

(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 octobre 2006 (12.10.2006)

PCT

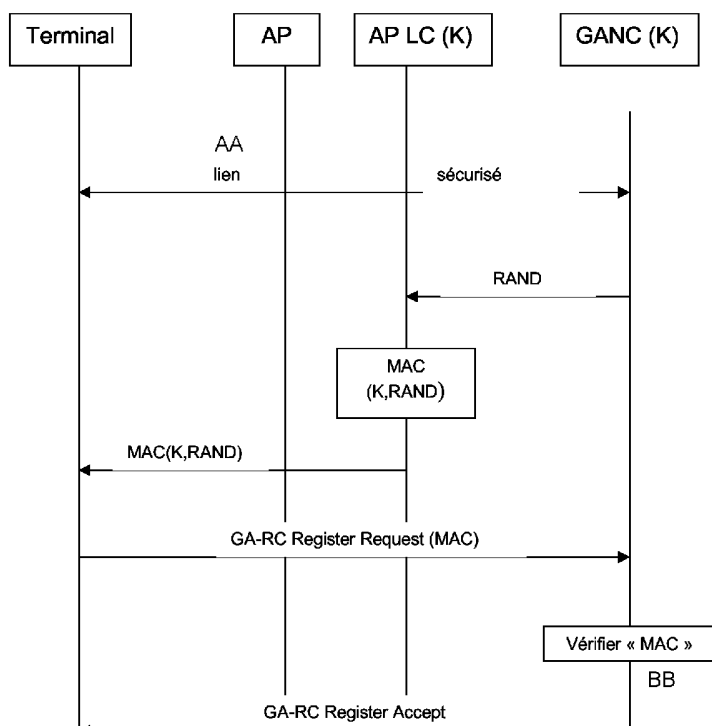
(10) Numéro de publication internationale
WO 2006/106261 A2

- (51) Classification internationale des brevets : **Non classée** (72) Inventeurs; et
(21) Numéro de la demande internationale : PCT/FR2006/050294 (75) Inventeurs/Déposants (pour US seulement) : **MARTI-QUET, Nicolas** [FR/FR]; 11, rue Auguste Chabrières, F-75015 Paris (FR). **FOUQUET, Sylvie** [FR/FR]; 171, avenue de Verdun, F-92190 Meudon (FR). **DRONNE, François** [FR/FR]; 34, rue Mozart, F-92330 Sceaux (FR).
(22) Date de dépôt international : 4 avril 2006 (04.04.2006)
(25) Langue de dépôt : français (74) Mandataire : **BENETIERE, Marion**; FRANCE TELECOM R & D/PIV/BREVETS, 38-40 rue du Général Leclerc, F-92794 Issy Les Moulineaux Cedex 9 (FR).
(26) Langue de publication : français
(30) Données relatives à la priorité : (81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, 05 03493 7 avril 2005 (07.04.2005) FR
(71) Déposant (pour tous les États désignés sauf US) : **FRANCE TELECOM** [FR/FR]; 6 place d'Alleray, F-75015 Paris (FR).

[Suite sur la page suivante]

(54) Title: METHOD FOR CONTROLLING PRESENCE OF TERMINAL ON AN ACCESS POINT TO A TELEPHONE NETWORK

(54) Titre : PROCÉDE DE CONTROLE DE PRESENCE D'UN TERMINAL SUR UN POINT D'ACCES A UN RESEAU DE TELEPHONIE



AA SECURE LINK
BB VERIFYING "MAC"

(57) Abstract: The invention concerns a method for controlling the presence of a terminal (10) on an access point (31) to a first telephone network via a second communication network, said access point (31) being defined by an address in said second communication network. The invention is characterized in that said method includes the following steps: in an initializing phase, associating with said access point (31) a certification module (33); establishing a correspondence table between an identifier of said terminal (10) and said access point (31) address; then in a second controlling phase, requesting from the terminal (10) its identifier and deducing therefrom by means of said correspondence table the address of said access point (31) in the second network; sending, to said address, a challenge (RAND) so as to provide same to the associated certification module (33); determination by the certification module (33) of a reply (MAC; RAND) to said challenge (RAND); transmitting said reply (MAC; RAND) to the terminal (10); returning by the terminal (10) a message (GA-RC Register Request) containing said reply; verifying the reply (MAC; RAND) contained in said message. The invention is applicable to access to a mobile telephone system operator's network via a stationary telephone network.

[Suite sur la page suivante]



MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

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

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** Procédé de contrôle de présence d'un terminal (10) sur un point (31) d'accès à un premier réseau de téléphonie à travers un deuxième réseau de communication, ledit point (31) d'accès étant défini par une adresse dans ledit deuxième réseau de communication. Selon l'invention, ledit procédé comprend les étapes consistant à : dans une phase d'initialisation, - associer audit point (31) d'accès un module (33) de certification, - établir une table de correspondance entre un identifiant dudit terminal (10) et l'adresse dudit point (31) d'accès, puis, dans une phase de contrôle, - requérir auprès du terminal (10) son identifiant et en déduire au moyen de ladite table de correspondance l'adresse dudit point (31) d'accès dans le deuxième réseau, - envoyer, à ladite adresse, un défi (RAND) afin de le fournir au module (33) de certification associé, - déterminer par le module (33) de certification une réponse (MAC; RAND) audit défi (RAND), - transmettre ladite réponse (MAC; RAND) au terminal (10), - retourner par le terminal (10) un message (GA-RC Register Request) contenant ladite réponse, - vérifier la réponse (MAC; RAND) contenue dans ledit message. Application à l'accès au réseau d'un opérateur de téléphonie mobile à travers un réseau de téléphonie fixe.

PROCEDE DE CONTROLE DE PRESENCE D'UN TERMINAL SUR UN POINT D'ACCES A UN RESEAU DE TELEPHONIE

La présente invention concerne un procédé de contrôle de présence d'un terminal sur un point d'accès à un premier réseau de téléphonie à travers un deuxième réseau de communication.

5 L'invention trouve une application particulièrement avantageuse dans le domaine des accès au réseau cœur d'un réseau de téléphonie mobile à travers un réseau IP, par exemple un réseau IP de type ADSL supporté au moins en partie par un réseau de téléphonie fixe.

A titre d'exemple, l'accès au réseau de téléphonie mobile peut être réalisé par un terminal mobile en se connectant à une borne radio, de type 10 Wi-Fi ou Bluetooth, laquelle est reliée au réseau cœur du réseau de téléphonie mobile par une liaison ADSL à travers une ligne de téléphonie fixe.

Ce type d'accès est régi par un consortium de constructeurs et d'opérateurs de télécommunications connu sous le nom d'UMA (Unlicensed Mobile Access) qui a défini une architecture pour connecter un réseau 15 d'accès générique basé sur IP au réseau cœur du réseau de téléphonie mobile de l'opérateur. Cette architecture a été introduite au 3GPP dans le document 3GPP TS 43.318 et fait appel à une nouvelle entité appelée UNC (UMA Network Controller) par le consortium UMA ou GANC (Generic Access Network Controller) par le 3GPP. Cette entité GANC/UNC sert d'interface 20 entre un réseau d'accès générique basé sur IP et le réseau cœur du réseau de téléphonie mobile. Elle est contrôlée par l'opérateur mobile.

Pour un opérateur de téléphonie mobile, la solution basée sur l'architecture UMA présente les avantages suivants :

25 - extension de la couverture géographique. En effet, pour un opérateur de téléphonie mobile ayant des difficultés de couverture de réseau (notamment en intérieur), cette solution permet d'utiliser le réseau de téléphonie fixe et la

couverture DSL auxquels l'abonné a déjà souscrit, pour étendre la couverture à moindre coût. Deux types d'extension de couverture peuvent alors être envisagés :

5 * couverture des zones blanches, c'est-à-dire non couvertes par le réseau mobile, GSM ou UMTS par exemple. L'opérateur peut de cette manière couvrir des secteurs géographiques dans lesquels il était absent auparavant.

10 * complément à la couverture existante. Même lorsque la couverture du réseau de téléphonie mobile existe, la solution UMA permet de décharger le réseau mobile et d'offrir plus de capacité à l'opérateur.

- tarification de type domestique ("Home Zone"). Un certain nombre d'opérateurs souhaitent offrir une tarification spéciale à ceux de leurs clients qui utilisent leur terminal mobile lorsqu'ils sont chez eux. A cet effet, une solution de type UMA peut être intéressante car elle permet également un accès moins coûteux pour l'opérateur. Cependant, un moyen technique est nécessaire pour s'assurer que le client est réellement à son domicile afin de lui appliquer le tarif domestique.

20 Comme cela vient d'être souligné, l'un des objectifs que peut avoir un opérateur de téléphonie mobile en adoptant une solution de type UMA est de pratiquer une tarification particulière au client lorsqu'il est chez lui.

En effet, si le client a un accès ADSL Wi-Fi à son domicile, il est intéressant pour l'opérateur de lui appliquer un tarif plus attractif, car :

25 - l'opérateur du réseau mobile attire ainsi sur son réseau coeur un client qui, sinon, aurait davantage intérêt à utiliser son téléphone fixe,
- tout en soulageant son réseau d'accès radio.

Afin de pratiquer ce type de tarification, l'opérateur a donc besoin d'être absolument certain que le client est bien chez lui.

Pour cela, les solutions actuellement proposées sont:

30 - utilisation de la couverture du réseau mobile du client pour obtenir sa localisation. Cela signifie cependant que la solution ne fonctionne pas dans les zones blanches (voir plus haut). D'autre part, il faut s'assurer que le client ne peut pas modifier la donnée de localisation envoyée par son terminal vers le réseau.

- identification du point d'accès. Mais, encore une fois, les solutions actuellement proposées par les constructeurs reposent principalement sur un envoi de l'identifiant du point d'accès par le terminal, ce qui n'est pas très difficile à détourner par le client, ce dernier pouvant envoyer l'identifiant du point d'accès « domicile » alors qu'il ne s'y trouve pas.

Dans les deux cas, un client mal intentionné est capable de détourner l'information afin d'obtenir une tarification de type domestique (« Home Zone ») même lorsqu'il n'est pas à son domicile.

Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de contrôle de présence d'un terminal sur un point d'accès à un premier réseau de téléphonie à travers un deuxième réseau de communication, ledit point d'accès étant défini par une adresse dans ledit deuxième réseau de communication, qui permettrait à l'opérateur dudit premier réseau de connaître avec certitude l'identité et la localisation du point d'accès effectivement utilisé par le terminal du client.

La solution au problème technique posé consiste, selon la présente invention, en ce que ledit procédé comprend les étapes consistant à :

dans une phase d'initialisation,

- associer audit point d'accès un module de certification,
 - établir une table de correspondance entre un identifiant dudit terminal et l'adresse dudit point d'accès,
- puis, dans une phase de contrôle,
- requérir auprès du terminal son identifiant et en déduire au moyen de ladite table de correspondance l'adresse dudit point d'accès dans le deuxième réseau,
 - envoyer, à ladite adresse, un défi afin de le fournir au module de certification associé,
 - déterminer par le module de certification une réponse audit défi,
 - transmettre ladite réponse au terminal,
 - retourner par le terminal un message contenant ladite réponse,
 - vérifier la réponse contenue dans ledit message.

Ainsi, on comprend, d'une part, que, grâce à la table de correspondance, le défi est bien envoyé au domicile du client, et d'autre part,

que, si la réponse au défi est correcte, le terminal se trouve bien à ce domicile.

Afin de garantir la sécurité de la table de correspondance, l'invention prévoit que ladite table de correspondance est gérée par ledit premier réseau.

5 De même, le niveau de sécurisation du procédé conforme à l'invention est encore augmenté si l'identifiant de terminal est requis à travers un lien sécurisé.

Selon un premier mode de réalisation particulier du procédé conforme à l'invention, il est prévu que, ledit défi étant constitué par un nombre aléatoire
10 fourni audit module de certification, la réponse audit défi est constituée par une signature calculée à partir dudit nombre aléatoire et d'une clé secrète préalablement fournie au module de certification.

Selon un deuxième mode de réalisation particulier du procédé conforme à l'invention, il est prévu que, ledit défi étant constitué par un
15 nombre aléatoire fourni audit module de certification, la réponse audit défi est constituée par le nombre aléatoire. Dans ce deuxième mode, il n'y a pas de clé secrète à provisionner dans le module de certification. Toutefois, l'unicité du défi permet d'associer de façon unique la réponse fournie à un module de certification particulier.

20 Par ailleurs, un module de certification d'un point d'accès pour la mise en œuvre du procédé selon l'invention, est remarquable en ce que ledit module de certification est apte à :

- recevoir un défi,
- déterminer une réponse audit défi,
- 25 - transmettre ladite réponse au terminal.

De plus, un contrôleur de réseau d'accès générique pour la mise en œuvre du procédé selon l'invention, est remarquable en ce que ledit contrôleur est apte à :

- fournir un défi à l'adresse dudit point d'accès,
- 30 - vérifier la réponse contenue dans le message retourné par ledit terminal.

Enfin, un système pour la mise en œuvre du procédé selon l'invention, est remarquable en ce que ledit système comprend un contrôleur selon

l'invention apte à gérer une pluralité de points d'accès, chaque point d'accès étant associé à un module respectif de certification selon l'invention.

La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma d'ensemble d'un système d'accès à un premier réseau, de téléphonie mobile, à travers un deuxième réseau de communication, en l'espèce un réseau IP, comme cela sera explicité plus loin.

La figure 2 est un diagramme des échanges d'informations effectués lors de la mise en œuvre du procédé conforme à l'invention selon un premier mode de réalisation.

La figure 3 est un diagramme des échanges d'informations effectués lors de la mise en œuvre du procédé conforme à l'invention selon un deuxième mode de réalisation.

Sur la figure 1 est représentée une architecture UMA pour l'accès d'un terminal 10, un téléphone mobile par exemple, au réseau cœur 20 du premier réseau de téléphonie mobile d'un opérateur de téléphonie mobile.

Le client abonné audit premier réseau de téléphonie mobile dispose à son domicile d'une liaison radio, notamment une liaison Wi-Fi, entre son terminal 10 et une borne 31 qui constitue un point d'accès AP au réseau de téléphonie mobile. La borne 31 est reliée à une ligne téléphonique fixe 32 du client sur laquelle est réalisée une liaison IP, ici de type ADSL, entre ladite borne 31 et un contrôleur GANC 40. La ligne téléphonique 32 appartient ainsi à un réseau IP (celui que l'on a appelé "deuxième réseau") supporté au moins en partie par le réseau de téléphonie fixe auquel appartient la ligne téléphonique 32. On rappelle ici qu'un contrôleur GANC (Generic Access Network Controller) joue le rôle d'interface entre un réseau d'accès générique basé sur IP, en l'espèce le réseau IP supporté par la ligne téléphonique 32, et le réseau cœur 20 du réseau de téléphonie mobile.

Comme le montre la figure 1, le procédé de contrôle de présence du terminal 10 au point 31 d'accès AP implique la présence d'une entité 33 appelée module de certification de localisation du point d'accès AP LC, qu'on désignera en abrégé par « module de certification ». Ce module, dont le

fonctionnement sera expliqué en détail plus loin, a pour but de s'assurer que le client utilise bien son point d'accès PA et qu'il est bien localisé au domicile du client, c'est-à-dire que celui-ci n'a pas déplacé son point d'accès à l'étranger, par exemple, pour éviter les frais de « roaming ».

5 Dans l'exemple particulier de la description, le point 31 d'accès et le module 33 de certification sont deux entités distinctes et connectées l'une à l'autre. Il faut noter que rien n'interdit que le module 33 de certification AP LC soit physiquement intégré au point 31 d'accès PA. Autrement dit, le point d'accès AP et le module AP LC peuvent être la même entité physique, mais ils
10 peuvent aussi être séparés.

De même, et préalablement à la mise en œuvre proprement dite du procédé selon l'invention, il est établi une table de correspondance entre un identifiant dudit terminal 10 et l'adresse dudit point 31 d'accès. A titre d'exemple, l'identifiant dudit terminal 10 est son numéro d'identification unique
15 dans le réseau mobile (IMSI « International Mobile Subscriber Identity »). L'adresse du point 31 d'accès est universelle et également connue sous le nom de MAC («Medium Access Control»).

De préférence, ladite table de correspondance est gérée par le réseau mobile et l'abonné du terminal 10 n'y a pas accès. A titre d'exemple, cette
20 table est établie par le GANC 40 et mémorisée dans celui-ci.

Dans un premier mode de réalisation, une clé secrète permanente K est partagée entre le module de certification AP LC et le contrôleur GANC 40. Cette clé K est unique pour chaque couple AP LC/GANC. Par les termes "clé
25 secrète", on entend bien entendu désigner une clé symétrique de chiffrement et de déchiffrement.

Après cette phase d'initialisation, le procédé conforme à l'invention se poursuit par une phase de contrôle qui va maintenant être décrite en référence aux figures 2 et 3, correspondant respectivement à deux modes de
réalisation.

30 Tout d'abord, le terminal 10 et le contrôleur GANC 40 établissent un lien, conformément à la procédure « Registration » décrite dans la section 8.4.1.6.1 du document 3GPP TS 43.318 v2.0.0. A l'issue de cette étape, les deux entités se sont authentifiées et sont capables de communiquer en toute

confidentialité. Lors de cette phase d'authentification, le terminal 10 fournit son identifiant au contrôleur GANC 40.

Ensuite, après avoir identifié le terminal 10, le contrôleur GANC 40 détermine au moyen de ladite table de correspondance l'adresse du point 31 d'accès AP au domicile du client

Puis, le contrôleur GANC 40 génère un défi sous forme d'un nombre aléatoire RAND et l'envoie au point 31 d'accès AP afin de le transmettre au module 33 de certification AP LC. Dans un mode particulier de réalisation, le point d'accès peut être identifié par le numéro de téléphone associé à la ligne téléphonique 32 fixe au domicile du client. Dans ce cas, le numéro de téléphone est inclus dans la table de correspondance. Le défi RAND peut être envoyé, par exemple, par un message court (SMS) fixe sur ladite ligne téléphonique fixe du client.

Selon le premier mode de réalisation, en réponse au défi, le module 33 de certification AP LC calcule alors une signature à partir de la clé secrète K et du nombre aléatoire RAND reçu du contrôleur GANC. Cette signature porte le nom de MAC (Message Authentication Code). Elle est basée sur la fonction HMAC définie dans le RFC 2104 (par exemple HMAC-SHA1). Elle constitue la réponse au défi.

Selon le deuxième mode de réalisation, en réponse au défi, le module 33 de certification renvoie le nombre aléatoire RAND lui-même, tel que reçu du contrôleur GANC sans modification.

Dans ces deux modes de réalisation, la réponse est transmise au terminal 10 via la liaison radio locale Wi-Fi, et le terminal 10 la retourne au contrôleur GANC 40 à travers la ligne téléphonique fixe 32. De manière pratique, on utilise pour cette transmission le message connu sous le nom de GA-RC Register Request conforme à la procédure « Registration » précitée, la réponse au défi étant incluse dans le champ AP-ID de ce message.

Enfin, le contrôleur GANC 40 vérifie la réponse qui lui est ainsi retournée par le terminal 10. Si la vérification est positive, on en conclut que client utilise bien son point 31 d'accès et, dans la variante décrite ci-dessus, à son domicile. Le contrôleur GANC 40 envoie alors au terminal 10 un message

d'acceptation GA-RC Register Accept conforme également à la procédure
« Registration » précitée.

REVENDICATIONS

5

1. Procédé de contrôle de présence d'un terminal (10) sur un point (31) d'accès à un premier réseau de téléphonie à travers un deuxième réseau de communication, ledit point (31) d'accès étant défini par une adresse dans ledit deuxième réseau de communication, caractérisé en ce que ledit procédé comprend les étapes consistant à :

10

dans une phase d'initialisation,

- associer audit point (31) d'accès un module (33) de certification,
- établir une table de correspondance entre un identifiant dudit terminal (10) et l'adresse dudit point (31) d'accès,

15

puis, dans une phase de contrôle,

- requérir auprès du terminal (10) son identifiant et en déduire au moyen de ladite table de correspondance l'adresse dudit point (31) d'accès dans le deuxième réseau,

20

- envoyer, à ladite adresse, un défi (RAND) afin de le fournir au module (33) de certification associé,

- déterminer par le module (33) de certification une réponse (MAC; RAND) audit défi (RAND),

25

- transmettre ladite réponse (MAC; RAND) au terminal (10),

- retourner par le terminal (10) un message (GA-RC Register Request) contenant ladite réponse,

- vérifier la réponse (MAC; RAND) contenue dans ledit message.

2. Procédé selon la revendication 1, caractérisé en ce que ladite table de correspondance est gérée par ledit premier réseau.

30

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que l'identifiant de terminal (10) est requis à travers un lien sécurisé.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que, ledit défi étant constitué par un nombre aléatoire (RAND) fourni audit module (33) de certification, la réponse audit défi est constituée par une signature (MAC) calculée à partir dudit nombre aléatoire (RAND) et d'une clé secrète (K) préalablement fournie au module (33) de certification.
- 5
5. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que, ledit défi étant constitué par un nombre aléatoire (RAND) fourni audit module (33) de certification, la réponse audit défi est constituée par ledit nombre aléatoire (RAND).
- 10
6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ledit premier réseau de téléphonie est un réseau de téléphonie mobile, et en ce que ledit deuxième réseau de communication est un réseau IP.
- 15
7. Procédé selon la revendication 6, caractérisé en ce que le point (31) d'accès est relié à une ligne de téléphonie fixe supportant une liaison IP et en ce que l'adresse dudit point (31) d'accès dans la table de correspondance comprend le numéro de ladite ligne téléphonique.
- 20
8. Procédé selon la revendication 7, caractérisé en ce que ledit défi (RAND) est envoyé par un message court (SMS) via la ligne de téléphonie fixe d'accès au réseau IP.
- 25
9. Module de certification d'un point (31) d'accès pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ledit module (33) de certification est apte à :
- recevoir un défi (RAND),
 - déterminer une réponse (MAC; RAND) audit défi (RAND),
 - transmettre ladite réponse (MAC; RAND) au terminal (10).
- 30

10. Contrôleur de réseau d'accès générique pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ledit contrôleur (40) est apte à :

- fournir un défi (RAND) à l'adresse dudit point (31) d'accès,
- 5 - vérifier la réponse (MAC; RAND) contenue dans le message (GA-RC Register Request) retourné par ledit terminal (10).

11. Système pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que ledit système comprend un
10 contrôleur (40) selon la revendication 10 apte à gérer une pluralité de points (31) d'accès, chaque point d'accès étant associé à un module respectif (33) de certification selon la revendication 9.

1/2

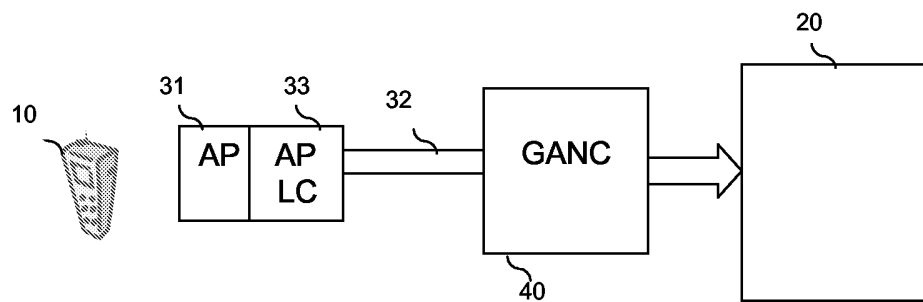


FIG. 1

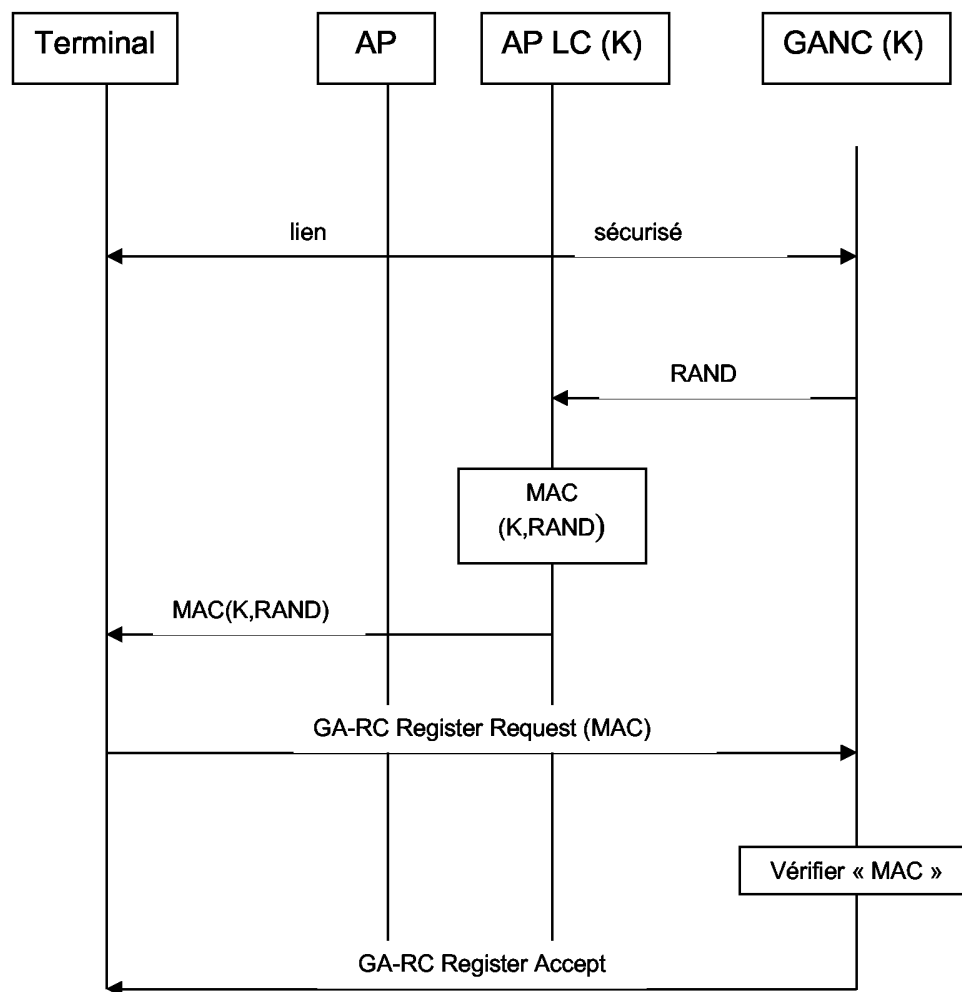


FIG. 2

2/2

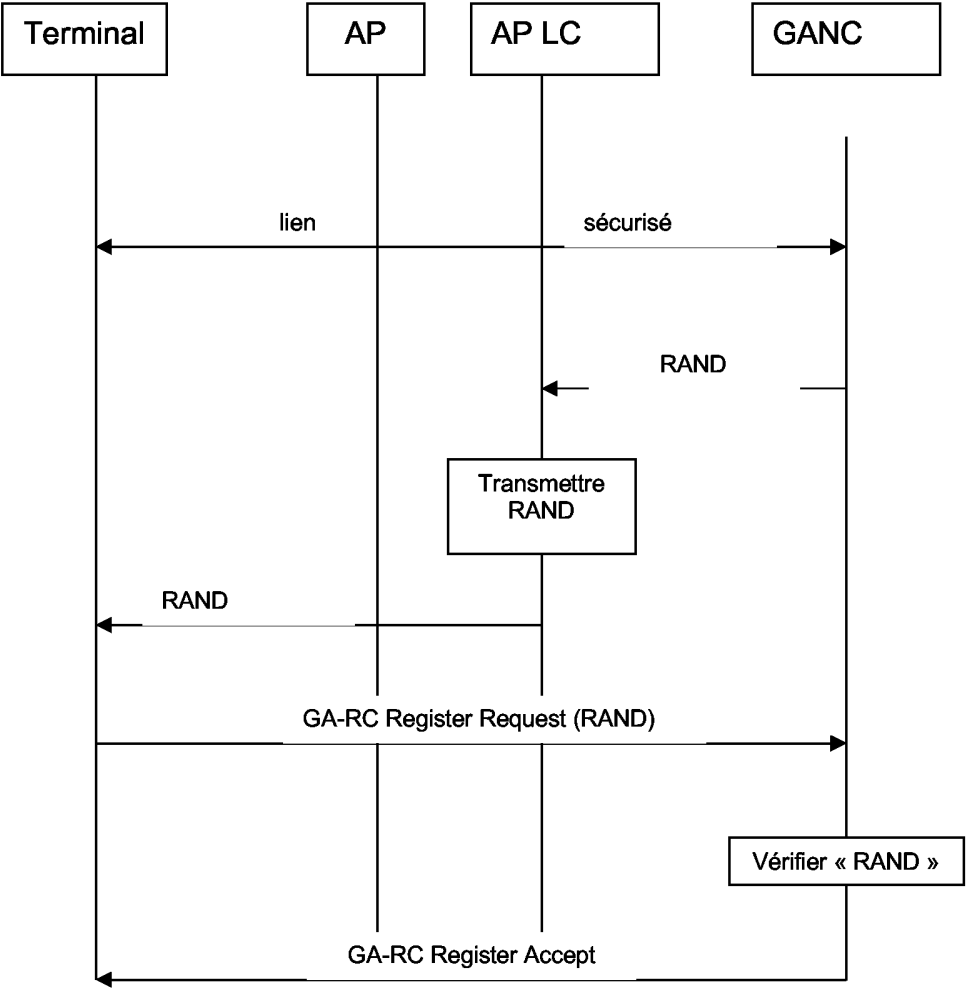


FIG. 3