(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
12 janvier 2017 (12.01.2017)

WIPO IPCT

(10) Numéro de publication internationale
WO 2017/005644 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01) *H04W 4/00* (2009.01)
H04L 9/32 (2006.01) *H04W 12/04* (2009.01)

(21) Numéro de la demande internationale :
PCT/EP2016/065563

(22) Date de dépôt international :
1juillet 2016 (01.07.2016)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1556335 3juillet 2015 (03.07.2015) FR

(71) Déposant : **IXXI** [FR/FR]; 8, avenue Montaigne, Immeuble Maille Nord II, 93160 Noisy-le-Grand (FR).

(72) Inventeurs : **TERREE, Pierre;** 9 rue Suffren, 97460 Saint-Paul La Réunion (FR). **DEMAILLY, Nicolas;** 2, passage du Charolais, 75012 Paris (FR).

(74) Mandataires : **GRAND, Guillaume** et al.; Lavoix, 62, rue de Bonnel, 69003 Lyon (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, 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, 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))*

(54) **Title** : METHOD AND SYSTEM FOR CONTROLLING ACCESS TO A SERVICE VIA A MOBILE MEDIA WITHOUT A TRUSTED INTERMEDIARY

(54) **Titre** : PROCÉDÉ ET SYSTÈME DE CONTRÔLE D'ACCÈS À UN SERVICE VIA UN MÉDIA MOBILE SANS INTERMEDIAIRE DE CONFIANCE

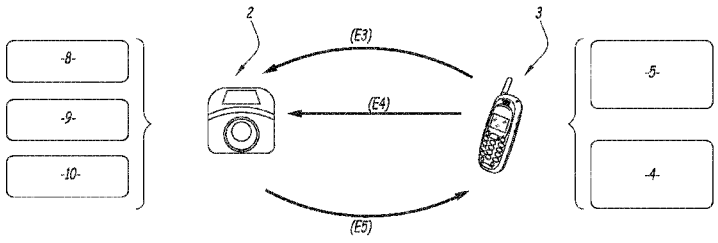


Fig.2

(57) **Abstract** : The invention relates to a method and a System for controlling access rights to a service which a user U accesses by means of a mobile média (3), having application in particular in secure transactions involving electronic ticketing, electronic money or access control to a transport network, for which a user equipped with a mobile média asserts, by the intermediary of said média, a right which must be controlled. The method comprises sending, by a rights transmission System (1), of a digital access right to the service associated with the mobile média (3), the transmission to, and storage in, the média (3) of the digital right transmitted by the sending System (1), and control of the validity of the digital right stored in the média (3) by a rights acceptance terminal (2), which comprises the transmission to the acceptance terminal (2) of the digital right stored in the média (3) and a single-use transaction certificate generated by the média (3), and the control by the acceptance terminal (2), in a mode disconnected from the sending System (1), of the authenticity of the digital right and of the validity of the transaction certificate.

(57) **Abrégé :**

[Suite sur la page suivante]

WO 2017/005644 A1

L'invention concerne un procédé et un système de contrôle des droits d'accès à un service auquel un utilisateur U accède au moyen d'un média mobile (3), trouvant notamment une application aux transactions sécurisées de billettique, de monétique, ou de contrôle d'accès à un réseau de transport, pour lesquelles un utilisateur équipé d'un média mobile fait valoir, par l'intermédiaire de ce média, un droit qui doit être contrôlé. Le procédé comprend l'émission, par un système d'émission de droits (1), d'un droit numérique d'accès au service associé au média mobile (3), la transmission au, et le stockage dans le, média (3) du droit numérique émis par le système d'émission (1), et le contrôle de validité du droit numérique stocké dans le média (3) par un terminal d'acceptation de droits (2), qui comprend la transmission au terminal d'acceptation (2) du droit numérique stocké dans le média (3) et d'un certificat de transaction à usage unique généré par le média (3), et le contrôle par le terminal d'acceptation (2), en mode déconnecté du système d'émission (1), de l'authenticité du droit numérique et de la validité du certificat de transaction.

Procédé et système de contrôle d'accès à un service via un média mobile sans intermédiaire de confiance

La présente invention concerne un procédé et un système de contrôle des droits d'accès à un service auquel un utilisateur accède au moyen d'un média mobile sans intermédiaire de confiance. Elle trouve en particulier une application aux transactions sécurisées de billettique, de monétique, ou de contrôle d'accès à un réseau de transport, pour lesquelles un utilisateur équipé d'un média mobile fait valoir, par l'intermédiaire de ce média, un droit qui doit être contrôlé.

Les procédés et systèmes de contrôle connus opèrent via un terminal qui est soit en ligne, c'est-à-dire connecté à un serveur distant, soit hors ligne, c'est-à-dire déconnecté de tout serveur distant.

Précisément, dans le premier cas, l'utilisateur s'authentifie auprès du terminal et celui-ci contacte alors le serveur distant afin de vérifier en ligne si l'utilisateur dispose des droits d'accès au service auquel il tente d'accéder.

Pour s'authentifier, l'utilisateur peut utiliser un média dont la fonction se limite à l'identification et qui ne stocke aucune information de droit d'accès.

Dans le deuxième cas, l'utilisateur dispose d'un média comprenant une mémoire sécurisée stockant des informations de droit d'accès, ce qui lui permet à la fois de s'authentifier auprès du terminal et de faire valoir hors ligne son droit d'accès.

Comme indiqué précédemment, dans ce deuxième cas, le média est pourvu d'une mémoire de stockage sécurisée, c'est-à-dire que les données qu'elle contient ne peuvent être modifiées sans disposer d'éléments cryptographiques. C'est généralement le cas des cartes à puce à microprocesseur.

Un des problèmes posés par les procédés et systèmes dans lesquels le terminal fonctionne en mode connecté au serveur, est celui de la vitesse de transaction limitée.

En effet, en fonction du domaine d'application, il peut être requis une vitesse de transaction importante pour la vérification des droits. Or, la qualité de la connectivité réseau du terminal peut être difficile à garantir, en particulier dans le cas où le terminal est embarqué dans un véhicule en mouvement. C'est pourquoi, dans le domaine de la billettique pour un réseau de transport, il est courant que la vérification du droit d'accès au réseau soit opérée par des terminaux en mode déconnecté.

Cependant, les procédés et systèmes dans lesquels le terminal fonctionne en mode déconnecté du serveur pose notamment le problème de l'utilisation d'un média pourvu d'une mémoire sécurisée.

En effet, la distribution de médias à mémoire sécurisée par un opérateur d'un service auprès des utilisateurs est complexe et onéreuse, en particulier en raison du fait que ces médias à mémoire sécurisée sont de nature fermée, avec des systèmes d'hébergement des données complexes et onéreux.

Les documents suivants sont également connus de l'état de la technique : WO 201 5/092261 -A1 , FR 2 950 450-A1 et US 2003/0093695-A1 .

Un des buts de l'invention est donc de résoudre les problèmes précités. Ainsi, l'invention a notamment pour objectif de proposer un procédé et un système fiable et rapide de contrôle des droits d'accès à un service auquel un utilisateur accède au moyen d'un média mobile pourvu d'une mémoire non sécurisée.

Ainsi, l'invention a pour objet, selon un premier aspect, un procédé de contrôle des droits d'accès à un service auquel un utilisateur accède au moyen d'un média mobile, tel que défini à la revendication 1.

Suivant certains modes de réalisation, le procédé comprend en outre une ou plusieurs des caractéristiques des revendications 2 à 7.

L'invention a également pour objet, selon un deuxième aspect, un système de contrôle des droits d'accès à un service accessible à un utilisateur au moyen d'un média mobile tel que défini à la revendication 8.

Suivant certains modes de réalisation, le système comprend en outre une ou plusieurs des caractéristiques des revendications 9 à 11.

Ainsi, le procédé et le système de l'invention permettent le contrôle rapide des droits d'accès d'un utilisateur à un service, dans la mesure où le terminal d'acceptation fonctionne de façon autonome, en mode déconnecté du système d'émission, pour la vérification des droits d'accès.

Par ailleurs, le procédé et le système de l'invention sont fiables, en termes de sécurisation des transactions, sans les contraintes de complexité et de coût de gestion, pour un opérateur de service, liées à l'utilisation de médias à mémoire sécurisée.

Cette sécurisation est apportée notamment par l'utilisation d'un certificat de transaction à usage unique, avec ainsi une protection contre la duplication et la falsification des droits d'accès.

En outre, les utilisateurs peuvent par exemple utiliser un média déjà en leur possession, indépendamment de leur inscription en tant qu'utilisateurs du service en question, tel qu'un téléphone mobile.

En effet, un téléphone mobile peut intégrer une puce disposant d'une mémoire sécurisée, telle qu'une carte SIM, mais intègre également une mémoire non sécurisée. Or

la possibilité de stocker des données dans cette mémoire non sécurisée est libre, simple à mettre en œuvre, et sans contrainte de capacité.

De plus, grâce au fait que la clef de chiffrement privée média est générée par le média mobile lui-même, au lieu d'être acquise auprès d'un tiers de confiance, la sécurité du média mobile et de l'accès au service s'en trouve améliorée. En effet, le risque de compromettre la sécurité de la clef média est réduit.

De plus, de cette manière, on se dispense d'avoir recours à un tiers de confiance pour acquérir la clef de chiffrement privée média, ce qui réduit le coût et la complexité de la mise en place du système de contrôle des droits d'accès. En outre, il est courant, dans les systèmes connus, qu'une clef de chiffrement privée média acquise auprès d'un tiers de confiance soit utilisée pour plusieurs applications différentes, ce qui augmente le risque d'en compromettre la sécurité.

Les caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple, et non limitative, en référence aux figures annexées suivantes :

- figure 1 : représentation schématique, dans un exemple de réalisation et de mise en œuvre, d'une première partie du système et du procédé selon l'invention ;
- figure 2 : représentation schématique, dans un exemple de réalisation et de mise en œuvre, d'une deuxième partie du système et du procédé selon l'invention ;
- figure 3 : représentation schématique, dans un exemple de mise en œuvre, de l'ensemble du procédé selon l'invention.

Le procédé selon l'invention se décompose en deux principales étapes. La première, illustrée à la figure 1 sur un exemple de mise en œuvre, concerne l'obtention d'un droit d'accès par un utilisateur auprès d'un opérateur émetteur et son chargement dans un média mobile. La deuxième, illustrée à la figure 2 sur un exemple de mise en œuvre, concerne la présentation du média par l'utilisateur à un terminal accepteur pour la validation de l'accès.

La figure 1 concerne donc plus particulièrement l'émission des droits d'accès par le système de contrôle, précisément par un système d'émission 1 de droits.

Ce système d'émission 1 peut être de type serveur informatique, comprenant une base de données d'utilisateurs et de droits 6, ainsi qu'un gestionnaire sécurisé de clef 7 incluant notamment une clef privée d'émission notée K_Priv_Em.

Le système d'émission 1 est ainsi apte à chiffrer et déchiffrer des informations au moyen de sa clef privée d'émission K_Priv_Em, selon le principe de chiffrement asymétrique ou chiffrement à clef publique. La clef privée d'émission K_Priv_Em est donc

associée à une clef publique d'émission K_Pub_Em sur laquelle nous reviendrons plus loin dans cette description.

Plus généralement, le système d'émission 1 est donc apte à gérer de manière sécurisée les certificats cryptographiques asymétriques, donc la génération de clefs et de signatures numériques de données.

La base de données d'utilisateurs et de droits 6 comprend notamment des identifiants d'utilisateurs associés à des données de droits, ainsi qu'à des clefs publiques médias K_PubJVIedia correspondant aux médias 3 mobiles utilisés par les utilisateurs respectifs.

Les médias 3 mobiles sont également aptes à gérer de manière sécurisée les certificats cryptographiques asymétriques, donc la génération de clefs et de signatures numériques de données, au moyen d'un gestionnaire sécurisé de clefs 5 comprenant notamment une clef privée média notée K_Priv_Media. Cette clef privée média K_Priv_Media est générée par le gestionnaire sécurisé de clefs 5 spécifiquement pour le service concerné.

De cette manière, la clef privée média K_Priv_Media est dès l'origine enregistrée dans la mémoire sécurisée du gestionnaire sécurisé des clefs 5. Il n'est pas nécessaire d'acquérir la clef privée média K_Priv_Media auprès d'un tiers de confiance, ou intermédiaire de confiance, extérieur au média 3, ce qui réduirait la sécurité du média 3.

Les médias 3 sont ainsi aptes à chiffrer et déchiffrer des informations au moyen de leurs clefs privées média K_Priv_Media respectives, selon le principe de chiffrement asymétrique ou chiffrement à clef publique. Les clefs privée média K_Priv_Media sont donc respectivement associées à des clefs publiques média K_PubJVIedia sur lesquelles nous reviendrons plus loin dans cette description.

Chaque média 3 raccordé au service concerné génère, par l'intermédiaire de son gestionnaire sécurisé de clefs 5, une seule clef K_Priv_Media, et son pendant public que constitue la clef publique média K_PubJVIedia, pour ce dit service.

Ces médias 3 disposent par ailleurs d'une mémoire non sécurisée 4, dont on verra plus loin qu'elle permet de stocker un droit numérique d'accès au service. Ces médias 3 sont donc aptes à traiter et mémoriser des données dans un environnement de stockage 4 non sécurisé.

Les médias 3 disposent d'interfaces de communication, qui peuvent être par exemple de type visuel, radio ou sonore, afin de permettre la communication avec le système d'émission 1 potentiellement distant, ainsi que la communication en proximité

avec des terminaux d'acceptation 2 de droits tel qu'illustré à la figure 2 qui sera décrite plus loin.

Dans une étape (E2), un droit numérique est émis par le système d'émission 1 et transmis par celui-ci au média 3. Il s'agit d'un droit numérique d'accès à un service donné associé au média 3 dans la base de données 6 du système d'émission 1. Ce droit numérique est ainsi récupéré et stocké dans la mémoire non sécurisée 4 du média 3.

Lors de l'initialisation du service sur le média 3, ce dernier génère une première fois, de manière sécurisée, un certificat pour ce service, lié au média 3, par l'intermédiaire du gestionnaire sécurisé de clefs 5.

A ce certificat correspond une clef privée média K_Priv_Media qui reste, sans jamais en sortir, dans la mémoire sécurisée du gestionnaire sécurisé de clefs 5 du média 3.

A ce certificat correspond par ailleurs une clef publique média K_PubJVIedia, qui peut être extraite et communiquée à des entités extérieures, de sorte qu'une telle entité extérieure soit en mesure, via cette clef publique média K_PubJVIedia d'authentifier de manière forte le média 3 en question.

Afin de récupérer le droit numérique de la part du système d'émission 1, le média 3 communique avec le système d'émission 1 lors d'une étape (E1) au cours de laquelle il s'authentifie auprès du système d'émission 1 et il lui transmet sa clef publique média K_Pub_Media.

La méthode d'authentification auprès du système d'émission 1 est liée à l'utilisateur, mais pas nécessairement au média 3, l'important étant que l'utilisateur porteur du média 3 soit authentifié auprès du système d'émission 1 de manière forte. Il peut s'agir par exemple d'un échange de nom d'utilisateur et de mot de passe, de l'enrichissement d'une requête réseau, etc..

Une fois l'utilisateur authentifié via le média 3, ce dernier transmet donc sa clef publique média K_PubJVIedia au système d'émission 1. Ce média 3 est alors enregistré dans la base de données 6 du système d'émission 1 comme appartenant à l'utilisateur préalablement authentifié.

Le système d'émission 1 dispose pour sa part de son propre certificat généré par son gestionnaire sécurisé de clefs 7.

A ce certificat correspond une clef privée d'émission K_Priv_Em qui reste, sans jamais en sortir, dans la mémoire sécurisée du gestionnaire sécurisé de clefs 7 du système d'émission 1.

A ce certificat correspond par ailleurs une clef publique d'émission K_Pub_Em, qui peut être extraite et communiquée à des entités extérieures.

Comme indiqué plus haut, lors de l'étape (E2), le système d'émission génère et transmet au média 3 un droit numérique d'accès au service, pour l'utilisateur préalablement authentifié lors de l'étape (E1) et le média 3 préalablement enregistré lors de cette étape (E1) comme appartenant à cet utilisateur authentifié.

Ainsi, l'étape (E2) est postérieure à l'étape (E1).

Un droit numérique correspond ainsi à des données de droit d'accès au service, certifiées comme rattachées à un média 3, donc indirectement à un utilisateur puisque qu'un média 3 est lié à un utilisateur dans la base de données 6 du système d'émission 1.

Mais ce droit numérique doit pouvoir être certifié comme ayant été émis par le système d'émission 1.

Ainsi, le système d'émission 1 fournit au média 3 un message de données formant le droit numérique, comprenant des données de droit associées au média 3 via sa clef publique média K_PubJVIedia, ainsi qu'une signature numérique des données de droit et de la clef publique média K_PubJVIedia du média 3 à partir de la clef privée d'émission K_Priv_Em du système d'émission 1.

Cette signature numérique correspondant donc au chiffrage, par la clef privée d'émission K_Priv_Em du système d'émission 1, des données de droit et de la clef publique média K_PubJVIedia du média 3.

Ce droit numérique est alors stocké dans la mémoire non sécurisée 4 du média 3.

La figure 2 concerne quant à elle plus particulièrement le contrôle des droits d'accès au service par un terminal d'acceptation 2 de droits, pour un média 3 porté par un utilisateur se présentant au contrôle pour accéder audit service.

Le terminal 2 fonctionne de manière autonome, en mode déconnecté du système d'émission 1 représenté à la figure 1.

Ce terminal d'acceptation 2 stocke la clef publique d'émission K_Pub_Em dans une zone de stockage 8 appropriée, clef obtenue par exemple lors de la mise en service du terminal d'acceptation 2 par une connexion au système d'émission 1. A défaut d'avoir été obtenue préalablement, cette clef publique d'émission K_Pub_Em peut éventuellement être incluse dans le droit numérique, de sorte que le terminal d'acceptation 2 puisse l'utiliser lors du contrôle du droit comme il sera expliqué plus loin. Dans ce cas, la clef publique d'émission K_Pub_Em doit avoir été certifiée par une autorité tierce de confiance reconnue par le terminal d'acceptation 2.

Par ailleurs, le terminal d'acceptation 2 peut comprendre un générateur d'aléa de transaction 9 dont la fonction sera expliquée plus loin, ainsi qu'un interpréteur de droits 10.

Ainsi, lorsque l'utilisateur présente son média 3 pour le contrôle du droit numérique préalablement obtenu auprès du système d'émission 1 et stocké dans sa mémoire non sécurisée 4, tel qu'expliqué plus haut, pour faire valoir ce droit numérique auprès du terminal d'acceptation 2, ce dernier n'a pas besoin d'être connecté au système d'émission 1 pour vérifier la validité du droit numérique présenté.

Pour opérer ce contrôle de validité, le droit numérique stocké dans le média 3 est transmis (E4) au terminal d'acceptation 2, qui va authentifier à la fois le média 3 et le droit numérique présenté. Une fois ce contrôle de validité réalisé par le terminal d'acceptation 2, les droits d'accès contenus dans le droit numérique validé sont interprétés par l'interpréteur de droit 10 du terminal d'acceptation 2.

Afin d'éviter que le droit numérique puisse être cloné, il est nécessaire de protéger la transaction de communication du droit numérique par le média 3 au terminal d'acceptation 2, contre le rejeu. Pour ce faire, le média 3 transmet au terminal d'acceptation 2, outre le droit numérique, un certificat de transaction à usage unique généré par ce média 3.

Ce certificat de transaction à usage unique est généré par le gestionnaire sécurisé de clefs 5 du média 3, en utilisant une valeur d'aléa à usage unique.

Si la communication entre le terminal d'acceptation 2 et le média 3 est bidirectionnelle, la valeur d'aléa est générée par le générateur d'aléa de transaction 9 du terminal d'acceptation 2 et transmise (E3) par ce dernier au média 3.

Si par contre, la communication entre le terminal d'acceptation 2 et le média 3 est unidirectionnelle du média 3 vers le terminal d'acceptation 2, cette valeur d'aléa peut être prédéterminée par le média 3, par exemple sous la forme d'un horodatage à durée de validité limitée (exemple : date et heure courantes).

Le terminal d'acceptation 2 obtient du média 3 à la fois le droit numérique, c'est-à-dire le message numérique préalablement émis et signé par le système d'émission 1 et contenant la clef publique média K_PubJVIedia, et le certificat de transaction généré par le média 3.

Ce certificat de transaction correspond à une contresignature numérique du droit numérique et de la valeur d'aléa à usage unique, par la clef privée média K_Priv_Media.

Pour la fiabilité du procédé de contrôle, il est nécessaire que le terminal d'acceptation 2 ait confiance envers le système d'émission 1. C'est la raison pour laquelle

le terminal d'acceptation 2 dispose de la clef publique d'émission K_Pub_Em du système d'émission 1, comme on l'a vu plus haut.

Pour le contrôle de validité du droit numérique, le terminal d'acceptation 2 peut donc contrôler deux signatures : la signature associée au droit numérique, générée par le système d'émission 1, pour l'authentification du droit ; la contresignature associée au certificat de transaction généré par le média 3, pour l'authentification du média 3 et de son utilisateur.

Les deux contrôles de signature correspondants peuvent être réalisés dans un ordre quelconque.

Ainsi, le contrôle de l'authenticité du droit numérique obtenu depuis le média 3 est réalisé par le terminal d'acceptation 2 par l'intermédiaire de la clef publique d'émission K_Pub_Em du système d'émission 1, clef à laquelle le terminal d'acceptation 2 fait implicitement confiance (voir plus haut quelques possibilités d'obtention par le terminal d'acceptation 2 de cette clef publique d'émission K_Pub_Em).

En déchiffrant la signature numérique contenue dans le droit numérique, au moyen de la clef publique d'émission K_Pub_Em, le terminal d'acceptation 2 vérifie l'authenticité du droit numérique. Il peut ainsi déterminer que le droit en question a bien été émis par le système d'émission 1 concerné, à destination du média 3 spécifique (puisque la clef publique média K_PubJVIedia fait partie des données contenues dans le droit numérique).

Si le droit numérique est authentifié, alors le terminal d'acceptation 2 accorde sa confiance au média 3.

Par ailleurs, le contrôle de la validité du certificat de transaction à usage unique obtenu depuis le média 3 est réalisé par le terminal d'acceptation 2 par l'intermédiaire de la clef publique média K_PubJVIedia.

En déchiffrant la contresignature numérique correspondant au certificat de transaction à usage unique, au moyen de la clef publique média K_PubJVIedia, le terminal d'acceptation 2 vérifie l'authenticité du média 3. Si l'aléa déchiffré est valide, le terminal d'acceptation 2 authentifie le média 3.

Ces deux vérifications de signature permettent au terminal d'acceptation 2 d'une part de déterminer que l'utilisateur présentant son média 3 au contrôle dispose bien des droits authentiques d'accès au service concerné, c'est-à-dire que le droit contrôlé est bien rattaché au média 3 enregistré dans la base de données 6 du système d'émission,, et d'autre part d'authentifier le média 3 et le droit, c'est-à-dire de vérifier que le droit n'a pas été cloné par un autre média.

La figure 3 illustre de manière synthétique l'ensemble du processus décomposé plus haut en référence aux figures 1 et 2.

L'utilisateur U procède à l'initialisation (a) du service concerné sur son média 3, qui génère alors la paire de clefs privée et publique média K_Priv_Media et K_PubJVIedia, par l'intermédiaire de son gestionnaire sécurisé de clefs 5.

Ensuite, l'utilisateur U, via le média 3, sélectionne (c) un droit d'accès qu'il souhaite obtenir auprès du système d'émission 1.

Le média 3 s'authentifie (d) alors auprès du système d'émission 1 et transmet (e) la sélection de l'utilisateur U.

Une fois l'authentification réalisée, le système d'émission 1 génère (f) puis émet (g), à destination du média 3, le droit numérique qui contient la signature des données de droit et de la clef publique média K_PubJVIedia par l'intermédiaire de la clef privée d'émission K_Priv_Em.

Ensuite, l'utilisateur U présente (h) le média 3 pour contrôle du droit d'accès par le terminal d'acceptation 2.

Le média 3 génère (i) alors le certificat de transaction à usage unique, donc la contresignature du droit numérique et de la valeur d'aléa à usage unique, par l'intermédiaire de la clef privée média K_Priv_Media.

Selon le type d'interface de communication utilisé, pour la communication entre le média 3 et le terminal d'acceptation 2, le droit numérique et le certificat de transaction à usage unique sont transmis par le média 3 au terminal d'acceptation 2, ou directement lues (j) par le terminal d'acceptation 2.

Le terminal d'acceptation 2 procède (k) alors au contrôle du droit numérique et du certificat de transaction à usage unique, puis, éventuellement, notifie (l) le résultat du contrôle au média 3 si l'interface le permet.

Une notification peut également être envoyée (m) directement par le terminal d'acceptation 2 à l'utilisateur U, via une interface visuelle ou sonore par exemple.

Les informations de validation sont éventuellement remontées ultérieurement au système d'émission 1, cette fois par fonctionnement du terminal d'acceptation 2 en mode connecté au système d'émission 1.

Eventuellement également, les informations de génération d'un certificat, tel qu'un certificat de transport lorsque le service en question concerne l'accès à un, et l'utilisation d'un, réseau de transport, peuvent être remontées (o) par le média 3 vers le système d'émission 1.

Dans la suite, deux exemples d'application du procédé et du système de l'invention sont décrits.

Le premier exemple concerne la billettique par tag radio avec un média 3 mobile de type NFC (« Near Field Communication ») - HCE (« Host Card Emulation »), correspondant à un système de billettique fonctionnant en système fermé, c'est-à-dire dans lequel le système d'émission 1 et les terminaux d'acceptation 2 sont gérés par un même opérateur.

Le système d'émission 1 correspond par exemple à un serveur billettique 1 en ligne, auprès duquel les utilisateurs du service sont enregistrés. Ces utilisateurs disposent ainsi de comptes clients par l'intermédiaire desquels ils peuvent s'authentifier en ligne, par exemple via un système d'authentification classique de type nom d'utilisateur / mot de passe.

Les terminaux d'acceptation 2 correspondent par exemple à des valideurs 2 équipés d'un coupleur de type NFC et disposant de la clef publique d'émission K_Pub_Em du serveur billettique 1.

Le serveur billettique 1 peut offrir la possibilité d'acheter en ligne des droits associés aux comptes clients des utilisateurs.

Le serveur billettique 1 peut par ailleurs proposer, via un magasin d'applications, une application mobile relative au service à télécharger sur les médias 3 mobiles des utilisateurs.

Lors du premier démarrage, l'application mobile procède à la génération du certificat du média 3 mobile sur laquelle elle est lancée, donc à la génération de la paire de clefs privée et publique média K_Priv_Media et K_PubJVIedia.

L'application peut aussi permettre l'enregistrement du client utilisateur auprès du serveur billettique 1.

Cette application mobile peut aussi servir d'interface utilisateur pour l'achat de droits sur le serveur billettique 1.

Lors de l'authentification de l'utilisateur auprès du serveur billettique 1 via l'application mobile, cette dernière peut transmettre au serveur billettique 1 le certificat du média 3 afin d'associer le média 3 au compte utilisateur correspondant.

Pour que l'utilisateur puisse faire valoir ses droits acquis d'accès au service concerné, l'application mobile télécharge au préalable dans la mémoire non sécurisée du média 3 les droits associés à ce média 3 (via la clef publique média K_PubJVIedia) et signés par la clef privée d'émission K_Priv_Em du serveur billettique 1, depuis ce serveur billettique 1.

Dans un deuxième temps, l'utilisateur peut présenter son média 3 auprès d'un valideur 2, afin de faire valoir ses droits. Avec un média 3 mobile de type NFC-HCE, disposant d'une antenne radio permettant une communication de proximité en mode émulation de carte, et si l'application mobile est définie comme un service de type HCE, alors cette application mobile peut être sélectionnée par le valideur 2 pour une communication radio.

La transaction est initiée par la sélection de l'application mobile par le valideur 2 suite à la détection d'une présence d'un média 3 mobile de type NFC dans le champ électromagnétique émis par le valideur 2.

Suite à cette sélection, le valideur 2 fournit une valeur d'aléa de transaction. L'application mobile génère alors le certificat de transaction et le transmet avec les droits au valideur 2.

Le valideur 2 vérifie ensuite que les droits ont bien été émis par le serveur billettique 1 concerné, et que le certificat de transaction est bien authentique, tel que décrit plus haut.

Si l'aléa est valide, le valideur 2 considère que le certificat de l'application mobile est bien associé aux droits présentés par l'utilisateur, et reconnaît ces droits.

Le deuxième exemple d'application concerne la billettique par tag visuel avec un média 3 mobile.

Dans cette variante, la communication entre le média 3 mobile et chaque valideur 2 est unidirectionnelle, du média 3 vers chaque valideur 2.

Ces valideur 2 sont équipés d'une caméra ou d'un capteur permettant la lecture des données présentées sur l'écran du média 3, ces données pouvant par exemple prendre la forme d'un code QR.

Les étapes d'acquisition et de chargement de droits sont strictement identiques à celles décrites ci-dessus relativement au premier exemple d'application.

Concernant la présentation des droits au valideur 2, faute de capacité à transmettre une valeur aléa, celle-ci est remplacée par une valeur prédéterminée, telle que l'heure courante, avec une durée de validité limitée par exemple à quelques secondes.

La transaction peut alors être déclenchée par une action de l'utilisateur dans l'application mobile, afin que le certificat de transaction soit généré et que les données de transaction et le droit numérique soient affichés sur l'écran du média 3.

Lorsque l'écran du média 3 est présenté au valideur 2, ce dernier récupère les données présentées et vérifie leur validité.

L'invention permet ainsi de garantir l'authenticité et l'intégrité des données de droits associées au porteur (le média 3 enregistré pour l'utilisateur).

L'invention est aisément mise en œuvre pour des droits d'accès à durée de validité déterminée. Durant la durée de validité, le droit peut être présenté à des terminaux d'acceptation à de multiples reprises. A chaque transaction, le média mobile génère un certificat de transaction à usage unique, mais les données de droit restent statiques.

Afin de palier la perte ou le vol d'un média mobile, le système peut proposer la possibilité de révocation d'un média mobile. Les clefs publiques d'un média mobile révoqué sont alors paramétrées en liste d'opposition sur les terminaux d'acceptation.

Dans le cas de droits consommables ou avec décompte suivant l'usage, il est nécessaire, lors des transactions de validation, de mettre à jour des données dans la mémoire non sécurisée du média mobile. Il peut alors être important de prévoir des contremesures côté système d'émission, avec une prise de risque limitée. En fonction des remontées de validation vers le système d'émission, une corrélation peut être effectuée par ce dernier. En cas d'écart de droits, le média mobile peut alors être automatiquement révoqué. L'intervalle de temps entre chaque contrôle de cohérence détermine le risque pris par l'opérateur du service.

La présente description est donnée à titre d'exemple et n'est pas limitative de l'invention.

En particulier, l'invention ne se limite pas au contrôle de l'accès à un service accessible à un utilisateur via un téléphone mobile, mais s'étend au contrôle de l'accès à un service accessible à un utilisateur via tout type de média mobile susceptible de stocker le droit numérique et générer un certificat de transaction à usage unique.

REVENDICATIONS

1.- Procédé de contrôle des droits d'accès à un service auquel un utilisateur (U) accède au moyen d'un média (3) mobile, ledit procédé comprenant l'émission (E2), par un système d'émission (1) de droits, d'un droit numérique d'accès au service associé à un média (3) mobile, la transmission (E2) au, et le stockage dans le, média (3) du droit numérique émis par le système d'émission (1), et le contrôle de validité du droit numérique stocké dans le média (3) par un terminal d'acceptation (2) de droits,
caractérisé en ce que le contrôle de validité du droit numérique par le terminal d'acceptation (2) comprend la transmission (E3, E4) au terminal d'acceptation (2) du droit numérique stocké dans le média (3) et d'un certificat de transaction à usage unique généré par le média (3), et le contrôle par le terminal d'acceptation (2), en mode déconnecté du système d'émission (1), de l'authenticité du droit numérique et de la validité du certificat de transaction, et en ce que, préalablement à l'émission du droit numérique par le système d'émission (1), le média (3) :

- génère une clef de chiffrement privée média (K_Priv_Media) et une clef de chiffrement publique média (K_PubJVIedia) au moyen d'un gestionnaire sécurisé de clefs (5) du média, et
- transmet (E1) sa clef publique média (K_PubJVIedia) au système d'émission (1).

2.- Procédé selon la revendication 1, le système d'émission (1) comprenant la clef de chiffrement privée d'émission (K_Priv_Em), et le média (3) comprenant une clef de chiffrement publique média (K_PubJVIedia), caractérisé en ce que le droit numérique émis par le système d'émission (1) comprend d'une part des données de droit associées au média (3) et d'autre part une signature numérique correspondant au chiffrage des données de droit et de la clef publique média (K_PubJVIedia) à partir de la clef privée d'émission (K_Priv_Em).

3.- Procédé selon la revendication 2, le média (3) comprenant la clef de chiffrement privée média (K_Priv_Media), caractérisé en ce que le média (3) génère le certificat de transaction à usage unique sous la forme d'une contresignature numérique correspondant au chiffrage des données de droit et d'une valeur d'aléa à usage unique à partir de la clef privée média (K_Priv_Media).

4.- Procédé selon la revendication 3, caractérisé en ce que la valeur d'aléa à usage unique est transmise (E3) par le terminal d'acceptation (2) au média (3) lors d'une initialisation de la communication entre le terminal d'acceptation (2) et le média (3), ou est prédéterminée par le média (3), par exemple sous la forme d'un horodatage à durée de validité limitée.

5.- Procédé selon l'une quelconque des revendications 3 et 4, caractérisé en ce que le contrôle de la validité du certificat de transaction par le terminal d'acceptation (2) comprend le déchiffrement de la contresignature numérique à partir de la clef publique média (K_PubJVIedia) et la vérification dans les données déchiffrées de la validité de la valeur d'aléa à usage unique.

6.- Procédé selon l'une quelconque des revendications 1 à 5, le système d'émission (1) comprenant une clef de chiffrement publique d'émission (K_Pub_Em), caractérisé en ce que la clef publique d'émission (K_Pub_Em) est préchargée dans le terminal d'acceptation (2), ou est incluse dans le droit numérique transmis au terminal d'acceptation (2).

7.- Procédé selon la revendication 6, caractérisé en ce que le contrôle de l'authenticité du droit numérique par le terminal d'acceptation (2) comprend le déchiffrement de la signature numérique à partir de la clef publique d'émission (K_Pub_Em) et la vérification dans les données déchiffrées que le droit numérique a bien été émis par le système d'émission (1) à destination du média (3).

8.- Système de contrôle des droits d'accès à un service accessible à un utilisateur (U) au moyen d'un média (3) mobile, ledit système de contrôle comprenant d'une part un système d'émission (1) de droits apte à émettre un droit numérique d'accès au service associé à un média (3) mobile et à transmettre le droit numérique pour stockage dans le média (3), et d'autre part au moins un terminal d'acceptation (2) de droits apte à contrôler la validité d'un droit numérique stocké dans un média (3) mobile,
caractérisé en ce que le terminal d'acceptation (2) est apte à contrôler la validité d'un droit numérique stocké dans un média (3) mobile par réception dudit droit numérique et d'un certificat de transaction à usage unique généré par le média (3), et par contrôle, en mode déconnecté du système d'émission (1), de l'authenticité dudit droit numérique et de la validité dudit certificat de transaction, et en ce que le média (3) comporte un gestionnaire

sécurisé de clés (5) apte à générer une clef de chiffrement privée média (K_Priv_Media) et une clef de chiffrement publique média (K_PubJVIedia) préalablement à l'émission du droit numérique, et en ce que le média (3) est apte à transmettre sa clef publique média (K_PubJVIedia) au système d'émission (1).

9.- Système de contrôle selon la revendication 8, le média (3) comprenant la clef de chiffrement publique média (K_PubJVIedia), caractérisé en ce que le système d'émission (1) comprend une clef de chiffrement privée d'émission (K_Priv_Em) et est apte à émettre un droit numérique comprenant d'une part des données de droit associées au média (3) et d'autre part une signature numérique correspondant au chiffrage des données de droit et de la clef publique média (K_PubJVIedia) à partir de la clef privée d'émission (K_Priv_Em).

10.- Système de contrôle selon la revendication 9, le média (3) comprenant la clef de chiffrement privée média (K_Priv_Media) et étant apte à générer le certificat de transaction à usage unique sous la forme d'une contresignature numérique correspondant au chiffrage des données de droit et d'une valeur d'aléa à usage unique à partir de la clef privée média (K_Priv_Media), caractérisé en ce que le terminal d'acceptation (2) est apte le contrôler la validité d'un certificat de transaction généré par le média (3), par déchiffrement de la contresignature numérique à partir de la clef publique média (K_PubJVIedia) et par vérification dans les données déchiffrées de la validité de la valeur d'aléa à usage unique.

11.- Système de contrôle selon l'une quelconque des revendications 8 à 10, caractérisé en ce que le système d'émission (1) comprend une clef de chiffrement publique d'émission (K_Pub_Em), le terminal d'acceptation (2) est apte à recevoir ladite clef publique d'émission (K_Pub_Em) par préchargement ou par inclusion de ladite clef publique d'émission (K_Pub_Em) dans le droit numérique réceptionné par le terminal d'acceptation (2), et en ce que le terminal d'acceptation (2) est apte à contrôler l'authenticité d'un droit numérique réceptionné depuis le média (3), par déchiffrement de la signature numérique à partir de la clef publique d'émission (K_Pub_Em) et par vérification dans les données déchiffrées que le droit numérique a bien été émis par le système d'émission (1) à destination du média (3).

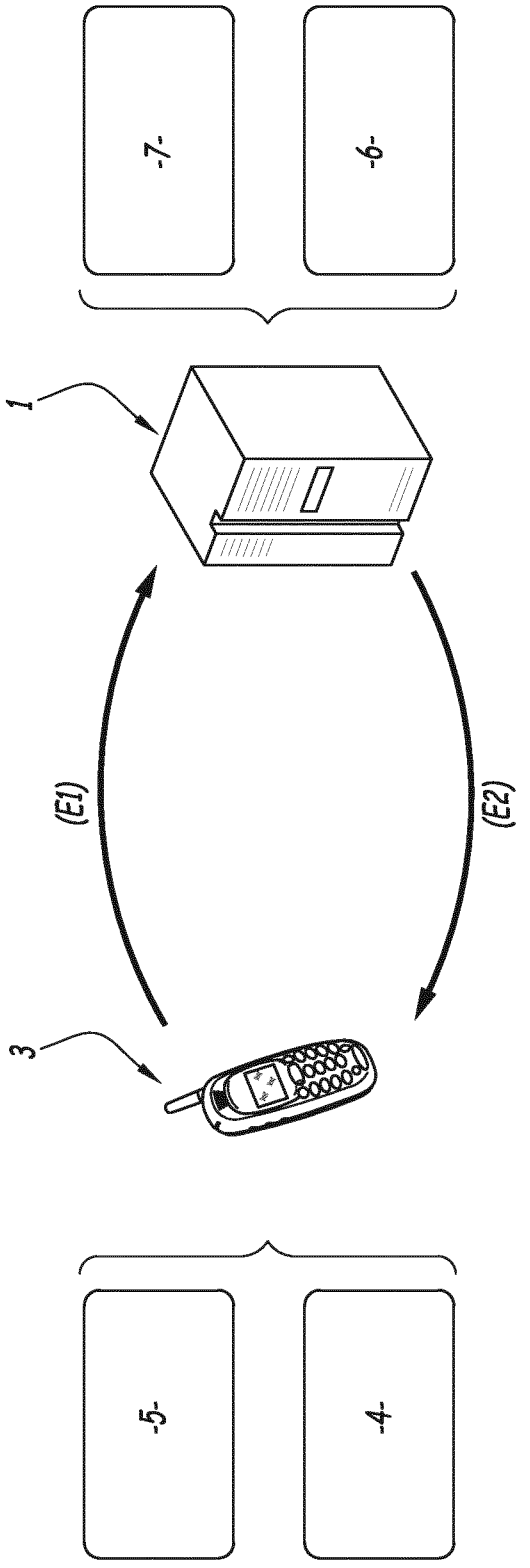


Fig.1

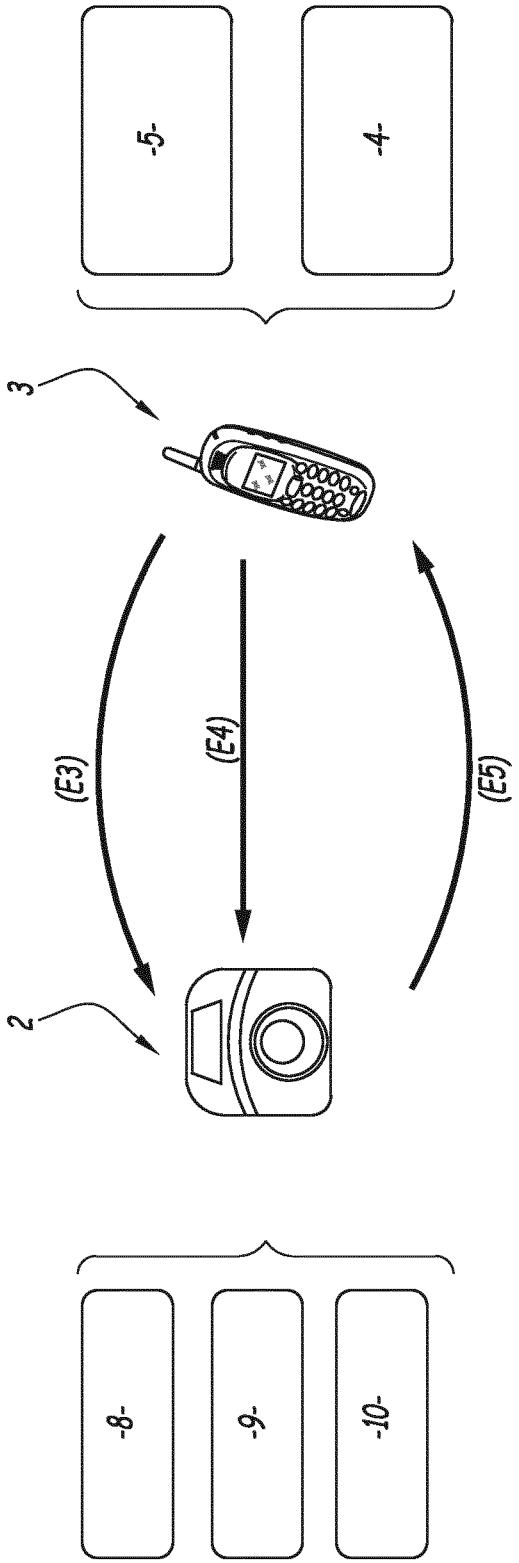
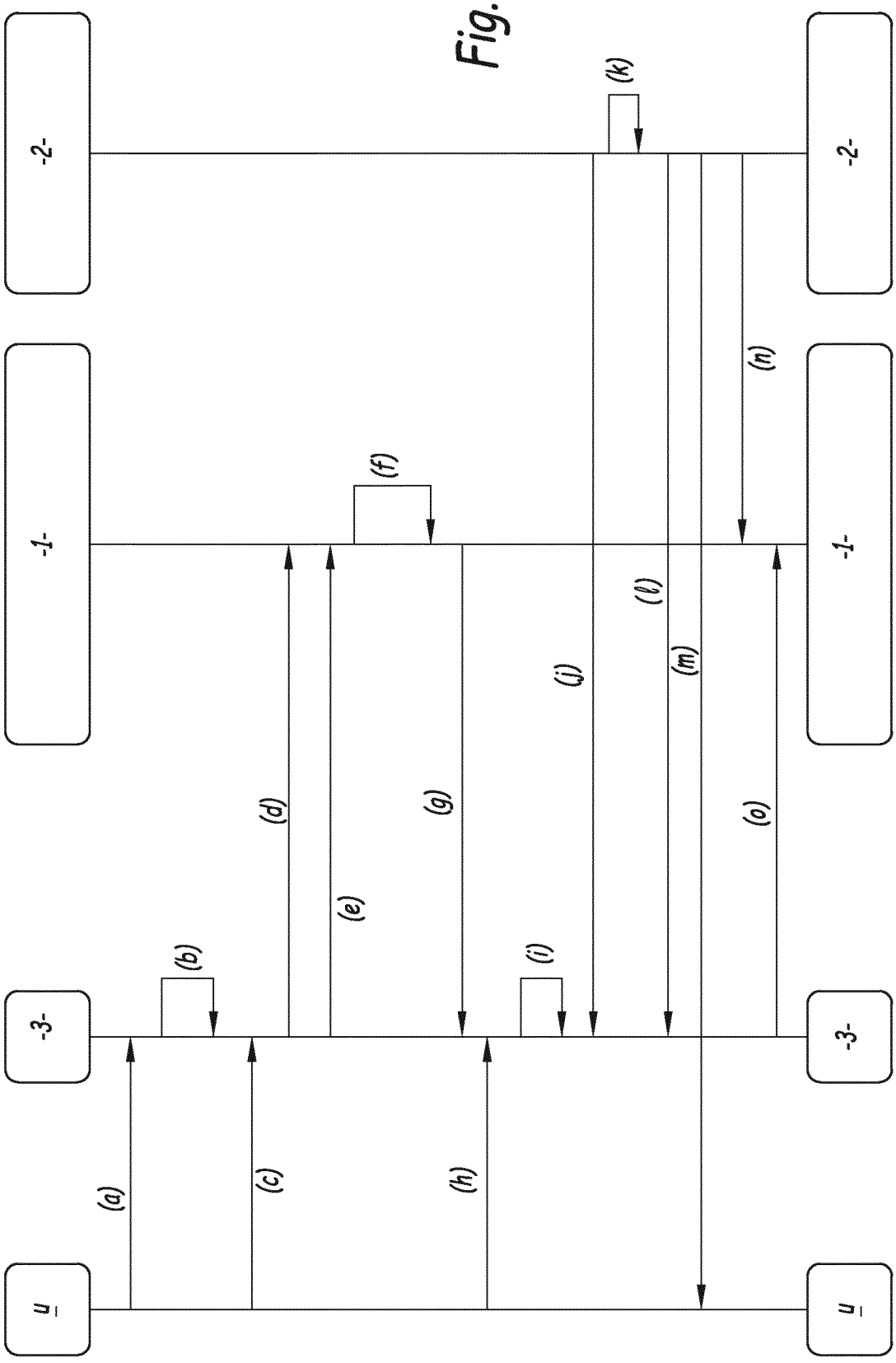


Fig.2

Fig.3



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/065563

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/32 H04W4/00 H04W12/04
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G06Q

Documentation searched otherthan minimum documentation to the extent that such documents are included in thefields 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 2015/092261 A1 (ORANGE [FR]) 25 June 2015 (2015-06-25) abstract page 9, line 29 - page 13, line 24 pages 2-8	1-11
X	FR 2 950 450 A1 (0BERTHUR TECHNOLOGIES [FR]) 25 March 2011 (2011-03-25) abstract page 4, line 16 - page 11, line 30	1-11
X	US 2003/093695 A1 (DUTTA SANTANU [US]) 15 May 2003 (2003-05-15) abstract paragraph [0034] - paragraph [0045] paragraph [0058] - paragraph [0067] figures 3, 4	1-11

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Spécial catégories of cited documents :

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

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

"L" document which may throw doubts on priority claim(s) orwhich is cited to establish the publication date of another citation or other spécial 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 ortheory 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
5 September 2016	12/09/2016

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	Bertolissi, Edy

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/065563

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"Chapter 10: Identification and Entity Authentication ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDB00K OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 385 - 424 , 1 October 1996 (1996-10-01) , XP001525010, ISBN: 978-0-8493-8523-0 Retrieved from the Internet: URL: http://www.cacr.math.uwaterloo.ca/hac/ (iii) Challenge-response based on digital signatures; page 404 - page 405	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/065563

Patent document cited in searoh report	Publication date	Patent family member(s)	Publication date
Wo 2015092261 Al	25-06-2015	FR 3015725 Al	26-06-2015
		Wo 2015092261 Al	25-06-2015
FR 2950450 Al	25-03--2011	EP 2306358 Al	06-04-2011
		FR 2950450 Al	25-03-2011
		US 2011068165 Al	24-03-2011
US 2003093695 Al	15-05--2003	AU 2003220339 Al	08-10-2003
		US 2003093695 Al	15-05-2003
		Wo 03081549 A2	02-10-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2016/065563

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06 H04L9/32 H04W4/00 H04W12/04
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 H04W G06Q

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

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal , 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 2015/092261 A1 (ORANGE [FR]) 25 juin 2015 (2015-06-25) abrégé page 9, ligne 29 - page 13, ligne 24 pages 2-8	1-11
X	FR 2 950 450 A1 (0BERTHUR TECHNOLOGIES [FR]) 25 mars 2011 (2011-03-25) abrégé page 4, ligne 16 - page 11, ligne 30	1-11
X	US 2003/093695 A1 (DUTTA SANTANU [US]) 15 mai 2003 (2003-05-15) abrégé alinéa [0034] - alinéa [0045] alinéa [0058] - alinéa [0067] figures 3, 4	1-11

-/ -

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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'appartenenant 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
5 septembre 2016	12/09/2016

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	Bertolissi, Edy

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2016/065563

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	"Chapter 10: Identification and Entity Authentication ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDB00K 0F APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 385 - 424 , 1 octobre 1996 (1996-10-01) , XP001525010, ISBN: 978-0-8493-8523-0 Extrait de l'Internet: URL: http://www.cacr.mathuwaterloo.ca/hac/ (iii) Challenge-response based on digital signatures; page 404 - page 405	1-11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2016/065563

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet (s)	Date de publication
WO 2015092261 A1	25-06-2015	FR 3015725 A1	26-06-2015
		WO 2015092261 A1	25-06-2015
FR 2950450 A1	25-03-2011	EP 2306358 A1	06-04-2011
		FR 2950450 A1	25-03-2011
		US 2011068165 A1	24-03-2011
US 2003093695 A1	15-05-2003	AU 2003220339 A1	08-10-2003
		US 2003093695 A1	15-05-2003
		WO 03081549 A2	02-10-2003