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

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 juillet 2014 (31.07.2014)

WIPO | PCT

(10) Numéro de publication internationale
WO 2014/114871 A1

(51) Classification internationale des brevets : *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2014/050110

(22) Date de dépôt international : 21 janvier 2014 (21.01.2014)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1350560 22 janvier 2013 (22.01.2013) FR

(71) Déposant : **ORANGE** [FR/FR]; 78 rue Olivier de Serres, F-75015 Paris (FR).

(72) Inventeurs : **MOUQUET, Antoine**; 9 avenue Puvis de Chavannes, Appartement 220, F-92400 Courbevoie (FR). **RENARD, Laurent**; 21 rue Etienne Ganneron, F-77600 Bussy Saint Georges (FR).

(74) Mandataire : **ORANGE/IMT/OLPS/IPL/PAT**; COCHET Bertrand, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

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

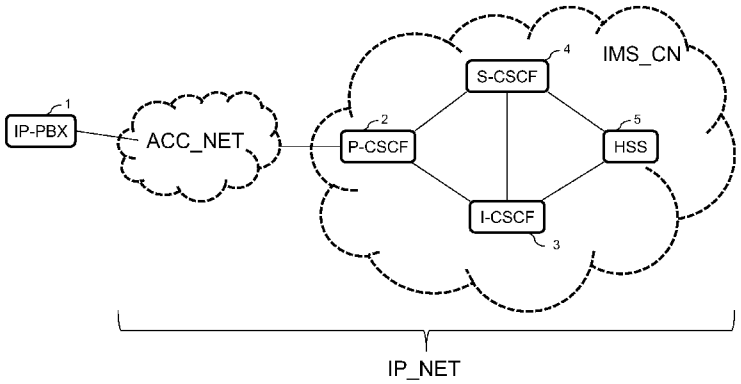
(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,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

[Suite sur la page suivante]

(54) Title : REGISTRATION OF A CLIENT DEVICE BY WAY OF AN AGENT SERVER IN A COMMUNICATION NETWORK

(54) Titre : ENREGISTREMENT D'UN EQUIPEMENT CLIENT PAR L'INTERMEDIAIRE D'UN SERVEUR MANDATAIRE DANS UN RESEAU DE COMMUNICATION

Fig. 1



(57) Abstract : The invention relates to a method of registration of a client device (1) with a registration server (4) of a communication network (IP_NET), by means of at least one registration request (REG_REQ) transmitted (17) by at least one agent server (2) of the communication network to a registration server (4) of the communication network, the method comprising the following steps, carried out by said at least one agent server (2) of the network: obtaining (13) of at least one identification datum (ID) of the client device in the network, on the basis of authentication data received (12) from said client device during a phase of authentication of said client device; and formulation (15) of the registration request (REG_REQ) of the client device, in which is inserted said at least one identification datum of the client device in the network. The invention also relates to an agent server (2) implementing the abovementioned method of registration and finds a particular application within the framework of the registration of a telephone routing device (PABX IP) in an IMS network, when this device does not have the capacity to register itself on its own or does not use this registration functionality when it does have it.

(57) Abrégé :

[Suite sur la page suivante]

WO 2014/114871 A1

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii))*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii))*

Publiée :

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

L'invention concerne un procédé d'enregistrement d'un équipement client (1) auprès d'un serveur d'enregistrement (4) d'un réseau de communication (IP_NET), au moyen d'au moins une requête d'enregistrement (REG_REQ) transmise (17) par au moins un serveur mandataire (2) du réseau de communication à un serveur d'enregistrement (4) du réseau de communication, le procédé comprenant les étapes suivantes, réalisées par ledit au moins un serveur mandataire (2) du réseau: obtention (13) d'au moins une donnée d'identification (ID) de l'équipement client dans le réseau, à partir de données d'authentification reçues (12) dudit équipement client lors d'une phase d'authentification dudit équipement client; et élaboration (15) de la requête d'enregistrement (REG_REQ) de l'équipement client, dans laquelle est insérée ladite au moins une donnée d'identification de l'équipement client dans le réseau. L'invention concerne également un serveur mandataire (2) mettant en œuvre le procédé d'enregistrement susmentionné et trouve une application particulière dans le cadre de l'enregistrement d'un équipement d'acheminement téléphonique (PABX IP) dans un réseau IMS, lorsque cet équipement n'a pas la capacité de s'enregistrer lui-même ou n'utilise pas cette fonctionnalité d'enregistrement quand il en dispose.

Enregistrement d'un équipement client par l'intermédiaire d'un serveur mandataire dans un réseau de communication

La présente invention concerne l'enregistrement d'équipements clients au sein d'un réseau de communication, et plus particulièrement l'enregistrement d'équipements de type IP-PBX dans un réseau IP comprenant un cœur de réseau disposant d'une architecture IMS (pour IP Multimedia System).

Lorsque l'on souhaite qu'un équipement client bénéficie des services offerts par un réseau de communication, il est habituellement nécessaire que cet équipement client s'enregistre auprès de ce réseau.

C'est en particulier la cas lorsque le réseau de communication est un réseau IP (i.e. un réseau utilisant le protocole IP) comprenant un réseau d'accès (de type ADSL, xDSL, WiFi, WiMAX, GSM, UMTS ou LTE, par exemple) associé à un cœur de réseau IMS, c'est-à-dire un cœur de réseau présentant une architecture de réseau IMS telle qu'introduite par l'organisme de normalisation 3GPP (« *3rd Generation Partnership Project* ») pour les réseaux mobiles, puis reprise par l'organisme TISPAN (« *Telecommunications and Internet Converged Services and Protocols for Advanced Networking* ») pour les réseaux fixes. L'architecture de réseau IMS permet notamment l'établissement dynamique et le contrôle de sessions multimédia entre deux clients ainsi que la réservation des ressources au niveau du réseau de transport des flux multimédias. Grâce à cette architecture, les opérateurs réseau peuvent commodément mettre en œuvre une politique de gestion, fournir une Qualité de Service prédéterminée, et calculer les montants à facturer aux clients. L'architecture IMS permet actuellement d'accéder à des services de type téléphonie, visiophonie, Présence et Messagerie Instantanée, dont elle gère aussi l'interaction.

Une telle architecture de réseau IMS comprend notamment :

- un ou plusieurs serveurs d'enregistrement, appelés « S-CSCF » (pour Serving-Call Server Control Function) aptes (entre autres fonctions) à gérer la procédure d'enregistrement des dispositifs connectés au réseau ;

- un ou plusieurs serveurs d'interrogation, appelés « I-CSCF » (pour Interrogating-Call Server Control Function) et d'ailleurs souvent combinés physiquement avec les serveurs de type S-CSCF pour constituer des serveurs dénotés « I/S-CSCF », qui, au moment de l'enregistrement d'un équipement client, interrogent un serveur d'abonnés appelé « HSS » (pour Home Subscriber Server), afin de pouvoir sélectionner un serveur S-CSCF possédant les caractéristiques requises pour atteindre le niveau de service souscrit

par l'utilisateur ;

- un ou plusieurs serveurs HSS, contenant chacun une base de données-clients. Chaque serveur HSS contient le « profil » d'un certain nombre d'équipements clients du réseau, ce profil comprenant leur état d'enregistrement, des données d'authentification et de localisation, et les services souscrits ;

- un ou plusieurs serveurs mandataires (aussi appelés serveurs « proxy »), désignés par « P-CSCF » (pour Proxy-Call Server Control Function), servant d'entité de raccordement entre le cœur de réseau IMS et le réseau d'accès utilisé par les équipements clients, et qui sont donc aptes à retransmettre tous les messages de signalisation entre les équipements clients d'une part et les serveurs S-CSCF ou I-CSCF d'autre part. Ces messages de signalisation sont notamment des messages selon le protocole SIP, tel que défini par l'IETF (*Internet Engineering Task Force*) dans le document RFC 3261, lequel permet l'établissement, la modification et la terminaison de sessions multimédia dans un réseau utilisant le protocole IP.

Ainsi, l'équipement client souhaitant s'enregistrer auprès d'un tel réseau IP envoie habituellement un message « SIP REGISTER » contenant des informations d'identification vers un serveur P-CSCF, lequel relaie ce message vers un serveur I-CSCF qui, après vérification auprès d'un serveur HSS, retransmet ce message d'enregistrement vers le serveur S-CSCF approprié afin que ce dernier procède à l'enregistrement de l'équipement client.

Il existe cependant des cas où des équipements clients n'ont pas la capacité de s'enregistrer (par exemple parce qu'ils supportent le protocole SIP mais pas l'architecture IMS) ou, s'ils ont cette capacité, ne l'utilisent pas. C'est notamment le cas de certains équipements d'acheminement téléphonique privés, désignés par « PABX IP » (« IP-PBX » en anglais), utilisés par des entreprises pour raccorder un ensemble de terminaux internes au réseau téléphonique.

Actuellement, deux modes de raccordement d'un équipement PABX IP à un réseau IMS sont normalisés par l'organisme TISPAN :

1) Le mode "Peering-based business trunking" : l'équipement PABX IP est alors considéré par l'opérateur comme étant un réseau tiers et raccordé à une passerelle IBCF (Interconnection Border Control Functions). Ce premier mode de raccordement pose cependant des problèmes pour raccorder un grand nombre de petits équipements PABX IP (c'est-à-dire les PABX IP gérant un faible nombre d'extensions), car la passerelle IBCF n'a pas été prévue pour raccorder des clients mais des gros réseaux, et la configuration

est fastidieuse.

2) Le mode "Subscription-based" : l'équipement PABX IP est alors considéré par le réseau comme un terminal IMS. Ce deuxième mode de raccordement est certes plus facile à gérer pour l'opérateur, notamment pour les petits équipements PABX IP. Cependant, ce deuxième mode de raccordement implique que l'équipement PABX IP doit s'enregistrer auprès du réseau IMS comme un terminal normal. Or de nombreux équipements PABX IP disponibles sur le marché ne supportent pas l'enregistrement, car ils sont en conformité avec une option de la recommandation « SIPconnect » du SIP Forum, appelée « Static mode ».

Des travaux sont actuellement en cours au 3GPP, sous le thème de travail "Feasibility study on IMS Business Trunking for IP-PBX in Static Mode of Operation", pour faire évoluer l'architecture IMS de façon à permettre le raccordement d'équipements PABX IP ne supportant pas l'enregistrement, tout en minimisant l'effort de configuration (« provisioning » en anglais). Dans le cadre de ces travaux, le rapport technique TR 23.897 v0.4.0 décrit, dans la clause 6.4 du TR 23.897, une solution basée sur une évolution du serveur P-CSCF pour raccorder à ce dernier des équipements PABX IP ne supportant pas l'enregistrement.

Un inconvénient majeur de cette solution est qu'elle requiert que les données de chaque équipement PABX IP (en particulier les adresses IMS publique et privée de ces PABX IP) soient préconfigurées dans un serveur P-CSCF, avant que ce serveur P-CSCF puisse initier une quelconque procédure d'enregistrement IMS pour le compte de ces équipements PABX IP. Ceci implique un effort important de configuration, puisqu'il faut intervenir (éventuellement manuellement) au niveau du serveur P-CSCF pour chaque ajout d'un nouveau client. Cette situation est problématique notamment quand il faut fournir un service de type "business trunking" à un nombre important de petits équipements PABX IP, puisque l'ajout d'un nouvel équipement PABX IP est fréquent dans ce cas.

De plus, pour permettre une plus haute disponibilité de service, il est recommandé de mettre en place une redondance au niveau du serveur P-CSCF, afin qu'en cas de défaillance d'un serveur P-CSCF, un autre serveur P-CSCF puisse prendre le relai. Ceci nécessite alors que les données des équipements PABX IP soient préconfigurées dans deux serveurs P-CSCF (voire plus), ce qui multiplie d'autant plus l'effort de configuration de ces serveurs.

La présente invention a pour objet de remédier aux inconvénients susmentionnés, en proposant une gestion de l'enregistrement d'un équipement client au niveau d'un équipement mandataire du réseau ne nécessitant aucune configuration particulière liée à cet équipement client au niveau de l'équipement mandataire.

Elle propose à cet effet un procédé d'élaboration d'une requête d'enregistrement d'un équipement client dans un réseau de communication, mis en œuvre par au moins un serveur mandataire dudit réseau, comprenant l'obtention d'au moins une donnée d'identification de l'équipement client dans le réseau, à partir de données d'authentification de cet équipement client reçues lors d'une phase d'authentification de cet équipement client, et l'élaboration de la requête d'enregistrement de l'équipement client, dans laquelle est insérée la au moins une donnée d'identification de l'équipement client dans le réseau. Ceci permet au serveur mandataire de déclencher l'enregistrement de l'équipement client dans le réseau, pour le compte de cet équipement client, sans avoir besoin de préconfigurer localement le serveur mandataire avec des données d'identification de cet équipement client, et ce de manière transparente aussi bien pour l'équipement client que pour le serveur d'enregistrement du réseau. Permet d'éviter également des enregistrements en masse lors du démarrage du serveur mandataire, ce qui est le cas lorsque ce dernier est préconfiguré localement.

Selon une caractéristique particulière, le procédé comprend en outre la configuration préalable dudit au moins un serveur mandataire, cette configuration préalable comprenant la mémorisation, dans ledit au moins un serveur mandataire, d'une règle de dérivation permettant de déduire la au moins une donnée d'identification de l'équipement client à partir d'au moins une partie des données d'authentification de cet équipement client, cette règle étant utilisée pour obtenir la au moins une donnée d'identification. Il est ainsi possible de configurer certains serveur mandataires du cœur de réseau pour la mise en œuvre de l'invention, et ce une fois pour toute. N'importe quel serveur mandataire du cœur de réseau peut être ainsi configuré, ce qui offre un gain en termes de flexibilité et de résilience.

Selon un mode de réalisation particulier, les données d'authentification de l'équipement client comprennent un identifiant de domaine associé à l'équipement client, ladite au moins une donnée d'identification comprenant au moins un identifiant parmi un identifiant public de l'équipement client dans le réseau de communication et un identifiant privé de l'équipement client dans le réseau de communication, généré à partir dudit identifiant de domaine.

Dans un autre mode de réalisation particulier dans lequel les étapes d'obtention et d'élaboration sont réalisées par plusieurs serveurs mandataires, une donnée d'identification unique d'instance est avantageusement obtenue en outre à partir des données d'authentification reçues dudit équipement client, cette donnée d'identification unique d'instance étant insérée dans les requêtes d'enregistrement élaborées par les serveurs mandataires. L'utilisation de plusieurs serveurs mandataires pour l'enregistrement de l'équipement client offre une résilience accrue : si un serveur mandataire principal, le chemin physique connectant ce serveur mandataire principal à l'équipement client ou le réseau d'accès connectant ce serveur mandataire principal à l'équipement client devenait défaillant, un autre serveur mandataire peut alors être utilisé par l'équipement client.

Dans cet autre mode de réalisation dans lequel les étapes d'obtention et d'élaboration sont réalisées par plusieurs serveurs mandataires, le procédé peut comprendre en outre, pour chacun des serveurs mandataires, la génération d'une donnée d'identification unique de ce serveur mandataire dans le réseau de communication et l'insertion de cette donnée d'identification unique de ce serveur mandataire dans la requête d'enregistrement élaborée par ledit serveur mandataire. Il est ainsi possible de distinguer les différents enregistrements d'un même équipement client, en fonction du serveur mandataire initiateur de l'enregistrement, pour éviter que l'enregistrement réalisé par le deuxième serveur mandataire, dans l'ordre chronologique, écrase l'enregistrement réalisé par le premier serveur mandataire.

Selon un mode de réalisation particulier, les données d'authentification sont sous forme d'un certificat d'authentification transmis, par l'équipement client, en réponse à une requête d'authentification émise par le au moins un serveur mandataire au cours d'une phase d'authentification. Dans un autre mode particulier de réalisation, le réseau de communication est un réseau IP comprenant un cœur de réseau présentant une architecture de type IMS et utilisant le protocole SIP, le message d'enregistrement est un message de type « SIP REGISTER », le serveur mandataire est un serveur P-CSCF et l'entité d'enregistrement est un serveur S-CSCF.

La présente invention propose en outre un procédé d'élaboration d'une requête de désenregistrement d'un équipement client dans un réseau de communication comprenant les étapes suivantes, mises en œuvre par au moins un serveur mandataire de ce réseau lorsque ce serveur mandataire ne reçoit aucun message de maintien en vie d'une connexion sécurisée établie avec l'équipement client pendant une durée déterminée ou lorsque ce serveur mandataire reçoit un message de déconnexion de ladite connexion

sécurisée :

récupération d'au moins une donnée d'identification de l'équipement client dans le réseau, cette au moins une donnée d'identification étant obtenue par le serveur mandataire à partir de données d'authentification de l'équipement client reçues lors d'une phase d'authentification dudit équipement client ; et

élaboration de la requête de désenregistrement de l'équipement client, dans laquelle est insérée ladite au moins une donnée d'identification de l'équipement client dans le réseau.

Il est ainsi possible de désenregistrer l'équipement client afin d'éviter de maintenir inutilement l'enregistrement de cet équipement dans le réseau après que la connexion sécurisée avec cet équipement client ait été interrompue, et ce de manière transparente aussi bien pour l'équipement client que pour le serveur d'enregistrement.

La présente invention propose par ailleurs un procédé d'enregistrement d'un équipement client dans un réseau de communication comprenant les étapes suivantes, mises en œuvre par au moins un serveur mandataire suite à la réception de données d'authentification de l'équipement client lors d'une phase d'authentification de cet équipement client :

élaboration d'une requête d'enregistrement de l'équipement client au moyen du procédé ci-avant ; et

envoi de cette requête d'enregistrement à un serveur d'enregistrement du réseau de communication, cette requête d'enregistrement étant utilisée par le serveur d'enregistrement pour enregistrer l'équipement client dans le réseau de communication.

Selon un mode de réalisation particulier, lorsque le serveur mandataire ne reçoit aucun message de maintien en vie d'une connexion sécurisée établie avec l'équipement client pendant une durée déterminée ou lorsque le serveur mandataire reçoit un message de déconnexion de ladite connexion sécurisée, le procédé d'enregistrement comprend l'élaboration d'une requête de désenregistrement de l'équipement client au moyen du procédé ci-avant et l'envoi de cette requête de désenregistrement au serveur d'enregistrement, cette requête de désenregistrement étant utilisée par le serveur d'enregistrement pour désenregistrer l'équipement client dans le réseau de communication.

La présente invention propose également un serveur mandataire d'un réseau de communication, apte à élaborer une requête d'enregistrement d'un équipement client dans le réseau de communication, destinée à être transmise à un serveur d'enregistrement du réseau de communication, comprenant un module de traitement de

données configuré pour, suite à la réception de données d'authentification émises par l'équipement client lors d'une phase d'authentification de cet équipement client, obtenir au moins une donnée d'identification de l'équipement client dans le réseau de communication, à partir des données d'authentification reçues dudit équipement client, et élaborer la requête d'enregistrement de l'équipement client, en y insérant cette au moins une donnée d'identification de l'équipement client dans le réseau.

La présente invention propose en outre un réseau de communication, comprenant un cœur de réseau et apte à enregistrer un équipement client afin de lui offrir un service, le cœur de réseau comprenant au moins un serveur mandataire tel que décrit ci-avant et un serveur d'enregistrement configuré pour enregistrer l'équipement client, suite à la réception d'une requête d'enregistrement de cet équipement client élaborée par le serveur mandataire.

Selon une implémentation particulière, les différentes étapes des procédés ci-avant sont mises en œuvre par un logiciel ou programme d'ordinateur, ce logiciel comprenant des instructions logicielles destinées à être exécutées par un processeur de données d'un serveur mandataire d'un réseau et étant conçu pour commander l'exécution des différentes étapes de ce procédé. En conséquence, l'invention vise aussi un programme, susceptible d'être exécuté par un ordinateur ou par un processeur de données, ce programme comportant des instructions pour commander l'exécution des étapes d'un procédé tel que mentionné ci-dessus. Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme d'un 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 lisible par un ordinateur ou processeur de données, et comportant des instructions d'un programme tel que mentionné ci-dessus. Ce support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD-ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette ou un disque dur. D'autre part, ce 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 selon l'invention peut être en particulier téléchargé sur un réseau de type Internet. Alternativement, ce 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 du procédé en question.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture dans la description détaillée ci-après de modes de réalisation particuliers, donnés à titre d'exemples non limitatifs, et des figures annexées dans lesquelles :

- la figure 1 illustre un système de communication dans lequel est mise en œuvre la présente invention ;
- la figure 2 illustre les étapes d'un procédé d'enregistrement selon un mode de réalisation particulier de l'invention, dans lequel la génération de la requête d'enregistrement de l'équipement client est confiée à un unique serveur mandataire du réseau de communication ;
- la figure 3 illustre les étapes d'un procédé d'enregistrement selon un autre mode de réalisation particulier de l'invention, dans lequel la génération de la requête d'enregistrement de l'équipement client est réalisée par plusieurs serveurs mandataires du réseau de communication ; et
- la figure 4 illustre un exemple particulier du procédé d'enregistrement selon un mode de réalisation particulier de l'invention utilisant un seul serveur mandataire, tel que décrit précédemment.

On se réfère tout d'abord à la **figure 1** qui illustre un système de communication dans lequel est mise en œuvre la présente invention.

Dans ce système, l'équipement client 1 est connecté au réseau IP_NET d'un opérateur de télécommunications, constitué d'un réseau d'accès ACC_NET et d'un cœur de réseau IMS_CN.

L'équipement client 1 est un équipement client à enregistrer dans le cœur de réseau IMS_CN, afin de lui permettre d'accéder à certains services offerts par le réseau IP_NET (téléphonie, voix sur IP, internet…), et qui n'a soit pas la possibilité d'effectuer un tel enregistrement parce qu'il ne dispose pas d'une telle fonctionnalité d'enregistrement, soit qui n'utilise pas lui-même cette fonctionnalité s'il en dispose. A titre d'exemple non limitatif, cet équipement client 1 peut être un équipement PABX IP tel que discuté précédemment.

Le réseau d'accès ACC_NET peut être un réseau radio, conforme ou non aux spécifications définies par l'organisme de normalisation 3GPP, ou bien un réseau filaire, optique ou xDSL.

Quant à cœur de réseau IMS_CN, il comprend notamment un équipement mandataire 2 connecté à un serveur d'interrogation 3 et un serveur d'enregistrement 4, lesquels sont eux-mêmes connectés entre eux ainsi qu'à un serveur d'abonnés 5.

L'équipement mandataire 2 sert notamment à relayer les messages de signalisation entre l'équipement client 1 et les autres serveurs du cœur de réseau IMS_CN, et dispose d'un module de traitement de données, typiquement sous forme d'un processeur associé à une mémoire, permettant de mettre en œuvre le procédé décrit par la suite.

Ainsi, dans le cas particulier où ce cœur de réseau IMS_CN présente une architecture de type IMS, le serveur mandataire 2 est un serveur P-CSCF, le serveur d'interrogation 3 est un serveur I-CSCF, le serveur d'enregistrement 4 est un serveur S-CSCF et le serveur d'abonnés 5 est un serveur HSS, certains de ces différents serveurs pouvant être rassemblés au sein d'une même entité, le cas échéant. Dans le cas d'une telle architecture IMS, le protocole de signalisation SIP est alors utilisé pour les échanges avec l'équipement client 1.

On se réfère maintenant à la **figure 2** qui illustre les étapes d'un procédé d'enregistrement selon un mode de réalisation particulier de l'invention, dans lequel la génération de la requête d'enregistrement de l'équipement client est effectuée par un unique serveur mandataire du réseau de communication.

Dans ce mode de réalisation, ce n'est pas l'équipement client 1 lui-même qui génère le message de requête d'enregistrement, pour s'enregistrer dans le réseau IMS_CN, mais le serveur mandataire 2. Pour ce faire, le serveur mandataire 2 est avantageusement configuré au préalable (étape 10) afin de pouvoir mettre en œuvre le procédé de la présente invention, cette configuration comprenant notamment la mémorisation d'une ou plusieurs règles permettant d'utiliser tout ou partie des données d'authentification reçues de l'équipement client 1 pour en déduire des informations d'identification permettant d'enregistrer cet équipement client 1, de manière transparente pour ce dernier, comme il sera vu plus loin. Une telle configuration préalable a typiquement lieu au moment de la mise en service du serveur mandataire, n'est pas spécifique à un type d'équipement client particulier et est la même pour tous les serveurs à laquelle elle s'applique.

Pour déduire ces informations d'identification de l'équipement client, le serveur mandataire 2 utilise des données d'authentification AUTH reçues de l'équipement client 1 (étape 23) durant une phase d'authentification (phase 20), déclenchée par la connexion de l'équipement client 1 au réseau IP_NET, qui est par exemple une phase d'authentification avec authentification client conforme au protocole TLS (pour Transport

Layer Security), préalable à tout échange d'informations entre l'équipement client 1 et le réseau IP_NET.

Ces données d'authentification AUTH de l'équipement client 1 sont typiquement mémorisées dans l'équipement client 1 (soit manuellement au préalable, soit au cours d'une préconfiguration automatique) et incluses dans un certificat d'authentification (désigné par CERT(AUTH) sur la figure 2) retourné par l'équipement client 1, suite à la réception (étape 21) d'une requête d'authentification émise par le serveur mandataire 2 lorsqu'il détecte la connexion de l'équipement client 1 au réseau IP_NET et qu'il lance la phase d'authentification.

Ainsi, dans le cas particulier d'un cœur de réseau IMS utilisant le protocole SIP, ces données d'authentification AUTH peuvent correspondre à un nom de domaine attribué à l'équipement PABX IP, identifié par une URI SIP ou un FQDN, et inséré dans le certificat d'authentification retourné par l'équipement client 1 lors de la phase d'authentification. En d'autres termes, les données d'authentification AUTH peuvent prendre la forme suivante :

AUTH= « sip : (Nom de domaine du PABX IP) »

Après avoir reçu un tel certificat d'authentification et authentifié l'équipement client 1, ce qui déclenche l'établissement d'une connexion sécurisée (phase 30) entre l'équipement client 1 et le réseau IP_NET, le serveur mandataire 2 peut extraire du certificat les données d'authentification AUTH de l'équipement client 1 pour en déduire (étape 31), au moyen d'une règle R de dérivation mémorisée lors de la configuration préalable susmentionnée du serveur mandataire 2, une ou plusieurs données d'identification ID de l'équipement client 1 dans le réseau de communication, cette/ces donnée(s) d'identification ID servant à enregistrer cet équipement dans le cœur de réseau IMS, et donc dans le réseau IP_NET.

La ou les données d'identification ID ainsi obtenues, à partir de ces données d'authentification et au moyen de cette règle R de dérivation, sont avantageusement également mémorisées, au préalable, au niveau d'un serveur d'abonnés (e.g. un serveur HSS dans le cas d'un cœur de réseau IMS) lors de la souscription de l'utilisateur de l'équipement client 1, afin de permettre la validation ultérieure de l'enregistrement.

Parmi ce(s) donnée(s) d'identification ID déduite(s) des données d'authentification AUTH reçues de l'équipement client 1, une première donnée d'identification ID1 peut ainsi être un identifiant public de l'équipement client 1 dans le réseau de communication, cet identifiant public ID1 étant construit à partir des données d'authentification, par exemple au moyen d'une règle R de dérivation prenant la forme d'une fonction injective associant

un identifiant public ID1 aux données d'authentification AUTH.

Une telle règle R peut par exemple consister à ajouter aux données d'authentification AUTH une extension EXT liée au réseau IMS_CN :

AUTH -> ID1=AUTH@EXT

Ainsi, dans le cas particulier d'un réseau cœur IMS utilisant le protocole SIP, cet identifiant public est l'identifiant public IMS (« IMS Public User Identity » en anglais ou IMPU) et peut prendre la forme suivante :

ID1 = « sip : (Nom de domaine du PABX IP)@(Nom de domaine dans le réseau IMS) »

Une deuxième donnée d'identification ID2, déduite également des données d'authentification AUTH reçues de l'équipement client 1, peut être un identifiant privé de l'équipement client 1 (i.e. une adresse privée utilisée par l'opérateur du réseau IP_NET), cet identifiant privé ID2 étant construit à partir des données d'authentification AUTH, par exemple au moyen d'une règle R' de dérivation prenant la forme d'une fonction injective associant un identifiant privé ID2 aux données d'authentification AUTH, par exemple en ajoutant à une partie des données d'authentification AUTH l'extension EXT liée au réseau IMS_CN.

Pour reprendre l'exemple d'un réseau cœur IMS utilisant le protocole SIP, cet identifiant privé est alors l'identifiant privé IMS (« IMS Private User Identity » en anglais ou IMPI), prenant typiquement la forme d'un identifiant d'accès au réseau (NAI en anglais), et peut prendre la forme suivante :

ID2 = « (Nom de domaine du PABX IP)@(Nom de domaine dans le réseau IMS) »

Une fois obtenue(s) la ou les donnée(s) d'identification de l'équipement client 1 dans le réseau, le serveur mandataire 2 mémorise d'une part ces données d'identification et élabore (étape 33) une requête d'enregistrement (REG_REQ) de l'équipement client, selon le protocole de signalisation utilisé dans le cœur de réseau IMS_CN (par exemple une requête « SIP REGISTER » lorsque ce réseau cœur est de type IMS utilisant le protocole SIP) dans laquelle est insérée cette ou ces donnée(s) d'identification.

Cette requête d'enregistrement REG_REQ est ensuite envoyée (étape 35) vers le serveur d'enregistrement 4, éventuellement par l'intermédiaire du serveur d'interrogation 3, afin que ce serveur d'enregistrement 4 procède à l'enregistrement (étape 37) de l'équipement client 1 dans le cœur de réseau IMS_CN, donc dans le réseau IP_NET, en utilisant les données d'identification de cet équipement client 1 dans le réseau. Cette dernière étape d'enregistrement, au niveau du serveur d'enregistrement, est classique et ne sera pas décrite en détail.

Ainsi, le cycle de vie de l'enregistrement de l'équipement client 1 est géré durant la connexion sécurisée 30, non pas par l'équipement client 1 lui-même, mais par le serveur mandataire 2, pour le compte de l'équipement client 1, et ce sur la base d'événements ayant lieu durant la phase d'authentification 20 de l'équipement client 1 auprès du réseau IP_NET. La connexion initiale de l'équipement client 1 au réseau IP_NET, entraînant le déclenchement de la phase d'authentification 20 de l'équipement client 1, déclenche également ainsi, indirectement et de manière transparente pour l'équipement client 1, l'enregistrement de ce dernier dans le cœur de réseau IMS_CN du réseau IP_NET.

Habituellement, la connexion authentifiée 30 établie suite à la phase d'authentification 10 est maintenue grâce à l'envoi (étape 38) de messages de type « keep-alive » au serveur mandataire 2. De tels messages peuvent être utilisés ici par le serveur mandataire 2 pour maintenir, ou supprimer, l'enregistrement de l'équipement client 1.

En particulier, tant que le serveur mandataire 2 reçoit des messages de type « keep-alive » de l'équipement client 1 (par exemple au moins un certain nombre de « keep-alive » durant une période de temps déterminée), signifiant que la connexion authentifiée est active, l'enregistrement de l'équipement client 1 est maintenu dans la mesure où le serveur mandataire 2 rafraîchit cet enregistrement auprès du serveur d'enregistrement 4 (par exemple en fonction d'une durée d'enregistrement fixée par ce serveur d'enregistrement 4) en lui renvoyant régulièrement la requête REG_REQ (étape 39) après la réception d'un ou plusieurs messages de type « keep-alive », en réutilisant les données d'identification mémorisées lors de l'élaboration de la requête REG_REQ initiale.

Par contre, si le serveur mandataire 2 ne reçoit plus de messages de type « keep-alive » de l'équipement client 1 durant une période de temps déterminée T0 (par ex. quelques minutes), ou encore s'il reçoit un message explicite de déconnexion de la connexion authentifiée, le serveur mandataire 2 peut décider d'interrompre l'enregistrement de l'équipement client 1 lors d'une phase de désenregistrement 40.

Cette phase de désenregistrement comprend la récupération de(s) donnée(s) d'identification ID insérées précédemment dans la requête d'enregistrement REG_REQ initiale, telles que mémorisées par le serveur mandataire 2, et l'élaboration (étape 41), par le serveur mandataire 2, d'une requête de désenregistrement UNREG_REQ (e.g. lorsque le protocole SIP est employé, une requête SIP « REGISTER » avec un en-tête « expires : 0 »), contenant notamment ce(s) donnée(s) d'identification ID, et l'envoi (étape 43) de cette requête UNREG_REQ vers le serveur d'enregistrement 4, afin que

celui-ci supprime (étape 45) l'enregistrement de l'équipement client 1 dans le réseau, au moyen de(s) donnée(s) d'identification ID de cet équipement client.

En même temps que le serveur mandataire 2 désenregistre l'équipement client auprès du serveur d'enregistrement 4, le serveur mandataire 2 peut mettre fin à la connexion authentifiée avec l'équipement client 1, en lui envoyant un message de fermeture de cette connexion (étape 47). Si ce message parvient à l'équipement client 1, ce dernier sera ainsi incité à initier une nouvelle connexion sécurisée, ce qui donnera lieu à un nouvel enregistrement par l'intermédiaire du serveur mandataire 2, et ainsi de suite.

La durée d'enregistrement de l'équipement client 1 dans le réseau correspond ainsi à la durée de la connexion sécurisée 30 entre cet équipement client 1 et le serveur mandataire 2. L'authentification de l'équipement client ayant été effectuée dès l'établissement de cette connexion sécurisée 30, il n'est plus nécessaire d'effectuer d'authentification supplémentaire tant que cette connexion sécurisée est maintenue (e.g. pour chaque requête SIP de type « SUBSCRIBE » ou « INVITE » émise par l'équipement client 1 pendant la connexion sécurisée 30).

On se réfère maintenant à la **figure 3** qui illustre les étapes d'un procédé d'enregistrement selon un autre mode de réalisation particulier de l'invention, dans lequel plusieurs requêtes d'enregistrement de l'équipement client sont construites par une pluralité de serveurs mandataires du réseau de communication.

En effet, il existe des situations dans lesquelles il convient de connecter l'équipement client au cœur de réseau IMS_CN par l'intermédiaire non pas d'un, mais de plusieurs serveurs mandataires. Ceci peut être le cas, par exemple, lorsqu'on souhaite se prémunir d'une éventuelle défaillance d'un unique serveur mandataire qui mettrait en œuvre le procédé tel que décrit précédemment en figure 2, et donc créer une redondance de serveurs mandataires capables de mettre en œuvre la présente invention. Ceci peut aussi être le cas notamment lorsque le volume de communications avec l'équipement client justifie une répartition de la charge entre plusieurs serveurs mandataires. Ainsi, sur la figure 3, deux serveurs mandataires 2_1 et 2_2 sont illustrés, sans que ce nombre soit limitatif.

Dans cet autre mode de réalisation, chacun des serveurs mandataires 2_1 et 2_2 est avantageusement configuré au préalable (étape 10), de manière identique et similairement à ce qui a été décrit en relation avec la figure 2.

Par la suite, l'équipement client 1 lance l'établissement d'une connexion sécurisée

avec chacun des serveurs mandataires 2_1 et 2_2 (phases d'établissement de connexion sécurisée 50 et 60) en envoyant (étapes 51 et 61) à chacun des serveurs mandataires 2_1 et 2_2, lors d'une phase initiale d'authentification de cet équipement, un message de réponse d'authentification contenant des données d'authentification AUTH telles que décrites précédemment.

Suite à la réception de ce message de réponse d'authentification, chacun des serveurs mandataires 2_1 et 2_2 procède, indépendamment et de manière identique, de la manière suivante :

- une ou plusieurs données d'identification ID de l'équipement client 1 dans le réseau de communication sont déduites des données d'authentification AUTH reçues (étapes 52, respectivement 62), similairement à l'étape 31 décrite précédemment ;

- une donnée d'identification unique d'instance, désignée par UUID sur la figure 3, est avantageusement obtenue en outre (étapes 53, respectivement 63) à partir des données d'authentification reçues dudit équipement client. Cet identifiant unique peut être construit à partir des données d'authentification AUTH au moyen d'une règle de dérivation mémorisée lors de la configuration préalable des serveurs mandataires, de manière à ce que, pour des données d'authentification données, ce soit toujours la même donnée d'identification unique d'instance UUID qui soit retournée. De plus, pour des données d'authentification distinctes, cette règle de dérivation retourne nécessairement des identifiants uniques d'instance différents. Pour reprendre l'exemple d'un réseau cœur IMS utilisant le protocole SIP, cet identifiant unique ID3 peut être un identifiant unique universel d'instance (UUID URN en anglais), obtenu au moyen d'une règle de dérivation utilisant l'algorithme décrit dans la clause 4.3 du document RFC 4122 ;

- une donnée d'identification unique dudit serveur mandataire dans le réseau de communication (REG-ID1 pour le serveur mandataire 2_1 et REG-ID2 pour le serveur mandataire 2_2 sur la figure 3) est avantageusement également générée (étapes 54, respectivement 64) par chaque serveur mandataire, afin de permettre l'identification de ces serveurs mandataires dans le processus d'enregistrement et identifier le chemin d'enregistrement. Ces données REG-ID1 et REG-ID2 désignant de manière unique leurs serveurs mandataires respectifs (i.e. il ne doit pas y avoir plusieurs serveurs mandataires associés à une même donnée REG-ID), elles peuvent par exemple prendre la forme d'un entier choisi aléatoirement entre 1 et 2^{31} associé au serveur mandataire lors de sa configuration préalable. Alternativement, elles peuvent être générées automatiquement par chaque serveur mandataire à partir d'une caractéristique distinctive de ces serveurs. La valeur REG-ID1, respectivement REG-ID2, est ainsi utilisée par le serveur mandataire

2_1, respectivement 2_2, pour tous les enregistrements effectués pour le compte d'équipements clients auxquels il procède.

Une fois les différentes données susmentionnées obtenues ou générées, chaque serveur mandataire élabore (étapes 55, respectivement 65) une requête d'enregistrement pour le compte de l'équipement client 1 (REG_REQ1 pour le serveur mandataire 2_1 et REG_REQ2 pour le serveur mandataire 2_2) dans laquelle il insère les données respectives susmentionnées, et transmet cette requête d'enregistrement (étapes 56, respectivement 66) vers le serveur d'enregistrement 4 afin de procéder à l'enregistrement (étapes 57, respectivement 67) de l'équipement client 1.

On se réfère maintenant à la **figure 4** qui illustre un exemple particulier du procédé d'enregistrement selon un mode de réalisation particulier de l'invention utilisant un seul serveur mandataire, tel que décrit précédemment en relation avec la figure 2.

Dans cet exemple particulier, l'équipement client 1 est un équipement d'acheminement téléphonique de type PABX IP, désigné ici par « IP-PBX », dont l'enregistrement est effectué auprès d'un réseau IMS lors de l'établissement d'une connexion sécurisée conforme au protocole TLS, de la manière suivante :

- dans un premier temps, typiquement lors de l'activation de l'équipement IP-PBX, cet équipement IP-PBX procède à l'établissement d'une session TCP avec un serveur P-CSCF du réseau IMS (étape 110), soit en utilisant l'adresse IP du P-CSCF si celle-ci est configurée dans l'équipement IP-PBX, soit en la déterminant au moyen d'un serveur DNS (en utilisant le principe décrit dans RFC 3263) ;

- une fois la session TCP établie, l'établissement d'une connexion sécurisée de type TLS (phase 120) entre l'équipement IP-PBX et le serveur P-CSCF peut démarrer par une phase d'authentification (phase 121). Au cours de cette phase d'authentification TLS, l'équipement IP-PBX signale tout d'abord qu'il vient de se connecter (étape 122) au serveur P-CSCF, lequel lui retourne alors un certain nombre d'informations (étape 123), notamment une requête d'authentification visant à obtenir un certificat numérique (« CertificateRequest » sur la figure 3) afin d'effectuer une authentification mutuelle.

- en réponse à cette requête d'authentification, l'équipement client IP-PBX renvoie au serveur P-CSCF (étape 124) le certificat d'authentification qui lui est assigné (« Certificate (subjectAltName : sip:site.enterprise.com) » sur la figure 3), lequel contient des données d'authentification sous la forme d'une URI SIP « sip:site.entreprise.com » désignant le nom de domaine associé à l'équipement client IP-PBX. L'équipement client IP-PBX retourne également une preuve associée à ce certificat, générée grâce à sa propre

clé privée, afin de permettre au serveur P-CSCF d'authentifier l'identité de cet équipement client.

- après avoir reçu le certificat d'authentification émis par l'équipement client IP-PBX, le serveur P-CSCF en extrait l'URI SIP « sip:site.entreprise.com » désignant le nom de domaine associé à l'équipement client IP-PBX et en déduit les données d'identification suivantes :

- l'IMPU de l'équipement client IP-PBX, sous la forme de l'URI SIP suivante : « sip:site.entreprise.com@busti.operator.com » ;

- l'IMPI de l'équipement client IP-PBX, sous la forme de l'identifiant NAI suivant « site.entreprise.com@busti.operator.com » ;

De manière optionnelle, dans le cas où l'enregistrement par un autre serveur P-CSCF est envisagé, le serveur P-CSCF peut également déduire un identifiant unique universel d'instance UUID URN à partir de l'URI SIP « sip:site.entreprise.com » et générer en outre un identifiant unique spécifique au serveur P-CSCF dans le réseau (ici la valeur « reg-id=1 »).

A partir des données susmentionnées, le serveur P-CSCF élabore alors une requête « SIP REGISTER » avec des champs d'en-tête remplis de la manière suivante :

- le champ « Request URI » est complété avec le nom de domaine du réseau IMS tel que configuré dans le P-CSCF (i.e. le même nom de domaine pour tous les équipements clients connectés au réseau IMS) ;

- les champs d'en-tête « From » et « To » sont complétés avec l'IMPU de l'équipement client IP-PBX, soit « sip:site.entreprise.com@busti.operator.com » ;

- le champ d'en-tête « Contact » est complété avec l'adresse IP source et le port de la connexion TLS. Dans le cas où plusieurs P-CSCF sont utilisés pour enregistrer l'équipement IP-PBX, chaque serveur P-CSCF peut insérer en outre dans ce champ « Contact » l'identifiant unique universel d'instance URN UUID obtenu à partir de l'URI SIP de l'équipement client IP-PBX, ainsi que la valeur « reg-id » spécifique au serveur P-CSCF (et non à l'équipement client IP-PBX) ;

- les autres champs d'en-tête sont complétés de manière classique, selon la spécification 3GPP TS 24.229.

Une fois la requête « SIP REGISTER » construite, elle est alors transmise (étape 131) par le serveur P-CSCF vers le serveur S-CSCF, par l'intermédiaire du serveur I-CSCF, afin que le serveur S-CSCF applique la procédure d'enregistrement selon la spécification TS 24.229, en utilisant l'IMPU et l'IMPI susmentionnés, ainsi qu'éventuellement l'identifiant unique d'instance URN UUID et la valeur reg-id susmentionnés.

Une fois l'enregistrement de l'équipement IP-PBX effectué, le serveur S-CSCF renvoie (étape 133) un message d'acquittement de type SIP « 200 OK » au serveur P-CSCF, par l'intermédiaire du serveur I-CSCF. Ce message d'acquittement n'est pas retransmis à l'équipement IP-PBX, de sorte à ce que cet enregistrement soit totalement transparent pour ce dernier.

Bien entendu, l'invention n'est pas limitée aux exemples de réalisation ci-dessus décrits et représentés, à partir desquels on pourra prévoir d'autres modes et d'autres formes de réalisation, sans pour autant sortir du cadre de l'invention.

Ainsi, dans le cas d'un réseau IMS, l'utilisation de requêtes d'enregistrement selon le protocole SIP a été décrite. L'invention ne se limite cependant pas à ce seul protocole, et peut s'étendre à tout autre protocole de signalisation d'un cœur de réseau présentant des requêtes d'enregistrement, tel que le protocole H.323 par exemple.

Par ailleurs, un équipement PABX IP a été cité comme exemple particulier d'équipement client s'enregistrant selon le procédé de la présente invention. Cependant, d'autres équipements peuvent être considérés, tels qu'un serveur vocal, un centre d'appels ou une plateforme de jeux interactifs.

En outre, la phase d'authentification mutuelle citée en exemple utilise le protocole TLS. L'invention ne se limite cependant pas à ce seul protocole d'authentification, et peut s'appliquer à tout autre protocole d'authentification dans lequel l'équipement client, cherchant à s'authentifier auprès du réseau, retourne, à un serveur mandataire du réseau en charge de valider cette authentification, un certificat d'authentification pouvant contenir des données d'authentification permettant la déduction de données d'identification, dans le réseau de communication, de cet équipement client. Ainsi, les protocoles SSL, SSH ou IPsec peuvent être employés.

Revendications

1. Procédé d'élaboration d'une requête d'enregistrement (REQ_REG) d'un équipement client (1) dans un réseau de communication (IP_NET), mis en œuvre par au moins un serveur mandataire (2) dudit réseau, comprenant les étapes suivantes :

obtention (13) d'au moins une donnée d'identification (ID) de l'équipement client dans le réseau, à partir de données d'authentification dudit équipement client reçues (12) lors d'une phase d'authentification dudit équipement client ; et

élaboration (15) de la requête d'enregistrement (REQ_REG) de l'équipement client, dans laquelle est insérée ladite au moins une donnée d'identification de l'équipement client dans le réseau.

2. Procédé selon la revendication 1, comprenant en outre la configuration préalable (11) dudit au moins un serveur mandataire, ladite configuration préalable comprenant la mémorisation, dans ledit au moins un serveur mandataire, d'au moins une règle (R) de dérivation permettant de déduire la au moins une donnée d'identification à partir d'au moins une partie des données d'authentification, ladite règle étant utilisée pour obtenir la au moins une donnée d'identification.

3. Procédé selon la revendication 1 ou 2, dans lequel les données d'authentification de l'équipement client comprennent un identifiant de domaine associé à l'équipement client, ladite au moins une donnée d'identification (ID) comprenant au moins un identifiant parmi un identifiant public de l'équipement client dans le réseau de communication et un identifiant privé de l'équipement client dans le réseau de communication, généré à partir dudit identifiant de domaine.

4. Procédé selon l'une des revendications 1 à 3, dans lequel les étapes d'obtention et d'élaboration sont réalisées par plusieurs serveurs mandataires (2_1,2_2), et où une donnée d'identification unique d'instance (UUID) est obtenue (53,63) en outre à partir des données d'authentification reçues dudit équipement client, ladite donnée d'identification unique d'instance étant insérée (55,65) dans les requêtes d'enregistrement (REG_REQ) élaborées par les serveurs mandataires.

5. Procédé selon l'une des revendications 1 à 4, dans lequel les étapes d'obtention et d'élaboration sont réalisées par plusieurs serveurs mandataires,

comprenant en outre, pour chacun des serveurs mandataires :

génération (54,64) d'une donnée d'identification unique (REG-ID1,REG-ID2) dudit serveur mandataire dans le réseau de communication ;

insertion (55,65) de ladite donnée d'identification unique dudit serveur mandataire dans la requête d'enregistrement (REQ_REG) élaborée par ledit serveur mandataire.

6. Procédé selon l'une des revendications précédentes, dans lequel les données d'authentification sont sous forme d'un certificat d'authentification (CERT(AUTH)) transmis (23), par l'équipement client, en réponse à une requête d'authentification émise (21) par le au moins un serveur mandataire au cours d'une phase d'authentification.

7. Procédé selon l'une des revendications précédentes, dans lequel le réseau de communication est un réseau IP comprenant un cœur de réseau présentant une architecture de type IMS et utilisant le protocole SIP, le message d'enregistrement est un message de type « SIP REGISTER », le serveur mandataire est un serveur P-CSCF et l'entité d'enregistrement est un serveur S-CSCF.

8. Procédé d'élaboration d'une requête de désenregistrement (UNREG_REQ) d'un équipement client (1) dans un réseau (IP_NET) comprenant les étapes suivantes, mises en œuvre par au moins un serveur mandataire (2) dudit réseau lorsque ledit serveur mandataire ne reçoit aucun message de maintien en vie d'une connexion sécurisée établie avec l'équipement client pendant une durée déterminée (T0) ou lorsque ledit serveur mandataire reçoit un message de déconnexion de ladite connexion sécurisée :

récupération d'au moins une donnée d'identification (ID) de l'équipement client dans le réseau, obtenue (31) par ledit serveur mandataire à partir de données d'authentification dudit équipement client reçues (23) lors d'une phase d'authentification dudit équipement client ; et

élaboration (41) de la requête de désenregistrement de l'équipement client, dans laquelle est insérée ladite au moins une donnée d'identification de l'équipement client dans le réseau.

9. Procédé d'enregistrement d'un équipement client (1) dans un réseau de communication (IP_NET) comprenant les étapes suivantes, mises en œuvre par au moins un serveur mandataire (2) suite à la réception (23) de données d'authentification dudit

équipement client lors d'une phase d'authentification dudit équipement client :

élaboration (33) d'une requête d'enregistrement (REG_REQ) de l'équipement client au moyen du procédé selon l'une des revendications 1 à 8 ; et

envoi (35) de ladite requête d'enregistrement à un serveur d'enregistrement (4) du réseau de communication, ladite requête d'enregistrement étant utilisée par le serveur d'enregistrement pour enregistrer (37) l'équipement client dans le réseau de communication.

10. Procédé d'enregistrement selon la revendication 9, comprenant en outre les étapes suivantes, lorsque ledit serveur mandataire ne reçoit aucun message de maintien en vie d'une connexion sécurisée établie avec l'équipement client pendant une durée déterminée ou lorsque ledit serveur mandataire reçoit un message de déconnexion de ladite connexion sécurisée :

élaboration (41) d'une requête de désenregistrement (UNREG_REQ) de l'équipement client au moyen du procédé selon la revendication 8 ; et

envoi (43) de ladite requête de désenregistrement au serveur d'enregistrement (4), ladite requête de désenregistrement étant utilisée par le serveur d'enregistrement pour désenregistrer (45) l'équipement client dans le réseau de communication.

11. Serveur mandataire (2) d'un réseau de communication, apte à élaborer une requête d'enregistrement d'un équipement client (1) dans le réseau de communication, destinée à être transmise à un serveur d'enregistrement (4) du réseau de communication, comprenant un module de traitement de données configuré pour, suite à la réception de données d'authentification (AUTH) émises (23) par ledit équipement client lors d'une phase d'authentification dudit équipement client :

obtenir (31) au moins une donnée d'identification (ID) de l'équipement client dans le réseau de communication, à partir des données d'authentification reçues dudit équipement client ;

élaborer (33) la requête d'enregistrement (REQ_REG) de l'équipement client, en y insérant ladite au moins une donnée d'identification de l'équipement client dans le réseau.

12. Réseau de communication (IP_NET), comprenant un cœur de réseau (IMS_CN) et apte à enregistrer un équipement client (1) afin de lui offrir un service, le cœur de réseau comprenant au moins un serveur mandataire (2) selon la revendication 11 et un serveur d'enregistrement (4) configuré pour enregistrer l'équipement client (1)

suite à la réception d'une requête d'enregistrement (REG_REQ) dudit équipement client élaborée par ledit serveur mandataire.

13. Programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé d'enregistrement d'un équipement client (1) dans un réseau de communication (IP_NET) selon l'une des revendications 1 à 8, lorsque ce programme est exécuté par le module de traitement de données d'un serveur mandataire (2) dudit réseau de communication.

14. Programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de désenregistrement d'un équipement client (1) dans un réseau de communication (IP_NET) selon la revendication 9, lorsque ce programme est exécuté par le module de traitement de données d'un serveur mandataire (2) dudit réseau de communication.

15. Support d'informations, lisible par un ordinateur ou un processeur de données, comportant des instructions d'un programme d'ordinateur selon l'une des revendications 13 ou 14.

Fig. 1

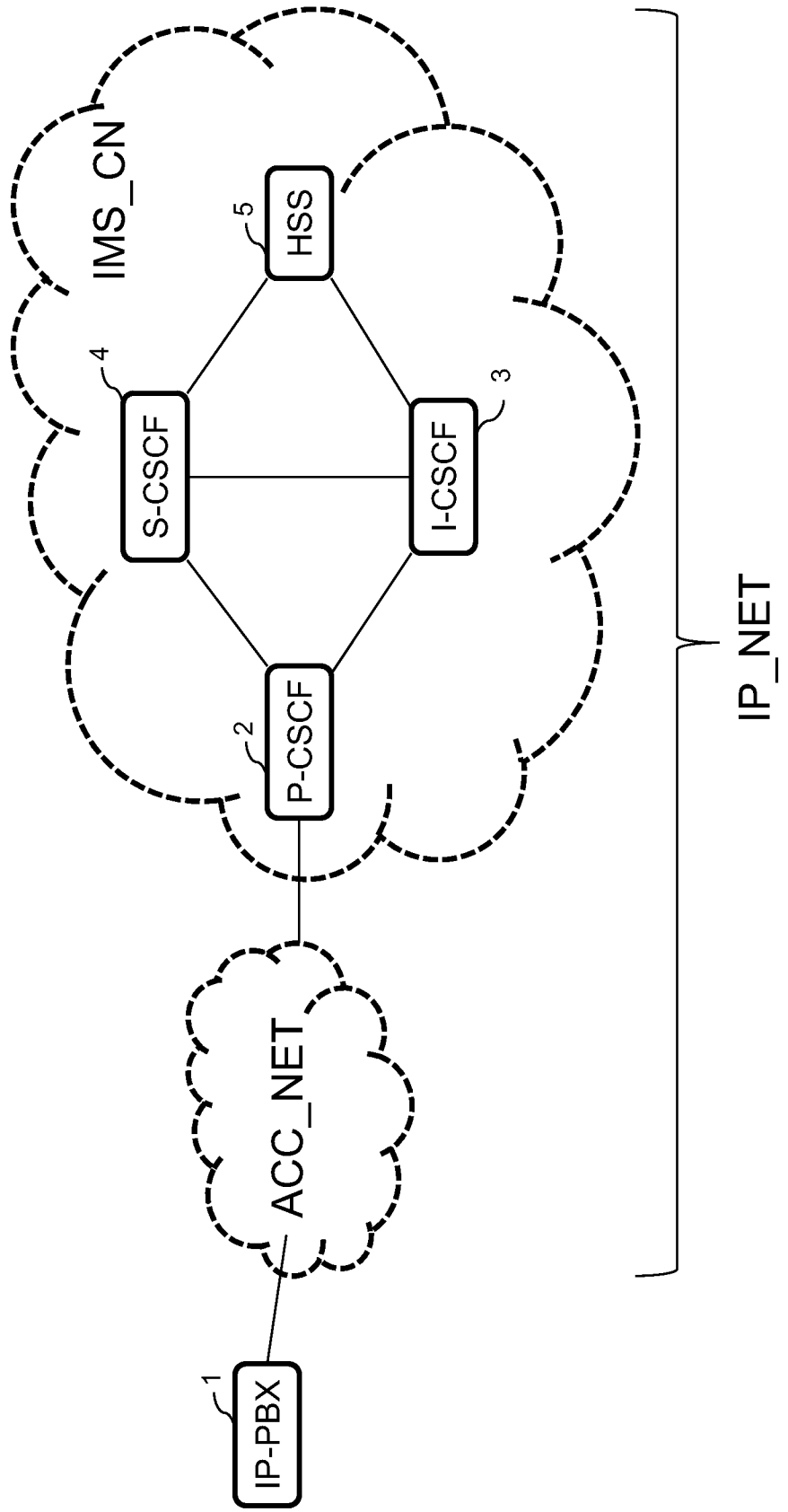


Fig. 2

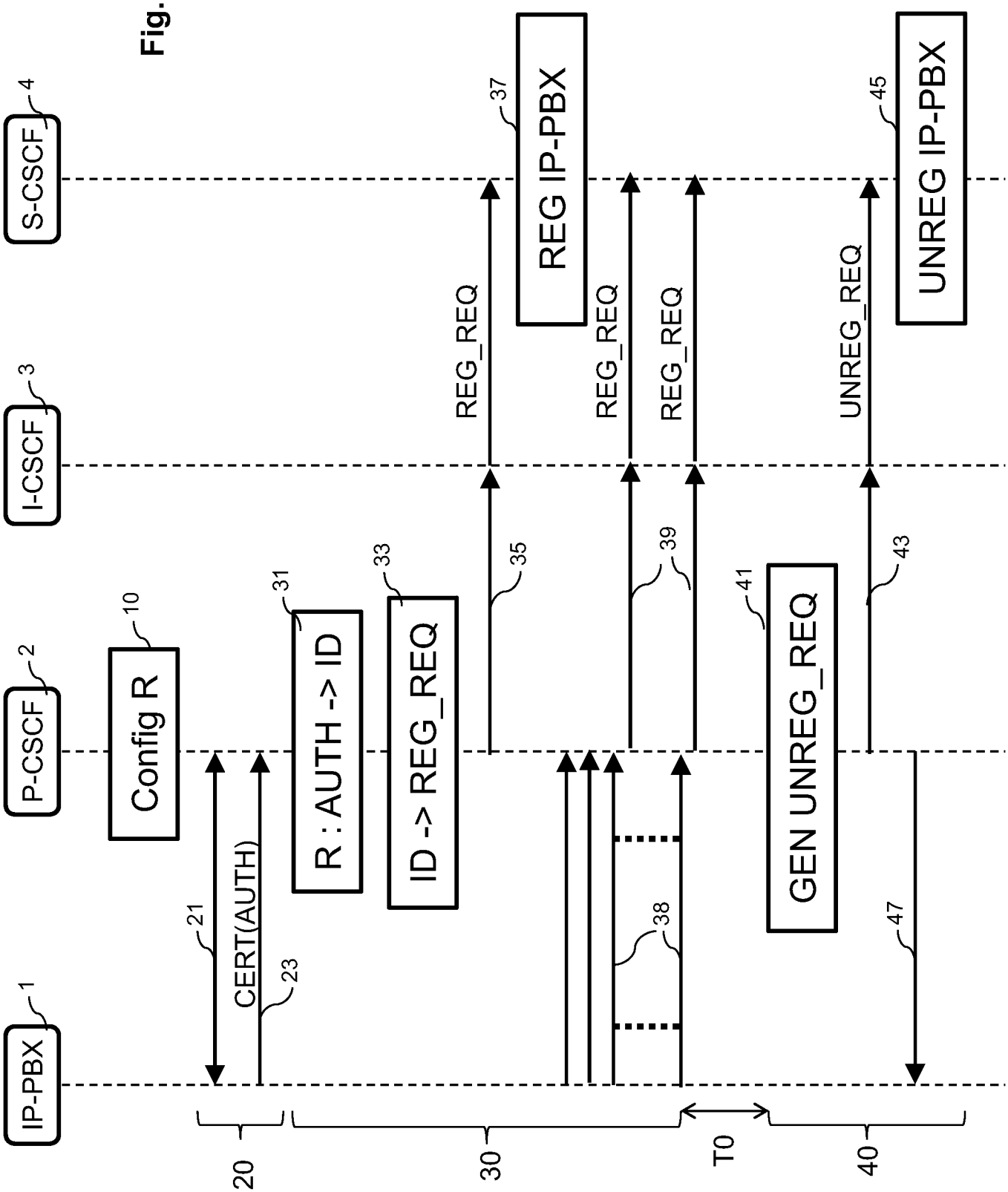
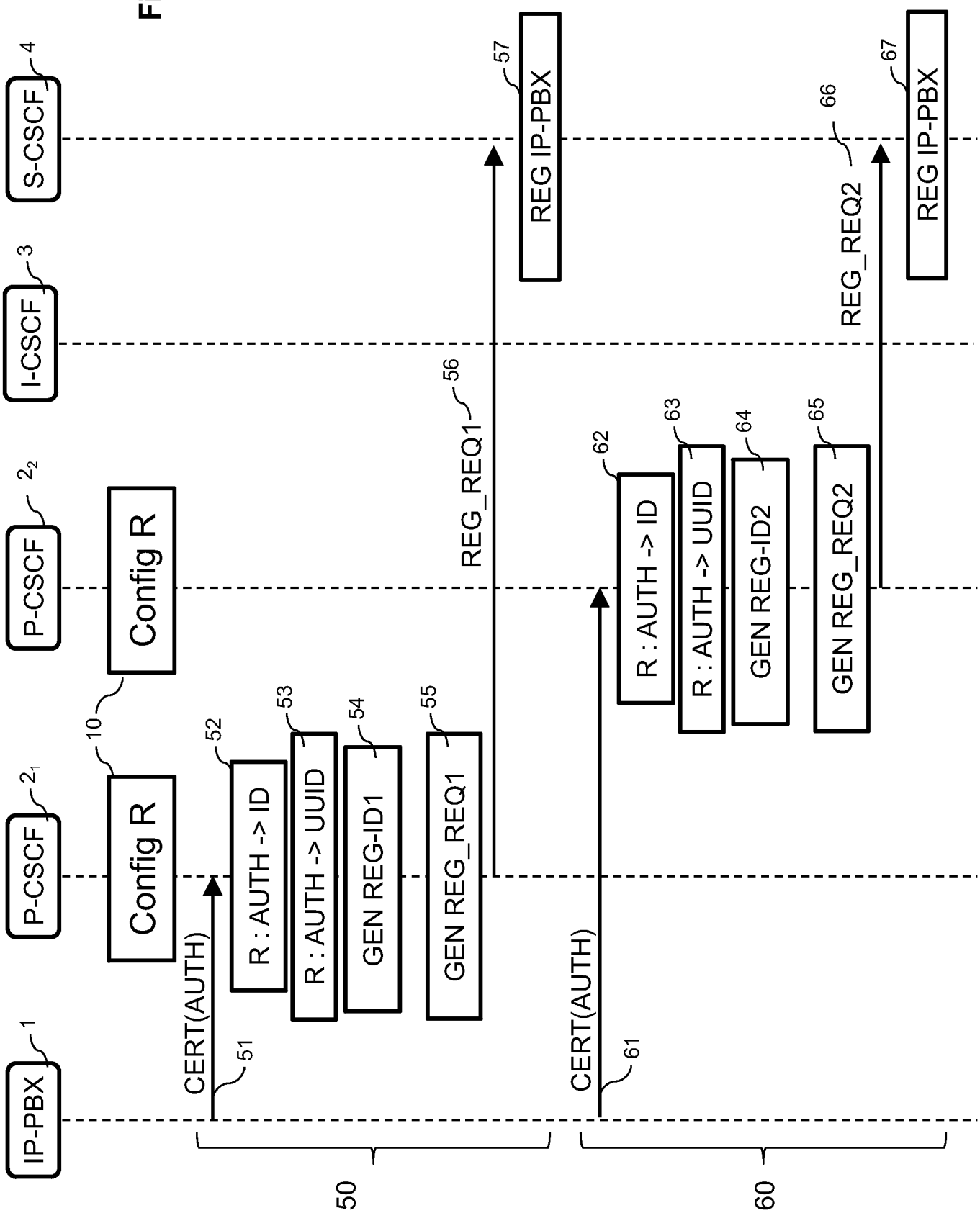

IP-PBX
1
P-CSCF
2
I-CSCF
3
S-CSCF
4
Config R
10
21
CERT(AUTH)
23
R : AUTH -> ID
31
ID -> REG_REQ
33
REG_REQ
35
REG IP-PBX
37
REG_REQ
39
38
REG_REQ
GEN UNREG_REQ
41
UNREG_REQ
43
UNREG IP-PBX
45
47
20
30
T0
40

Fig. 3


IP-PBX
1
P-CSCF
2₁
P-CSCF
2₂
I-CSCF
3
S-CSCF
4
Config R
10
CERT(AUTH)
51
R : AUTH -> ID
52
R : AUTH -> UUID
53
GEN REG-ID1
54
GEN REG_REQ1
55
REG_REQ1
56
REG IP-PBX
57
50
CERT(AUTH)
61
R : AUTH -> ID
62
R : AUTH -> UUID
63
GEN REG-ID2
64
GEN REG_REQ2
65
REG_REQ2
66
REG IP-PBX
67
60

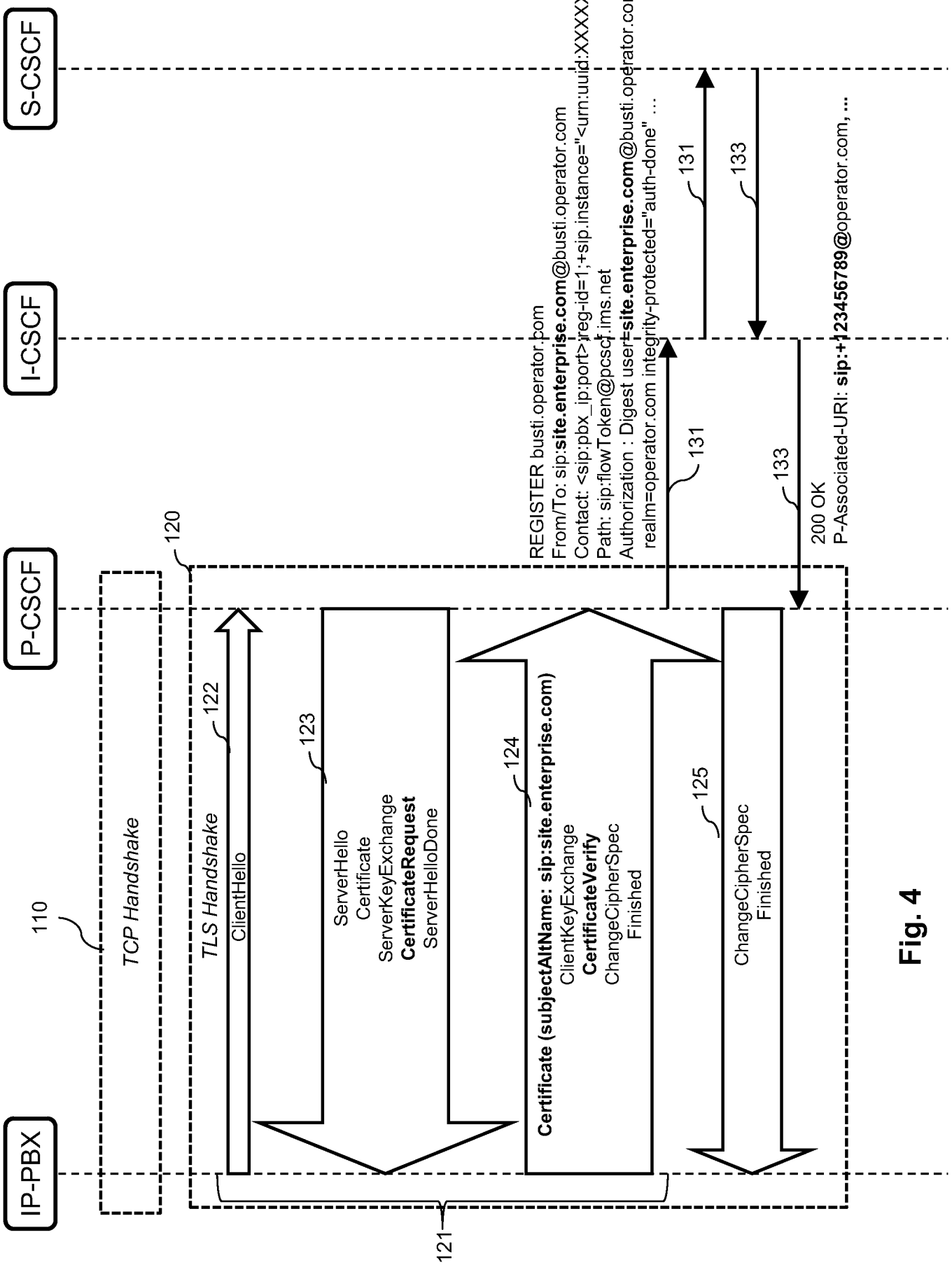

IP-PBX
P-CSCF
I-CSCF
S-CSCF
110
120
121
TCP Handshake
TLS Handshake
122
ClientHello
123
ServerHello
Certificate
ServerKeyExchange
CertificateRequest
ServerHelloDone
124
Certificate (subjectAltName: sip:site.enterprise.com)
ClientKeyExchange
CertificateVerify
ChangeCipherSpec
Finished
125
ChangeCipherSpec
Finished
REGISTER busti.operator.com
From/To: sip:site.enterprise.com@busti.operator.com
Contact: <sip:pbx_ip:port>;reg-id=1;+sip.instance="<urn:uuid:XXXXX>"
Path: sip:flowToken@pcscf.ims.net
Authorization : Digest user=site.enterprise.com@busti.operator.com
realm=operator.com integrity-protected="auth-done" ...
131
133
200 OK
P-Associated-URI: sip:+123456789@operator.com, ...
131
133

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2014/050110

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 009 934 A1 (HUAWEI TECH CO LTD [CN]) 31 December 2008 (2008-12-31) abstract paragraph [0098] - paragraph [0161] -----	1-15
X	US 2008/014939 A1 (CHANG DEUGKU [KR]) 17 January 2008 (2008-01-17) abstract paragraph [0073] - paragraph [0131] -----	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 April 2014	14/04/2014

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2014/050110

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2009934 A1	31-12-2008	AT 520268 T	15-08-2011
		CN 1984004 A	20-06-2007
		EP 2009934 A1	31-12-2008
		ES 2371109 T3	27-12-2011
		US 2009093249 A1	09-04-2009
		WO 2007121663 A1	01-11-2007
US 2008014939 A1	17-01-2008	KR 20080002326 A	04-01-2008
		US 2008014939 A1	17-01-2008

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2014/050110

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 2 009 934 A1 (HUAWEI TECH CO LTD [CN]) 31 décembre 2008 (2008-12-31) abrégé alinéa [0098] - alinéa [0161] -----	1-15
X	US 2008/014939 A1 (CHANG DEUGKU [KR]) 17 janvier 2008 (2008-01-17) abrégé alinéa [0073] - alinéa [0131] -----	1-15

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
7 avril 2014	14/04/2014

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Stergiou, Christos

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2014/050110

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 2009934 A1	31-12-2008	AT 520268 T	15-08-2011
		CN 1984004 A	20-06-2007
		EP 2009934 A1	31-12-2008
		ES 2371109 T3	27-12-2011
		US 2009093249 A1	09-04-2009
		WO 2007121663 A1	01-11-2007
US 2008014939 A1	17-01-2008	KR 20080002326 A	04-01-2008
		US 2008014939 A1	17-01-2008