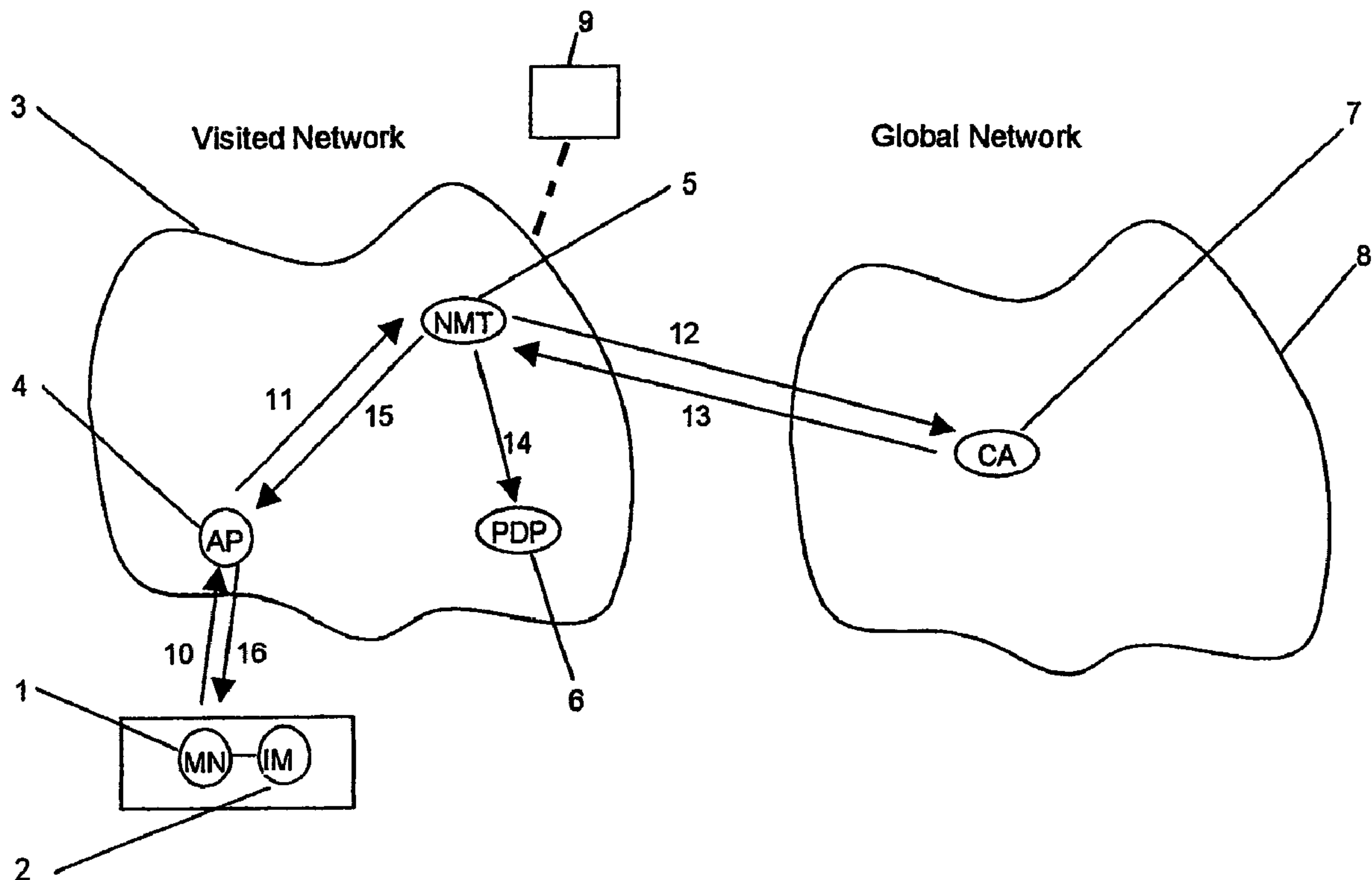




(86) Date de dépôt PCT/PCT Filing Date: 2001/11/29
(87) Date publication PCT/PCT Publication Date: 2003/06/12
(45) Date de délivrance/Issue Date: 2011/08/30
(85) Entrée phase nationale/National Entry: 2004/05/27
(86) N° demande PCT/PCT Application No.: DE 2001/004461
(87) N° publication PCT/PCT Publication No.: 2003/049365

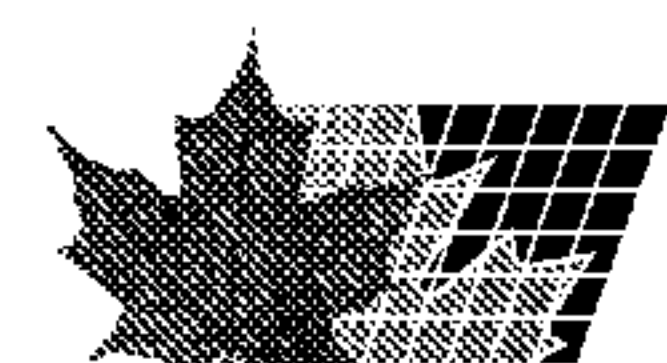
(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01),
H04L 9/30 (2006.01), *H04W 12/06* (2009.01)
(72) Inventeurs/Inventors:
CUELLAR, JORGE, DE;
MARHOEFER, MICHAEL, DE
(73) Propriétaire/Owner:
SIEMENS AKTIENGESELLSCHAFT, DE
(74) Agent: SMART & BIGGAR

(54) Titre : UTILISATION D'UNE PAIRE DE CLES PUBLIQUES DANS UN TERMINAL POUR L'AUTHENTIFICATION ET L'AUTORISATION DE L'ABONNE DE TELECOMMUNICATION PAR RAPPORT AU FOURNISSEUR DE RESEAU ET DES PARTENAIRES COMMERCIAUX
(54) Title: USE OF A PUBLIC KEY KEY PAIR IN THE TERMINAL FOR AUTHENTICATION AND AUTHORIZATION OF THE TELECOMMUNICATION SUBSCRIBER IN RESPECT OF THE NETWORK OPERATOR AND BUSINESS PARTNERS



(57) Abrégé/Abstract:

A very efficient authentication and authorisation check in n: m relationships is possible with a method for checking the entitlement of a user of a telecommunication terminal (1) to a service, whereby an access device (4) on a telecommunication network (3)



(57) **Abrégé(suite)/Abstract(continued):**

obtains at least one certificate and a proof of identity (10) from the telecommunication terminal (1), whereupon NMT (5) together with a certification device (7) carries out a check of whether the certificate giving the identity is valid and has a positive status and whether particular authorisation may be obtained from complementary certificates. Should the above be the case, a secret (for example a session key) is transmitted (15) to the access device (4) which is also sent (15, 16) to the telecommunication terminal (1, 2), encoded with at least the public key. The access device (4) is then activated with a policy corresponding to the rights of the telecommunication user.

Abstract

A very efficient authentication and authorisation check in n: m relationships is possible with a method for checking the entitlement of a user of a telecommunication terminal (1) to a service, whereby an access device (4) on a telecommunication network (3) obtains at least one certificate and a proof of identity (10) from the telecommunication terminal (1), whereupon NMT (5) together with a certification device (7) carries out a check of whether the certificate giving the identity is valid and has a positive status and whether particular authorisation may be obtained from complementary certificates. Should the above be the case, a secret (for example a session key) is transmitted (15) to the access device (4) which is also sent (15, 16) to the telecommunication terminal (1, 2), encoded with at least the public key. The access device (4) is then activated with a policy corresponding to the rights of the telecommunication user.

54106-62

1

Description

Use of a public key key pair in the terminal for authentication and authorization of the telecommunication subscriber in respect of the network operator and business partners.

- 5 The invention relates to devices and methods for checking the entitlement (authentication and/or authorization) of a subscriber in respect of an access device of a telecommunication network or in respect of a further service provider available via said network.

EP-A2-0903887 discloses a secret generated by an authentication unit of a mobile
10 radio network, which is transmitted to a mobile station, which uses the secret to authenticate the mobile station in respect of a base station of the mobile radio network, whereby the base station can implement an authentication check with the assistance of the authentication unit. It is proposed particularly that a service provider with an RSA key pair (F, G) sends the result $F(E)$ of encoding the public
15 key E of the mobile station with the private key F of the service provider to a mobile station, which has its own key pair (D, E), whereupon the mobile station can send E and $F(E)$ to the mobile radio network, whereupon the service provider can use their private key G to recover E from $F(E)$; the service provider then sends a random number $E(X)$ encoded with the public key E of the mobile radio
20 terminal to the mobile radio terminal, which can use its private key D to recover the random number X from $E(X)$ and send it back unencoded to the service provider for authentication.

XP10314761, ISBN 0-7803-4872-9 by Stefan Pütz discloses an authentication method for third generation mobile radio networks, with which authentication is
25 effected by means of a challenge response method.

According to the GSM standard for example, a GSM mobile station (mobile phone) uses the SIM card of a user, which contains a secret identifying the SIM card, said secret being also known to the network operator (shared secret), and a PIN number requested from the subscriber using the mobile radio station. A
30 network operator can use an appropriate protocol (e.g. the challenge response

54106-62

2

protocol for GSM authentication) to identify a user's SIM card and to permit or refuse the subscriber the use of the mobile radio network for example. This method is however only suitable for authentication in n:1 relationships (authentication of for example n potential users of a mobile radio network in respect of one network operator) but is not suitable for authenticating the subscriber in respect of a plurality of potential business partners (not known definitively in advance) (n: m relationship).

The object of the present invention is therefore to facilitate simple and efficient authentication and authorization of a telecommunication subscriber for specific services or transactions via a telecommunication network in respect of an access device of a telecommunication network, which the telecommunication subscriber wishes to use by means of a telecommunication terminal with a subscriber identity module.

The invention allow simple and efficient authentication of a telecommunication subscriber in respect of the telecommunication network, via which said subscriber communicates (to process services such as transactions) and also simple and efficient authentication and/or authorization in respect of third parties for predefined services such as transactions (confidential emails, banking transactions, payments, etc.).

The inventive method also functions with n: m relationships such as authentication of potential telecommunication subscribers by means of telecommunication subscriber identity modules in telecommunication terminals in respect of a plurality of (m) connectivity providers for peer-to-peer transactions between end subscribers, in ad hoc networks, etc., allows the generation of a value-added facility (for the legal validity of orders, transfers, etc.) with the use of public key key pairs, allows multiples use of existing components (telecommunication subscriber identity modules) without increasing terminal-side hardware costs and provides a high level of security.

The method is particularly suitable for authenticating mobile terminals in respect of an internet protocol network for the use of said network itself and for services offered by third parties via the internet protocol network.

54106-62

2a

According to one aspect of the present invention, there is provided a method for checking the entitlement of a subscriber of a telecommunication terminal with a subscriber identity module to utilize a service or use a telecommunication network, characterized in that an access device of a telecommunication network obtains at
5 least one certificate and identity data from the telecommunication terminal, whereupon a network management device (NMT 5) or a certification device carries out a check to establish whether the certificate confirms the identity data and has a positive status, whereby, if this is the case, a secret (session key) is transmitted to the access device, said secret encoded with at least a public key of
10 the subscriber identity module also being sent to the telecommunication terminal.

In accordance with another aspect of the present invention, there is provided a telecommunication network, particularly for implementing the method according to the invention herein, characterized in that it comprises the following: an access device for receiving a certificate and identity data sent from telecommunication
15 terminal, access to a certification device with a certificate generation method for generating certificates from public keys, which certification device gives notification of the validity of a certificate and associated status data on request, whereby the access of a telecommunication terminal to a service of a provider permitted for holders of a certificate is only granted by a device of the
20 telecommunication network in so far as the check on a certificate/ the certificates of the telecommunication terminal by the certification device using the public key was successful.

Further features and advantages of the invention will emerge from the description which follows of an exemplary embodiment with reference to the drawing, in
25 which:

FIG. 1 shows a schematic representation of an inventive entitlement check

3

Figure 1 shows a telecommunication terminal 1 (mobile node MN, e.g. a cellular mobile radio terminal for GSM, UMTS, etc.) with a connected (for example insertable therein) telecommunication subscriber identity module 2 (e.g. SIM, W-SIM, UICC of a U-SIM, etc.), a visited telecommunication network 3 (for example an internet protocol network of a mobile telecommunication network, etc.) with an access device 4 (AP = access point) to the telecommunication network 3, with a network management device 5 (NMT = network management tool) and an access management entity 6 (PDP = policy decision point). A certification device 7, which also provides a publicly accessible directory of certificates it has generated and the status data assigned to said certificates (in the same telecommunication network 3 or in a different telecommunication network 8 or with a different operator or in a trust center, which can be accessed by elements of the telecommunication network 3), can be contacted by the telecommunication network 3, which the user of the telecommunication terminal 1 wishes to use, to check identity data (MSISDN, etc.) and certificates stored in the telecommunication terminal 1 and to request the associated status data of the telecommunication subscriber 1 with regard to the implementation of services. These services for example include transport services, particularly use of the telecommunication network 3 itself, and/or application services, such as location-related services and/or transactions such as orders, transfers, etc. with providers 9 via the telecommunication network 3.

The user of the telecommunication terminal 1 wishes to prove their entitlement in respect of the operator of the network 3 and/or a provider 9 (within the telecommunication network 3 or outside the telecommunication network 3, for example even a third party provider independent of the telecommunication network, offering their services only via the telecommunication network 3) to utilize

4

services of the provider of 3 or 9, in other words to implement an authentication and/or authorization. The authentication and/or authorization is effected in respect of the telecommunication network 3 or the provider of the service 9 (e.g. by the NMT (5))

5 once the identity data (MSISDN, etc.) and entitlement of the telecommunication subscriber 1 (or of the telecommunication subscriber identity module 2) has been checked.

The identity data and entitlement of the telecommunication subscriber 1 are checked here by checking one or a plurality of
10 certificate(s) stored in said subscriber's telecommunication subscriber identity module 2 and using a private key of an asymmetrical (PKI-based) key pair also stored in the subscriber identity module 2. The check is for example implemented when an attempt is made to log the telecommunication subscriber terminal 1
15 onto the telecommunication network 3 as part of an authorization check method between the NMT, access device AP 4 and the telecommunication subscriber terminal 1 by checking the certificate/certificates and requesting the assigned status data in the certification device 7. The NMT verifies the validity of the
20 certificate by means of an OCSP or CRL inquiry to CA 7.

When it wishes to be authorized in respect of the access device 4, the telecommunication subscriber identity module 1 inputs a PIN or another input specific to the telecommunication subscriber
25 (fingerprint, etc.) and sends the access device 4 (for example in response to a challenge by the access device 4 with a challenge number) identity data (relating to the identity of the telecommunication subscriber identity module or the terminal and/or the subscriber), one or a plurality of certificates (that can be
30 generated from identity or assigned entitlement data, a public key of an asymmetrical key pair with a certificate generation method known only to the certification device 7) and protection signed by

5

the private key from the telecommunication subscriber identity module against unauthorized repetition of an intercepted request by a third party (replay protection, nonce). The access point (AP, 4) checks correct delivery (e.g. challenge sufficiently recent, nonce correct and signed by means of the private key stored in the subscriber identity module) and transmits the certificate(s) to a network management device 5 (NMT = network management tool) responsible for part of the network 3 or the entire network 3 in stage 11.

10

In stage 12 the network management device 5 sends the certificate(s) to a certification device 7 (CA = certification authority), which uses an OCSP responder and a list of revoked certificates (certificate revocation list, CRL) to check the validity of the certificate(s) and the correctness of the identity data and in some cases entitlements given and provides information about the status (e.g. valid/invalid, etc.) of the certificate(s) and in some cases the entitlements of the telecommunication subscriber. The certificate confirms the identity data, if the certification device can generate the identity data from the certificate using a method known to it.

15

20

If the public key and the identity/entitlements of the telecommunication subscriber 1, 2 and/or the mobile radio terminal can be obtained from the certificate(s) by the certification device 7 and the status information (certificate not expired, not revoked, entitlements, etc.) can be determined, notification of the status of the certificate is given by the certification device 7 to the network management device 5 in the network 3 (13). The network management device 5 uses the status data and entitlements provided to decide on the scope of the entitlement of the MN 1 to utilize services and resources of the telecommunication network 3 and

25

30

6

informs the access management entity PDP 6 of this in stage 14. Depending on this decision, the PDP 6 then transmits a corresponding policy to the AP4 to release the use of the telecommunication network 3 for the telecommunication subscriber 1 or it remains blocked in the event of a completely negative decision on the part of the NMT 5.

The network management device 5 can notify the network 3 centrally at the request of third parties 9, whether and for which services, etc. a mobile radio terminal (1) is currently deemed to be entitled by the certification device 7. In the case of a positive certificate status (certificate valid, etc.) a secret (e.g. session key) generated by the NMT (5) with an encoding method used in the network 3 is also sent to the access device 4 and decoded there.

15 The same secret is also encoded by the network management device 5 with the public key of the telecommunication identity module 2 (which public key can be obtained by the network management device at the start of the logging in process for the terminal 1 via the access device 4 in stage 10). The NMT 5 can also transmit its own

20 certificate via the AP 4 to the NM 1. The secret is then decoded by the access device 4 with the key known to it (and provided in the telecommunication network) and in stage 16 the secret, which is still encoded with the public key of the telecommunication subscriber identity module 2 is transmitted to the

25 telecommunication subscriber identity module 2. The private key associated with the said public key is also stored in the telecommunication subscriber identity module 2 and this is used to decode the secret. This secret can then be used for example for confidential communication between the terminal 1 and the access

30 device 4.

The access device (4) adds the subscriber to a list of telecommunication

7

subscribers with access to the telecommunication network (3) and/or service (9) and grants access to the telecommunication network and/or service (9) only to subscribers included in the list.

- 5 A telecommunication terminal 1 with the telecommunication subscriber identity module 2 can also utilize further services and resources, order goods, make electronic payments, etc. in respect of a third party (9) for example (depending on what the certificate(s) permit(s)), whereby the third party (9) either
- 10 confirms the degree of entitlement at a device NMT 5 of the telecommunication network 3 or requests this from the CA 7 (see above).

54106-62

8

CLAIMS:

1. A method for checking the entitlement of a subscriber of a telecommunication terminal (1) with a subscriber identity module to utilize a service (9) or use a telecommunication network,

5 characterized in that an access device (4) of a telecommunication network (3) obtains at least one certificate and identity data from the telecommunication terminal (1) (10),

whereupon a network management device (NMT 5) or a certification device (7) carries out a check to establish whether the certificate confirms the
10 identity data and has a positive status,

whereby, if this is the case, a secret (session key 15) is transmitted to the access device (4), said secret encoded with at least a public key of the subscriber identity module also being sent to the telecommunication terminal (1, 2) (15, 16).

15 2. The method according to Claim 1,
characterized in that

after the secret has been sent, the access device (4) adds the subscriber to a list of telecommunication users with access to the telecommunication network (3) or service (9),

20 whereby the access device (4) grants access to the telecommunication network (3) or to the service (9) only to the users included in the list.

3. The method according to Claim 1 or 2,
characterized in that

25 the access device (4) sends the certificate obtained from the telecommunication terminal (1), the identity and replay protection to the network management device (5) of the telecommunication network (3), which has the

54106-62

9

check carried out by the certification device (7) and if the check is positive, sends the secret to the access device (4) and via the access device (4) to the telecommunication terminal (1) (15, 16).

4. The method according to any one of Claims 1 to 3,

5 characterized in that

notification of the result of the check by the certification device (7) is given by the network management device (5) to a service management device (6).

5. The method according to any one of Claims 1 to 4,

characterized in that

10 the certification entity (7) is arranged in a different network from the access device (4).

6. The method according to any one of Claims 1 to 4,

characterized in that

15 the certification device (7) is arranged in the same telecommunication network as the access device (4).

7. The method according to any one of Claims 1 to 6,

characterized in that

the private key of the key pair is only stored in a telecommunication subscriber identity module (2) of the telecommunication terminal (1).

20 8. The method according to any one of Claims 1 to 7,

characterized in that

the telecommunication network is an internet protocol network.

9. The method according to any one of Claims 1 to 8,

54106-62

10

characterized in that

the telecommunication network is a cellular mobile radio network.

10. The method according to any one of Claims 1 to 9,

characterized in that

5 a plurality of certificates, particularly attribute certificates, can be used for a telecommunication subscriber identity module, a positive check of which permits the telecommunication terminal at least one type of transaction or other services or entitlements respectively.

11. The method according to any one of Claims 1 to 10,

10 characterized in that

in the case of a positive check (7) the telecommunication terminal is permitted to use transactions or services provided by third parties (9) via the telecommunication network (3).

12. The method according to any one of Claims 1 to 11,

15 characterized in that

the telecommunication subscriber identity module (2) has stored a private key belonging to the public key, which it uses to decode the secret encoded with the public key.

13. A telecommunication network, particularly for implementing the
20 method according to any one of Claims 1 to 12,

characterized in that it comprises the following:

- an access device (4) for receiving a certificate and identity data sent from telecommunication terminal (1),

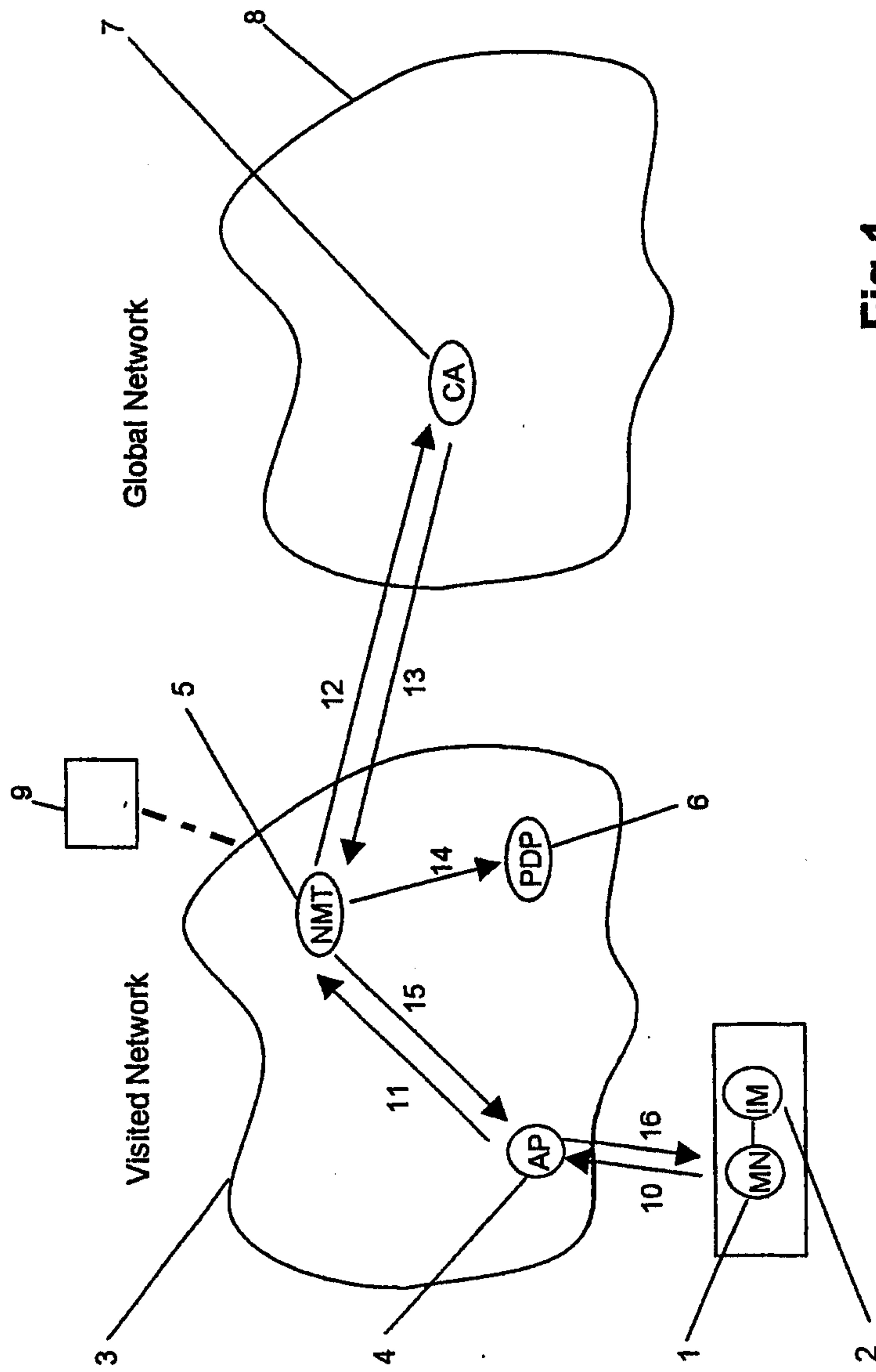
- access to a certification device (7) with a certificate generation
25 method for generating certificates from public keys, which certification device

54106-62

11

gives notification of the validity of a certificate and associated status data on request (13), whereby the access of a telecommunication terminal (1) to a service of a provider (9) permitted for holders (1) of a certificate is only granted by a device (4; 6) of the telecommunication network (3) in so far as the check on a
5 certificate/ the certificates of the telecommunication terminal by the certification device (7) using the public key was successful.

2001E06926DE

**Fig.1**

