



(51) Classification internationale des brevets :

H04W 12/02 (2009.01) *H04W 12/12* (2009.01)
H04W 8/18 (2009.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01)

(21) Numéro de la demande internationale :

PCT/FR2017/052694

(22) Date de dépôt international :

02 octobre 2017 (02.10.2017)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

1659585 04 octobre 2016 (04.10.2016) FR

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

(72) **Inventeurs :** RICHARD, Benjamin ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR). GAMISHEV, Todor ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR). MACARIO-RAT, Gilles ; ORANGE GARDENS - IMT/OLR/IPL/PATENTS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR).

(74) **Mandataire :** ORANGE IMT/OLR/IPL/PATENTS ; RENARD Béatrice, ORANGE GARDENS -, 44 avenue de la République - CS 50010, 92326 CHÂTILLON CEDEX (FR).

(54) Title: METHOD FOR REGISTERING USER EQUIPMENT IN A COMMUNICATIONS NETWORK

(54) Titre : PROCÉDÉ D'ENREGISTREMENT D'UN ÉQUIPEMENT UTILISATEUR DANS UN RÉSEAU DE COMMUNICATION

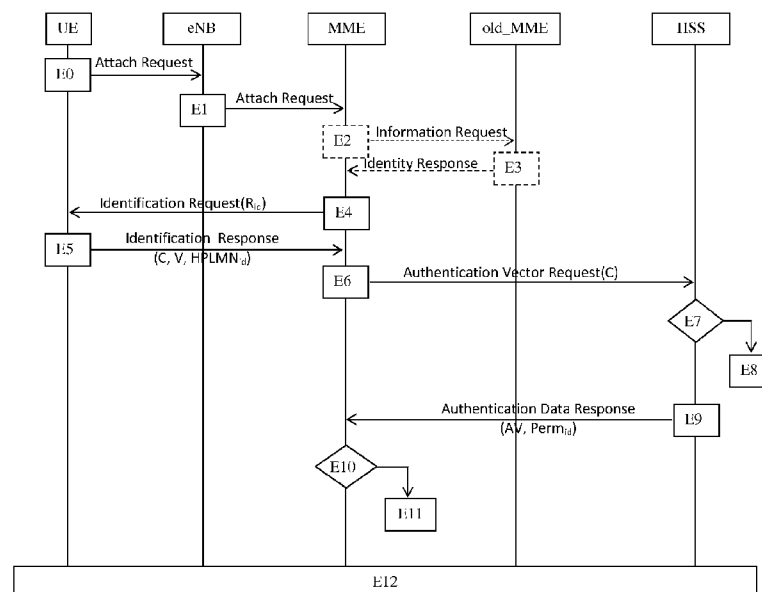


Figure 1

(57) **Abstract:** The invention relates to a method for registering user equipment (UE) in a communications network, said network comprising a mobility management entity (MME) and a home subscriber server (HSS), said method, implemented by the management entity, comprising: a step (E0) of receiving a request, from the user equipment, for attachment to the network; a step (E4) of sending an identification request to the user equipment; a step (E5) of receiving an identification response comprising an encrypted value (C) for the subscriber server, said encrypted value being based on an identifier of the user equipment, and a verification value (V) based on said identifier; a step (E6) of sending a vector authentication request to the home subscriber server, the request comprising the encrypted value; a step (E9) of receiving an authentication response comprising the identifier of the user equipment obtained from the subscriber

(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, JO, JP, KE, KG, KH, 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, 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))

server by decryption of the encrypted value; and a step (E10) of verification, by means of the verification value, that the identifier of the user equipment, received from the subscriber server, corresponds to the identifier used to calculate the control value.

(57) **Abrégé** : L'invention concerne un procédé d'enregistrement d'un équipement utilisateur (UE) dans un réseau de communication, ledit réseau comprenant une entité de gestion (MME) et un serveur d'abonnés (HSS), le procédé, mis en œuvre par l'entité de gestion, comprenant : - une étape (E0) de réception d'une requête d'attachement au réseau en provenance de l'équipement utilisateur, - une étape (E4) d'envoi à l'équipement utilisateur d'une requête d'identification, - une étape (E5) de réception d'une réponse d'identification, comprenant une valeur chiffrée (C) pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification (V), fonction dudit identifiant, - une étape (E6) d'envoi d'une requête de vecteur d'authentification au serveur d'abonnés, la requête comprenant la valeur chiffrée, - une étape (E9) de réception d'une réponse d'authentification comprenant l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée, - une étape (E10) de vérification au moyen de la valeur de vérification que l'identifiant de l'équipement utilisateur reçu du serveur d'abonnés correspond à l'identifiant utilisé pour calculer la valeur de contrôle.

Procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication

La présente invention concerne le domaine de l'accès à un réseau mobile de communication, et plus particulièrement la sécurité lors de l'accès à ce réseau.

5 Dans le cadre des réseaux mobiles de type 3G et 4G, l'organisme « 3GPP » (« Third Generation Partnership Project ») a défini des protocoles destinés à garantir la sécurité de l'accès d'un client à un réseau mobile. En particulier, les protocoles « UMTS AKA » (de l'anglais « Universal Mobile Telecommunications System » et « Authentication and Key Agreement »), et « EPS AKA » (de l'anglais « Evolved Packet System ») décrivent une
10 authentification mutuelle entre le réseau et le client, et l'établissement de clés de session destinées à assurer la confidentialité et l'intégrité des données échangées entre le client et le réseau lors de l'accès à ce dernier.

Cependant, certaines attaques sont susceptibles de remettre en cause la sécurité offerte par l'authentification mutuelle, plus précisément de porter atteinte à la vie privée d'un client.

15 Les protocoles AKA sont mis en œuvre après que le réseau a reçu d'un client une demande d'attachement au réseau. Une telle demande d'attachement implique d'envoyer un identifiant du client dans le réseau. Un tel identifiant, qui identifie la souscription du client au réseau est soit un identifiant permanent appelé « IMSI » (de l'anglais « International Mobile Subscriber Identity »), soit un identifiant temporaire appelé « TMSI » (« Temporary Mobile
20 Subscriber Identity ») dans le protocole UMTS AKA et « GUTI » (« Globally Unique Temporary UE Identity ») dans le protocole EPS AKA.

L'IMSI est un numéro unique, stocké dans un élément de sécurité (« Secure Element » en anglais), par exemple une carte UICC/USIM (pour « Universal Integrated Circuit Card/Universal Subscriber Identity Module ») comprise dans un équipement utilisateur tel
25 qu'un terminal mobile, et qui permet au réseau mobile d'identifier le client en tant qu'abonné. Ce numéro est connu du réseau et utilisé pour initier le mécanisme d'authentification mutuelle et de génération de clés tel que défini dans les protocoles AKA. La procédure d'attachement au réseau, et de ce fait les protocoles d'authentification, tentent de minimiser l'échange en clair de l'identifiant IMSI sur l'interface radio en utilisant des identifiants temporaires. En effet, pour
30 des questions de sécurité l'IMSI est transporter aussi rarement que possible sur l'interface radio : pour éviter qu'un attaquant ne l'intercepte et ne l'utilise pour tracer les déplacements de ce client.

Les identifiants temporaires sont assignés et modifiés par le réseau une fois le client authentifié. Ainsi, avant d'utiliser un identifiant temporaire, le client doit avoir procédé à une
35 première authentification en utilisant son identifiant permanent IMSI. Lors de cette première

authentification, l'IMSI est alors transmis en clair sur la voie radio entre l'équipement utilisateur et un équipement du réseau. Un risque d'interception de l'identifiant permanent IMSI existe. Il existe en effet des outils capables d'obtenir d'un équipement utilisateur son identifiant IMSI. Un tel outil, appelé « IMSI Catcher », se comporte comme une fausse antenne relais, 5 située entre l'équipement utilisateur et une antenne relais d'un opérateur. L'IMSI Catcher intercepte le trafic en provenance du terminal et peut ainsi récupérer l'IMSI.

L'obtention de l'identifiant IMSI d'un abonné permet de le localiser et de le tracer dans ses déplacements. Cela porte atteinte à la vie privée de l'abonné (on parle de « privacy » en anglais) et remet également en cause l'anonymisation des services d'accès au réseau.

10

Un des buts de l'invention est de remédier à des insuffisances/inconvénients de l'état de la technique et/ou d'y apporter des améliorations.

A cette fin, l'invention propose un procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication, ledit réseau comprenant une entité de gestion et un 15 serveur d'abonnés, le procédé, mis en œuvre par l'entité de gestion, comprenant :

- une étape de réception d'une requête d'attachement au réseau en provenance de l'équipement utilisateur,
- une étape d'envoi à l'équipement utilisateur d'une requête d'identification,
- une étape de réception d'une réponse d'identification, comprenant une valeur chiffrée 20 pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification, fonction dudit identifiant,
- une étape d'envoi d'une requête de vecteur d'authentification au serveur d'abonnés, la requête comprenant la valeur chiffrée,
- une étape de réception d'une réponse d'authentification comprenant l'identifiant de 25 l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée,
- une étape de vérification au moyen de la valeur de vérification que l'identifiant de l'équipement utilisateur reçu du serveur d'abonnés correspond à l'identifiant utilisé pour calculer la valeur de contrôle.

Avec le procédé décrit ici, un identifiant unique d'abonné n'est plus transmis en clair 30 sur la voie radio mais de façon chiffrée. Il est transmis en même temps qu'une valeur de vérification adaptée pour permettre à l'entité de gestion de la mobilité qui appartient à un réseau visité de s'assurer que l'équipement utilisateur qui s'attache au réseau correspond bien à un équipement utilisateur dont l'identifiant lui est transmis par le serveur d'abonnés du réseau nominal, ou réseau « home » de l'équipement utilisateur. Le chiffrement est en effet effectué

dans le réseau nominal, le déchiffrement ne pouvant être effectué que par un serveur du réseau nominal, ici le serveur d'abonnés.

A noter que le procédé est mis en œuvre lorsque l'équipement utilisateur ne dispose pas d'un identifiant temporaire, ou lorsque l'entité de gestion de la mobilité n'a pas réussi à obtenir, d'une entité d'enregistrement précédente impliquée dans l'enregistrement précédent de l'équipement au réseau et à partir d'un identifiant temporaire fourni par l'équipement utilisateur, l'identifiant de l'équipement utilisateur.

Le procédé garantit ainsi la non localisation d'un abonné et sa non traçabilité lors de ses déplacements. Le procédé contribue ainsi au respect de la vie privée de l'abonné.

Par ailleurs, l'entité de gestion de la mobilité du réseau visitée via laquelle l'équipement utilisateur s'enregistre dans le réseau est capable d'associer un flux reçu de l'équipement utilisateur à un identifiant d'abonné reçu d'un serveur du réseau nominal. Il respecte ainsi des obligations inhérentes à la mise en œuvre de certaines procédures exceptionnelles, par exemple l'écoute légale en France.

Dans un exemple de réalisation, la requête d'attachement comprend une valeur représentative d'une absence de possession d'un identifiant temporaire par l'équipement utilisateur.

Cet exemple correspond au cas où l'équipement utilisateur ne dispose pas d'un identifiant temporaire. Dans ce cas les étapes de requête d'identification et de réponse d'identification sont mises en œuvre entre l'entité de gestion de la mobilité et une entité d'enregistrement précédente.

Dans un exemple de réalisation, la réponse d'identification comprend un identifiant du réseau nominal.

La présence d'un identifiant du réseau nominal dans la requête d'identification envoyée par l'équipement utilisateur permet à l'entité de gestion de la mobilité d'identifier le serveur d'abonnés à contacter pour obtenir un identifiant de l'équipement utilisateur. En effet, elle ne peut déduire cette information de l'identifiant de l'équipement utilisateur qu'elle a reçu chiffré.

Dans un exemple de réalisation, la requête d'identification comprend un aléa, ledit aléa étant utilisé par l'équipement utilisateur pour calculer la valeur chiffrée et la valeur de vérification.

Cet exemple permet d'éviter des attaques par rejeu au cours desquelles un attaquant transmettrait à l'entité de gestion de la mobilité une réponse d'identification qu'il aurait interceptée précédemment sur la voie radio, afin d'obtenir un vecteurs d'authentification.

Dans un exemple de réalisation, la valeur chiffrée est également fonction d'un message d'authentification calculé à partir de l'identifiant de l'équipement utilisateur et de l'aléa.

Le message d'authentification ainsi calculé est destiné à être vérifié par le serveur d'abonnés du réseau nominal. Celui-ci s'assure ainsi que l'équipement utilisateur possède bien la clé d'authentification utilisée pour calculer le message d'authentification et qui est associée par le serveur à l'équipement utilisateur.

5 L'invention concerne également un procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication, ledit réseau comprenant une entité de gestion et un serveur d'abonnés, le procédé, mis en œuvre par l'équipement utilisateur comprenant :

- une étape d'envoi à l'entité de gestion d'une requête d'attachement au réseau,
- une étape de réception d'une requête d'identification,

10 - une étape de calcul d'une valeur chiffrée pour le serveur d'abonnés et d'une valeur de vérification, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et ladite valeur de vérification étant fonction dudit identifiant et envoi d'une réponse d'identification comprenant la valeur chiffrée et la valeur de vérification.

L'invention porte également sur un procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication, ledit réseau comprenant une entité de gestion et un serveur d'abonnés, le procédé, mis en œuvre par le serveur d'abonnés comprenant :

15 - une étape de réception d'une requête de vecteur d'authentification en provenance de l'entité de gestion, ladite requête comprenant une valeur chiffrée par l'équipement utilisateur pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur,

20 - une étape d'envoi d'une réponse d'authentification comprenant un vecteur d'authentification et l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée.

Dans un exemple de réalisation, la valeur chiffrée est fonction d'un aléa et d'un message d'authentification calculé par l'équipement utilisateur à partir de l'identifiant de l'équipement utilisateur et de l'aléa, le procédé comprenant une étape de vérification du message d'authentification au moyen d'une clé d'authentification associée à l'identifiant de l'équipement utilisateur.

L'invention concerne aussi une entité de gestion d'un réseau de communication, ledit réseau comprenant au moins un équipement utilisateur et un serveur d'abonnés, ladite entité comprenant :

30 - des premiers moyens de réception, agencés pour recevoir une requête d'attachement au réseau en provenance de l'équipement utilisateur,

- des premiers moyens d'envoi, agencés pour envoyer à l'équipement utilisateur une

35 requête d'identification,

- des deuxièmes moyens de réception, agencés pour recevoir une réponse d'identification, ladite réponse d'identification comprenant une valeur chiffrée pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification, fonction dudit identifiant,

5 - des deuxièmes moyens d'envoi, agencés pour envoyer une requête de vecteur d'authentification au serveur d'abonnés, la requête comprenant la valeur chiffrée,

- des troisièmes moyens de réception, agencés recevoir une réponse d'authentification comprenant l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée,

10 - des moyens de vérification, agencés pour vérifier au moyen de la valeur de vérification que l'identifiant de l'équipement utilisateur reçu du serveur d'abonnés correspond à l'identifiant utilisé pour calculer la valeur de contrôle.

L'invention porte aussi sur un programme pour une entité de gestion d'un réseau de communication, comprenant des instructions de code de programme destinées à commander l'exécution des étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau, décrit précédemment, lorsque le programme est exécuté sur ladite entité.

L'invention concerne aussi un équipement utilisateur dans un réseau de communication, ledit réseau comprenant une entité de gestion et un serveur d'abonnés, comprenant :

20 - des moyens d'envoi, agencés pour envoyer à l'entité de gestion une requête d'attachement au réseau,

- des moyens de réception, agencés pour recevoir une requête d'identification,

- des moyens de calcul et d'envoi, agencés pour calculer une valeur chiffrée pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification fonction dudit identifiant et pour envoyer une réponse d'identification comprenant ladite valeur chiffrée et ladite valeur de vérification.

25 L'invention porte aussi sur un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un équipement utilisateur, le programme comprenant des portions de code pour l'exécution des étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau tel que décrit précédemment, lorsque le programme est exécuté sur ledit équipement utilisateur.

L'invention concerne aussi un serveur d'abonnés dans un réseau de communication, ledit réseau comprenant une entité de gestion et au moins un équipement utilisateur, comprenant :

35 - des moyens de réception, agencés pour recevoir une requête de vecteur d'authentification en provenance de l'entité de gestion, ladite requête comprenant une valeur

chiffrée par l'équipement utilisateur pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur,

- des moyens d'envoi, agencés pour envoyer une réponse d'authentification comprenant un vecteur d'authentification et l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée.

L'invention porte aussi sur un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un serveur d'abonnés, le programme comprenant des portions de code pour l'exécution des étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau tel que décrit précédemment, lorsque le programme est exécuté sur ledit équipement utilisateur.

L'invention concerne également un système d'enregistrement d'au moins un équipement utilisateur dans à un réseau de communication comprenant :

- une entité de gestion telle que décrite précédemment,
- au moins un équipement utilisateur tel que décrit précédemment, et
- un serveur d'abonnés tel que décrit précédemment.

D'autres caractéristiques et avantages de la présente invention seront mieux compris de la description et des dessins annexés parmi lesquels :

- la figure 1 présente les étapes d'un procédé d'enregistrement dans le réseau, selon un exemple de réalisation ;

- la figure 2 est une représentation schématique d'un équipement utilisateur, apte à mettre en œuvre le procédé d'enregistrement dans le réseau, selon un exemple de réalisation ;

- la figure 3 est une représentation schématique d'une entité de gestion de la mobilité, apte à mettre en œuvre le procédé d'enregistrement dans le réseau, selon un exemple de réalisation.

- la figure 4 est une représentation schématique d'un serveur d'abonnés, apte à mettre en œuvre le procédé d'enregistrement dans le réseau, selon un exemple de réalisation.

Les étapes d'un protocole d'enregistrement d'un équipement utilisateur auprès d'un réseau, selon un exemple de réalisation, vont maintenant être décrites en relation avec la figure 1.

Un utilisateur (non représenté sur la figure 1) est équipé d'un équipement utilisateur UE agencé pour accéder à un réseau mobile. L'équipement utilisateur UE comprend habituellement un terminal et un élément de sécurité (« Secure Element » en anglais), par exemple une carte UICC/USIM (pour « Universal Integrated Circuit Card/Universal Subscriber Identity

Module »). Un tel élément de sécurité est agencé pour stocker et traiter des données sensibles, par exemple une application d'accès au réseau et des données associées (on parle de « credentials » en anglais), telles que des clés et des algorithmes cryptographiques. De telles données sont destinées à être utilisées par un protocole d'authentification mutuelle avec le réseau lors de l'accès à ce dernier. L'invention n'est pas limitée à un équipement utilisateur de ce type et dans un autre exemple de réalisation, l'équipement utilisateur UE comprend une zone logicielle sécurisée agencée pour traiter les données sensibles d'accès au réseau.

L'architecture du réseau mobile et le procédé d'attachement au réseau sont illustrés ici dans le cadre d'un réseau de type « EPS » (pour « Evolved Packet System »). L'invention n'est cependant pas limitée à ce type de réseau et s'applique également à d'autres types de réseaux mobiles tels que par exemple le réseau « GPRS » (de l'anglais « General Packet Radio Service »), ou « UMTS » (de l'anglais « Universal Mobile Telecommunications System »).

Une station de base eNB est agencée pour gérer la transmission et la réception radio avec l'équipement utilisateur UE. L'équipement utilisateur UE est par exemple un smartphone, un téléphone portable, une tablette, etc.

Une entité de gestion de la mobilité MME est, de manière classique, responsable du contrôle dans un réseau « EPC » (« Evolved Packet Core »). Elle est en charge entre autres de la gestion de la signalisation du réseau et de l'équipement utilisateur UE, de l'établissement des connexions, de la gestion de la mobilité de l'équipement UE et de son authentification à partir de données obtenues d'un serveur d'abonnés HSS (ou « AuC » pour « Authentication Center », ou centre d'authentification). La gestion de la mobilité, ou handover, peut impliquer plusieurs entités dont une entité d'enregistrement du réseau old_MME, impliquée lors de l'enregistrement précédent de l'équipement utilisateur auprès du réseau. Cette entité d'enregistrement est agencée pour fournir sur demande des informations sur un contexte propre à l'équipement utilisateur UE et créé lors du précédent enregistrement de l'équipement dans le réseau. Cette entité d'enregistrement old_MME est par exemple une entité de gestion de la mobilité MME, ou une autre entité de gestion locale de la mobilité, ou une passerelle SGSN qui assure des fonctions de gestion de la mobilité dans le cas d'un réseau GPRS.

Une passerelle de service S-GW (pour « Serving Gateway ») est agencée pour router des paquets IP entre l'équipement utilisateur UE et le réseau cœur et une passerelle de paquets P-GW (pour « Packet Data Network Gateway ») est agencée pour fournir une connectivité vers des réseaux externes. Une entité réseau d'enregistrement d'identités « EIR » (pour « Equipment Identity Register ») est agencée pour mémoriser des informations de sécurité et d'identification relatives à des terminaux mobiles. C'est grâce à cette entité qu'un opérateur peut bloquer un équipement mobile volé. Enfin, une entité de gestion PCRF (de l'anglais « Policy and Charging

Rules Function ») est en charge de la gestion et du contrôle en temps réel d'une session et offre une interface de paiement et de facturation. Les fonctions de la passerelle de service S-GW, de la passerelle de paquets P-GW, de l'entité d'enregistrement EIR, de l'entité de gestion PCRF, les fonctions classiques de l'entité de gestion de la mobilité MME, de l'entité d'enregistrement
5 old_MME et les interfaces entre les différentes entités sont décrites en détail dans la spécification TS 23.401. Les passerelles de service S-GW, de paquets P-GW, l'entité d'enregistrement EIR et l'entité de gestion PCRF ne sont pas représentées sur la figure 1 pour des raisons de lisibilité.

A des fins d'accès au réseau, l'équipement utilisateur UE mémorise une clé
10 d'authentification, notée K, partagée avec le serveur d'abonnés HSS. La clé d'authentification K est destinée à être utilisée pour la génération de données d'authentification et pour dériver des clés telles que des clés de chiffrement de la voie radio et de contrôle d'intégrité. Plus précisément la clé d'authentification K est mémorisée dans l'élément de sécurité de l'équipement utilisateur UE. L'équipement utilisateur UE mémorise également une clé publique
15 pke d'un couple de clés asymétriques de chiffrement pke/ske. La clé secrète ske est détenue uniquement par le serveur d'abonnés HSS tandis que la clé publique associée pke est distribuée à l'ensemble des équipements utilisateur qui sont gérés par le même serveur d'abonnés HSS.

Le serveur d'abonnés HSS est agencé pour authentifier les équipements utilisateur UE qu'il gère. A cet effet il accède à une base d'abonnés qui comprend l'ensemble des clés
20 d'authentification K des équipements utilisateur qu'il gère, une clé d'authentification étant associée dans cette base de données à un identifiant permanent associé à un équipement utilisateur. Le serveur d'abonnés HSS mémorise également le couple de clés de chiffrement asymétrique pke/ske. Il distribue la clé publique de chiffrement pke à l'ensemble des abonnés qu'il gère.

Certains échanges décrits ci-dessous sont conformes à ceux de la procédure d'enregistrement d'un terminal mobile dans un réseau telle que décrite dans la spécification TS
25 23.401, paragraphe 5.3.2.1. En particulier les messages échangés, lorsqu'ils ont le même nom, ainsi que leurs paramètres, sont identiques à ceux de la spécification. Ils ne sont donc pas décrits dans le détail.

Dans une étape initiale E0, l'équipement utilisateur UE émet sur la voie radio une requête d'attachement Attach Request, reçue par la station de base eNB et retransmise dans une
30 étape E1 de retransmission à l'entité de gestion de la mobilité MME.

La requête d'attachement comprend un identifiant de l'équipement utilisateur UE. Cet identifiant est soit un identifiant temporaire de type « GUTI » (pour « Globally Unique
35 Temporary Identifier ») s'il en possède un, ou une valeur prédéterminée NoID. Dans un

exemple de réalisation, l'identifiant temporaire n'a jamais été utilisé pour un attachement au réseau. Un identifiant temporaire qui n'a jamais été utilisé pour un attachement au réseau garantit une absence de traçabilité de l'équipement utilisateur UE. En effet, dans ce cas l'identifiant temporaire n'est utilisé qu'une fois et ne circule qu'une fois sur la voie radio.

- 5 L'envoi de la valeur prédéterminée NoID indique que l'équipement utilisateur UE ne possède pas d'identifiant temporaire ou n'en possède pas qui n'a jamais été utilisé. Dans un autre exemple de réalisation, correspondant à un réseau UMTS, l'identifiant temporaire est de type « TMSI » (« Temporary Mobile Subscriber Identity »).

10 Dans un cas où l'équipement utilisateur UE possède déjà un identifiant temporaire de type GUTI ou TMSI, celui-ci lui a été affecté lors d'un précédent attachement de l'équipement UE auprès du réseau par l'entité d'enregistrement old_MME, impliquée dans l'attachement précédent.

Lorsque l'équipement utilisateur UE possède déjà un identifiant temporaire, dans une étape E2 d'envoi, l'entité de gestion de la mobilité MME envoie de manière classique une
15 requête d'identification, Identification Request, à destination de l'entité d'enregistrement old_MME qui a alloué l'identifiant temporaire à l'équipement utilisateur UE.

L'entité d'enregistrement old_MME envoie une réponse d'identification, Identification Response, à l'entité de gestion de la mobilité MME dans une étape E3 de réponse. La réponse d'identification comprend un contexte propre à l'équipement utilisateur UE qui
20 comprend un identifiant d'abonné Perm_{ID}, auquel a été associé l'identifiant temporaire GUTI, ainsi que des informations de sécurité. Dans un exemple de réalisation, l'identifiant permanent Perm_{ID} est le numéro unique d'abonné IMSI (de l'anglais « International Mobile Subscriber Identity »). L'IMSI est un numéro unique, stocké dans l'élément de sécurité de l'équipement utilisateur UE ; il permet au réseau mobile d'identifier le l'utilisateur de l'équipement UE en
25 tant qu'abonné. Les étapes E2 et E3 étant optionnelles, puisqu'exécutées uniquement lorsque l'équipement utilisateur UE possède un identifiant temporaire, elles apparaissent en pointillés sur la figure 1.

Dans un cas où l'équipement utilisateur UE était inconnu de l'entité d'enregistrement old_MME, ou lorsque la requête d'attachement envoyée par l'équipement utilisateur UE au
30 cours de l'étape E0 comprend la valeur prédéterminée NoID, l'entité de gestion de la mobilité MME envoie à l'équipement utilisateur UE dans une étape E4 une requête d'identification, Identification Request, relayée par la station de base eNB. La requête d'identification envoyée à l'équipement utilisateur UE comprend une valeur aléatoire R_{id}. Cette requête est destinée à obtenir de manière sécurisée l'identifiant Perm_{ID} de l'abonné, utilisateur de l'équipement UE.

L'aléa Rid est destiné à éviter des attaques par rejeu au cours desquelles un attaquant enverrait un message d'identification précédemment envoyé et qu'il aurait intercepté.

L'équipement utilisateur UE envoie, dans une étape E5 de réponse, une réponse d'identification, Identification Response, qui comprend un triplé de valeurs noté (C, V, HPLMN_{id}). Le triplé comprend un identifiant HPLMN_{id} du réseau nominal HPLMN (de l'anglais « Home Public Land Mobile Network »), une première valeur C, une deuxième valeur V. Le réseau nominal HPLMN est le réseau auprès duquel l'abonné a souscrit un abonnement. En d'autres termes c'est le réseau de souscription, ou le réseau qui fournit le service à l'abonné. La première valeur C est destinée à transmettre l'identifiant Perm_{id} de l'abonné de manière chiffrée. La deuxième valeur V est une valeur de contrôle, destinée à permettre à l'entité de gestion de la mobilité MME de s'assurer qu'un identifiant permanent reçu du serveur d'abonnés HSS du réseau nominal HPLMN_{id} correspond à celui qui a été transmis qui a été utilisé pour calculer la première valeur C. Les première et deuxième valeurs C, V, sont calculées comme suit :

- $C = \text{PKE.Enc}(\text{pke} ; H_5(K ; R_{id}, \text{Perm}_{id}), R_{id}, \text{Perm}_{id})$, où PKE.Enc représente un algorithme de chiffrement asymétrique et H_5 une fonction de hachage avec clé secrète de type message d'authentification HMAC (pour « Hash Message Authentication Code »). Dans un exemple de réalisation, l'algorithme de chiffrement asymétrique est RSA (pour « Rivest, Shamir et Adleman ») et la fonction de hachage H_5 fait partie d'un ensemble de fonctions standardisées tel que Millenage, ou Tuak. Le message d'authentification HMAC permet au serveur d'abonnés HSS d'être assuré que l'équipement utilisateur UE possède bien la clé d'authentification K.

- $V = H^*(R_{id}, \text{Perm}_{id})$, où H^* correspond à une fonction de hachage, par exemple SHA-2 (pour « Secure Hash Algorithm »).

La première valeur C permet à l'équipement utilisateur UE de transmettre son identifiant Perm_{id} de manière confidentielle. A noter que l'entité de gestion de la mobilité MME ne peut pas accéder à l'identifiant permanent Perm_{id} du terminal UE, celui-ci étant transmis chiffré et l'entité de gestion de la mobilité MME ne disposant pas du matériel cryptographique lui permettant de le déchiffrer. Seul le serveur d'abonnés HSS du réseau nominal de l'équipement utilisateur UE, qui détient la clé secrète ske associée à la clé publique de chiffrement pke est agencé pour déchiffrer l'identité permanente Perm_{id} du terminal UE.

La deuxième valeur V est une valeur de vérification destinée à permettre à l'entité de gestion de la mobilité MME de vérifier que l'identifiant permanent Perm_{id} utilisé pour calculer la première valeur C reçue de l'équipement utilisateur UE dans le message de réponse, correspond à l'identifiant permanent qu'elle va recevoir du serveur d'abonnés HSS en réponse à une requête de données d'authentification suivante.

L'identifiant du réseau nominal $HPLMN_{id}$ permet à l'entité de gestion de la mobilité MME d'identifier le serveur d'abonnés HSS associé à l'équipement utilisateur UE sans connaissance de l'identifiant $Perm_{id}$ de celui-ci.

5 Dans une étape suivante E6, l'entité de gestion de la mobilité MME envoie une requête de vecteur d'authentification, Authentication Vector Request au serveur d'abonnés HSS associé à l'identifiant de réseau $HPLMN_{id}$. La requête de vecteur d'authentification comprend la première valeur C reçue précédemment.

10 Dans une étape suivante E7 de traitement et de vérification, le serveur d'abonnés HSS déchiffre la valeur C en appliquant l'algorithme de déchiffrement asymétrique PKE.Dec au moyen de sa clé secrète ske . Il obtient ainsi l'identifiant $Perm_{id}$ associé à l'équipement utilisateur UE, l'aléa R_{id} et le message d'authentification HMAC, $H_5(K, R_{id}, Perm_{id})$. Le serveur d'abonnés HSS extrait ensuite de sa base d'abonnés la clé d'authentification K associée à l'équipement utilisateur UE dont l'identifiant permanent est $Perm_{id}$ et il vérifie le message d'authentification HMAC obtenu par le déchiffrement. A cette fin il calcule une valeur de

15 contrôle en appliquant la fonction H_5 à la clé d'authentification K qu'il vient d'extraire de sa base de données, à l'aléa R_{id} et à l'identifiant permanent $Perm_{id}$ qu'il a obtenus en déchiffrant la première valeur C reçue au cours de l'étape E6. En d'autres termes il calcule $H_5(K_c, R_{id}, Perm_{id})$.

Si cette valeur n'est pas égale au message d'authentification HMAC du triplé C reçu au cours de l'étape E5 (branche 'nok' sur la figure 1), le procédé se termine dans une étape E8 de

20 fin. En effet, dans ce cas, l'équipement utilisateur UE a calculé le message d'authentification avec une clé d'authentification différente de la clé qui lui est associée par le serveur d'abonnés HSS.

Dans le cas contraire, (branche 'ok' sur la figure 1), les données que le serveur d'abonnés HSS a reçu sont cohérentes avec des données d'un abonné. Dans une étape suivante

25 E9 de calcul et d'envoi d'un vecteur d'authentification, le serveur d'abonnés HSS calcul un vecteur d'authentification AV conformément à la procédure d'attachement décrite dans la spécification TS 33.102. Le serveur d'abonnés HSS envoie en fin d'étape E9 une réponse d'authentification, Authentication Vector Answer qui comprend l'identifiant permanent $Perm_{id}$ de l'équipement utilisateur UE et le vecteur d'authentification AV calculé précédemment.

30 Dans une étape E10 de vérification, l'entité de gestion de la mobilité MME vérifie que l'identifiant permanent $Perm_{id}$ reçu du serveur d'abonnés HSS dans la réponse d'authentification au cours de l'étape E9 correspond à l'équipement utilisateur UE qui a envoyé une réponse d'identification au cours de l'étape E5 pour la demande d'attachement courante. A cette fin, l'entité de gestion de la mobilité MME calcule $H^*(R_{id}, Perm_{id})$ à partir de l'identifiant

$Perm_{id}$ reçu et de l'aléa R_{id} . Il vérifie ensuite que la valeur calculée est égale à la valeur de vérification V qu'il a reçue de l'équipement utilisateur au cours de l'étape E5.

Dans un premier cas (branche « ok » sur la figure 1) où les valeurs sont égales, cela signifie que l'identifiant permanent $Perm_{id}$ reçu du serveur d'abonnés HSS correspond à l'identifiant de l'équipement utilisateur UE reçu chiffré au cours de l'étape E5. Ainsi, grâce au
5 procédé d'attachement décrit ici, l'identifiant permanent $Perm_{id}$ de l'équipement utilisateur UE n'est plus transmis en clair sur la voie radio lors de la procédure d'attachement au réseau.

Dans un deuxième cas (branche 'nok' sur la figure 1) où les valeurs sont différentes, indiquant que l'identifiant permanent $Perm_{id}$ reçu du serveur d'abonnés ne correspond pas à l'identifiant qui a été utilisé pour calculer la valeur de vérification V , le procédé s'arrête dans
10 une étape E11 de fin.

Ainsi, la sécurité, mise en avant par les protocoles d'authentification, ne présente pas la faiblesse inhérente à un envoi en clair par l'équipement utilisateur de l'identifiant $Perm_{id}$ de l'équipement utilisateur UE lors de l'attachement au réseau.

Par ailleurs, l'entité de gestion de la mobilité MME obtient l'identifiant permanent $Perm_{id}$ de l'équipement utilisateur UE du serveur d'abonnés HSS du réseau nominal de l'équipement utilisateur UE. Ainsi, des contraintes inhérentes à des procédures exceptionnelles, telles que des procédures d'écoute légale, sont respectées. En effet, il est possible pour l'entité de gestion de la mobilité MME d'associer à un flux en provenance d'un équipement utilisateur à
15 un identifiant d'abonné. Ces informations sont nécessaires pour la mise en œuvre de ces procédures exceptionnelles.

La procédure d'attachement au réseau se poursuit, conformément à la fin de l'étape 5a et jusqu'à l'étape à 26 de la procédure d'enregistrement décrite dans la spécification TS 23.401, faisant intervenir les passerelles de service S-GW et de paquet P-GW, l'entité d'enregistrement
25 EIR et l'entité de gestion PCRF non représentées sur la figure 1. L'exécution de ces étapes de la procédure d'enregistrement est représentée sur la figure par l'étape E13.

Une entité de gestion de la mobilité, selon un exemple de réalisation, va maintenant être décrite en relation avec la figure 2.

Une entité de gestion de la mobilité MME, est une entité réseau en charge du contrôle dans un réseau de communication mobile. Elle est responsable de l'enregistrement des équipements utilisateur, de leur authentification et de leur capacité à être joignable.
30

L'entité de gestion de la mobilité MME est un serveur informatique qui comprend :

- une unité de traitement ou processeur 201, ou « CPU » (de l'anglais « Central Processing Unit »), destinée à charger des instructions en mémoire, à les exécuter, à effectuer des opérations ;

5 - un ensemble de mémoires, dont une mémoire volatile 202, ou « RAM » (pour « Random Access Memory »), utilisée pour exécuter des instructions de code, stocker des variables, etc., et une mémoire de stockage 203 de type « EEPROM » (de l'anglais « Electrically Erasable Programmable Read Only Memory »). En particulier, la mémoire de stockage 203 est agencée pour mémoriser un module logiciel comprenant des instructions de code pour mettre en œuvre celles des étapes du procédé d'enregistrement d'un équipement
10 utilisateur dans un réseau tel que décrit précédemment qui sont exécutées par l'entité de gestion de la mobilité MME ;

- un ensemble 203 d'interfaces, agencées pour communiquer avec des entités du réseau, telles que l'équipement utilisateur UE via la station de base eNB, d'autres entités de gestion dans le réseau, le serveur d'abonnés HSS.

15 L'entité de gestion de la mobilité MME comprend également :

- un premier module de réception 205, agencé pour recevoir une requête d'attachement au réseau en provenance de l'équipement utilisateur. Le premier module de réception 205 est agencé pour mettre en œuvre l'étape E1 du procédé décrit précédemment ;

20 - un premier module d'envoi 206, agencé pour envoyer à l'équipement utilisateur une requête d'identification. Le premier module d'envoi 206 est agencé pour mettre en œuvre l'étape E4 du procédé d'enregistrement décrit en relation avec la figure 5 ;

- un deuxième module de réception 207, agencé pour recevoir une réponse d'identification, ladite réponse d'identification comprenant une valeur chiffrée C à l'attention du serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement
25 utilisateur. Le deuxième module de réception 207 est également agencé pour recevoir une valeur de vérification V, fonction dudit identifiant. Le deuxième module de réception 207 est agencé pour mettre en œuvre l'étape E5 du procédé d'enregistrement décrit précédemment ;

30 - un deuxième module d'envoi 208, agencé pour envoyer une requête de vecteur d'authentification au serveur d'abonnés HSS, la requête comprenant la valeur chiffrée C. Le deuxième module d'envoi 208 est agencé pour mettre en œuvre l'étape E6 du procédé décrit précédemment ;

- un troisième module de réception 209, agencé pour recevoir une réponse d'authentification comprenant l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée. Le troisième module de réception 209 est

agencé pour mettre en œuvre l'étape E9 du procédé d'enregistrement tel que décrit précédemment ; et

- un module de vérification 210, agencés pour vérifier au moyen de la valeur de vérification que l'identifiant de l'équipement utilisateur reçu du serveur d'abonnés correspond à l'identifiant utilisé pour calculer la valeur de contrôle. Le module de vérification 210 est agencé pour mettre en œuvre l'étape E10 du procédé décrit précédemment.

L'ensemble d'interfaces 204, le premier module d'envoi 205, le premier module de réception 206, le deuxième module de réception 207, le deuxième module d'envoi 208, le troisième module de réception 209 et le module de vérification sont de préférence des modules logiciels comprenant des instructions logicielles pour mettre en œuvre les étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication qui sont exécutées par l'entité de gestion de la mobilité MME.

L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé d'enregistrement d'un terminal mobile tel que décrit précédemment lorsque ce programme est exécuté par un processeur de l'entité de gestion de la mobilité MME, et
- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

Un équipement utilisateur UE selon un exemple de réalisation, va maintenant être décrit en relation avec la figure 3.

Un équipement utilisateur UE comprend habituellement un équipement mobile équipé d'une interface radio agencée pour s'interfacer avec un réseau mobile de communication, et un élément de sécurité (« Secure Element » en anglais), par exemple une carte UICC/USIM (pour « Universal Integrated Circuit Card/Universal Subscriber Identity Module »). Un tel élément de sécurité est agencé pour stocker et traiter des données sensibles, telles que des clés et des algorithmes cryptographiques. De telles données et algorithmes sont destinés à être utilisés lors de l'enregistrement de l'équipement utilisateur UE dans le réseau, et notamment au cours de la procédure d'authentification entre l'équipement utilisateur et le réseau. Les interactions entre le terminal mobile et l'élément de sécurité dans l'équipement utilisateur UE étant très étroites lors d'un accès de l'équipement utilisateur UE au réseau et pour des raisons de lisibilité, on ne distingue pas dans la suite l'équipement mobile de l'élément de sécurité, qui sont ainsi regroupés dans l'équipement utilisateur UE.

L'invention n'est pas limitée à un équipement utilisateur de ce type et dans un autre exemple de réalisation, l'équipement utilisateur UE comprend une zone logicielle sécurisée agencée pour traiter les données sensibles d'accès au réseau.

Dans l'exemple décrit ici, l'équipement utilisateur UE comprend :

- 5 - une unité de traitement 301, ou CPU, agencée pour exécuter des instructions de code,
- une interface radio 302, agencée pour s'interfacer avec le réseau mobile de communication ;
- un ensemble de mémoires, dont une mémoire volatile 303 de type RAM, utilisée
10 pour exécuter des instructions de code, stocker des variables, etc., et une mémoire de stockage 304 de type mémoire flash ou EEPROM. La mémoire de stockage 304 est agencée pour mémoriser des données et des applications. En particulier, la mémoire de stockage 304 mémorise un module logiciel d'enregistrement dans le
15 réseau agencé pour mettre en œuvre celles des étapes du procédé d'enregistrement dans le réseau décrit précédemment qui sont mises en œuvre par l'équipement utilisateur UE. La mémoire de stockage 304 mémorise également une clé d'authentification K, un identifiant du réseau nominal $HPLMN_{id}$, une clé publique pke associée à une clé secrète ske détenue par le serveur d'abonnés HSS, et une
20 valeur NoID destinée à être envoyée par l'équipement utilisateur dans une requête d'attachement au réseau lorsque l'équipement ne possède pas d'identifiant temporaire ;

L'équipement utilisateur UE comprend également :

- un module d'envoi 305, agencé pour envoyer à l'entité de gestion une requête d'attachement au réseau. Le module d'envoi 305 est agencé pour mettre en œuvre l'étape E0 du
25 procédé d'enregistrement tel que décrit précédemment ;
- un module de réception 306, agencé pour recevoir une requête d'identification. Le module de réception 306 est agencé pour mettre en œuvre l'étape E4 du procédé décrit précédemment ;
- un module de calcul et d'envoi 307, agencé pour calculer une valeur chiffrée pour le
30 serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification fonction dudit identifiant. Le module de calcul et d'envoi 307 est également agencé pour envoyer une réponse d'identification comprenant ladite valeur chiffrée et ladite valeur de vérification. Le module de calcul et d'envoi 307 est agencé pour mettre en œuvre l'étape E5 du procédé d'enregistrement tel que décrit en relation avec la
35 figure 1.

Le module d'envoi 305, le module de réception 306 et le module de calcul et d'envoi 307 sont de préférence des modules logiciels comprenant des instructions logicielles pour mettre en œuvre les étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication qui sont exécutées par l'équipement utilisateur UE.

5 L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé d'enregistrement d'un terminal mobile tel que décrit précédemment lorsque ce programme est exécuté par un processeur de l'équipement utilisateur UE, et

- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur

10 décrit ci-dessus.

Un serveur d'abonnés, selon un exemple de réalisation, va maintenant être décrit en relation avec la figure 4.

15 Un serveur d'abonnés HSS est un serveur informatique agencé pour gérer des données d'accès d'abonnés à un réseau de communication. Il est également agencé pour authentifier un équipement utilisateur lors de l'accès de celui-ci au réseau et pour s'authentifier auprès de cet équipement.

Le serveur d'abonnés HSS comprend :

- une unité de traitement ou processeur 401, destinée à charger des instructions en

20 mémoire, à les exécuter, à effectuer des opérations ;

- un ensemble de mémoires, dont une mémoire volatile 402, ou RAM, utilisée pour exécuter des instructions de code, stocker des variables, etc., et une mémoire de stockage 403 de type EEPROM. En particulier, la mémoire de stockage 403 est agencée pour mémoriser un module logiciel comprenant des instructions de code pour mettre en œuvre celles des étapes du

25 procédé d'enregistrement d'un équipement utilisateur dans un réseau de communication tel que décrit précédemment qui sont exécutées par le serveur d'abonnés HSS. Le serveur d'abonnés HSS est agencé pour accéder à une base d'abonnés 404 qui comprend des données d'accès au réseau propres à chacun des abonnés au réseau. En particulier, pour chacun des abonnés du réseau, le serveur d'abonnés HSS mémorise une clé d'authentification K de l'abonné. Le

30 serveur d'abonnés HSS mémorise également un couple de clés de chiffrement asymétrique pke/ske. Il distribue la clé publique de chiffrement pke à l'ensemble des abonnés qu'il gère ;

- un ensemble d'interfaces 405 agencées pour communiquer avec des entités du réseau, par exemple l'entité de gestion de la mobilité MME.

Le serveur d'abonnés HSS comprend également :

- un module de réception 406, agencé pour recevoir une requête de vecteur d'authentification en provenance de l'entité de gestion, ladite requête comprenant une valeur chiffrée C par l'équipement utilisateur pour le serveur d'abonnés. La valeur chiffrée est fonction d'un identifiant de l'équipement utilisateur. Le module de réception 406 est agencé pour mettre en œuvre l'étape E6 du procédé d'enregistrement décrit précédemment ;

- un module d'envoi 407, agencé pour envoyer une réponse d'authentification comprenant un vecteur d'authentification et l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée. Le module d'envoi 407 est agencé pour mettre en œuvre l'étape E9 du procédé d'enregistrement décrit en relation avec la figure 1.

Dans un exemple de réalisation, où la valeur chiffrée est fonction d'un aléa Rid et d'un message d'authentification calculé par l'équipement utilisateur à partir de l'identifiant de l'équipement utilisateur et de l'aléa, le serveur d'abonnés comprend également un module (non représenté sur la figure 4) de vérification, agencé pour vérifier le message d'authentification au moyen d'une clé d'authentification associée à l'identifiant de l'équipement utilisateur.

Les interfaces 405, le module de réception 406 et le module d'envoi sont de préférence des modules logiciels comprenant des instructions logicielles pour mettre en œuvre les étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau tel que décrit précédemment qui sont exécutées par le serveur d'abonnés HSS.

L'invention concerne donc aussi :

- un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé d'enregistrement d'un équipement utilisateur dans un réseau tel que décrit précédemment lorsque ce programme est exécuté par un processeur du serveur d'abonnés HSS, et

- un support d'enregistrement lisible sur lequel est enregistré le programme d'ordinateur décrit ci-dessus.

L'invention concerne aussi un système d'enregistrement dans un réseau de communication. Ce système comprend au moins un équipement utilisateur UE tel que décrit en relation avec la figure 3, un serveur d'abonnés HSS tel que décrit en relation avec la figure 4 et une entité de gestion de la mobilité telle que décrite en relation avec la figure 2. Un tel système est agencé pour mettre en œuvre les étapes du procédé d'enregistrement tel que décrit précédemment.

REVENDICATIONS

1. Procédé d'enregistrement d'un équipement utilisateur (UE) dans un réseau de communication, ledit réseau comprenant une entité de gestion (MME) et un serveur d'abonnés (HSS), le procédé, mis en œuvre par l'entité de gestion, comprenant :
- une étape (E0) de réception d'une requête d'attachement au réseau en provenance de l'équipement utilisateur,
 - une étape (E4) d'envoi à l'équipement utilisateur d'une requête d'identification,
 - une étape (E5) de réception d'une réponse d'identification, comprenant une valeur chiffrée (C) pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification (V), fonction dudit identifiant,
 - une étape (E6) d'envoi d'une requête de vecteur d'authentification au serveur d'abonnés, la requête comprenant la valeur chiffrée,
 - une étape (E9) de réception d'une réponse d'authentification comprenant l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée,
 - une étape (E10) de vérification au moyen de la valeur de vérification que l'identifiant de l'équipement utilisateur reçu du serveur d'abonnés correspond à l'identifiant utilisé pour calculer la valeur de contrôle.
2. Procédé selon la revendication 1, dans lequel la requête d'attachement comprend une valeur représentative (NoID) d'une absence de possession d'un identifiant temporaire par l'équipement utilisateur.
3. Procédé selon l'une des revendications précédentes, dans lequel la réponse d'identification comprend un identifiant du réseau nominal.
4. Procédé selon l'une des revendications précédentes, dans lequel la requête d'identification comprend un aléa (R_{id}), ledit aléa étant utilisé par l'équipement utilisateur pour calculer la valeur chiffrée et la valeur de vérification.
5. Procédé selon la revendication 4 dans lequel la valeur chiffrée est également fonction d'un message d'authentification calculé à partir de l'identifiant de l'équipement utilisateur et de l'aléa.

6. Procédé d'enregistrement d'un équipement utilisateur (UE) dans un réseau de communication, ledit réseau comprenant une entité de gestion (MME) et un serveur d'abonnés (HSS), le procédé, mis en œuvre par l'équipement utilisateur comprenant :

- une étape (E0) d'envoi à l'entité de gestion d'une requête d'attachement au réseau,
- 5 - une étape (E4) de réception d'une requête d'identification,
- une étape (E5) de calcul d'une valeur chiffrée (C) pour le serveur d'abonnés et d'une valeur de vérification (V), ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et ladite valeur de vérification (V) étant fonction dudit identifiant et envoi d'une réponse d'identification comprenant la valeur chiffrée et la valeur de vérification.

10

7. Procédé d'enregistrement d'un équipement utilisateur (UE) dans un réseau de communication, ledit réseau comprenant une entité de gestion (MME) et un serveur d'abonnés (HSS), le procédé, mis en œuvre par le serveur d'abonnés comprenant :

- une étape (E6) de réception d'une requête de vecteur d'authentification en provenance de l'entité de gestion, ladite requête comprenant une valeur chiffrée (C) par l'équipement utilisateur pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur,
- 15 - une étape (E9) d'envoi d'une réponse d'authentification comprenant un vecteur d'authentification et l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée.

20

8. Procédé selon la revendication 7 dans lequel la valeur chiffrée est fonction d'un aléa (R_{id}) et d'un message d'authentification calculé par l'équipement utilisateur à partir de l'identifiant de l'équipement utilisateur et de l'aléa, le procédé comprenant une étape de vérification du message d'authentification au moyen d'une clé d'authentification associée à l'identifiant de l'équipement utilisateur.

25

9. Entité de gestion (MME) d'un réseau, ledit réseau comprenant au moins un équipement utilisateur (UE) et un serveur d'abonnés (HSS), ladite entité comprenant :

- 30 - des premiers moyens de réception (205), agencés pour recevoir une requête d'attachement au réseau en provenance de l'équipement utilisateur,
- des premiers moyens d'envoi (206), agencés pour envoyer à l'équipement utilisateur une requête d'identification,
- des deuxièmes moyens de réception (207), agencés pour recevoir une réponse
- 35 d'identification, ladite réponse d'identification comprenant une valeur chiffrée (C) pour le

serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification (V), fonction dudit identifiant,

- des deuxièmes moyens d'envoi (208), agencés pour envoyer une requête de vecteur d'authentification au serveur d'abonnés, la requête comprenant la valeur chiffrée,
- 5 - des troisièmes moyens de réception (209), agencés recevoir une réponse d'authentification comprenant l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée,
- des moyens de vérification (210), agencés pour vérifier au moyen de la valeur de vérification que l'identifiant de l'équipement utilisateur reçu du serveur d'abonnés correspond à
- 10 l'identifiant utilisé pour calculer la valeur de contrôle.

10. Programme pour une entité de gestion d'un réseau de communication, comprenant des instructions de code de programme destinées à commander l'exécution des étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau, selon l'une des
15 revendications 1 à 5, lorsque le programme est exécuté sur ladite entité.

11. Equipement utilisateur (UE) dans un réseau de communication, ledit réseau comprenant une entité de gestion (MME) et un serveur d'abonnés (HSS), comprenant :

- des moyens d'envoi (305), agencés pour envoyer à l'entité de gestion une requête
- 20 d'attachement au réseau,
- des moyens de réception (306), agencés pour recevoir une requête d'identification,
- des moyens de calcul et d'envoi (307), agencés pour calculer une valeur chiffrée pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur, et une valeur de vérification fonction dudit identifiant et pour envoyer une réponse
- 25 d'identification comprenant ladite valeur chiffrée et ladite valeur de vérification.

12. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un équipement utilisateur, le programme comprenant des portions de code pour l'exécution des étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau selon l'une
30 quelconque des revendications 6, lorsque le programme est exécuté sur ledit équipement utilisateur.

13. Serveur d'abonnés (HSS) dans un réseau de communication, ledit réseau comprenant une entité de gestion (MME) et au moins un équipement utilisateur UE,
35 comprenant :

- des moyens de réception (406), agencés pour recevoir une requête de vecteur d'authentification en provenance de l'entité de gestion, ladite requête comprenant une valeur chiffrée (C) par l'équipement utilisateur pour le serveur d'abonnés, ladite valeur chiffrée étant fonction d'un identifiant de l'équipement utilisateur,

- 5 - des moyens d'envoi (407), agencés pour envoyer une réponse d'authentification comprenant un vecteur d'authentification et l'identifiant de l'équipement utilisateur obtenu du serveur d'abonnés par déchiffrement de la valeur chiffrée.

10 14. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un serveur d'abonnés, le programme comprenant des portions de code pour l'exécution des étapes du procédé d'enregistrement d'un équipement utilisateur dans un réseau selon l'une quelconque des revendications 5, lorsque le programme est exécuté sur ledit équipement utilisateur.

15 15. Système d'enregistrement d'au moins un équipement utilisateur dans à un réseau de communication comprenant :

- une entité de gestion (MME) selon la revendication 9,
- au moins un équipement utilisateur (UE) selon la revendication 11, et
- un serveur d'abonnés (HSS) selon la revendication 13.

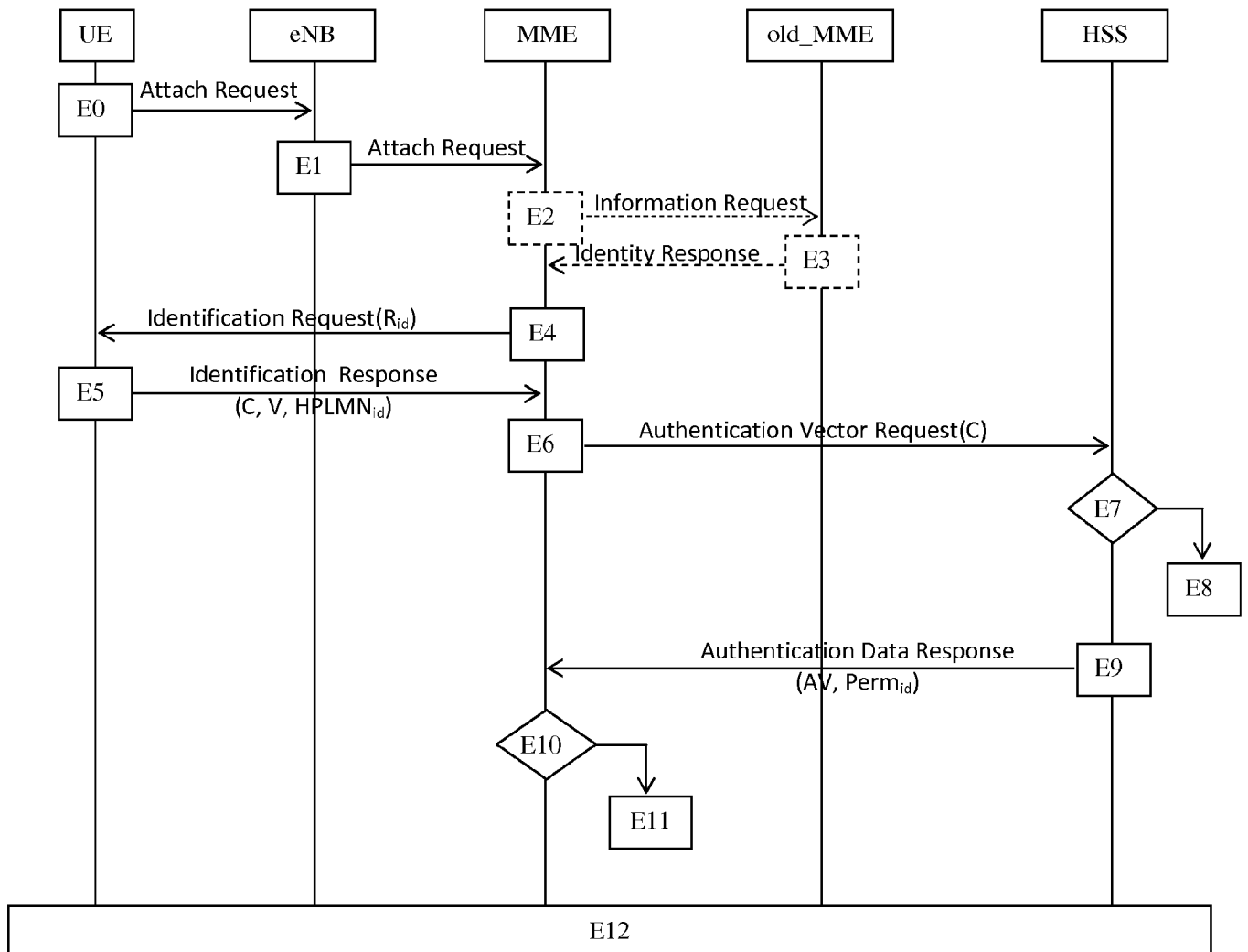


Figure 1

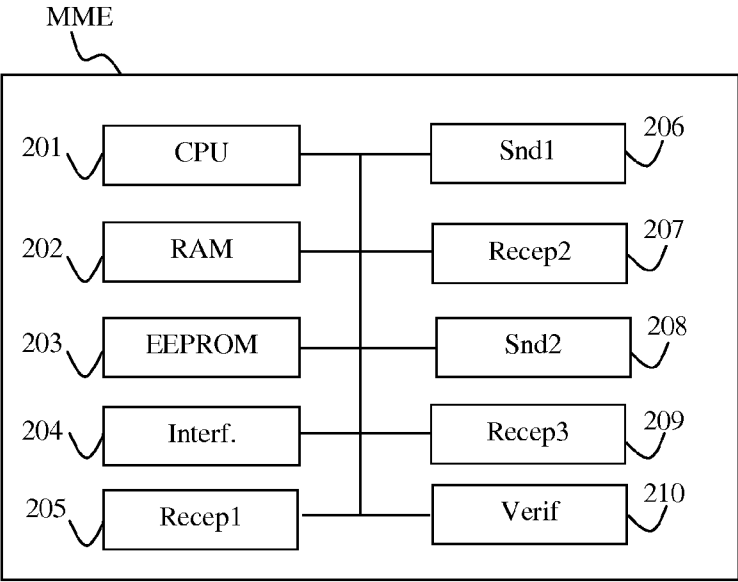


Figure 2

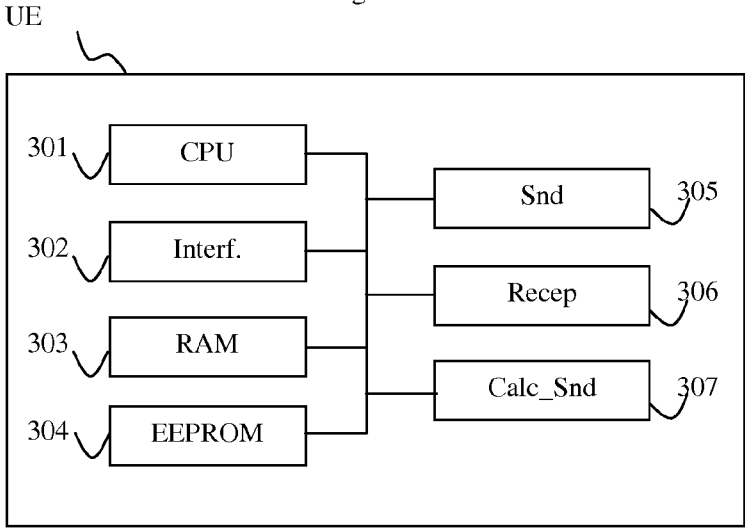


Figure 3

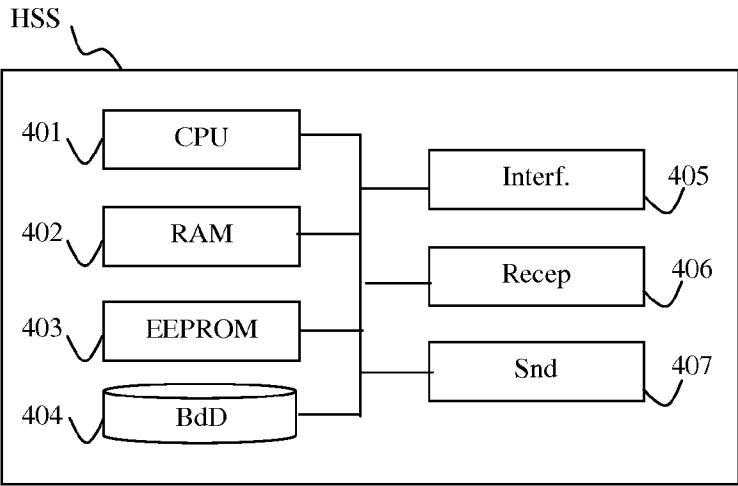


Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052694

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/02 H04W8/18 H04W12/06 H04W12/12 H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04W

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	US 2009/305671 A1 (LUFT ACHIM [DE] ET AL) 10 December 2009 (2009-12-10)	7,13,14
A	paragraph [0110] - paragraph [0118]; figure 5	1-6, 8-12,15

X	US 2008/130898 A1 (HOLTMANN SILKE [FI] ET AL) 5 June 2008 (2008-06-05)	1-12,15
	paragraph [0038] - paragraph [0055]; figure 3	

	-/--	



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

22 November 2017

Date of mailing of the international search report

29/11/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Jardak, Christine

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052694

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3gpp: "3GPP TS 24.008 3rd generation Partnership Project; Technical specification group core network; mobile radio interface layer 3 specification ; core network protocols; stage 3 (release 1999)", 31 December 2005 (2005-12-31), pages 1-451, XP055358595, Retrieved from the Internet: URL:http://www.arib.or.jp/IMT-2000/V740Dec09/5_Appendix/R99/24/24008-3k0.pdf [retrieved on 2017-03-24] paragraph [9.4.1.3] -----	1-12,15
A	Wikipedia: "Code d'authentification de message - Wikipédia", 6 June 2016 (2016-06-06), pages 1-2, XP055358599, Retrieved from the Internet: URL:https://fr.wikipedia.org/wiki/Code_d'authentification_de_message [retrieved on 2017-03-24] page 1 -----	1-12,15
X	EP 1 873 998 A1 (NOKIA CORP [FI]) 2 January 2008 (2008-01-02) paragraph [0040] - paragraph [0047]; figure 4 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2017/052694

Patent document cited in search report			Publication date		Patent family member(s)			Publication date	
US 2009305671	A1	10-12-2009	US	2009305671	A1			10-12-2009	
			US	2015245207	A1			27-08-2015	
			US	2016249217	A1			25-08-2016	

US 2008130898	A1	05-06-2008	US	2008130898	A1			05-06-2008	
			US	2013080779	A1			28-03-2013	
			WO	2008047195	A1			24-04-2008	

EP 1873998	A1	02-01-2008	EP	1873998	A1			02-01-2008	
			US	2008002829	A1			03-01-2008	
			US	2013003971	A1			03-01-2013	

Demande internationale n°
PCT/FR2017/052694

INV.	H04W12/02	H04W8/18	H04W12/06	H04W12/12	H04L29/06
ADD.					

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L H04W

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

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2009/305671 A1 (LUFT ACHIM [DE] ET AL) 10 décembre 2009 (2009-12-10)	7,13,14
A	alinéa [0110] - alinéa [0118]; figure 5	1-6, 8-12,15

X	US 2008/130898 A1 (HOLTMANN SILKE [FI] ET AL) 5 juin 2008 (2008-06-05)	1-12,15
	alinéa [0038] - alinéa [0055]; figure 3	

	-/--	

☒ Les documents de familles de brevets sont indiqués en annexe

- "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 d'expédition du présent rapport de recherche internationale

29/11/2017

Fonctionnaire autorisé

Jardak, Christine

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	3gpp: "3GPP TS 24.008 3rd generation Partnership Project; Technical specification group core network; mobile radio interface layer 3 specification ; core network protocols; stage 3 (release 1999)", 31 décembre 2005 (2005-12-31), pages 1-451, XP055358595, Extrait de l'Internet: URL: http://www.arib.or.jp/IMT-2000/V740Dec09/5_Appendix/R99/24/24008-3k0.pdf [extrait le 2017-03-24] alinéa [9.4.1.3] -----	1-12,15
A	Wikipedia: "Code d'authentification de message - Wikipédia", 6 juin 2016 (2016-06-06), pages 1-2, XP055358599, Extrait de l'Internet: URL: https://fr.wikipedia.org/wiki/Code_d'authentification_de_message [extrait le 2017-03-24] page 1 -----	1-12,15
X	EP 1 873 998 A1 (NOKIA CORP [FI]) 2 janvier 2008 (2008-01-02) alinéa [0040] - alinéa [0047]; figure 4 -----	1-15

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2017/052694

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009305671 A1	10-12-2009	US 2009305671 A1	10-12-2009
		US 2015245207 A1	27-08-2015
		US 2016249217 A1	25-08-2016

US 2008130898 A1	05-06-2008	US 2008130898 A1	05-06-2008
		US 2013080779 A1	28-03-2013
		WO 2008047195 A1	24-04-2008

EP 1873998 A1	02-01-2008	EP 1873998 A1	02-01-2008
		US 2008002829 A1	03-01-2008
		US 2013003971 A1	03-01-2013
