(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
1 juin 2017 (01.06.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/089710 A1

(51) Classification internationale des brevets : *H04L 12/18* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2016/053072

(22) Date de dépôt international : 24 novembre 2016 (24.11.2016)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1561351 25 novembre 2015 (25.11.2015) FR

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

(72) Inventeurs : **BERTIN, Emmanuel**; 41 rue du Point du Jour, 14530 Luc sur Mer (FR). **CAZEAUX, Stéphane**; 5 rue Saint-Vigor, 14280 Authie (FR).

(74) Mandataire : **ORANGE IMT/OLPS/IPL/PATENTS**; MILET Isabelle, ORANGE GARDENS, 44 avenue de la République - CS 50010, 92326 Chatillon Cedex (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, DJ, 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, KW, KZ, LA, LC, LK, LR, LS, 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, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE,

[Suite sur la page suivante]

(54) Title : METHOD FOR DISTRIBUTING RIGHTS TO A SERVICE AND SERVICE PLATFORM

(54) Titre : PROCÉDÉ DE DISTRIBUTION DE DROITS SUR UN SERVICE ET PLATEFORME DE SERVICE

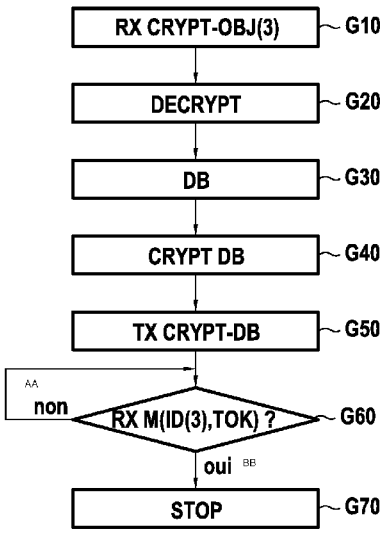


FIG.6

AA no
BB yes

(57) Abstract : The method for distributing rights to a service according to the invention is intended to be implemented by a service platform and comprises: - a step of constructing (G30) a database (DB) referred to as an identities and rights database, comprising, for each device participating in the service, an identity (ID(3)) intended to be used by said device during participation thereof in the service and, associated with said identity, at least one item of information representative of the rights to the service allocated to the device; and - a step of transmitting (G50) of said identity and rights database to each device participating in the service.

(57) Abrégé : Le procédé de distribution de droits sur un service selon l'invention est destiné à être mis en œuvre par une plateforme de service et comprend : - une étape de construction (G30) d'une base de données dite d'identités et de droits (DB) comprenant, pour chaque dispositif participant au service, une identité (ID(3)) destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information représentative de droits sur le service alloués au dispositif; et - une étape de transmission (G50) de cette base d'identités et de droits à chaque dispositif participant au service.

WO 2017/089710 A1

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée :

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

Procédé de distribution de droits sur un service et plateforme de service

Arrière-plan de l'invention

L'invention se rapporte au domaine général des communications.

Elle concerne plus particulièrement la mise en œuvre de services tels que des services de communication comme par exemple un service de conférence (visio-conférence, audioconférence ou encore conférence de type audio/vidéo) ou un service de diffusion de flux de données multimédia, ou tout autre type de services impliquant une pluralité d'acteurs, ainsi que la gestion des droits y afférents.

La plupart des systèmes de conférence connus sont basés sur l'utilisation d'une plateforme de service (audio, vidéo, web, etc.), aussi appelée pont de conférence, qui centralise et contrôle l'ensemble des ressources mises en œuvre lors de la conférence. Cette plateforme de service s'appuie sur une gestion centralisée des accès et des droits afférents à la conférence (par exemple droit de modérer la conférence, droit de clore la conférence, etc.).

Ainsi, lorsqu'un utilisateur souhaite réaliser une action lors de la conférence, telle que par exemple entrer dans la conférence, couper le microphone de l'un des dispositifs participant à la conférence ou encore clore la conférence, la plateforme de service contrôle que l'utilisateur a bien le droit de requérir une telle action, et le cas échéant, exécute elle-même ladite action.

Or l'émergence de nouvelles technologies et en particulier des technologies web telles que la technologie WebRTC (Web Real-Time Communication) développée au sein des consortiums W3C et IETF, permet aujourd'hui d'envisager une évolution des services de communication et notamment des services de conférence, qui ne nécessite plus la mise en œuvre de ressources centralisées au niveau d'une seule et même plateforme de service. Un tel service est par exemple décrit dans la demande de brevet FR 1 359 692.

Selon l'approche retenue dans le document FR 1 359 692, les terminaux des utilisateurs participant à un service de communication tel un service de conférence peuvent, en fonction de leurs capacités respectives, mettre à disposition du service de conférence leurs propres ressources pour établir directement entre eux des canaux de transmission de flux, ces canaux servant alors de supports à une session de communication mise en œuvre dans le cadre du service de conférence. Le rendu du service de conférence n'est alors plus centralisé au niveau de la plateforme de service (c'est-à-dire du pont de conférence), mais est délocalisé et distribué en tout ou partie sur les terminaux des utilisateurs participant au service.

Dans un tel contexte, le recours à une gestion centralisée au niveau de la plateforme de service des droits et des accès afférents au service de conférence peut s'avérer complexe, voire inapproprié. Il existe donc un besoin d'un mécanisme alternatif de gestion des droits afférents à un service tel que par exemple un service de communication, qui permet notamment de gérer efficacement ces droits lorsque le rendu du service est distribué sur plusieurs dispositifs, et en particulier sur des terminaux d'utilisateurs du service.

Objet et résumé de l'invention

L'invention répond notamment à ce besoin en proposant un procédé de distribution de droits sur un service, destiné à être mis en œuvre par une plateforme de service et comprenant :

- une étape de construction d'une base de données dite d'identités et de droits comprenant, pour chaque dispositif participant au service, une identité destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information représentative de droits sur le service alloués au dispositif; et
- une étape de transmission de cette base d'identités et de droits à chaque dispositif participant au service.

L'invention vise corrélativement une plateforme de service apte à diffuser des droits sur un service, cette plateforme de service comprenant :

- un module de construction, configuré pour construire une base de données dite d'identités et de droits comprenant, pour chaque dispositif participant au service, une identité destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information représentative de droits sur le service alloués au dispositif ; et
- un module de transmission, configuré pour transmettre cette base d'identités et de droits à au moins un autre dispositif participant au service.

L'invention propose ainsi avantageusement de construire, au niveau d'une plateforme de service centralisée, une base d'identités et de droits sur le service, et de diffuser ensuite cette base d'identités et de droits aux différents dispositifs participant au service pour qu'ils puissent disposer en local d'informations sur les droits de chacun des dispositifs participant au service.

Cette base d'identités et de droits a par exemple la forme d'une matrice regroupant, pour chacun des dispositifs participant au service, l'identité utilisée par ce dispositif lors de sa participation au service et une ou plusieurs informations relatives aux droits affectés à ce dispositif sur le service. L'identité du dispositif stockée dans la base d'identités et de droits est typiquement une information de joignabilité du dispositif lors du service, telle que par exemple un numéro de téléphone, une adresse mél, etc. Les informations relatives aux droits affectés à un dispositif sur le service peuvent se présenter quant à elles sous la forme d'actions autorisées au dispositif (par exemple couper le microphone d'un autre dispositif lors de la conférence, clore la conférence, etc.), et/ou d'un ou de plusieurs rôles associés au dispositif lors de sa participation au service (par exemple un rôle de modérateur), chaque dispositif disposant de la connaissance préalable de la correspondance entre un rôle et les actions autorisées par ce rôle, ou ayant la possibilité d'y accéder librement.

De façon avantageuse, la base d'identités et de droits ainsi construite est transmise conformément à l'invention aux dispositifs participant au service. De cette sorte, chaque utilisateur du service est informé des droits et des rôles affectés aux autres utilisateurs du service. Ainsi, lorsqu'un dispositif A requiert auprès d'un dispositif B une action lors de la mise en œuvre du

service, celui-ci peut, à partir des informations contenues dans la base de données qui lui a été transmise, déterminer si le dispositif A est autorisé à requérir une telle action et le cas échéant exécuter l'action ou au contraire refuser d'exécuter cette action. Cette vérification peut être réalisée très rapidement, grâce à la base de données stockée localement au niveau du dispositif B, sans consulter la plateforme de service.

L'invention a donc une application privilégiée, mais non limitative, lorsque les ressources de rendu d'un service sont distribuées sur plusieurs dispositifs (terminal(ux) d'utilisateur(s), plateforme(s) de service, serveur(s), etc.), en couplant la gestion des droits sur le service avec le rendu même du service, un contrôle des droits pouvant être effectué grâce à la base des identités et des droits diffusée par la plateforme de service au niveau de chaque dispositif participant au rendu du service.

On note qu'aucune limitation n'est attachée au type de service rendu. Il peut s'agir par exemple d'un service de distribution de flux média ou de conférence tels que mentionnés précédemment, comme d'un service auxquels plusieurs objets connectés participent en coopérant entre eux de sorte à réaliser différentes actions (ex. mesure de paramètres, traitement des mesures, rendu des mesures, etc.).

Selon une première variante de réalisation de l'invention, pour au moins un dispositif participant au service, l'identité et ladite au moins une information représentative des droits sur le service alloués à ce dispositif sont obtenus, par la plateforme de service, du dispositif lors de son enregistrement auprès de celle-ci.

Cette identité et les droits y afférents peuvent avoir notamment été transmis au dispositif préalablement par une plateforme d'affection de droits sur le service.

Selon une seconde variante de réalisation de l'invention, pour au moins un dispositif participant au service, ladite au moins une information représentative des droits sur le service alloués à ce dispositif comprend un rôle associé au dispositif lors de sa participation au service.

Le recours à l'une ou l'autre des variantes précitées dépend de l'architecture envisagée pour le rendu du service, la plateforme d'affectation des droits sur le service permettant de préciser à chaque utilisateur et/ou participant au service les droits et les rôles qui lui sont attribués.

Dans un mode particulier de réalisation, la base d'identités et de droits est chiffrée et/ou signée par la plateforme de service avant d'être transmise à chaque dispositif.

En particulier, la base d'identités et de droits peut être chiffrée et/ou signée selon un schéma connu de cryptographique asymétrique, à l'aide d'une clé privée allouée à la plateforme de service, la clé publique associée à cette clé privée étant accessible par les dispositifs participant au service (par exemple stockée en mémoire de ces dispositifs).

Grâce à un tel chiffrement et/ou signature, les dispositifs peuvent s'assurer de l'origine et de l'intégrité de la base d'identités et de droits qui leur est transmise.

Ainsi, grâce à l'invention, les dispositifs participant au service n'ont pas besoin d'établir entre eux une relation de confiance (par exemple via une authentification ou un mécanisme

d'appairage deux à deux), puisqu'une entité de confiance, à savoir la plateforme de service gérant les droits sur le service, leur a certifié par le biais de la transmission de la base d'identités et de droits qu'ils peuvent se faire confiance entre eux. L'invention permet donc de simplifier la mise en œuvre du service.

En variante, d'autres mécanismes peuvent être envisagés pour permettre à chaque dispositif de vérifier l'origine de la base d'identités et de droits qui lui est transmise, comme par exemple un contrôle de l'adresse IP (Internet Protocol) source à l'origine de la transmission de la base de données, ou du nom de domaine auquel est rattaché la plateforme de service, ou encore un mécanisme d'authentification préalable mis en œuvre entre chaque dispositif et la plateforme de service, etc. Le choix de l'un ou l'autre de ces mécanismes peut dépendre notamment du niveau de sécurité imposé par le contexte d'utilisation du service.

Dans un mode de réalisation particulier, le procédé de distribution comprend :

- une étape de réception d'un dispositif participant au service d'une indication d'un changement des droits alloués à ce dispositif sur le service ;
- une étape de mise à jour de la base d'identités et de droits pour l'identité utilisée par le dispositif conformément à ladite indication ; et
- une étape de transmission de la base d'identités et de droits mise à jour à chaque dispositif participant au service.

Ce mode de réalisation permet avantageusement de prendre en compte une évolution des droits et/ou des rôles des dispositifs au cours de l'utilisation du service.

Dans un mode particulier de réalisation l'indication de changement de droits comprend un jeton d'authentification correspondant à au moins un nouveau droit affecté au dispositif.

Ceci permet à la plateforme de service de s'assurer que le dispositif est bien autorisé à changer de droits en cours de service.

Comme mentionné précédemment, l'invention s'appuie donc sur la construction et la diffusion auprès des dispositifs participant à un service d'une base d'identités et de droits par une plateforme de service centralisée gérant les droits sur ce service, mais également sur l'utilisation de cette base d'identités et de droits par les dispositifs lors de leur participation au service.

Ainsi, selon un autre aspect, l'invention vise également un procédé de traitement d'une requête par un premier dispositif destiné à être mis en œuvre lors d'une participation du premier dispositif à un service, ce procédé comprenant :

- une étape d'obtention d'une base d'identités et de droits transmise par une plateforme de service suite à l'exécution par ladite plateforme d'un procédé de distribution de droits sur le service selon l'invention, ladite base d'identité et de droits comprenant, pour chaque dispositif participant au service, une identité destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information représentative de droits sur le service alloués au dispositif ;

— une étape de réception d'une requête en provenance d'un deuxième dispositif participant au service, cette requête comprenant une identité utilisée par le deuxième dispositif lors de sa participation au service et une action destinée à être réalisée par le premier dispositif ;
— une étape de vérification, dans la base d'identités et de droits, si l'identité comprise dans la requête a le droit de requérir l'exécution de ladite action par le premier dispositif ; et
— le cas échéant, une étape d'exécution de l'action requise.

Corrélativement, l'invention vise aussi un dispositif, dit premier dispositif, apte à participer à un service, ce premier dispositif comprenant :

— un module d'obtention, apte à obtenir une base d'identités et de droits transmise par une plateforme de service selon l'invention apte à diffuser des droits sur le service, ladite base d'identité et de droits comprenant, pour chaque dispositif participant au service, une identité destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information représentative de droits sur le service alloués au dispositif ;
— un module de réception, apte à recevoir une requête en provenance d'un deuxième dispositif apte à participer au service, cette requête comprenant une identité utilisée par le deuxième dispositif lors de sa participation au service et une action destinée à être exécutée par le premier dispositif ;
— un module de vérification, activé par le module de réception suite à la réception de la requête en provenance du deuxième dispositif, et configuré pour vérifier dans la base d'identités et de droits si l'identité comprise dans la requête a le droit de requérir l'exécution de ladite action par le premier dispositif ; et
— un module d'exécution configuré pour exécuter l'action requise dans la requête, activé si le module de vérification détermine que l'identité comprise dans la requête a le droit de requérir l'exécution de cette action par le premier dispositif.

En outre, dans un mode particulier de réalisation, la base d'identités et de droits transmise par la plateforme de service est chiffrée et/ou signée, le procédé de traitement comprenant une étape de déchiffrement et/ou de validation de la signature de la base d'identités et de droits avant de mettre en œuvre l'étape de vérification.

Le procédé de traitement et le dispositif selon l'invention bénéficient des mêmes avantages cités précédemment que le procédé de distribution des droits et la plateforme de service selon l'invention.

Dans un mode particulier de réalisation, les différentes étapes du procédé de distribution et/ou du procédé de traitement sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans une plateforme de services ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de distribution tel que décrit ci-dessus.

L'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un dispositif tel un terminal, une plateforme de service, un serveur ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de traitement tel que décrit ci-dessus.

L'un ou l'autre de ces programmes peut utiliser n'importe quel langage de programmation, et être 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 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 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 un disque dur.

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 selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, 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 du procédé en question.

Selon un autre aspect, l'invention vise également un système offrant un service et comprenant :

— une plateforme de service selon l'invention, apte à diffuser des droits sur le service ; et
— une pluralité de dispositifs selon l'invention aptes à participer au service.

Le système selon l'invention bénéficie des mêmes avantages cités précédemment que le procédé de distribution des droits, le procédé de traitement, la plateforme de service et le dispositif selon l'invention.

Dans un mode particulier de réalisation, le système peut comporter en outre une plateforme d'affectation de droits sur le service, cette plateforme d'affectation de droits comprenant :

— un module d'authentification, configuré pour authentifier un dispositif destiné à participer au service ;
— un module d'affectation à ce dispositif d'une identité destinée à être utilisée par le dispositif lors de sa participation au service et de droits sur le service ; et

— un module de transmission, au dispositif et/ou à la plateforme de service, de l'identité et d'au moins une information représentative des droits affectés au dispositif par le module d'affectation.

Ce mode de réalisation a une application privilégiée lorsque l'affectation des droits et la distribution des droits sont distribuées sur des plateformes distinctes, par exemple dans l'éventualité d'une architecture de service distribuée.

On peut également envisager, dans d'autres modes de réalisation, que le procédé de distribution des droits, le procédé de traitement, la plateforme de service, le dispositif et le système selon l'invention présentent en combinaison tout ou partie des caractéristiques précitées.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

— la figure 1 représente un système offrant un service de conférence conforme à l'invention dans un mode particulier de réalisation ;

— les figures 2 et 3 représentent respectivement un exemple d'architecture matérielle d'une plateforme de service et d'un dispositif conformes à l'invention dans un mode particulier de réalisation ;

— la figure 4 représente, sous forme d'ordinogramme, les principales étapes d'un procédé mis en œuvre par un dispositif du système de la figure 1, conforme à l'invention, dans un mode particulier de réalisation ;

— la figure 5 représente, sous forme d'ordinogramme, les principales étapes d'un procédé mis en œuvre par une plateforme d'affectation de droits sur le service de conférence offert par le système de la figure 1, dans un mode particulier de réalisation ;

— la figure 6 représente, sous forme d'ordinogramme, les principales étapes d'un procédé de distribution des droits sur le service de conférence offert par le système de la figure 1 tel qu'il est mis en œuvre par une plateforme de distribution des droits du système de la figure 1, dans un mode particulier de réalisation ;

— la figure 7 illustre un premier exemple de base d'identités et de droits pouvant être utilisée par le système de la figure 1 ;

— la figure 8 représente, sous forme d'ordinogramme, les principales étapes d'un procédé de traitement mis en œuvre par un dispositif du système de la figure 1, dans un mode particulier de réalisation ; et

— la figure 9 illustre un second exemple de base d'identités et de droits pouvant être utilisée dans le cadre de l'invention pour un système comprenant une pluralité d'objets connectés.

Description détaillée de l'invention

La **figure 1** représente, dans son environnement, un système 1 conforme à l'invention, offrant à une pluralité de dispositifs un service tel que par exemple un service de communication CONF de type conférence (audioconférence, visio-conférence ou conférence audio/vidéo).

Aucune limitation n'est attachée toutefois à la nature du service offert par le système 1, et d'autres services peuvent être envisagés comme par exemple un autre service de diffusion de flux de données multimédia (audio, vidéo, texte, etc.), un service de jeu en ligne, un service s'appuyant sur plusieurs objets connectés entre eux, etc.

Dans l'exemple envisagé à la figure 1, le rendu du service de conférence CONF est distribué sur plusieurs dispositifs 3 du système 1 participant à une même session du service, ces dispositifs 3 étant conformes à l'invention et aptes à communiquer entre eux via un réseau 2 de télécommunications (ex. Internet, intranet, réseau fixe ou mobile, etc.). Les dispositifs 3 comprennent plus particulièrement ici une pluralité de terminaux d'utilisateurs (trois dans l'exemple de la figure 1 référencés par 3-1, 3-2, 3-3) et une plateforme de service 3-4, cette plateforme de service étant par exemple un pont de conférence connu en soi.

Chaque terminal 3-1, 3-2, 3-3 héberge ici une application web (ou « web app » en anglais) de conférence décentralisée, accessible de façon connue en soi par l'utilisateur du terminal via un navigateur web. Le rendu du service de conférence est par exemple distribué sur les terminaux 3-1, 3-2, 3-3 et sur la plateforme de service 3-4 de façon similaire ou identique à ce qui est proposé dans le document FR 1 359 692, non repris en détail ici.

Cet exemple n'est bien entendu donné qu'à titre illustratif, et aucune limitation n'est attachée à la nature des dispositifs 3 sur lesquels s'appuie le rendu du service de communication CONF. Il peut ainsi s'agir de terminaux d'utilisateurs tels que des téléphones portables, des tablettes numériques ou des ordinateurs de type PC ou portables, de serveurs, de plateformes de service, d'objets connectés, etc. De même aucune limitation n'est attachée au nombre de dispositifs considérés.

Dans le mode de réalisation décrit ici, le système 1 comprend également, pour assurer la gestion des droits sur le service de conférence CONF :

- une plateforme de service 4 en charge de l'affectation des droits sur le service CONF (désignée ci-après par plateforme 4 d'affectation des droits). C'est cette plateforme qui, dans l'exemple envisagé à la figure 1, affecte à chacun des dispositifs 3 du système 1 une identité destinée à être utilisée par chaque dispositif lors de sa participation au service de conférence CONF, ainsi que des droits, ou de manière équivalente, un ou des rôles sur ce service ; et
- une plateforme de service 5 en charge de la distribution des droits affectés sur le service CONF auprès des dispositifs 3 du système 1, conformément à l'invention (désignée ci-après par plateforme 5 de distribution des droits).

La plateforme 5 de distribution des droits est hébergée ici par un serveur de gestion 6 tel que décrit dans le document FR 1 359 692, apte à permettre un rendu du service de conférence

CONF distribué sur les dispositifs 3 du système 1. La façon dont le serveur de gestion 6 procède à cet effet est décrite en détail dans le document FR 1 359 692 et n'est pas repris ici.

La plateforme 4 d'affectation des droits peut également être hébergée par le serveur 6, ou en variante, comme dans l'exemple illustré à la figure 1, par un serveur 7 distinct du serveur 6 mais apte à communiquer avec le serveur 6, par exemple via le réseau de télécommunications 2, de sorte à permettre une interaction entre les deux plateformes 4 et 5.

Dans le mode de réalisation décrit ici, la plateforme 5 de distribution des droits a l'architecture matérielle d'un ordinateur, telle que représentée à la **figure 2**. Elle comprend notamment un processeur 8, une mémoire morte 9, une mémoire vive 10, une mémoire non volatile 11 et un module de communication 12 comprenant notamment des moyens connus en soi pour communiquer sur le réseau de télécommunications 2 (ex. en fonction du réseau considéré, une carte réseau, une carte SIM (Subscriber Identity Module), etc.). La mémoire morte 9 constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 8 et sur lequel est enregistré un programme d'ordinateur PROG1 (ou logiciel) conforme à l'invention comportant des instructions pour l'exécution des étapes du procédé de diffusion conforme à l'invention.

Le programme d'ordinateur PROG1 définit ici des modules ou composants fonctionnels et logiciels de la plateforme 5 de distribution des droits, aptes à mettre en œuvre les étapes du procédé de diffusion selon l'invention. Ces modules logiciels sont susceptibles d'accéder aux et/ou de commander les ressources matérielles de la plateforme 5 (et notamment les ressources matérielles 9-13 citées précédemment). Ils comprennent ici :

— un module de construction 5A d'une base de données DB dite d'identités et de droits sur le service de conférence CONF ; et
— un module de distribution 5B de la base de données DB aux dispositifs du système 1.

Les fonctions des modules 5A et 5B sont détaillées ultérieurement en référence aux étapes correspondantes du procédé de distribution selon l'invention.

Dans le mode de réalisation décrit ici, la plateforme 4 d'affectation des droits a également l'architecture matérielle d'un ordinateur, cette architecture étant identique ou similaire à celle de la plateforme 5 de distribution des droits illustrée à la figure 2. La mémoire morte de la plateforme 4 d'affectation des droits constitue un support d'enregistrement, lisible par le processeur de la plateforme 4, et sur lequel est enregistré un programme d'ordinateur définissant ici divers modules (composants) fonctionnels et logiciels de la plateforme 4. Ces modules logiciels sont susceptibles d'accéder aux et/ou de commander les ressources matérielles de la plateforme de service 5 et comprennent ici :

— un module d'authentification 4A, configuré pour authentifier les dispositifs 3 du système 1 souhaitant participer au service de conférence CONF ;
— un module d'affectation 4B à ces dispositifs d'identités et de droits sur le service de conférence CONF ; et

— un module de transmission 4C de ces identités et de ces droits aux dispositifs du système 1. En variante, le module de transmission 4C peut être configuré pour transmettre ces identités et ces droits à la plateforme 5 de distribution des droits, via le réseau de télécommunications 2 par exemple, ou si les deux plateformes 4 et 5 sont hébergées par un même serveur, via un bus de données ou de communication propre au serveur.

Les fonctions des modules 4A-4C sont détaillées ultérieurement.

De façon similaire, dans le mode de réalisation décrit ici, chaque dispositif 3 du système 1 (i.e. terminaux 3-1, 3-2, 3-3, et pont de conférence 3-4), ont l'architecture matérielle d'un ordinateur telle que représentée à la **figure 3**. Il comprend notamment un processeur 13, une mémoire morte 14, une mémoire vive 15, une mémoire non volatile 16 et un module de communication 17 comprenant notamment des moyens connus en soi pour communiquer sur le réseau de télécommunications 2 (ex. en fonction du réseau considéré, une carte réseau, une carte SIM (Subscriber Identity Module), etc.). La mémoire morte 14 constitue un support d'enregistrement conforme à l'invention, lisible par le processeur 13 et sur lequel est enregistré un programme d'ordinateur PROG2 (i.e. logiciel) conforme à l'invention comportant des instructions pour l'exécution des étapes du procédé de traitement d'une requête conforme à l'invention.

Le programme d'ordinateur PROG2 définit ici des modules ou composants fonctionnels et logiciels des dispositifs 3, aptes à mettre en œuvre les étapes du procédé de traitement selon l'invention. Ces modules logiciels sont susceptibles d'accéder aux et/ou de commander les ressources matérielles du dispositif (et notamment les ressources matérielles 13-17 citées précédemment). Ils comprennent ici :

— un module d'obtention 3A de la base de données DB distribuée par la plateforme 5 de distribution des droits ;
— un module de réception 3B de requêtes relatives au service de conférence CONF ;
— un module de vérification 3C apte à interroger la base de données DB ; et
— un module d'exécution 3D, apte à exécuter diverses actions requises au dispositif dans le cadre du service de conférence CONF et des fonctions qu'il assure pour le rendu du service de conférence CONF.

Les fonctions des modules 3A-3D sont détaillées ultérieurement en référence aux étapes correspondantes du procédé de traitement selon l'invention.

Nous allons maintenant décrire, en référence aux **figures 4 à 6**, les principales étapes des procédés mis en œuvre respectivement conformément à l'invention, par les dispositifs 3 du système 1 (figure 4), par la plateforme 4 d'affectation des droits (figure 5), et par la plateforme 5 de distribution des droits (figure 6) , dans un mode particulier de réalisation. La figure 4 représente le procédé de traitement mis en œuvre par chacun des dispositifs 3 du système 1 participant au rendu du service de conférence CONF lors d'une session impliquant ces dispositifs, c'est-à-dire par les terminaux 3-1, 3-2, 3-3 et par le pont de conférence 3-4. Par souci de simplification dans la suite de la description, sauf référence explicite à l'un des dispositifs 3-1, 3-2, 3-3 ou 3-4, on utilise

la référence générale 3 pour désigner l'un quelconque de ces dispositifs. Lorsque cette référence générale 3 est utilisée, cela signifie que les étapes et autres paramètres décrits en relation avec cette référence générale sont appliqués à chacun des dispositifs 3-1, 3-2, 3-3 et 3-4.

En référence tout d'abord aux figures 4 et 5, on suppose ici que pour pouvoir accéder au service de conférence CONF, chacun des dispositifs 3 du système 1 s'est enregistré préalablement à ce service (étape E10), par exemple auprès de la plateforme 4 d'affectation des droits. Lors de cet enregistrement, de façon connue en soi, chaque dispositif 3 a convenu avec la plateforme 4, d'un identifiant (ou « login » en anglais) et d'un mot de passe pour s'authentifier auprès de celle-ci.

On suppose maintenant que les dispositifs 3 du système 1 souhaitent établir entre eux une conférence via le service CONF (autrement désignée par « session » du service de conférence dans la description). A cet effet, chaque dispositif 3 s'authentifie ici dans un premier temps auprès de la plateforme 4 d'affectation des droits (étapes E20 et F10), de façon connue en soi, en utilisant l'identifiant et le mot de passe échangés lors de l'enregistrement préalable du dispositif 3.

En référence à la figure 5, suite à l'authentification d'un dispositif 3 via son module d'authentification 4A, la plateforme 4, responsable de la gestion des droits d'accès au service de conférence CONF, établit par l'intermédiaire de son module d'affectation 4B l'identité ID(3) destinée à être utilisée par ce dispositif sur le service (i.e. identité ID(3-1) pour le terminal 3-1, identité ID(3-2) pour le terminal 3-2, identité ID(3-3) pour le terminal 3-3 et identité ID(3-4) pour le dispositif 3-4 respectivement) (étape F20). Cette identité traduit la façon dont le dispositif 3 en question va être reconnu par les autres dispositifs participant au service. Par exemple, pour un service de conférence, il peut s'agir de l'adresse IP du dispositif 3. On suppose ainsi ici, que la plateforme 4 affecte :

- au terminal 3-1, l'identité ID(3-1) correspondant à l'adresse IP @3-1 du dispositif 3-1 ;
- au terminal 3-2, l'identité ID(3-2) correspondant à l'adresse IP @3-2 du dispositif 3-2 ;
- au terminal 3-3, l'identité ID(3-3) correspondant à l'adresse IP @3-3 du terminal 3-3 ; et
- au dispositif 3-4, l'identité ID(3-4) correspondant à l'adresse IP @3-1 du dispositif 3-4.

En variante, d'autres identités peuvent être envisagées, en fonction notamment du service considéré. Ainsi par exemple, l'identité établie par la plateforme 4 pour un dispositif 3 peut correspondre à son numéro de téléphone, à un surnom, etc.

Cette identité est établie ici par la plateforme 4 à partir d'informations préalablement stockées dans une mémoire non volatile de la plateforme, et obtenues par exemple lors de l'enregistrement du dispositif 3 (ce peut être notamment des informations fournies par l'utilisateur du dispositif 3 lors de son enregistrement au service de conférence ou choisies par la plateforme 4). Il convient de noter que l'identité ID(3) établie lors de l'étape F20 par la plateforme 4 pour le dispositif 3 n'est pas nécessairement liée à l'identifiant utilisé par le dispositif 3 pour s'authentifier auprès de la plateforme 4.

La plateforme 4 d'affectation des droits affecte (i.e. alloue) par ailleurs au dispositif 3, par l'intermédiaire de son module d'affectation 4B, des droits RGT(3) sur le service de conférence CONF (i.e. des droits RGT(3-1) pour le terminal 3-1, des droits RGT(3-2) pour le terminal 3-2, des droits RGT(3-3) pour le terminal 3-3 et des droits RGT(3-4) pour le dispositif 3-4 respectivement) (étape F30). Par allocation de droits, on entend ici que la plateforme 4 autorise certaines actions spécifiques au dispositif 3 dans le cadre du service CONF au dispositif 3. Il peut s'agir d'actions consistant à requérir auprès d'un ou de plusieurs autres dispositifs l'exécution d'une action particulière (ex. couper le microphone d'un dispositif, déconnecter un dispositif, obtenir des informations d'un dispositif, etc.), ou d'actions pouvant s'appliquer au dispositif lui-même si cela est pertinent, au service de manière générale (ex. rebooter le service), ou encore à l'ensemble des dispositifs (ex. mettre fin à la conférence). Aucune limitation n'est attachée à la nature des droits alloués à chacun des dispositifs 3 par la plateforme 4, ces droits dépendant bien entendu du service considéré.

Les droits affectés à un dispositif 3 peuvent être spécifiés directement en tant que tels ou de façon codée, ou encore découler indirectement d'un ou de plusieurs rôles affectés par la plateforme 4 au dispositif 3 vis-à-vis d'un ou plusieurs dispositifs du système 1 (ex. dans le cas d'un service de conférence : organisateur, modérateur, participant, etc.). La correspondance entre rôle et droits afférents est supposée ici connue de chacun des dispositifs 3 participant au service de conférence CONF et des plateformes de service 4 et 5. Elle est par exemple communiquée à chaque dispositif 3 lors de son enregistrement au service de conférence CONF.

Quelle que soit la forme sous laquelle ils sont représentés, les droits RGT(3) constituent des informations représentatives des droits sur le service CONF alloués au dispositif 3 au sens de l'invention.

Dans l'exemple du service de conférence CONF envisagé ici à titre illustratif, on considère deux rôles distincts, i.e. « modérateur » (ou superviseur) ou « participant », pouvant être attribués par la plateforme 4 aux dispositifs 3, pour lesquels les droits associés en découlant sont les suivants :

- rôle de « modérateur » (ou superviseur) :
  - droit de couper le microphone d'un autre dispositif ;
  - droit de déconnecter un autre dispositif ; et
  - droit d'obtenir des informations d'un autre dispositif ;
- rôle de « participant » :
  - droit d'obtenir des informations d'un autre dispositif.

Plus précisément, on suppose ici que la plateforme 4 attribue au terminal 3-1 le rôle de modérateur, et aux terminaux 3-2, 3-3 et au dispositif 3-4 des rôles de participant à la conférence.

Dans le mode de réalisation décrit ici, le module d'affectation 4B de la plateforme 4 d'affectation des droits construit ensuite, pour chaque dispositif 3, un objet OBJ(3) (i.e. une

structure de données) comprenant l'identité ID(3) et les droits RGT(3) affectés au dispositif 3 (étape F40).

Puis elle chiffre cet objet OBJ(3) à l'aide d'un algorithme de chiffrement asymétrique mis en œuvre par son module de transmission 4C, de façon connue en soi, en utilisant une clé de chiffrement privée PrivK4 caractéristique du service CONF et préalablement allouée à la plateforme 4 par une autorité de confiance (étape F50). Cette clé de chiffrement privée PrivK4 est par exemple stockée dans la mémoire non volatile de la plateforme 4, et associée à une clé de chiffrement publique PubK4. Aucune limitation n'est attachée à l'algorithme de chiffrement asymétrique utilisé par le module de transmission 4C de la plateforme 4 pour chiffrer l'objet OBJ(3). L'objet chiffré obtenu est désigné par CRYPT_OBJ(3).

En variante, un algorithme de chiffrement symétrique peut être envisagé pour chiffrer l'objet OBJ(3), celui-ci utilisant une clé de chiffrement secrète SK4 partagée entre la plateforme 4 d'affectation des droits et la plateforme 5. Cette clé partagée SK4 a par exemple été échangée entre la plateforme 5 et la plateforme 4 lors de l'enregistrement du dispositif 3 au service CONF.

Dans une autre variante encore, la plateforme 4 signe l'objet OBJ(3) ou l'objet chiffré CRYPT_OBJ(3) au moyen d'un algorithme de signature numérique connu en soi et de la clé de chiffrement privée PrivK4.

L'objet chiffré CRYPT_OBJ(3) est ensuite transmis au dispositif 3 par le module de transmission 4C de la plateforme 4 d'affection de droits, via le réseau de télécommunications 2 (étape F60).

Il convient de noter que le chiffrement, respectivement la signature, de l'objet OBJ(3) permet de s'assurer que l'identité et les droits affectés au dispositif 3 par la plateforme 4 d'affectation des droits ne sont pas modifiés par un tiers (dispositif 3 ou autre), seule la plateforme 4 en tant qu'entité de confiance disposant de la connaissance de la clé privée PrivK4 ayant permis de chiffrer, respectivement de signer, l'objet OBJ(3).

En référence de nouveau à la figure 4, l'objet chiffré CRYPT_OBJ(3) est reçu, via le réseau de télécommunications 2, par le module d'obtention 3A du dispositif 3 (étape E30).

Dans le mode de réalisation décrit ici, le dispositif 3 s'enregistre alors auprès de la plateforme 5 de distribution des droits et lui transmet lors de cet enregistrement, via le réseau de télécommunications 2, l'objet chiffré CRYPT_OBJ(3) reçu de la plateforme d'affection de droits 4 (étape E40). Il convient de noter que le dispositif 3, dans le mode de réalisation décrit ici, ne déchiffre pas l'objet chiffré CRYPT_OBJ(3), mais le transmet en l'état à la plateforme 5.

En référence à la figure 6, la plateforme 5 de distribution des droits reçoit donc, de chaque dispositif 3, un objet chiffré CRYPT_OBJ(3) comprenant l'identité ID(3) établie par la plateforme 4 pour ce dispositif 3, ainsi que les droits RGT(3) qui lui ont été affectés (étape G10).

On suppose ici que la plateforme 5 de distribution des droits dispose, stockée par exemple dans sa mémoire non volatile 11, la clé publique PubK4 associée à la clé privée PrivK4 utilisée par la plateforme 4 d'affectation des droits pour chiffrer l'objet OBJ(3).

Dans le mode de réalisation décrit ici, la plateforme 5 de distribution des droits déchiffre, par l'intermédiaire de son module 5A de construction, l'objet chiffré CRYPT_OBJ(3) reçu du dispositif 3 en utilisant de façon connue en soi la clé publique PubK4 (étape G20). Le module 5A obtient à l'issue de cette étape de déchiffrement l'objet OBJ(3) comprenant l'identité ID(3) et les droits RGT(3) affectés pour l'utilisation du service CONF au dispositif 3.

Il convient de noter que si l'objet chiffré CRYPT_OBJ(3) est issu d'un autre dispositif que la plateforme 4 et n'a pas été chiffré à l'aide de la clé privée PrivK4 affectée au service CONF et détenue par la plateforme 4, cette étape de déchiffrement n'est pas possible.

Dans un autre mode de réalisation dans lequel l'objet CRYPT_OBJ(3) est un objet signé par la plateforme 4, la plateforme 5 vérifie lors de l'étape G20 la signature numérique de l'objet de façon connue en soi.

Dans un autre mode de réalisation, l'objet chiffré CRYPT_OBJ(3) associé au dispositif 3 est transmis directement par la plateforme 4 d'affectation des droits à la plateforme 5 de distribution des droits, sans intervention du dispositif 3, par exemple via un bus de données interne si les deux plateformes sont localisées sur un même serveur, ou via une application de type API (Application Programming Interface) ou via le réseau de télécommunications 2.

Le module 5A de construction de la plateforme 5 de distribution des droits extrait de l'objet déchiffré OBJ(3) l'identité ID(3) du dispositif 3 ainsi que les droits (3) qui lui ont été affectés et les stocke dans une structure de données, et plus particulièrement dans la base de données DB dite d'identités et de droits (étape G30).

Le module 5A de construction met en œuvre les étapes G10, G20 et G30 pour chacun des dispositifs 3-1, 3-2, 3-3 et 3-4 de sorte à construire une base d'identités et de droits DB regroupant les droits RGT(3) et les identités ID(3) de tous les dispositifs participant au service CONF et en relation les uns avec les autres. On a donc une base DB pour chaque utilisation (i.e. chaque session) du service CONF (autrement dit, pour chaque conférence établie dans le cadre de ce service entre plusieurs dispositifs).

Dans le mode de réalisation décrit ici, la base DB d'identités et de droits a plus particulièrement la forme d'une matrice, c'est-à-dire d'un tableau à deux dimensions, dont un exemple est illustré à la **figure 7**.

Selon cet exemple, chaque ligne Li de la matrice est associée à un dispositif 3-i du système 1 et indique les droits affectés par la plateforme 4 à ce dispositif sur les dispositifs 3-j identifiés dans les colonnes Cj de la matrice, où i,j=1,...,N et N désigne le nombre de dispositifs 3 du système 1 participant à la session du service à laquelle se rapporte la base DB (N=4 dans l'exemple illustré). Les dispositifs 3-i et 3-j sont identifiés en ligne et en colonne par l'identité qu'a établie la plateforme 4 d'affection de droits.

Ainsi, la ligne L1 indique que le dispositif 3-1 dont l'identité est ID(3-1)=@3-1 a un rôle de modérateur (indiqué par « SUP » dans la matrice DB) vis-à-vis des dispositifs 3-2, 3-3 et 3-4. Autrement dit, la ligne L1 reprend l'ensemble des droits spécifiés par l'information RGT(3-1).

De façon similaire, les lignes L2, L3 et L4 (reprenant l'ensemble des droits spécifiés dans les informations RGT(3-2), RGT(3-3), RGT(3-4)) indiquent respectivement que :

- le dispositif 3-2 dont l'identité est ID(3-2)=@3-2 a un rôle de participant (indiqué par « PART » dans la matrice DB) vis-à-vis des dispositifs 3-1, 3-3 et 3-4 ;
- le dispositif 3-3 dont l'identité est ID(3-3)=@3-3 a un rôle de participant (indiqué par « PART » dans la matrice DB) vis-à-vis des dispositifs 3-1, 3-2 et 3-4 ;
- le dispositif 3-4 dont l'identité est ID(3-4)=@3-4 a un rôle de participant (indiqué par « PART » dans la matrice DB) vis-à-vis des dispositifs 3-1, 3-2 et 3-3.

Autrement dit, au vu de la correspondance établie précédemment, le dispositif 3-1 en tant que modérateur du service CONF dispose des droits de couper le microphone des dispositifs 3-2, 3-3 et 3-4, de déconnecter les dispositifs 3-2, 3-3 et 3-4 et d'obtenir des informations sur les dispositifs 3-2, 3-3 et 3-4. Les dispositifs 3-2, 3-3 et 3-4 en tant que participant au service CONF dispose uniquement du droit d'obtenir des informations des autres dispositifs du système 1.

La base ou matrice DB ainsi construite par la plateforme 5 donne donc une vue d'ensemble synthétique de tous les dispositifs participant à la session considérée du service de conférence et des droits et identités afférents à ces dispositifs. Elle est stockée par le module de construction 5A dans la mémoire non volatile 11 de la plateforme 5.

Dans le mode de réalisation décrit ici, la plateforme 5 de distribution des droits chiffre, via son module de transmission 5B, la base DB d'identités et de droits ainsi construite (étape G40). Elle utilise à cet effet ici un algorithme de chiffrement asymétrique, connu en soi, et une clé privée PrivK5, associée au service de conférence CONF, et affectée par une autorité de confiance à la plateforme 5. Cette clé privée PrivK5 est par exemple stockée dans la mémoire non volatile 11 de la plateforme 5. Aucune limitation n'est attachée à l'algorithme de chiffrement asymétrique utilisé par le module de transmission 5B de la plateforme 5 pour chiffrer la base DB d'identités et de droits. La base DB chiffrée obtenue est désignée par CRYPT_DB.

En variante, un algorithme de chiffrement symétrique peut être envisagé pour chiffrer la base DB, celui-ci utilisant une clé de chiffrement secrète SK5 partagée entre la plateforme 5 d'affectation des droits et les dispositifs 3. Cette clé partagée SK5 a par exemple été échangée entre le dispositif 3 et la plateforme 5 lors de l'enregistrement du dispositif 3 auprès de la plateforme 5.

Selon une autre variante encore, la plateforme 5 signe la base d'identité et de droits DB ou sa version chiffrée au moyen d'un algorithme de signature numérique connu en soi et de la clé de chiffrement privée PrivK5.

Puis le module de transmission 5C de la plateforme 5 transmet la base d'identité et de droits chiffrée CRYPT_DB à chacun des dispositifs 3 du système 1 (étape G50).

En référence de nouveau à la figure 4, chaque dispositif 3 reçoit la base d'identité et de droits chiffrée CRYPT_DB distribuée par la plateforme 5 (étape E50), et la déchiffre à l'aide de la clé publique PubK5 associée à la clé de chiffrement privée PrivK5 (étape E60). La base

d'identités et de droits DB ainsi déchiffrée est stockée par chaque dispositif 3, par exemple dans sa mémoire non volatile.

Ainsi, via la base d'identités et de droits DB distribuée par la plateforme 5 de distribution des droits sur le service CONF, chaque dispositif 3 participant à la session de conférence est informé de son propre rôle et de ses droits, ainsi que des rôles et des droits des autres dispositifs participant à cette session.

Nous allons maintenant décrire, en référence à la **figure 8**, la façon dont les dispositifs 3 se servent, lors de la conférence, de cette base DB distribuée par la plateforme 5 et stockée localement au niveau de chaque dispositif, notamment pour traiter des requêtes en provenance d'un autre dispositif participant à la conférence conformément à l'invention.

On suppose donc maintenant que, suite à la distribution de la base DB, les dispositifs 3 participent à proprement parler à une conférence mise en œuvre dans le cadre du service CONF.

On suppose par ailleurs que l'utilisateur de l'un des dispositifs, par exemple du terminal 3-1, souhaite couper le microphone du terminal de l'un des participants à la conférence, par exemple du terminal 3-2. La figure 8 illustre les étapes mises en œuvre par le terminal 3-2 (étapes d'un procédé de traitement conforme à l'invention).

Pour couper le microphone du terminal 3-2, le terminal 3-1 envoie, via le réseau de télécommunications 2 par exemple, une requête REQ au terminal 3-2 contenant son identité ID(3-1) ainsi qu'une action ACT à réaliser par le terminal 3-2, à savoir ici couper son microphone.

Sur réception par son module de réception 3B de la requête REQ envoyée par le terminal 3-1 (étape H10), le terminal 3-2 extrait l'identité ID(3-1) de la requête REQ et vérifie, au moyen de son module de vérification 3C, dans la base DB d'identités et de droits stockée dans sa mémoire si cette identité a le droit de lui demander d'exécuter l'action ACT contenue dans la requête REQ, à savoir de couper son microphone (étape H20). Cette étape de vérification est mise en œuvre par le module de vérification 3C via des moyens d'interrogation ou de consultation d'une base de données connus en soi, en contrôlant si parmi les droits RGT(3-1) reportés dans la base DB pour l'identité ID(3-1) figure l'autorisation de demander au dispositif 3-2 de couper son microphone.

Dans l'exemple décrit à la figure 7, la base DB indique au terminal 3-2 que le terminal 3-1 correspondant à l'identité ID(3-1) a le rôle de modérateur de la conférence vis-à-vis de lui. Conformément à la correspondance rôle/droits préétablie mentionnée précédemment, le module de vérification 3C du terminal 3-2 déduit de ce rôle que le terminal 3-1 a le droit de requérir auprès du terminal 3-2 qu'il exécute l'action ACT, autrement dit qu'il coupe son microphone (réponse oui à l'étape test H30).

Suite à cette vérification positive, le module d'exécution 3D du terminal 3-2 exécute l'action ACT requise par le terminal 3-1 et coupe le microphone du terminal 3-2 (étape H40).

Si au contraire, le module de vérification 3C du terminal 3-2 détermine au regard des informations contenues dans la base DB que le terminal 3-1 n'est pas en droit de requérir

l'exécution de l'action ACT par le terminal 3-2 (réponse non à l'étape test H30), le module d'exécution 3D refuse d'exécuter l'action et rejette la requête REQ du terminal 3-1 (étape H40).

Ainsi, grâce à l'invention, chaque dispositif 3 participant au rendu du service de conférence CONF peut connaître les droits et les rôles de chacun des autres dispositifs, et exécuter directement des actions distantes selon un procédé de communication directe entre les dispositifs.

On note que l'invention permet également de s'accommoder aisément d'une mise à jour des droits affectés à un dispositif 3 en cours d'utilisation du service de conférence. Ainsi en référence à la figure 4, si l'un des dispositifs 3 participant au service change par exemple de rôle et devient à titre illustratif « modérateur » plutôt que simple « participant » (réponse oui à l'étape test E70), il envoie via le réseau de télécommunications 2 un message M à la plateforme 5 de distribution des droits pour lui notifier (indiquer) ce changement de rôle (étape E80). Ce message comprend son identité ID(3) ainsi que, dans le mode de réalisation décrit ici, un jeton d'authentification TOK (aussi appelé jeton de sécurité ou token) associé au nouveau rôle qui lui a été affecté, par exemple via la plateforme 4 d'affectation des droits qui lui transmet à cet effet le jeton TOK associé au nouveau rôle de façon sécurisée. En variante, le dispositif 3 ou son utilisateur peut acquérir le jeton TOK par tout autre moyen de manière sécurisée pour s'assurer que seul un dispositif ou un utilisateur autorisé dispose de ce jeton.

Dans ce mode de réalisation, chaque rôle est associé à un jeton de sécurité distinct, de sorte que le jeton d'authentification TOK en lui-même représente une information représentative des droits sur le service alloués au dispositif au sens de l'invention. Un tel jeton d'authentification offre de façon connue en soi une solution d'authentification forte permettant de prouver à la plateforme 5 le droit du dispositif à prétendre à ce nouveau rôle. Il peut s'agir par exemple d'un mot de passe associé au nouveau rôle revendiqué par le dispositif 3.

Le jeton d'authentification associé à un rôle peut être géré par le dispositif 3 de façon transparente pour son utilisateur. En variante, le jeton peut être fourni à la plateforme 5 par l'utilisateur du dispositif 3 auquel cas le message M comprend, en plus de l'identité ID(3), une indication du changement de rôle du dispositif 3 (ex. une information représentative des nouveaux droits alloués à ce dispositif sur le service ou simplement un message de changement de rôle ou de mise à jour de ces droits).

Dans une autre variante encore, le jeton TOK est fourni sous la forme d'un nouvel objet N_OBJ(3) chiffré par la plateforme 4 au dispositif 3, ce nouvel objet reflétant le nouveau rôle affecté au dispositif 3. Dans cette variante, le message M transmis par le dispositif 3 à la plateforme 5 pour lui signaler son changement de rôle comprend le nouvel objet N_OBJ(3) chiffré.

Dans une autre variante encore, le jeton TOK peut être fourni à la plateforme 5 par le dispositif 3 ou par son utilisateur en plus d'un nouvel objet N_OBJ(3) chiffré et fourni au dispositif 3 par la plateforme 4, ce nouvel objet reflétant le nouveau rôle affecté au dispositif 3.

En référence à la figure 6, sur réception du message M (réponse oui à l'étape test G60), la plateforme 5 contrôle le jeton TOK inclus dans le message et met à jour par l'intermédiaire

de son module de construction 5A, dans la base d'identités et de droits DB, les droits RGT(3) associés à l'identité ID(3) avec le rôle correspondant au jeton envoyé par le dispositif 3 (étape G30). Pour contrôler le jeton TOK, la plateforme 5 consulte par exemple une table préconfigurée et stockée dans sa mémoire non volatile, dans laquelle est associé à chaque rôle pouvant être affecté à un dispositif participant au service CONF un jeton TOK devant être présenté par le dispositif pour accéder à ce rôle si celui-ci diffère du rôle qui lui a été attribué initialement dans l'objet OBJ(3) qu'il a transmis à la plateforme 5. Les jetons TOK associés à chacun des rôles peuvent avoir été inclus par la plateforme 4 dans l'objet initial OBJ(3) par exemple, et transmis à la plateforme 5 via le dispositif 3 comme décrit précédemment.

Dans la variante décrite précédemment dans laquelle un nouvel objet N_OBJ(3) chiffré est transmis en tant que jeton TOK dans le message M, le fait pour la plateforme 5 de pouvoir déchiffrer cet objet à l'aide de la clé publique PubK4 associée à la clé privée de la plateforme 4 permet de contrôler le jeton TOK et de déterminer que le dispositif 3 est bien en droit d'accéder à ce nouveau rôle. La plateforme 5 met alors à jour par l'intermédiaire de son module de construction 5A, dans la base d'identités et de droits DB, les droits associés à l'identité ID(3) avec les droits RGT(3) indiqués dans le nouvel objet N_OBJ(3) (étape G30).

Puis la plateforme 5 transmet via son module de transmission 5B aux dispositifs 3 du système 1 la base DB d'identités et de droits ainsi mise à jour, comme décrit précédemment en référence aux étapes G40 et G50.

Les dispositifs 3 traitent et utilisent la base DB ainsi mise à jour de façon similaire à ce qui a été décrit précédemment en référence aux étapes E50 et E60 et à la figure 8.

Dans l'exemple envisagé ici, on a considéré un service de conférence (audio, visio ou audio/vidéo). Toutefois, comme mentionné précédemment, cet exemple n'est donné qu'à titre illustratif et l'invention s'applique à d'autres types de service dont le rendu peut être distribué sur une pluralité de dispositifs. Ainsi, notamment, l'invention s'applique également à un système comprenant une pluralité d'objets connectés.

Pour mieux illustrer cet autre exemple, considérons par exemple un système comprenant quatre objets connectés entre eux via un réseau de télécommunications, tels qu'une caméra O1, une porte O2, un objet O3 embarquant une application de reconnaissance faciale et une chaudière O4. Ces objets offrent un service tel que lorsque l'application reconnaissance faciale reconnaît sur une image saisie par la caméra un membre de la famille devant la porte, elle demande à la porte de s'ouvrir et augmente la température de la chaudière. Selon un tel exemple, on peut définir les droits suivants sur le service :

- droit R1 d'obtenir un état du dispositif ;
- droit R2 de redémarrer le dispositif ;
- droit R3 d'obtenir un flux média du dispositif ;
- droit R4 d'ouvrir la porte ;
- droit R5 de modifier la température ;

et construire la base DB' d'identités et de service représentée à la **figure 9**, où ID(O1), ID(O2), ID(O3), ID(O4) désignent les identités établies pour ce service pour les objets O1, O2, O3 et O4 respectivement.

REVENDICATIONS

1. Procédé de distribution de droits sur un service (CONF), destiné à être mis en œuvre par une plateforme de service (5) et comprenant :

— une étape de construction (G30) d'une base de données dite d'identités et de droits (DB) comprenant, pour chaque dispositif (3) participant au service, une identité (ID(3)) destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information (RGT(3)) représentative de droits sur le service alloués au dispositif; et

— une étape de transmission (G50) de cette base d'identités et de droits à chaque dispositif participant au service.

2. Procédé selon la revendication 1 dans lequel, pour au moins un dispositif participant au service, l'identité et ladite au moins une information représentative des droits sur le service alloués à ce dispositif sont obtenus, par la plateforme de service, dudit dispositif lors de son enregistrement (E40) auprès de la plateforme de service.

3. Procédé selon la revendication 1 ou 2 dans lequel, pour au moins un dispositif participant au service, ladite au moins une information représentative des droits sur le service alloués à ce dispositif comprend un rôle (PART,SUP) associé au dispositif lors de sa participation au service.

4. Procédé selon l'une quelconque des revendications 1 à 3 dans lequel, pour au moins un dispositif participant au service, l'identité et ladite au moins une information représentative des droits sur le service alloués à ce dispositif sont obtenus d'une plateforme (4) d'affectation de droits sur le service.

5. Procédé selon l'une quelconque des revendications 1 à 4 dans lequel la base d'identités et de droits est chiffrée et/ou signée (G40) par la plateforme de service avant d'être transmise à chaque dispositif.

6. Procédé selon l'une quelconque des revendications 1 à 5 comprenant :

— une étape de réception (G60) d'un dispositif participant au service d'une indication d'un changement des droits alloués à ce dispositif sur le service ;

— une étape de mise à jour (G30) de la base d'identités et de droits pour l'identité utilisée par le dispositif conformément à ladite indication ; et

— une étape de transmission (G50) de la base d'identités et de droits mise à jour à chaque dispositif participant au service.

7. Procédé selon la revendication 6 dans lequel ladite indication comprend un jeton d'authentification (TOK) correspondant à au moins un nouveau droit affecté au dispositif.

8. Procédé de traitement d'une requête par un premier dispositif destiné à être mis en œuvre lors d'une participation du premier dispositif à un service, ce procédé comprenant :

— une étape d'obtention (E50) d'une base d'identités et de droits transmise par une plateforme de service suite à l'exécution par ladite plateforme d'un procédé de distribution de droits sur le service selon l'une quelconque des revendications 1 à 6, ladite base d'identité et de droits comprenant, pour chaque dispositif (3) participant au service, une identité (ID(3)) destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information (RGT(3)) représentative de droits sur le service alloués au dispositif ;

— une étape de réception (H10) d'une requête en provenance d'un deuxième dispositif participant au service, cette requête comprenant une identité utilisée par le deuxième dispositif lors de sa participation au service et une action destinée à être exécutée par le premier dispositif ;

— une étape de vérification (H20), dans la base d'identités et de droits, si l'identité comprise dans la requête a le droit de requérir l'exécution de ladite action par le premier dispositif ; et

— le cas échéant (H30), une étape d'exécution (H40) de l'action requise.

9. Procédé de traitement selon la revendication 8 dans lequel la base d'identités et de droits transmise par la plateforme de service est chiffrée et/ou signée, le procédé de traitement comprenant une étape de déchiffrement et/ou de validation de la signature (E60) de la base d'identités et de droits avant de mettre en œuvre l'étape de vérification.

10. Programme d'ordinateur comportant des instructions pour l'exécution des étapes du procédé de distribution de droits sur un service selon l'une quelconque des revendications 1 à 7 et/ou du procédé de traitement selon la revendication 8 ou 9 lorsque ledit programme est exécuté par un ordinateur.

11. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé de distribution de droits sur un service selon l'une quelconque des revendications 1 à 7 et/ou du procédé de traitement selon la revendication 8 ou 9.

12. Plateforme de service (5) apte à diffuser des droits sur un service, cette plateforme de service comprenant :

— un module de construction (5A), configuré pour construire une base de données dite d'identités et de droits comprenant, pour chaque dispositif participant au service, une identité

destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information représentative de droits sur le service alloués au dispositif ; et

— un module de transmission (5B), configuré pour transmettre cette base d'identités et de droits à au moins un autre dispositif participant au service.

13. Dispositif (3), dit premier dispositif, apte à participer à un service, ce premier dispositif comprenant :

— un module d'obtention (3A), apte à obtenir une base d'identités et de droits transmise par une plateforme de service selon la revendication 10 apte à diffuser des droits sur le service, ladite base d'identité et de droits comprenant, pour chaque dispositif (3) participant au service, une identité (ID(3)) destinée à être utilisée par ce dispositif lors de sa participation au service et, associée à cette identité, au moins une information (RGT(3)) représentative de droits sur le service alloués au dispositif ;

— un module de réception (3B), apte à recevoir une requête en provenance d'un deuxième dispositif apte à participer au service, cette requête comprenant une identité utilisée par le deuxième dispositif lors de sa participation au service et une action destinée à être exécutée par le premier dispositif ;

— un module de vérification (3D), activé par le module de réception suite à la réception de la requête en provenance du deuxième dispositif, et configuré pour vérifier dans la base d'identités et de droits si l'identité comprise dans la requête a le droit de requérir l'exécution de ladite action par le premier dispositif ; et

— un module d'exécution (3D) configuré pour exécuter l'action requise dans la requête, activé si le module de vérification détermine que l'identité comprise dans la requête a le droit de requérir l'exécution de cette action par le premier dispositif.

14. Système (1) offrant un service et comprenant :

— une plateforme de service selon la revendication 12, apte à diffuser des droits sur le service ; et

— une pluralité de dispositifs selon la revendication 13 aptes à participer audit service.

15. Système selon la revendication 14 comprenant en outre une plateforme (4) d'affectation de droits sur le service, cette plateforme d'affectation de droits comprenant :

— un module d'authentification (4A), configuré pour authentifier un dispositif destiné à participer au service ;

— un module d'affectation (4B) à ce dispositif d'une identité destinée à être utilisée par le dispositif lors de sa participation au service et de droits sur le service ; et

— un module de transmission (4C), au dispositif et/ou à la plateforme de service, de l'identité et d'au moins une information représentative des droits affectés au dispositif par le module d'affectation.

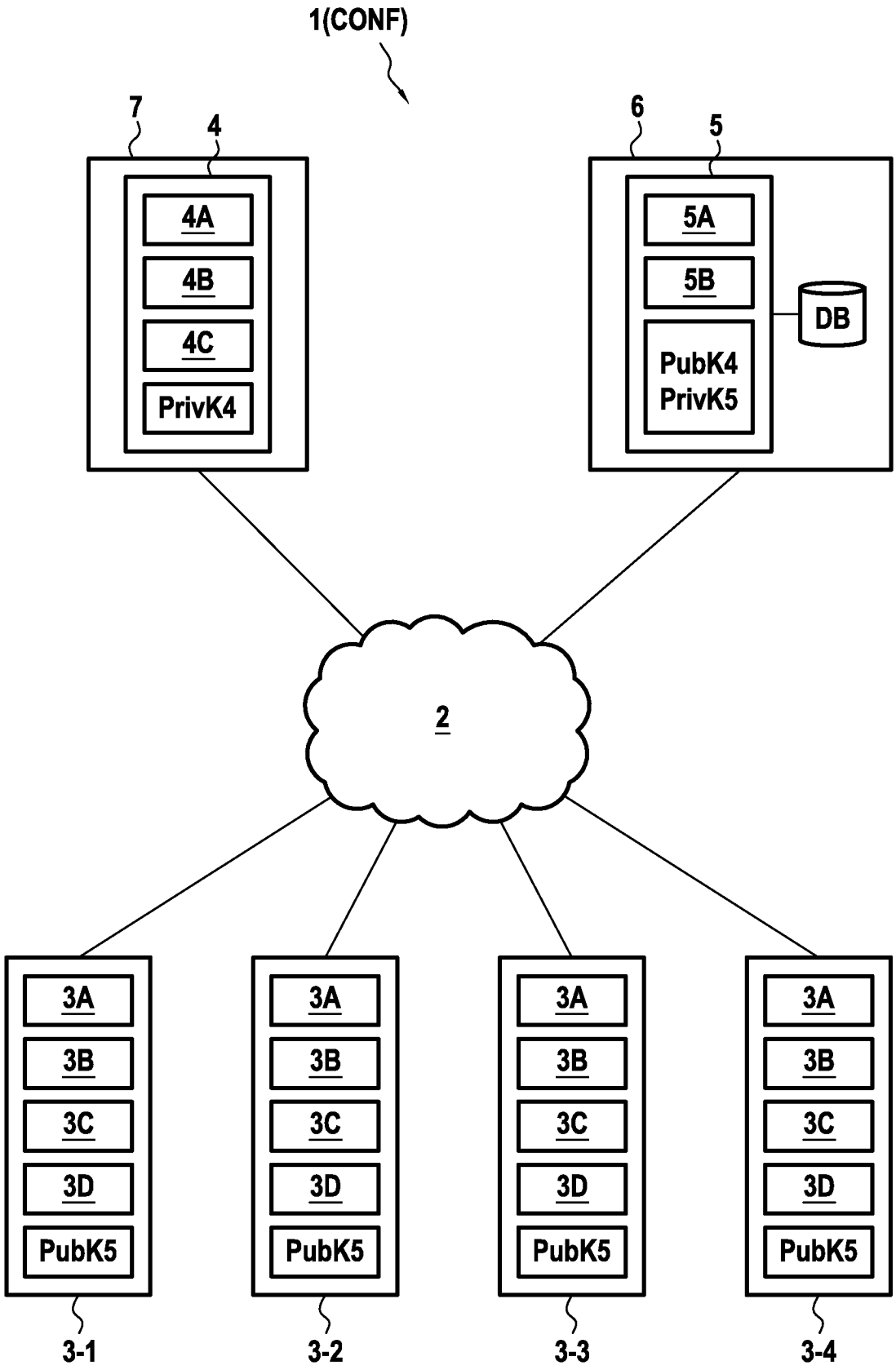

1(CONF)
7
4
4A
4B
4C
PrivK4
6
5
5A
5B
DB
PubK4
PrivK5
2
3A
3B
3C
3D
PubK5
3-1
3-2
3-3
3-4

FIG.1

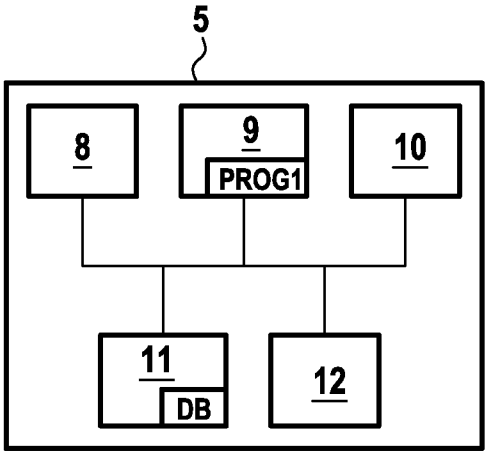


FIG.2

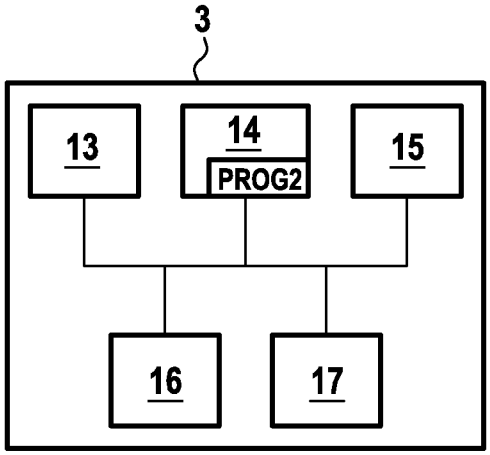
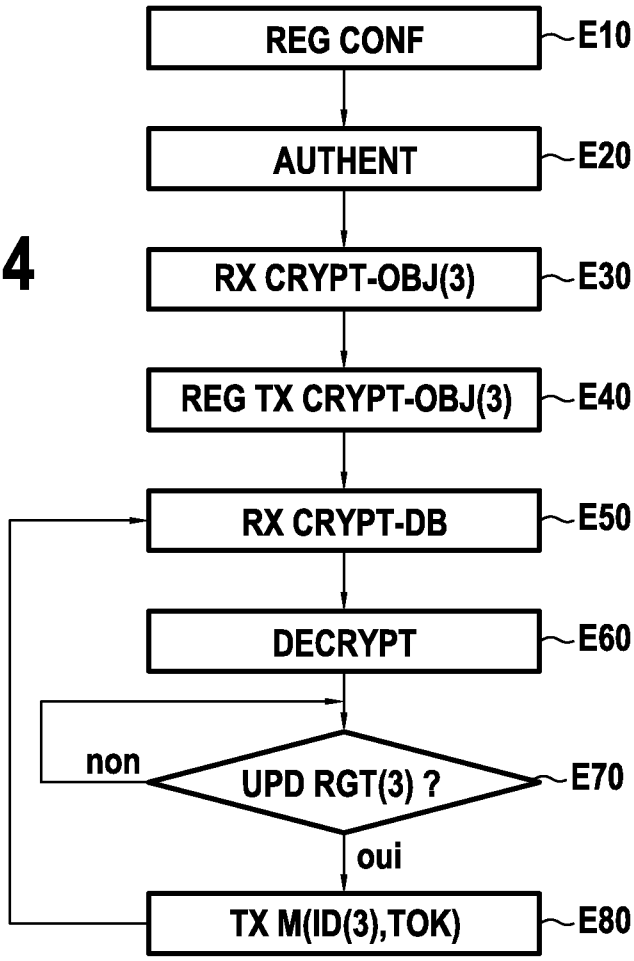


FIG.3

FIG.4



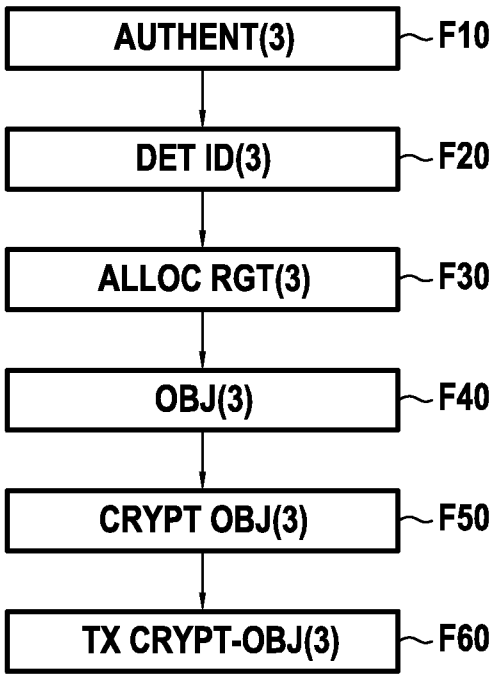


FIG.5

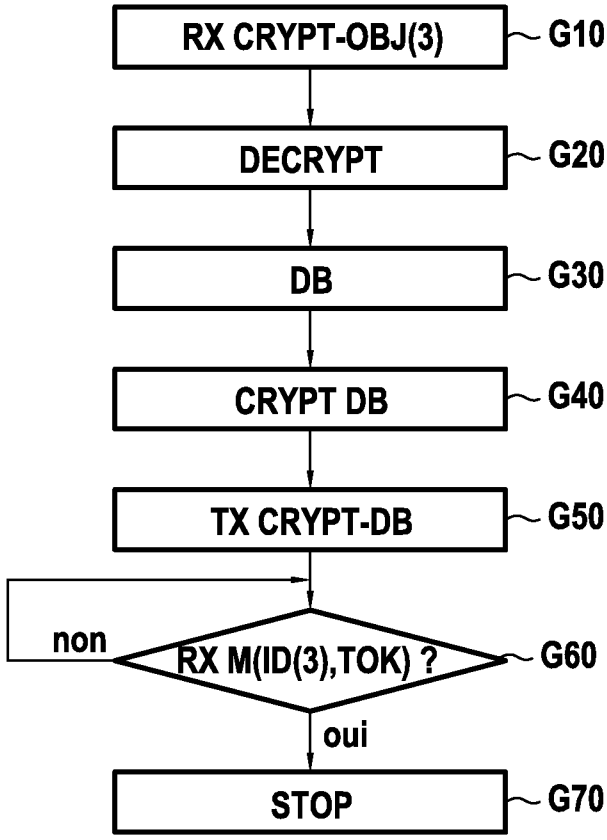


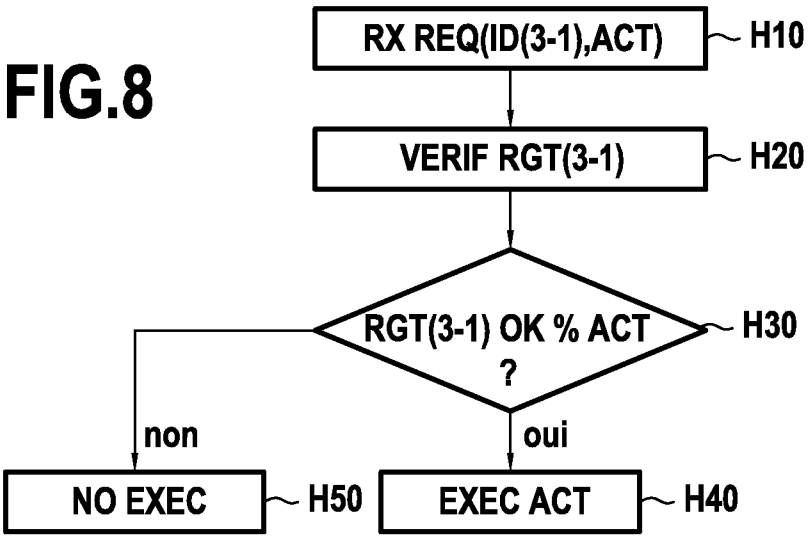
FIG.6

DB

		C1	C2	C3	C4
		ID(3-1)	ID(3-2)	ID(3-3)	ID(3-4)
L1	ID(3-1)	—	SUP	SUP	SUP
L2	ID(3-2)	PART	—	PART	PART
L3	ID(3-3)	PART	PART	—	PART
L4	ID(3-4)	PART	PART	PART	—

FIG.7

FIG.8



DB'

	ID(O1)	ID(O2)	ID(O3)	ID(O4)
ID(O1)	—	—	R1	—
ID(O2)	—	—	R1	—
ID(O3)	R1,R2,R3	R1,R2,R3	—	R1,R2,R4
ID(O4)	—	—	R1	—

FIG.9

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2016/053072

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/18
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 G06F

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	WO 2012/170786 A1 (SGROUPLES INC [US]; WEINSTEIN MARK [US]; WOLFE JONATHAN [US]) 13 December 2012 (2012-12-13) paragraph [0008] - paragraph [0009] paragraph [0039] - paragraph [0156] paragraph [0168] - paragraph [0173]; claims 1-13; figures 1-32	1-15
X	WO 2006/124138 A2 (MICROSOFT CORP [US]) 23 November 2006 (2006-11-23) paragraph [0012] - paragraph [0049]; claims 1-15; figures 2-5	1-15
X	US 2014/033067 A1 (PITTENGER JASON T [US] ET AL) 30 January 2014 (2014-01-30) paragraph [0015] - paragraph [0082]; claims 1-13; figures 1-11	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
2 February 2017	10/02/2017

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	Camba, Sonia

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2016/053072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012170786 A1	13-12-2012	CA 2875847 A1	13-12-2012
		EP 2718832 A1	16-04-2014
		JP 2014527208 A	09-10-2014
		US 2012331568 A1	27-12-2012
		WO 2012170786 A1	13-12-2012
WO 2006124138 A2	23-11-2006	EP 1872217 A2	02-01-2008
		JP 4851515 B2	11-01-2012
		JP 2008546052 A	18-12-2008
		KR 20080016536 A	21-02-2008
		US 2006265262 A1	23-11-2006
		WO 2006124138 A2	23-11-2006
US 2014033067 A1	30-01-2014	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2016/053072

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L12/18
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 G06F

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	WO 2012/170786 A1 (SGROUPLES INC [US]; WEINSTEIN MARK [US]; WOLFE JONATHAN [US]) 13 décembre 2012 (2012-12-13) alinéa [0008] - alinéa [0009] alinéa [0039] - alinéa [0156] alinéa [0168] - alinéa [0173]; revendications 1-13; figures 1-32	1-15
X	WO 2006/124138 A2 (MICROSOFT CORP [US]) 23 novembre 2006 (2006-11-23) alinéa [0012] - alinéa [0049]; revendications 1-15; figures 2-5	1-15
X	US 2014/033067 A1 (PITTENGER JASON T [US] ET AL) 30 janvier 2014 (2014-01-30) alinéa [0015] - alinéa [0082]; revendications 1-13; figures 1-11	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
2 février 2017	10/02/2017

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	Camba, Sonia

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2016/053072

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2012170786 A1	13-12-2012	CA 2875847 A1	13-12-2012
		EP 2718832 A1	16-04-2014
		JP 2014527208 A	09-10-2014
		US 2012331568 A1	27-12-2012
		WO 2012170786 A1	13-12-2012
WO 2006124138 A2	23-11-2006	EP 1872217 A2	02-01-2008
		JP 4851515 B2	11-01-2012
		JP 2008546052 A	18-12-2008
		KR 20080016536 A	21-02-2008
		US 2006265262 A1	23-11-2006
		WO 2006124138 A2	23-11-2006
US 2014033067 A1	30-01-2014	AUCUN	