(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 052 006**

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

(21) **N° d'enregistrement national :** **16 54901**

(51) Int Cl[8] : ***H 04 M 1/57*** *(2017.01), H 04 L 29/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 31.05.16.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.12.17 Bulletin 17/48.

(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 :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *ORANGE Société anonyme* — FR.

(72) **Inventeur(s) :** MOHALI MARIANNE et BOUVET BERTRAND.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** ORANGE IMT/OLPS/IPL/PAT Société anonyme.

(54) PROCEDE DE QUALIFICATION DE L'IDENTITE D'UN TERMINAL APPELANT.

(57) La présente invention concerne un procédé de qualification d'identité dans un réseau de communication, comprenant les étapes suivantes: un premier terminal, dit appelant, initie une communication à destination d'un second terminal, dit appelé; et ledit terminal appelé reçoit dans la signalisation d'appel au moins une identité dudit terminal appelant. Ledit procédé est remarquable en ce qu'il comprend en outre les étapes suivantes: le terminal appelé détermine une information de qualification selon laquelle ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance; et le terminal appelé présente à son utilisateur une information représentative de ladite au moins une identité du terminal appelant, accompagnée d'une indication représentative de ladite information de qualification.

FR 3 052 006 - A1

PROCEDE DE QUALIFICATION DE L'IDENTITE D'UN TERMINAL APPELANT

L'invention se rapporte au domaine général des télécommunications.

Elle concerne plus particulièrement le domaine du traitement de la signalisation destinée à initier une communication telle qu'un appel téléphonique, un appel passé dans le cadre d'une vidéoconférence, un message instantané, un message textuel (SMS) ou un message multimédia (MMS), de manière à fournir à l'utilisateur du terminal destinataire (dit « appelé ») des informations concernant l'initiateur de la communication (dit « appelant »).

On notera que dans le cadre de la présente invention, on utilise, aux fins de concision, le terme de « terminal » pour désigner n'importe quel type d'équipement communicant, fixe ou mobile, muni d'un (ou associé à un) moyen d'affichage ou tout autre moyen de restitution (sonore par exemple).

On notera également que les réseaux de communication visés par la présente invention peuvent être de nature très variée : il peut s'agir par exemple de réseaux ISDN (Integrated Service Digital Network), ou de réseaux PSTN (Public Switch Telephony Network), ou de réseaux PLMN (Public Landing Mobile Network), ou encore de réseaux IP (Internet Protocol).

On rappelle en particulier que les services de communication sur réseaux IP sont capables d'identifier des ressources physiques ou virtuelles au moyen de chaînes de caractères telles qu'une « URI » (initiales des mots anglais « *Uniform Resource Identifier* » signifiant « Identifiant Uniforme de Ressource »). La syntaxe des URIs est définie dans le document RFC 3986 de l'IETF (Internet Engineering Task Force) ; la connaissance de l'URI d'une ressource permet d'obtenir l'adresse IP d'un équipement du réseau de l'opérateur gérant cette ressource. Dans la présente description, nous appellerons « URI » tout type d'identifiant de ressource applicative physique ou virtuelle accessible sur un réseau.

Les réseaux IP évolués utilisent des protocoles dits de contrôle de session, qui permettent l'établissement, la modification et la terminaison de sessions multimédia. Ces protocoles utilisent des messages dits de « signalisation », qui permettent à un terminal de demander une connexion avec un autre terminal, de signaler qu'une ligne téléphonique est occupée, de signaler

qu'un téléphone appelé sonne, ou encore de signaler que tel téléphone est connecté au réseau et peut être joint de telle ou telle manière.

Un des protocoles de contrôle de session les plus utilisés est le protocole SIP (initiales des mots anglais « *Session Initiation Protocol* » signifiant « Protocole d'Initiation de Session »). Le protocole SIP a été défini par l'IETF dans les documents RFC 3261, RFC 3265 et RFC 3325, ainsi que leurs évolutions. Dans les réseaux mettant en œuvre le protocole SIP, tels que les réseaux « IMS » (IP Multimedia Subsystem), on distingue deux types d'identifiants de ressource : ceux de la forme « SIP-URI » telle que définie dans la RFC 3261, ou ceux de la forme « tel-URI » telle que définie dans la RFC 3966. Une SIP-URI est de la forme « sip:user@host » (par exemple, sip:alice@domaine1), où la partie « host » identifie le domaine de l'opérateur responsable de l'identité représentée par la partie « user ». Une tel-URI est de la forme « tel:numéro_de_téléphone » (par exemple, « tel:+33123456789 ») en référence aux numéros de téléphone publics internationaux, ou de la forme « tel:numéro_de_téléphone ; phone-context=... » (par exemple, « tel:0623456789 ; phone-context=+33 ») en référence aux numéros de téléphone dont le format n'est valable que dans un contexte plus restreint (dans cet exemple, le format de numéro à dix chiffres « 0623456789 » n'est valable que dans le plan de numérotation français).

Dans l'état de l'art, deux identités du terminal appelant (désignées parfois ci-dessous par « identités de l'appelant » par souci de brièveté) peuvent être véhiculées sur un réseau de communication de bout en bout, à savoir :

- une identité dite « non-certifiée » pouvant être insérée par un appelant, par exemple un terminal ou un PBX, dans le cas où cet appelant n'est pas certifié par un tiers de confiance, et
- une identité dite « certifiée » insérée par un tiers de confiance.

L'opérateur réseau ayant en charge cet appelant constitue, vis-à-vis de l'utilisateur du terminal appelé et des services règlementaires (chargés par exemple des interceptions légales, ou de la traçabilité des appels), un tiers de confiance apte à établir l'identité certifiée et garantissant sa teneur, lors de la transmission de cette identité certifiée via la signalisation jusqu'à l'appelé. Lorsque l'identité certifiée est insérée dans la signalisation par un fournisseur de

service de type OTT (initiales des mots anglais « *Over the Top* »), c'est ce fournisseur qui constitue le tiers de confiance ; on rappelle à cet égard (cf. « Wikipédia ») que l'on appelle « OTT » un service de fourniture de contenus sur Internet sans la participation de l'opérateur de connectivité réseau sous-jacent (comme une compagnie de câble, de téléphone ou de satellite) dans le contrôle ou la distribution dudit contenu. Comme autre exemple, l'identité certifiée peut être insérée dans la signalisation d'appel par un tiers de confiance dans le cadre d'une communication de type « WebRTC ».

Il en résulte, dans tous ces systèmes de communication, que l'identité certifiée ne peut être falsifiée par l'appelant.

L'identité certifiée peut être insérée par exemple dans un champ dédié d'un message de signalisation de la communication. Ainsi, les messages de signalisation du protocole SIP comportent un champ appelé « P_Asserted_Id », qui contient une identité certifiée de l'appelant au sens de l'invention.

Mais cela ne signifie pas que l'identité certifiée est nécessairement destinée à être *présentée* aux utilisateurs des terminaux appelés. En effet, dans de nombreux systèmes de communication, le message de signalisation de la communication véhicule également l'identité non-certifiée, et c'est cette dernière qui est prévue, dans le cadre d'un service de présentation du numéro ou de l'identité de l'appelant, pour être présentée au terminal appelé à la place de l'identité certifiée. Par exemple, les messages de signalisation du protocole SIP comportent un champ « From » dont le contenu représente une identité non-certifiée susceptible d'être présentée sur le terminal appelé dans le cadre d'un service de présentation de l'identité de l'appelant.

De même :

- les messages de signalisation dans les réseaux ISDN contiennent un « NDI » (numéro de désignation de l'installation, certifié), et un « NDS » (numéro de désignation supplémentaire, déclaratif, non-certifié) ;

- les messages de signalisation dans les réseaux PSTN, qui utilisent le protocole de signalisation « ISUP » (ISDN Signaling User Part), ainsi que dans les réseaux PLMN, qui utilisent le protocole de signalisation « BICC » (Bearer Independant Call Control), comprennent un champ appelé « Calling Party Number », dont le contenu représente une identité fournie par le réseau, et donc

certifiée, de l'appelant, et un champ appelé « Generic Number » ou « Additional Calling Party Number », dont le contenu représente une identité déclarative, et donc non-certifiée, de l'appelant.

On distingue dans l'état de l'art plusieurs cas en ce qui concerne le traitement des identités de l'appelant.

Selon un premier cas, le réseau délivre les deux identités de l'appelant jusqu'au terminal/équipement appelé : c'est typiquement le cas des réseaux SIP/IMS.

Dans ce cas toutefois, lorsque le terminal appelé est compatible avec le protocole SIP, il est habituellement configuré « en dur » (« *firmware* » en anglais) pour n'afficher qu'une seule des deux identités. En France par exemple, en réponse à la demande des opérateurs téléphoniques, les terminaux mobiles sont configurés « en dur » de manière à n'afficher que l'identité d'appelant non-certifiée.

La **figure 1** illustre un message d'appel entrant SIP INVITE présenté à la pile SIP d'une passerelle résidentielle. On y voit l'identité de l'appelant non-certifiée (au format SIP URI) dans le champ « From », ainsi que, sous deux formats (SIP-URI, et TEL-URI), l'identité de l'appelant certifiée dans le champ « P-Asserted-Identity ». On notera que, dans le message de la figure 1, les deux identités (certifiée et non-certifiée) sous format SIP-URI sont quasi-identiques, à savoir « sip :(+33)(0)296100432@sip.france.fr » ; toutefois, de manière générale, les identités certifiée et non-certifiée de l'appelant peuvent fort bien être tout-à-fait différentes.

En France, dans une communication sur le réseau fixe de VoIP destinée à une passerelle résidentielle, les deux identités de l'appelant sont fournies à la pile SIP de la passerelle, et cette passerelle est configurée pour n'exploiter que l'identité non-certifiée de l'appelant ; par exemple :

- lorsque l'appelé est un terminal téléphonique analogique connecté à la passerelle à travers une interface FXS, la passerelle insère l'identité de l'appelant non-certifiée dans le champ « Calling Line Identity » du message « Call Setup » engendré pour l'interfonctionnement avec le protocole V.23 utilisé sur l'interface FXS ;

- lorsque l'appelé est un terminal téléphonique sans-fil DECT, la passerelle insère l'identité de l'appelant non-certifiée dans le champ « IPUI » (International Portable User Identity) du message « Call Control Setup » envoyé à la base DECT.

De même, la **figure 2** illustre un message d'appel entrant SIP INVITE destiné à un terminal VoLTE (Voix sur LTE). Dans cet exemple, l'identité d'appelant certifiée (représentée par le contenu du champ « P-Asserted-Identity ») et l'identité d'appelant non-certifiée (représentée par le contenu du champ « From »), qui sont toutes deux au format SIP-URI, se trouvent être identiques — mais encore une fois, ce n'est pas une obligation en général.

Selon un deuxième cas, le réseau ne délivre qu'une seule de ces identités de l'appelant jusqu'au terminal/équipement appelé, et ce, au choix de l'opérateur ayant la charge de l'appelé. C'est notamment le cas sur les réseaux mobiles 2G ou 3G en France.

La **figure 3** illustre un message d'appel entrant présenté en France à un terminal mobile 2G ou 3G par un équipement V-MSC (initiales des mots anglais « *Visited Mobile Switching Center* » signifiant « Centre de Commutation Mobile Visité », qui constitue le dernier nœud réseau avant le terminal appelé). Un tel équipement V-MSC reçoit les deux identités de l'appelant en provenance du réseau amont ; par exemple, dans le cas du protocole ISUP/BICC, l'identité certifiée est contenue dans le champ « Calling Party BCD Number » et l'identité non-certifiée est contenue dans le champ « Generic Number »).

Dans cet exemple, le champ « Calling Party BCD Number », qui transporte toujours l'identité de l'appelant certifiée au niveau de la signalisation réseau *interne*, transporte *au final* l'identité non-certifiée entre l'équipement V-MSC et le terminal appelé.

Plus précisément, l'équipement V-MSC applique la procédure de traitement suivante :

- si l'identité de l'appelant certifiée est identique à l'identité de l'appelant non-certifiée, il n'y a alors pas de changement de l'identité contenue dans le champ « Calling Party BCD Number » ; et

- si l'identité de l'appelant certifiée est différente de l'identité de l'appelant non-certifiée, la signalisation d'appel utilise là aussi le champ « Calling Party

BCD Number » pour transmettre l'identité de l'appelant au terminal appelé ; comme mentionné ci-dessus, ce champ du protocole « Call Control » (protocole de communication entre l'équipement V-MSC et le terminal appelé) est, sémantiquement parlant, l'identité certifiée, mais comme la réglementation en France impose d'afficher l'identité de l'appelant non-certifiée, l'équipement V-MSC insère l'identité de l'appelant non-certifiée dans le champ « Calling Party BCD Number » transmis au terminal appelé.

Les deux cas décrits ci-dessus illustrent le fait que, bien souvent, c'est l'identité non-certifiée, et elle seule, qui est affichée sur le terminal appelé lors de la présentation de l'identité de l'appelant ; comme mentionné ci-dessus, c'est en particulier le cas en France (à cause d'une règlementation qui impose aux centres d'appels offrant un service de démarchage commercial d'insérer dans l'identité non-certifiée l'identité de l'entreprise tierce pour laquelle un centre d'appel appelle, de façon à ce que l'appelé puisse ensuite entrer en contact avec cette entreprise tierce). De plus, l'identité non-certifiée peut être plus compréhensible et exploitable par l'utilisateur, par exemple pour pouvoir rappeler un appelant appartenant à une entreprise sans avoir à passer par le standard de l'entreprise.

Paradoxalement, la plupart des normes recommandent de présenter uniquement l'identité certifiée sur le terminal de l'appelé. De ce fait, les terminaux du marché non contrôlés par un opérateur réseau sont configurés pour présenter (uniquement) l'identité certifiée. Les normes sont toutefois en train d'évoluer pour permettre à un opérateur réseau de configurer les terminaux SIP de manière à ce qu'ils présentent à leurs utilisateurs soit l'identité certifiée, soit l'identité de non-certifiée des appelants.

Quoi qu'il en soit, et quelle que soit la configuration du terminal appelé quant à l'identité de l'appelant à afficher, il n'existe pas dans l'état de l'art de moyen pour indiquer à l'utilisateur du terminal appelé si l'identité du terminal appelant qui lui est présentée est une identité certifiée (par le réseau, ou par un autre tiers de confiance), ou une identité déclarée par le terminal appelant.

La présente invention concerne donc un procédé de qualification d'identité dans un réseau de communication, comprenant les étapes suivantes :

- un premier terminal, dit appelant, initie une communication à destination d'un second terminal, dit appelé, et

- ledit terminal appelé reçoit dans la signalisation d'appel au moins une identité dudit terminal appelant.

Ledit procédé est remarquable en ce qu'il comprend en outre les étapes suivantes :

- le terminal appelé détermine une information de qualification selon laquelle ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance, et

- le terminal appelé présente à son utilisateur une information représentative de ladite au moins une identité du terminal appelant, accompagnée d'une indication représentative de ladite information de qualification.

Ladite information représentative de l'identité peut, par exemple, être un numéro de téléphone, ou un nom associé à ce numéro de téléphone dans la liste de contacts du terminal appelé, ou un nom fourni par le réseau via le service CNIP (Calling Name Identification Présentation).

Grâce à ces dispositions, le client appelé (utilisateur du terminal appelé) peut distinguer les appelants dont l'identité est totalement fiable (certifiée) de ceux pour lesquels il peut y avoir un doute sur l'identité réelle de l'appelant (non-certifiée/déclarative). Ce client appelé peut alors adapter son comportement, par exemple décrocher ou rejeter l'appel ; on peut en outre prévoir un rejet automatique (configurable par exemple via un commutateur ON/OFF sur le terminal) des appels entrants dès lors que l'identité de l'appelant affichée n'est pas certifiée. La présente invention est donc particulièrement avantageuse dans le contexte actuel où le nombre d'appels indésirables sur les réseaux fixe et mobile ne cesse de progresser, de sorte que de plus en plus d'abonnés réclament à leurs opérateurs respectifs de trouver une solution au harcèlement dû à ces appels indésirables.

En ce qui concerne ladite indication selon laquelle l'identité de l'appelant est certifiée ou non par le réseau, on pourra commodément choisir parmi des formes très variées. Selon un premier exemple, ladite indication peut prendre la forme d'un texte ou d'un logo dédié, ou d'une couleur dédiée. Selon un deuxième

exemple, ladite indication peut prendre la forme d'une sonnerie différente selon que l'identité de l'appelant est certifiée ou non-certifiée. Selon un troisième exemple, ladite indication peut prendre la forme d'une activation ou d'une non-activation d'un vibreur du terminal appelé selon que l'identité de l'appelant est certifiée ou non-certifiée.

Selon des caractéristiques particulières, ledit terminal appelé reçoit dans la signalisation d'appel seulement l'identité certifiée, ou seulement l'identité non-certifiée, dudit terminal appelant.

Grâce à ces dispositions, on met les dispositifs de cœur de réseau en conformité avec les normes qui prévoient, comme mentionné ci-dessus, que le terminal de l'appelé ne présentera à son utilisateur qu'une seule identité de l'appelant.

Selon d'autres caractéristiques particulières, ledit terminal appelé reçoit dans la signalisation d'appel à la fois l'identité certifiée et l'identité non-certifiée dudit terminal appelant.

Grâce à ces dispositions, on laisse ouverte la possibilité que les futures normes, ou une règlementation nationale, permettent au terminal de l'appelé de présenter à son utilisateur les deux identités de l'appelant, et donc une information plus complète sur cet appelant.

Selon des caractéristiques encore plus particulières, ledit procédé comprend en outre les étapes suivantes :

- le terminal appelé compare l'identité certifiée avec l'identité non-certifiée du terminal appelant,

- et

- si le terminal détermine que l'identité certifiée du terminal appelant est identique à son identité non-certifiée, le terminal affiche cette identité identique avec une indication de certification, et
- si le terminal détermine que l'identité certifiée du terminal appelant est différente de son identité non-certifiée, le terminal affiche les deux identités, avec une indication de certification accompagnant l'identité certifiée et/ou une indication de non-certification accompagnant l'identité non-certifiée.

Corrélativement, l'invention concerne divers dispositifs.

Elle concerne ainsi, premièrement, un terminal, dit terminal appelé, possédant des moyens pour, lorsqu'il est le destinataire d'une communication initiée par un autre terminal, dit terminal appelant, recevoir dans la signalisation d'appel au moins une identité dudit terminal appelant. Ledit terminal est remarquable en ce qu'il possède en outre des moyens pour :

- déterminer une information de qualification selon laquelle ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance, et
- présenter à son utilisateur une information représentative de ladite au moins une identité du terminal appelant, accompagnée d'une indication représentative de ladite information de qualification.

Selon des caractéristiques particulières, ledit terminal possède en outre des moyens pour, lorsqu'il reçoit dans la signalisation d'appel à la fois l'identité certifiée et l'identité non-certifiée dudit terminal appelant, présenter ces deux identités du terminal appelant.

Selon d'autres caractéristiques particulières, ledit terminal possède en outre des moyens pour déterminer si les identités certifiée et non-certifiée du terminal appelant sont identiques ou non.

L'invention concerne aussi, deuxièmement, un dispositif de cœur de réseau comprenant des moyens pour délivrer à un terminal destinataire d'une communication, dit terminal appelé, au moins une identité d'un terminal, dit terminal appelant, ayant initié ladite communication, ainsi que des moyens pour fournir audit terminal appelé une information de qualification permettant au terminal appelé de déterminer si ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance. Ledit dispositif de cœur de réseau est remarquable en ce que lesdits moyens pour fournir audit terminal appelé une information de qualification comprennent :

- l'ajout à ladite au moins une identité du terminal appelant, dans un champ prévu pour véhiculer une identité du terminal appelant, d'un préfixe ou d'un suffixe dédié, et/ou
- l'ajout d'une extension dédiée dans un champ prévu pour véhiculer une identité du terminal appelant, et/ou
- l'insertion de ladite information de qualification dans un champ de signalisation dédié, et/ou

- l'insertion de ladite au moins une identité du terminal appelant dans un champ sélectionné, parmi une pluralité de champs prévus pour véhiculer une identité du terminal appelant, en fonction de ladite information de qualification.

Ce dispositif de cœur de réseau pourra par exemple, dans le cas d'un réseau mobile 2G ou 3G, être un équipement V-MSC tel que mentionné ci-dessus.

Les avantages offerts par ces divers dispositifs sont essentiellement les mêmes que ceux offerts par les procédés corrélatifs succinctement exposés ci-dessus.

On notera qu'il est possible de réaliser ces dispositifs dans le contexte d'instructions logicielles et/ou dans le contexte de circuits électroniques.

L'invention vise également un système de qualification d'identité dans un réseau de communication, ledit système comprenant :

- au moins un terminal tel que décrit succinctement ci-dessus, et
- au moins un dispositif de cœur de réseau tel que décrit succinctement ci-dessus.

L'invention vise également un programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur. Ce programme d'ordinateur est remarquable en ce qu'il comprend des instructions pour l'exécution des étapes du procédé de qualification d'identité succinctement exposé ci-dessus, lorsqu'il est exécuté sur un ordinateur.

Les avantages offerts par ce programme d'ordinateur sont essentiellement les mêmes que ceux offerts par ledit procédé.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous de modes de réalisation particuliers, donnés à titre d'exemples non limitatifs. La description se réfère aux figures, décrites ci-dessus, qui l'accompagnent, dans lesquelles :

- la figure 1 illustre un message d'appel entrant SIP INVITE présenté à une passerelle résidentielle,
- la figure 2 illustre un message d'appel entrant SIP INVITE présenté à un terminal VoLTE, et

- la figure 3 illustre un message d'appel entrant présenté à un terminal mobile 2G ou 3G.

On va décrire à présent un premier mode de réalisation de l'invention. Dans ce premier mode, on suppose que les deux identités de l'appelant (certifiée, et non-certifiée) sont fournies au terminal appelé.

Dans le cas d'un réseau 2G ou 3G, on pourra prévoir à cet effet que l'équipement V-MSC soit apte à envoyer les deux identités de l'appelant au terminal appelé (contrairement à l'état de l'art, du moins en France). Les dispositifs V-MSC laissent alors passer en transparence les deux identités de l'appelant (reçues de l'amont via ISUP/BICC) vers le terminal appelé via le protocole CC Call Control. Cette disposition permet avantageusement d'avoir un fonctionnement identique entre les réseaux 2G/3G et les réseaux SIP/IMS, et donc des traitements identiques au niveau du terminal appelé quel que soit le réseau d'accès utilisé par ce terminal.

Selon une première variante de ce mode de réalisation, le terminal appelé est configuré pour n'afficher qu'une seule des deux identités de l'appelant (selon le choix de l'opérateur). Il peut s'agir d'une configuration « en dur » (*firmware*), ou d'un comportement dynamique en fonction d'informations disponibles au niveau du terminal, par exemple l'identifiant international du code-pays MCC (Mobile Country Code) et/ou l'identifiant international du code-opérateur MNC (Mobile Network Code). Dans ce cas :

- si c'est l'identité non-certifiée qui a été choisie, le terminal affiche le numéro de téléphone de l'appelant (ou le nom associé à ce numéro de téléphone inscrit dans le carnet d'adresse ou fourni par le réseau via le service CNIP) avec une indication de non-certification (par exemple, la couleur orange), et

- si c'est l'identité certifiée qui a été choisie, le terminal affiche le numéro de téléphone de l'appelant (ou le nom associé à ce numéro de téléphone inscrit dans le carnet d'adresse ou fourni par le réseau via le service CNIP) avec une indication de certification (par exemple, la couleur verte).

Selon une deuxième variante de ce premier mode de réalisation, le terminal appelé est apte à afficher les deux identités de l'appelant. Cette deuxième variante permet, avantageusement, de fournir une plus grande richesse d'information à l'utilisateur de ce terminal.

Dans ce cas, on peut prévoir que le terminal se contente d'afficher l'identité certifiée accompagnée de l'indication de certification, et l'identité non-certifiée accompagnée de l'indication de non-certification. Toutefois, cela pourrait porter à confusion pour l'utilisateur lorsque ces deux identités se trouvent être identiques.

C'est pourquoi l'on prévoira de préférence une étape au cours de laquelle le terminal (que l'on suppose ici muni des moyens nécessaires à cette opération) compare l'identité certifiée avec l'identité non-certifiée de l'appelant. Ensuite :

- si le terminal détermine que l'identité certifiée de l'appelant est identique à son identité non-certifiée, le terminal affiche cette identité avec une indication de certification (par exemple, la couleur verte), et
- si le terminal détermine que l'identité certifiée de l'appelant est différente de son identité non-certifiée, le terminal affiche les deux identités, avec une indication de certification (par exemple, la couleur verte) accompagnant l'identité certifiée et une indication de non-certification (par exemple, la couleur orange) accompagnant l'identité non-certifiée ; cependant, dans ce cas, on peut se contenter de l'indication accompagnant une seule de ces identités, l'autre indication étant dès lors implicite.

On va décrire à présent un deuxième mode de réalisation de l'invention. Dans ce deuxième mode, on suppose qu'une seule identité de l'appelant (soit certifiée, soit non-certifiée) est fournie au terminal appelé.

Le dispositif de cœur de réseau (par exemple, un équipement V-MSC dans un réseau mobile 2G ou 3G) en charge de sélectionner l'identité de l'appelant à délivrer au terminal appelé fournit une information, dite information de qualification, permettant au terminal appelé de déterminer si cette identité de l'appelant est certifiée ou non-certifiée. Voici, à titre d'exemples, quelques moyens possibles pour fournir ladite information de qualification.

Selon une première variante, l'information de qualification est ajoutée dans un champ classique prévu pour véhiculer une identité de l'appelant (par exemple, le champ « Calling Party BCD Number » sur un réseau 2G ou 3G), par exemple :

- en préfixant/suffixant l'identité de l'appelant (par exemple, son numéro de téléphone) avec un caractère spécifique pour indiquer s'il s'agit d'une identité certifiée ou non-certifiée, ou
- en ajoutant une extension : un seul bit suffit pour indiquer la qualification du numéro de téléphone de l'appelant, par exemple 1=certifié, 0=non-certifié.

Selon une deuxième variante, l'information de qualification est insérée dans un champ de signalisation dédié à la mise en œuvre de la présente invention.

Un avantage de ces deux variantes est qu'elles permettent au terminal d'aller chercher l'information de qualification toujours au même endroit dans la signalisation. Toutefois, ces variantes requièrent une modification de la signalisation classique, et donc des dispositifs de cœur de réseau (émettant cette signalisation) ainsi que des terminaux (recevant cette signalisation).

Selon une troisième variante, l'information de qualification est fournie implicitement en envoyant au terminal appelé un seul des deux champs classiques (par exemple, Calling Party BCD Number et Generic Number) prévus pour véhiculer une identité de l'appelant ; ainsi :

- si le terminal appelé reçoit le « Calling Party BCD Number », alors c'est l'identité certifiée qui lui a été fournie, et
- si le terminal appelé reçoit le « Generic Number », alors c'est l'identité non-certifiée qui lui a été fournie.

Un avantage de cette troisième variante est que, après réception du signal d'appel, le terminal n'a plus qu'à afficher l'identité reçue et l'indication de qualification associée. Toutefois, cette troisième variante exige que le terminal soit apte à lire *les deux* champs classiques prévus pour véhiculer une identité de l'appelant ; de plus, cette troisième variante exige que le réseau soit apte à sélectionner le champ à envoyer au terminal (et donc à filtrer l'autre).

Ensuite, le terminal appelé présente à son utilisateur l'identité de l'appelant et, en fonction de la qualification de cette identité qu'il a ainsi déterminée, l'indication de certification correspondante.

On notera que la présente invention peut être mise en œuvre dans les terminaux de façon mixte : par exemple, le terminal appelé pourrait mettre en

œuvre le premier mode de réalisation décrit ci-dessus lorsqu'il se trouve sous couverture VoLTE ou VoWiFi (Voix sur WiFi), et le deuxième mode de réalisation décrit ci-dessus lorsqu'il se trouve sous couverture 2G/3G.

On notera également que l'invention peut être mise en œuvre au sein des nœuds de réseaux de communication, par exemple des terminaux ou des dispositifs de cœur de réseau, au moyen de composants logiciels et/ou matériels.

Les composants logiciels pourront être intégrés à un programme d'ordinateur classique de gestion de nœud de réseau. C'est pourquoi, comme indiqué ci-dessus, la présente invention concerne également un système informatique. Ce système informatique comporte de manière classique une unité centrale de traitement commandant par des signaux une mémoire, ainsi qu'une unité d'entrée et une unité de sortie. De plus, ce système informatique peut être utilisé pour exécuter un programme d'ordinateur comportant des instructions pour la mise en œuvre de l'un quelconque des procédés de qualification d'identité selon l'invention.

En effet, l'invention vise aussi un programme d'ordinateur téléchargeable depuis un réseau de communication comprenant des instructions pour l'exécution des étapes d'un procédé de qualification d'identité selon l'invention, lorsqu'il est exécuté sur un ordinateur. Ce programme d'ordinateur peut être stocké sur un support lisible par ordinateur et peut être exécutable par un microprocesseur.

Ce programme peut utiliser n'importe quel langage de programmation, et se présenter sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations, inamovible, ou partiellement ou totalement amovible, lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comprendre un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de

circuit microélectronique, ou un moyen d'enregistrement magnétique, tel qu'un disque dur, ou encore une clé USB (« *USB flash drive* » en anglais).

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme d'ordinateur selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

En variante, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution de l'un quelconque des procédés de qualification d'identité selon l'invention.

REVENDICATIONS

1. Procédé de qualification d'identité dans un réseau de communication, comprenant les étapes suivantes :

- un premier terminal, dit appelant, initie une communication à destination d'un second terminal, dit appelé, et

- ledit terminal appelé reçoit dans la signalisation d'appel au moins une identité dudit terminal appelant,

caractérisé en ce qu'il comprend en outre les étapes suivantes :

- le terminal appelé détermine une information de qualification selon laquelle ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance, et

- le terminal appelé présente à son utilisateur une information représentative de ladite au moins une identité du terminal appelant, accompagnée d'une indication représentative de ladite information de qualification.

2. Procédé de qualification d'identité selon la revendication 1, caractérisé en ce que ledit terminal appelé reçoit dans la signalisation d'appel seulement l'identité certifiée, ou seulement l'identité non-certifiée, dudit terminal appelant.

3. Procédé de qualification d'identité selon la revendication 1, caractérisé en ce que ledit terminal appelé reçoit dans la signalisation d'appel à la fois l'identité certifiée et l'identité non-certifiée dudit terminal appelant.

4. Procédé de qualification d'identité selon la revendication 3, caractérisé en ce qu'il comprend en outre les étapes suivantes :

- le terminal appelé compare l'identité certifiée avec l'identité non-certifiée du terminal appelant,

- et

- si le terminal détermine que l'identité certifiée du terminal appelant est identique à son identité non-certifiée, le terminal affiche cette identité identique avec une indication de certification, et

- si le terminal détermine que l'identité certifiée du terminal appelant est différente de son identité non-certifiée, le terminal affiche les deux identités, avec une indication de certification accompagnant l'identité certifiée et/ou une indication de non-certification accompagnant l'identité non-certifiée.

5. Terminal, dit terminal appelé, possédant des moyens pour, lorsqu'il est le destinataire d'une communication initiée par un autre terminal, dit terminal appelant, recevoir dans la signalisation d'appel au moins une identité dudit terminal appelant, caractérisé en ce qu'il possède en outre des moyens pour :

- déterminer une information de qualification selon laquelle ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance, et

- présenter à son utilisateur une information représentative de ladite au moins une identité du terminal appelant, accompagnée d'une indication représentative de ladite information de qualification.

6. Terminal selon la revendication 5, caractérisé en ce qu'il possède en outre des moyens pour, lorsqu'il reçoit dans la signalisation d'appel à la fois l'identité certifiée et l'identité non-certifiée dudit terminal appelant, présenter ces deux identités du terminal appelant.

7. Terminal selon la revendication 5 ou la revendication 6, caractérisé en ce qu'il possède en outre des moyens pour déterminer si les identités certifiée et non-certifiée du terminal appelant sont identiques ou non.

8. Dispositif de cœur de réseau, comprenant des moyens pour délivrer à un terminal destinataire d'une communication, dit terminal appelé, au moins une identité d'un terminal, dit terminal appelant, ayant initié ladite communication, ainsi que des moyens pour fournir audit terminal appelé une information de qualification permettant au terminal appelé de déterminer si ladite au moins une identité du terminal appelant est certifiée ou non par un tiers de confiance, caractérisé en ce que lesdits moyens pour fournir audit terminal appelé une information de qualification comprennent :

- l'ajout à ladite au moins une identité du terminal appelant, dans un champ prévu pour véhiculer une identité du terminal appelant, d'un préfixe ou d'un suffixe dédié, et/ou

- l'ajout d'une extension dédiée dans un champ prévu pour véhiculer une identité du terminal appelant, et/ou

- l'insertion de ladite information de qualification dans un champ de signalisation dédié, et/ou

- l'insertion de ladite au moins une identité du terminal appelant dans un champ sélectionné, parmi une pluralité de champs prévus pour véhiculer une identité du terminal appelant, en fonction de ladite information de qualification.

9. Système de qualification d'identité dans un réseau de communication, ledit système comprenant :

- au moins un terminal selon l'une quelconque des revendications 5 à 7, et

- au moins un dispositif de cœur de réseau selon la revendication 8.

10. Programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions pour l'exécution des étapes d'un procédé de qualification d'identité selon l'une quelconque des revendications 1 à 4, lorsqu'il est exécuté sur un ordinateur.

```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:+33296092334@172.20.33.195:5060 SIP/2.0
    Method: INVITE
    Request-URI: sip:+33296092334@172.20.33.195:5060
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 172.20.193.67:5060;branch=z9hG4bKceb44t20a0i0dekln540.1
    To: "De 092334"<sip:+33296092334@sip.france.fr>
    From: "De 100432"<sip:0296100432@sip.france.fr;user=phone>;tag=SDg4ffe01-255055905-1268331609345-
    Call-ID: SDg4ffe01-646301328c818db9bbaf33e54ab04aff-c552s51
    CSeq: 658128513 INVITE
    Max-Forwards: 8
    Content-Length: 257
    Contact: <sip:0296100432@172.20.193.67:5060;transport=udp>
    Content-Type: application/sdp
    Allow: ACK, BYE, CANCEL, INFO, INVITE, OPTIONS, PRACK, REFER, NOTIFY, UPDATE
    Accept: multipart/mixed
    Accept: application/media_control+xml
    Accept: application/sdp
    P-Asserted-Identity: "De 100432"<sip:+33296100432@sip.france.fr>
    P-Asserted-Identity: "De 100432"<tel:+33296100432>
    Privacy: none
    Session-Expires: 86400
    Min-SE: 86400
  Message Body
```

FIG. 1

```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:+33789145220@OSP.NOKIMS.EU;user=phone SIP/2.0
  Message Header
    From: <sip:+33296103701@QZ37.SIP.OFR.COM;user=phone>;tag=05003949270914
    To: <sip:+33789145220@OSP.NOKIMS.EU;user=phone>
    Max-Forwards: 70
    Via: SIP/2.0/UDP  172.20.9.170:5060;branch=z9hG4bK00000080388873217338
    Record-Route: <sip:172.20.9.170:5060;transport=UDP;lr>
    Call-ID: 49fR2574918151PQbcGhEfCeMdk@QZ37.SIP.OFR.COM
    CSeq: 41985 INVITE
    P-Asserted-Identity: <sip:+33296103701@QZ37.SIP.OFR.COM;user=phone>
      SIP PAI Address: sip:+33296103701@QZ37.SIP.OFR.COM;user=phone
        SIP PAI User Part: +33296103701
        SIP PAI Host Part: QZ37.SIP.OFR.COM
        SIP PAI URI parameter: user=phone
    Accept: application/sdp
    Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,PRACK,UPDATE
    P-Charging-Vector: icid-value=4799300104-1215-18495702;icid-generated-at=QZ37.SIP.OFR.COM;orig-ioi=SIP.OFR.COM
    P-Early-Media: supported
    Supported: 100rel,precondition,histinfo
    Content-Type: application/sdp
    Contact: <sip:172.20.9.170:5060;transport=UDP>
    Content-Length:  566
  Message Body
    Session Description Protocol
```

FIG. 2

```
⊞ MTP 3 User Adaptation Layer
⊞ Signalling Connection Control Part
⊞ Radio Access Network Application Part
⊟ GSM A-I/F DTAP - Setup
  ⊞ Protocol Discriminator: Call Control; call related SS messages (3)
    00.. .... = Sequence number: 0
    ..00 0101 = DTAP Call Control Message Type: Setup (0x05)
  ⊞ Bearer Capability 1 - (Full rate support only MS/fullrate speech version 1 supported)
  ⊞ Progress Indicator
  ⊟ Calling Party BCD Number - (33296103701)
      Element ID: 0x5c
      Length: 8
      0... .... = Extension: Extended
      .001 .... = Type of number: International Number (0x01)
      .... 0001 = Numbering plan identification: ISDN/Telephony Numbering (ITU-T Rec. E.164 / ITU-T Rec. E.163) (0x01)
      1... .... = Extension: No Extension
      .00. .... = Presentation indicator: Presentation allowed (0x00)
      ...0 00.. = Spare bit(s): 0
      .... ..11 = Screening indicator: Network provided (0x03)
      Calling Party BCD Number: 33296103701
      BCD Digits: 33296103701
```

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 828542
FR 1654901

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	EP 1 294 157 A2 (HEWLETT PACKARD CO [US]) 19 mars 2003 (2003-03-19) * alinéas [0027] - [0057]; figures 1-4 *	1,2,5, 8-10	H04M1/57 H04L29/06
X	WO 2016/072736 A1 (LG ELECTRONICS INC [KR]) 12 mai 2016 (2016-05-12) * alinéas [0040] - [0168]; figures 1-9 *	1,2,5, 8-10	
X	US 2008/181379 A1 (CHOW STANLEY TAIHAI [CA] ET AL) 31 juillet 2008 (2008-07-31) * alinéas [0023] - [0048]; figures 1-6 *	1-10	
X	US 2015/236857 A1 (FELTHAM ANDREW S [GB] ET AL) 20 août 2015 (2015-08-20) * alinéas [0034] - [0051]; figures 2-4 *	1,3-7,10	
X	US 2008/084975 A1 (SCHWARTZ RONALD [CA]) 10 avril 2008 (2008-04-10) * alinéas [0031] - [0335]; figures 1-20 *	1-3,5, 8-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04M

Date d'achèvement de la recherche: 2 mars 2017

Examinateur: Agreda Labrador, A

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1654901 FA 828542

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 02-03-2017
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1294157 A2	19-03-2003	DE 60207500 D1	29-12-2005
		DE 60207500 T2	06-07-2006
		EP 1294157 A2	19-03-2003
		GB 2379829 A	19-03-2003
		US 2003051133 A1	13-03-2003
WO 2016072736 A1	12-05-2016	AUCUN	
US 2008181379 A1	31-07-2008	CN 101595708 A	02-12-2009
		EP 2132916 A2	16-12-2009
		US 2008181379 A1	31-07-2008
		WO 2008093306 A2	07-08-2008
US 2015236857 A1	20-08-2015	US 2015236857 A1	20-08-2015
		US 2015237201 A1	20-08-2015
		US 2016135051 A1	12-05-2016
US 2008084975 A1	10-04-2008	AUCUN	

EPO FORM P0465