dérivée à l'entité distante.

15. Entité de vérification pour la mise en œuvre au moins de l'étape courante du procédé selon l'une des revendications 1 à 12, 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
S15
STO S-GO
S161
STO IS
S162
CODE
S21
TEL NUM
S22
IHM / TER
S23
CODE
VERIF
OK
S24
VERIF
OK
S25
VALID

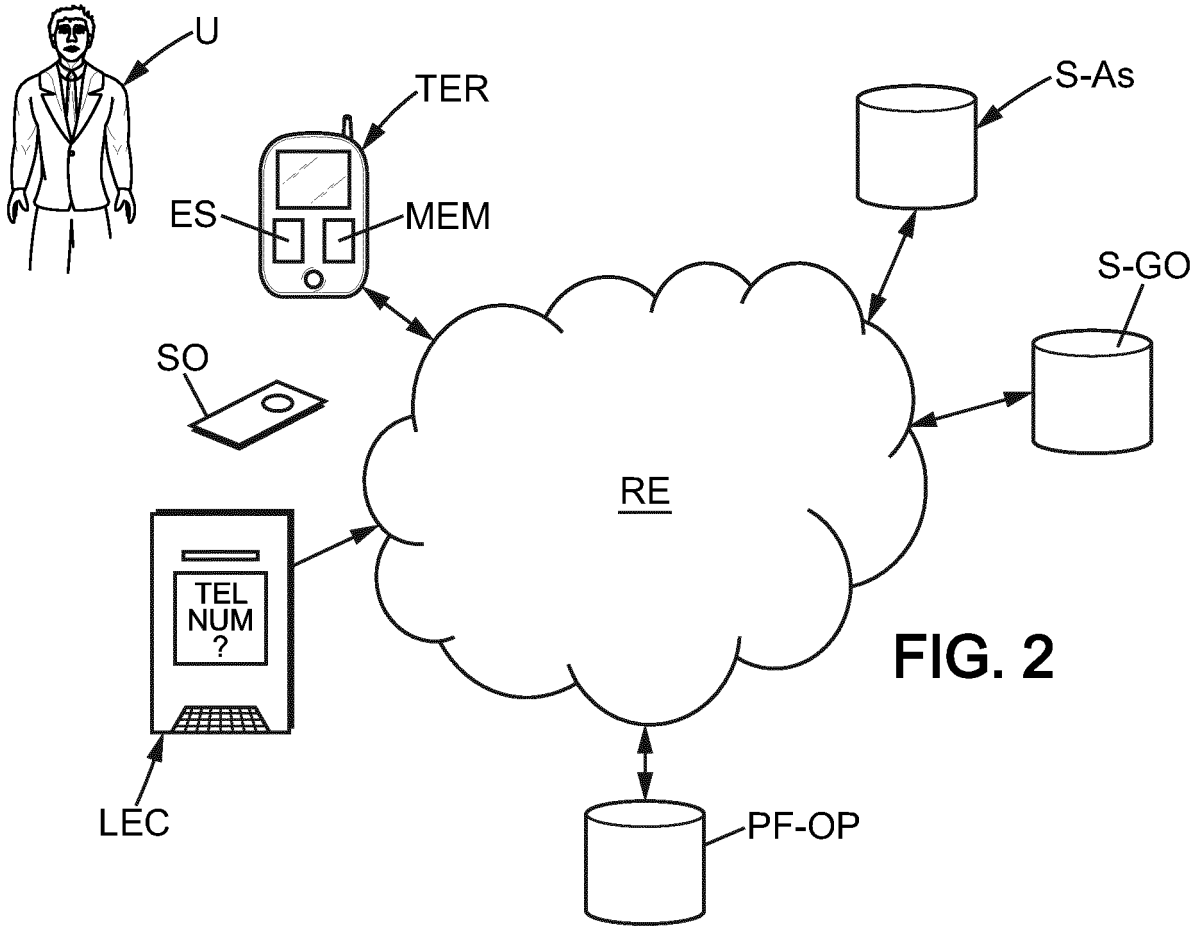

U
TER
S-As
ES
MEM
S-GO
SO
RE
TEL
NUM
?
LEC
PF-OP

FIG. 2

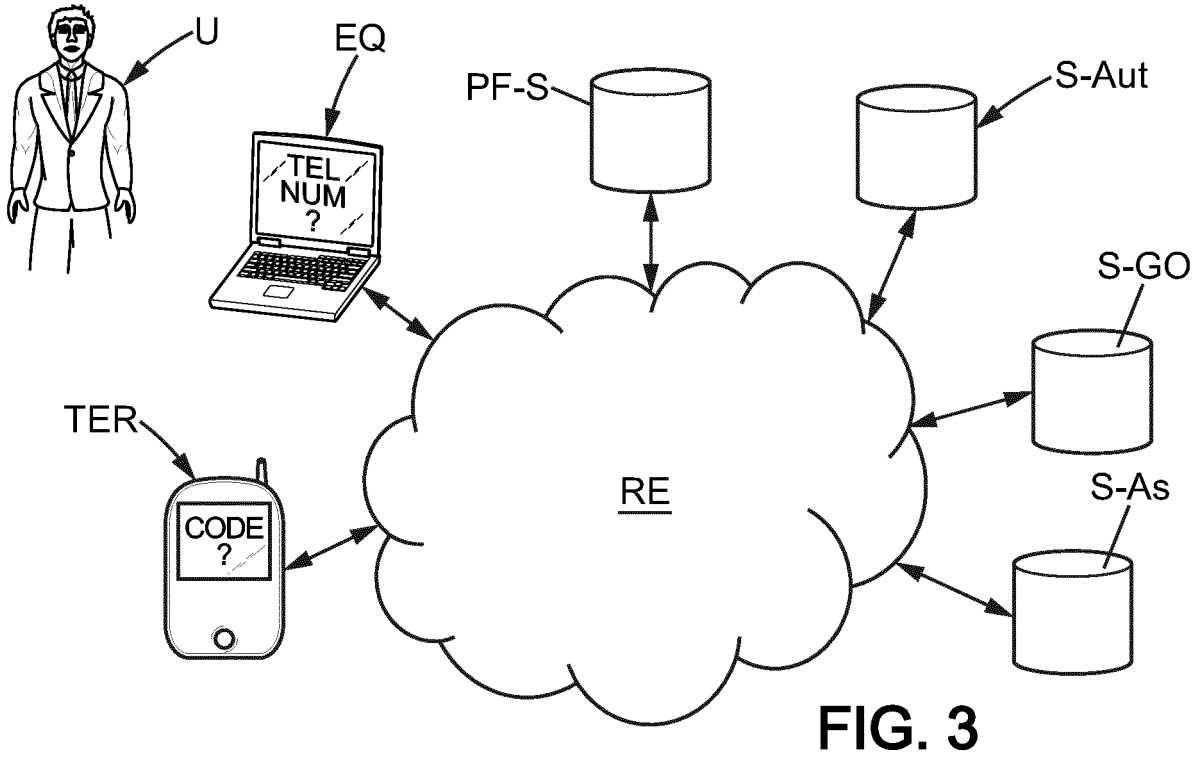

U
EQ
PF-S
S-Aut
TEL
NUM
?
S-GO
TER
RE
CODE
?
S-As

FIG. 3

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 764812
FR 1251438

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	"Secure Authentication for Mobile Internet Services", , 31 décembre 2011 (2011-12-31), XP55043212, 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 * -----	1-15	H04L9/32
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 * -----	1-15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q

Date d'achèvement de la recherche	Examinateur
6 novembre 2012	Dedek, Frédéric

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)