

(51) International Patent Classification:  
*H04W 12/08* (2009.01)(21) International Application Number:  
PCT/EP2009/055494(22) International Filing Date:  
6 May 2009 (06.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ZHANG, Yi** [CN/CN]; Nanshan 2#, Chaoyang District, Beijing, 100101 (CN). **KROESELBERG, Dirk** [DE/DE]; Pestalozzistraße 27, 80469 München (DE).(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR, Patent Administration, 80240 Munich (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: ADMISSION CONTROL TO A FEMTO ACCESS POINT

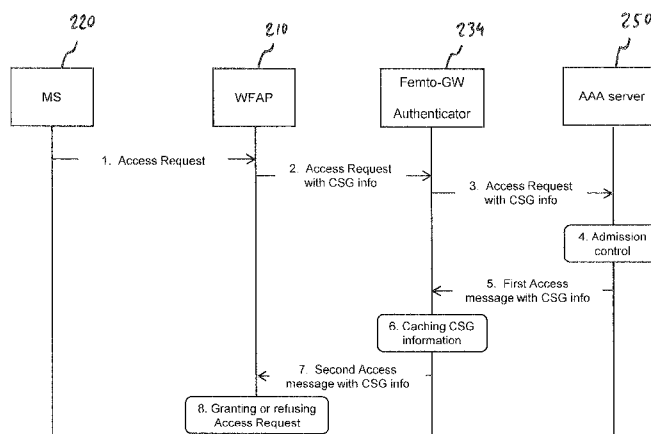


Fig. 2a

(57) **Abstract:** It is described a method for controlling an admission of a mobile station (MS) (220) to a femto access point (FAP) (210). The method comprises (a) receiving an access request message by an AAA server (250), wherein the access request message comprises a closed subscriber group (CSG) information being assigned to the FAP and wherein the access request message is indicative for an access request of the MS to the FAP, which is connected via a femto gateway (234) and/or via a FAP management system (132) to the AAA server, (b) performing an admission control by the AAA server, whereby the CSG information of the access request message is compared with admission control data being stored in the AAA, (c) returning a first access message from the AAA server to the femto gateway and/or to the FAP management system, wherein the first access message is indicative for a match or a missing match between the CSG information and the admission control data, (d) transmitting a second access message from the femto gateway and/or from the FAP management system to the FAP based on first access message, and (e) granting or refusing the access request to the MS by the FAP based on the second access message. It is further described an AAA server and a computer program for executing the described admission control method.

## DESCRIPTION

Admission control to a Femto Access Point

5

Field of invention

The present invention generally relates to the field of tele-  
communication networks. In particular, the present invention  
10 relates to a method for controlling an admission of a mobile  
station to a femto access point of a mobile telecommunication  
network, in particular to a WiMAX femto access point of a Wi-  
MAX telecommunication network. Further, the present invention  
relates to an authentication, authorization and accounting  
15 server and to a computer program for controlling an admission  
of a mobile station to a femto access point in accordance  
with the mentioned admission control method.

20 Art Background

In the past the demand for handling wireless broadband data  
traffic (e.g. multimedia and/or video data traffic) over the  
internet has been increased. Therefore, also home users and  
25 office users have become important target customers for wire-  
less operators and solution providers in order to boost their  
Average Revenue per User (ARPU) or their operating margin.  
This trend seems to be unbowed.

30 Work related to WiMAX (Worldwide Interoperability for Micro-  
wave Access) femto cells and networks and specifically, the  
concept of WiMAX Femto Access Points (WFAP) targets to extend  
the reliable high data rate of a WiMAX access inside a home  
and/or inside an office environment. On the one hand a WFAP  
35 may provide wireless broadband access to all Mobile Stations  
(MSs). In this respect there may be no conceptual difference  
compared to a so called macro Base Station (BS). On the other  
hand the WFAP may only provide service to a limited number of

users. The latter can also mean that the WFAP provides radio access only for a Closed Subscriber Group (CSG) that allows only a small group of explicitly listed subscribers and devices access to the network infrastructure and broadband IP connectivity through the respective WFAP.

Information about a CSG such as for instance its members shall be administered or maintained by each WFAP of a telecommunication network. Thereby, for all allowed users (a) Mobile Station Identifiers (MSIDs), (b) Network Access Identifiers (NAIs) and/or (c) any other identities of devices or subscribers of the respective WiMAX telecommunication system are stored within a memory of the respective WFAP. At the same time, one system requirement for WiMAX Femto Systems is that the MS or the WiMAX subscription shall maintain a list of WFAP identities for the WFAPs where the MS or the WiMAX subscription is a member of the WFAP's CSG. Because a WFAP is not expected to be configured with more than one CSG, a CSG Identifier (ID) can be used to identify the CSG information for a specific WFAP and also to denote this WFAP uniquely. Thereby, the CSG ID may have several forms such as for instance a string or the same form as a BS identifier (BSID). A corresponding list identifying CSGs a MS is assigned to, which list is maintained on the MS, can be called as CSG ID list.

A CSG configuration of a WiMAX femto cell within a WiMAX telecommunication network typically comprises one or more WFAPs, which are connected via one or more Femto Gateways (GW) to an Authentication, Authorization and Accounting (AAA) server. The related CSG ID list being assigned to the subscriber or MS is stored not only in a MS. The CSG ID list is rather also stored in the AAA server that is responsible for the subscription together with the actual subscription information of the WiMAX home operator.

A proper working CSG concept is very important for a WiMAX femto system. Whenever a MS tries to access the WFAP, admis-

sion control should be done. Thereby, admission control means that by means of a policy of the CSG and/or any other femto-related policy it is checked whether or not the MS can access to this WFAP. If a MS wants to access the WFAP, and is not on  
5 the respective CSG ID list of the WFAP, this MS should be rejected by the telecommunication network. In addition, the admission control may include that when a CSG information is modified such as for instance by adding a new subscriber/MS to a specific CSG of a WFAP and extending the subscription or  
10 the MS CSG ID list, the network operator has to authorize this modification prior to implementing the actual modification.

If the CSG information can be synchronized between the WFAP  
15 and the AAA server, the admission control may be done only on WFAP or on the respective Femto-GW the WFAP is connected to. However, if synchronization couldn't be guaranteed to 100%, the admission control cannot be executed by the WFAP or Femto-GW alone.

20 There may be a need for providing an effective and reliable admission control to a Femto Access Point (FAP) of a telecommunication network.

25 Summary of the Invention

This need may be met by the subject matter according to the independent claims. Advantageous embodiments of the present  
30 invention are described by the dependent claims.

According to a first aspect of the invention a method is provided for controlling an admission of a mobile station to a femto access point of a mobile telecommunication network, in  
35 particular to a WiMAX femto access point of a WiMAX telecommunication network. The provided method comprises (a) receiving an access request message by an authentication, authorization and accounting server, wherein the access re-

quest message comprises a closed subscriber group information being assigned to the femto access point and wherein the access request message is indicative for an access request of the mobile station to the femto access point, which is connected via a femto gateway and/or via a femto access point management system to the authentication, authorization and accounting server, (b) performing an admission control by the authentication, authorization and accounting server, whereby the closed subscriber group information of the access request message is compared with admission control data being stored in the authentication, authorization and accounting server, (c) returning a first access message from the authentication, authorization and accounting server to the femto gateway and/or to the femto access point management system, wherein the first access message is indicative for a match or a missing match between the closed subscriber group information and the admission control data, (d) transmitting a second access message from the femto gateway and/or from the femto access point management system to the femto access point based on first access message, and (e) granting or refusing the access request to the mobile station by the femto access point based on the second access message.

The described method is based on the idea that when an subscriber does the initial network entry with a specific MS via a Femto Access Point (FAP), the Authentication, Authorization and Accounting (AAA) server, which is responsible for the subscription, shall do the admission control in order to determine whether this MS is eligible to access the telecommunication network through this FAP, or not.

If the FAP is a WiMAX femto access point (WFAP) and the telecommunication network is a WiMAX telecommunication network, the access request message may be an extension of a standardized RADIUS Access-Request message or Diameter Extensible Authentication Protocol (EAP) Request message, which is transmitted from the Femto gateway (GW) and/or from the FAP management system to the AAA server. In this message, which may

be abbreviated "DER" message, besides the EAP data, also the identification (ID) of the Closed Subscriber Group (CSG) may be attached for instance as a new RADIUS attribute or a Diameter attributed value pair (AVP). In this respect the abbreviation RADIUS is used Remote Authentication Dial In User Service.

After receiving the Access Request or the DER message including CSG ID, the AAA server shall do admission control for the MS by matching the "CSG\_ID" or the CSG information against admission control data stored as part of the subscription data in the AAA server and/or in any data base being connected to the AAA server. Thereby, the admission control data may comprise for this particular subscription or MS a list of WFAP identities, which may serve as an access point for this MS. The AAA server can perform the comparison respectively the matching either based on the subscription ID (permanent ID or Network Access Identifier (NAI)) and/or based on the ID of the MS (MS\_ID) used by the subscriber.

If Admission Control has succeeded in the AAA server, the first access message is an Access Accept message, which may contain also the CSG ID list or CSG information of the subscription or of this specific MS. Further, other femto-related policy may be included in this Access Accept message. The first access message respectively the Access Accept message may be of the type of a Diameter EAP message.

Transferring the CSG ID list or the CSG information to the Femto-GW and/or to the FAP management system may provide the advantage that an Access Service Network (ASN), after receiving such information from the Femto GW, can execute handover (HO) decisions based on femto cell specific policy of the subscription or MS locally without being forced to contact the AAA server for every handover decision.

Granting or refusing the access request of the mobile station can be carried out by the Femto-GW and/or by the FAP manage-

ment system by returning the admission control result including the received data to the WFAP in a message being based on an AuthRelay\_EAP Transfer message or on a Key\_Change\_Directive message. Alternatively, the access request can be granted or refused directly by the WFAP.

It is mentioned that the second access message is also indicative for a match or a missing match between the closed subscriber group information and the admission control data. The first access message and the second access message may be the same, i.e. the femto gateway and/or to the FAP management system may simply forward the first message to the FAP.

The described method may allow to synchronize CSG-related information for admission control and Femto policy control between the WFAP, the Femto-GW and/or to the FAP management system respectively the Access Service Network (ASN) GW and the AAA server, wherein the last one is responsible for authenticating and authorizing network entry for a subscriber or MS entering the network with femto support for instance using a WFAP for network access or handing over to a WFAP after initial an entry of the network.

According to an embodiment of the invention the method further comprises performing an authentication procedure with respect to the mobile station.

The authentication procedure may be carried out for instance in the femto GW and/or in the FAP management system. In this case (a) the femto GW and/or the FAP management system represents an authenticator and (b) the access request message transmitted from the femto GW and/or from the FAP management system and received by the AAA server comprises an information element being indicative for an authentication of the mobile station.

It is pointed out that of course the described method may be stopped or terminated in case the authentication of the MS is

not successful. In this case the access request of the MS will not be successful, i.e. the FAP provides no access to the respective MS.

5 The authenticator respectively the femto GW and/or the FAP management system may cache the CSG information, a CSG ID list and/or other femto-related policy locally as part of the MS context for the specific session of the MS. This may provide the advantage that this information is present at the  
10 femto GW and/or in the FAP management system when it will be needed.

According to a further embodiment of the invention the method further comprises transferring the closed subscriber group  
15 information from the femto gateway and/or from the femto access point management system to the authentication, authorization and accounting server. This means that the femto GW and/or the FAP management system contributes at least partially to the authentication of the MS. Thereby, the CSG in-  
20 formation may be included in the above described access request message, which is received by the authentication, authorization and accounting server.

According to a further embodiment of the invention the method  
25 further comprises transferring the closed subscriber group information from the femto access point to the femto gateway and/or to the FAP management system. This may provide the advantage that it is not necessary that the femto GW and/or the FAP management system has to be preconfigured with the CSG-ID  
30 information of all the WFAPs being assigned to the Femto-GW.

The described transfer of the closed subscriber group information may be done already during an initial network entry of the mobile station.

35

The CSG information being assigned to and transferred by the FAP may be for instance the corresponding CSG ID. Upon receiving the CSG information respectively the CSG ID the femto

gateway and/or the FAP management system may act as the authenticator in charge for handling the MS's network entry over the standardized R6 reference point respectively an appropriate R6 interface between the FAP and the femto GW  
5 and/or the FAP management system. In case of a WiMAX system this can be realized for example by extending the known MS\_PreAttachment\_Req message or the known AuthRelay\_EAP Transfer message from the WFAP to the femto GW/FAP management system respectively the Authenticator. Thereby, the respective  
10 information is transferred in addition to the EAP data which have been obtained from the MS, which requests the network entry.

Further, the femto GW/FAP management system respectively the  
15 authenticator can be statically configured with the CSG ID or CSG information for each WFAP and can derive the correct CSG information based on the source identity of the entity (WFAP) that sent the R6 respective message.

20 According to a further embodiment of the invention the method further comprises using the closed subscriber group information by an Access Service Network for carrying out a handover decision for the mobile station between a source access point and a target access point.

25 The source access point and/or the target access point may be any point of attachment such as for instance the FAP, another FAP, a relay node or a base station.

30 Generally speaking, when a HO action or preparation takes place in the ASN or between different ASNs, the ASN (i.e. an ASN-GW, a femto GW, a relay node, a BS or a FAP respectively a WFAP) may use the CSG information such as the CSG\_ID and possibly also additional femto-specific policy received by  
35 the above described admission control method to assist any HO decision. The femto GW/FAP management system respectively the authenticator for the subscription/MS may assist the admis-

sion control through an Authentication Key (AK) context retrieve procedure.

Specifically, the CSG information or the CSG ID of the target point of attachment may be included in an extended Context Transfer (e.g. Context\_Request) message as a new Type Length Value (TLV) information element.

Further, an anchor authenticator, i.e. the authenticator being assigned to the first point of attachment (e.g. the FAP) may carry out the HO admission control for the MS based on the cached CSG info and/or another femto-related policy.

If admission control succeeds, an AK context is sent. By contrast, if the admission does not succeed, the authenticator rejects to feedback an AK context and the reject reason is given in a result code of the context response message.

Further, if the AK context retrieve procedure happens during a HO preparation phase and is triggered by the target point of attachment, the reject reason for admission control may be added into an HO response message (HO\_Rsp) from the target point of attachment to the source point of attachment.

The described usage of the closed subscriber group information by an Access Service Network for carrying out a handover decision may provide the advantage that the ASN can carry out local handover decisions based on a femto specific policy like a CSG information or FAP IDs, without the requirement to contact the AAA server responsible for the actual subscription or the MS which is requesting a HO. This is considered as a major performance optimization that significantly reduces signalling load between WiMAX ASN and Connectivity Serving Network (CSN) or between a Network Access Provider (NAP) and a Network Service Provider (NSP) (if NAP and NSP are different business entities).

According to a further embodiment of the invention the method further comprises sending a message from the authentication, authorization and accounting server to an access serving network being associated with the femto gateway, wherein the message comprises the closed subscriber group information and/or policy information for admission control of the femto access point. This may mean that the CSG information and/or other femto-related policy for admission control is provided or updated from the AAA server to the ASN. In addition, dynamic updates of femto-related information can be realized by the AAA server.

The femto-related information may be distributed for instance by means of an extended RADIUS COA (Change-of-Authorization) message including the updated femto-related information. Alternatively, the femto-related information may be distributed by sending a Diameter WiMAX Change-of-Authorization-Request (WCAR) message with the same information.

The distribution of femto-related information may provide the advantage to enable dynamic changes of the femto-related policy information for a subscription or MS, e.g. mid-session updates of the CSG information. Further, this enables users for instance to update the list of allowed WFAPs for a MS in a mid-session respectively during an open session. It may not be necessary to power cycle the respective network device.

It is mentioned that the described message from the AAA server to the ASN may also be used for other parameters for updating procedures from the AAA server to the femto GW or to an ASN GW.

According to a further embodiment of the invention the method further comprises (a) receiving a user identification of the subscriber of the mobile station, which is requesting access to the femto access point, by the authentication, authorization and accounting server from the femto access point and/or from the femto access point management system, (b) looking up

for subscription information of the mobile station based on the user identification, wherein subscription data stored in the authentication, authorization and accounting server are taken into account, (c) transferring the subscription information from the authentication, authorization and accounting server to the femto access point.

The user identification may be transferred directly or indirectly from the femto access point to the AAA server. In the latter case the FAP may contact the AAA server through a local network entity like the femto GW and/or the FAP management system, which is controlling the FAP and send the user identification of the subscription respectively the MS, which wants to enter the mobile telecommunication network, to the AAA server. The correct AAA server (in case it is not the same as the AAA server owning the subscription for the FAP) can be found based on the operator realm that is part of the user identification information.

In case the AAA server comprises a first server component being used for authentication, authorization and accounting of FAPs and a second server component being used for authentication, authorization and accounting of MSs the user identification can be sent first to the first AAA server component (AAA (FAP)), which can then contact the second AAA server component (AAA (MS)) for resolution of the subscription information of the MS. Alternatively the AAA (MS) can be directly contacted by the femto GW and the subscription information of the MS can be obtained directly.

After receiving the subscription information from the authentication, authorization and accounting server the FAP may at least temporarily store the subscription information in a CSG being assigned to the FAP.

Generally speaking, the described method allows the owner of the FAP to configure the respective CSG information and add new users or new MSs to the respective CSG. This can be done

by entering a human-readable information instead of the MSID respectively the Media Access Control (MAC) address of the MS. The entering of the human-readable information can be done with the help of an appropriate network backend infrastructure such as for instance an I/O device or an appropriate administration interface.

It is mentioned that it is not necessary to transmit the whole subscription information of the mobile station from the authentication, authorization and accounting server to the femto access point. This might be in conflict with privacy concerns because the WFAP may not be allowed to have a full knowledge of the MS subscription information. Preferably, the subscription information comprises and/or may be limited to the MS-ID respectively the MS MAC address.

According to a further embodiment of the invention the user identification is the username of the subscriber of the mobile station. This may provide the information that the user identification can be easily handled, recognized and remembered by human being.

By contrast to the procedure of entering the MSID manually by the FAP owner, which is a considerably inconvenient and faulty process (the MSID is typically a 48-bit MAC address that needs to be typed into the administration interface by the user as hexadecimal encoding), the described usage of the human readable username is much simpler. Therefore, the chance of a human error with respect to the user identification can be reduced.

The username may be a human-readable name in Network Access Identifier (NAI) format that is similar to an e-mail address, like for instance first.lastname@wimaxoperator.com. This holds in particular for a WiMAX femto system, wherein the FAP is a WFAP and, if applicable, the FAP management system is a WFAP management system.

According to a further embodiment of the invention (a) the user identification is received by the authentication, authorization and accounting server from the femto access point via the femto gateway and/or via a femto access point management system and/or (b) the subscription information is transferred from the authentication, authorization and accounting server to the femto access point via the femto gateway and/or via the femto access point management system.

10 In this respect it is mentioned that the FAP Management System may also be integrated into the femto GW.

According to a further embodiment of the invention the method further comprises updating the closed subscriber group information being assigned to the femto access point by the authentication, authorization and accounting server.

Generally speaking, the AAA server, when receiving the request from the FAP and/or from the femto GW or the FAP management system with the user identification information, can update the CSG information of the FAP. It is mentioned that this only works in case the above described first AAA server component being used for authentication, authorization and accounting of FAPs and a the above second AAA server component being used for authentication, authorization and accounting of MSs is the same network entity, which can return the updated CSG information to the Femto-GW and/or to the FAP.

30 According to a further embodiment of the invention the subscription information is an identification of the mobile station. The identification of the MS may be the well known MSID of the MS used by the user. As has already been mentioned above the MSID may be read from the subscription data stored in the AAA server and is returned to the femto GW, the FAP management system or to the FAP.

In this respect it is mentioned that the AAA server is typically the only network entity in a WiMAX telecommunication network that is able to resolve a MSID to a username for a specific subscription.

5

According to a further embodiment of the invention the subscription information comprises a list of mobile station identifications that are valid for a specific user owning the subscription. This may mean that the AAA server can return to  
10 the FAP, to the femto GW and/or to the above described FAP management system a whole list of MSIDs. In this case, the CSG of the FAP can be updated with all possible mobile devices for this user in a single step.

15 According to a further embodiment of the invention the method further comprises entering the user identification in an administration interface of the femto access point. This may provide the advantage that the user identification can be easily entered.

20

It is mentioned that at time of entering by the MS the FAP is typically not yet aware of the subscription information respectively of the MSID that is required for updating the CSG being assigned to the FAP.

25

According to a further aspect of the invention an authentication, authorization and accounting server is provided for controlling an admission of a mobile station to a femto access point of a mobile telecommunication network, in particular to a WiMAX femto access point of a WiMAX telecommunication network. The provided authentication, authorization and accounting server comprises (a) a receiving unit for receiving an access request message, wherein the access request message comprises a closed subscriber group information being  
30 assigned to the femto access point and wherein the access request message is indicative for an access request of the mobile station to the femto access point, which is connected via a femto gateway and/or via a femto access point manage-

35

ment system to the authentication, authorization and accounting server, (b) a storage unit for storing admission control data, (c) a processor unit for performing an admission control, whereby the closed subscriber group information of the  
5 access request message is compared with the admission control data, and (d) a transmitting unit for returning a first access message to the femto gateway and/or to the femto access point management system, wherein the first access message is indicative for a match or a missing match between the closed  
10 subscriber group information and the admission control data.

Also this further aspect of the invention is based on the idea that when an subscriber does the initial network entry with a specific MS via a FAP, the described AAA server, which  
15 is responsible for the subscription, shall do the admission control in order to determine whether this MS is eligible to access the telecommunication network or not.

The admission control information may be transferred from the femto gateway and/or from the FAP management system to the  
20 femto access point by means of a second access message, which is based on the first access message. Thereby, the first access message and the second access message may be the same, i.e. the femto gateway may simply forward the first message  
25 to the FAP.

Further, based on the second access message the FAP may grant or refuse the access request to the mobile station

30 According to a further aspect of the invention there is provided a computer program for controlling an admission of a mobile station to a femto access point of a mobile telecommunication network, in particular to a WiMAX femto access point of a WiMAX telecommunication network. The computer program,  
35 when being executed by a data processor, is adapted for controlling the above described admission control method.

As used herein, reference to a computer program is intended to be equivalent to a reference to a program element and/or to a computer readable medium containing instructions for controlling a computer system to coordinate the performance  
5 of the above described method.

The computer program may be implemented as computer readable instruction code in any suitable programming language, such as, for example, JAVA, C++, and may be stored on a computer-  
10 readable medium (removable disk, volatile or non-volatile memory, embedded memory/processor, etc.). The instruction code is operable to program a computer or any other program-  
mable device to carry out the intended functions. The computer program may be available from a network, such as the  
15 World Wide Web, from which it may be downloaded.

The invention may be realized by means of a computer program respectively software. However, the invention may also be realized by means of one or more specific electronic circuits  
20 respectively hardware. Furthermore, the invention may also be realized in a hybrid form, i.e. in a combination of software modules and hardware modules.

It has to be noted that embodiments of the invention have  
25 been described with reference to different subject matters. In particular, some embodiments have been described with reference to method type claims whereas other embodiments have been described with reference to apparatus type claims. However, a person skilled in the art will gather from the above  
30 and the following description that, unless other notified, in addition to any combination of features belonging to one type of subject matter also any combination between features relating to different subject matters, in particular between features of the method type claims and features of the apparatus type claims is considered as to be disclosed with this  
35 application.

The aspects defined above and further aspects of the present invention are apparent from the examples of embodiment to be described hereinafter and are explained with reference to the examples of embodiment. The invention will be described in  
5 more detail hereinafter with reference to examples of embodiment but to which the invention is not limited.

#### Brief Description of the Drawings

10

Figure 1a shows a femto system network architecture for a Closed Subscriber Group configuration within a Mobile Station, a WiMAX Femto Access Point, a Femto Gateway and a WiMAX Femto Access Point management system and two AAA servers.

15

Figure 1b shows a simplified femto system network architecture for a Closed Subscriber Group configuration within a Mobile Station, a WiMAX Femto Access Point, a combined device including the functionality of a Femto Gateway and a WiMAX  
20 Femto Access Point management system and two AAA servers.

Figure 2a shows a transactional flow diagram for performing an admission control for a Mobile Station to a femto system.

25

Figure 2b shows a transactional flow diagram for updating a Closed Subscriber Group information with a resolution from a Network Access Identifier to a Mobile Station Identifier.

30

Figure 2c shows a transactional flow diagram for updating a Closed Subscriber Group information with a resolution from a Network Access Identifier to a Mobile Station Identifier via an administration portal.

35

#### Detailed Description

The illustration in the drawing is schematically. It is noted that in different figures, similar or identical elements are

provided with the same reference signs or with reference signs, which are different from the corresponding reference signs only within the first digit.

5

Figure 1a shows a network architecture of a femto system 100. The femto system 100 comprises a WiMAX Femto Access Point (WFAP) 110, which currently serves a Mobile Station (MS) 120. The WFAP 110 is connected to a WFAP Management System 132 and  
10 to a Femto Gateway (GW) 134 by respectively an extended R6 interface. The Femto-GW 134 and the WFAP Management System 132 are connected to each other via an extended R3 interface. The Femto-GW 134 is adapted for connecting the WFAP 110 to a Connective Service Network (CSN) 140.

15

As can be seen from Figure 1a, the MS 120 has an identification MSID equal to "1". Further, a list comprising different CSG ID's is stored in the MS 120. According to the embodiment described here the MS 120 is assigned at least to a first CSG  
20 having a CSG ID "x" and to a second CSG having a CSG ID "z".

As can be further seen from Figure 1a, the WFAP 110 serves the above mentioned CSG being identified with the CSG ID "x". Further, the WFAP 110 has stored ID's about different MS  
25 which are assigned to the CSG "x". According to the embodiment described here at least the MS 120 having the MSID "1" and a further not depicted MS having the MSID "2" are members of the CSG "x".

30 The CSN 140 comprises (a) a first AAA server 152 being used for authentication, authorization and accounting (AAA) of WFAPs and (b) a second AAA server 154 being used for AAA of MSs. According to the embodiment described here the first AAA server 152, which is abbreviated with "AAA (WFAP)", is as-  
35 signed to a first operator such as for instance a first Network Service Provider (NSP) and the second AAA server 154, which is abbreviated with "AAA (MS)", is assigned to a second operator such as for instance a second NSP. The AAA (WFAP)

server 152 stores all CSG profiles of the WFAP 110. The AAA (MS) server 154 stores all CSG identification profiles the MS 120 is assigned to. Further, also CSG identification profiles of other MSs, which are not depicted in Figure 1a, may be stored in the AAA (MS) server 154. Generally speaking, the AAA (WFAP) server 152 manages WFAP related CSG information, e.g. CSG ID and CSG, etc. The AAA (MS) server 154 manages the MS related CSG information such as CSG ID list, MSID, etc. More general, the AAA (WFAP) may be a data base.

The two AAA servers 152 and 154 are respectively connected the WFAP management system 132 and to the Femto-GW 134 via an extension of the standardized R3 interface.

It has to be mentioned that the two AAA servers 152 and 154 could also be realized by one single AAA server.

Preferred procedures for updating a Closed Subscriber Group information with a resolution from a Network Access Identifier to a Mobile Station Identifier will be described beneath in detail with reference to Figures 2b and 2c.

Figure 1b shows a simplified femto system network architecture 100 for a configuration of a Closed Subscriber Group within a MS 120, a WFAP 110 and two AAA servers 152 and 154. As can be easily seen from the Figures 1b and 1c, the network architecture 100 shown in Figure 1c differs from the network architecture 100 shown in Figure 1a by the merge of the WFAP Management System 132 and the Femto-GW 134 (see Figure 1a) into a single network element 130. Further, the WFAP 110 and the network element 130 are connected with each other via an extended R6 interface. Furthermore, extended R3 interfaces are used both for the connection of the network element 130 with the AAA (MS) server 154 and the connection of the network element 130 with the AAA (WFAP) server 152. Apart from these differences the femto system network architecture 100b

is at least substantially the same as the femto system network architecture 100a.

- 5 Figure 2a shows a transactional flow diagram for performing an admission control for a Mobile Station 220 to a femto system as shown in Figure 1a.

10 When the subscriber does the initial network entry with a specific MS 120 via a WFAP 210, an AAA server 250 being responsible for the subscription will take care of the admission control to determine whether this MS 120 is eligible to access or not.

15 Step 1: As can be seen from Figure 2a, during an initial Network entry in a first step, the MS 220, which wants to get an access to the WFAP 210, sends an Access Request message to the WFAP 210.

20 Step 2: In a second step, still during the initial Network entry of the MS 120, the WFAP transfers the Access Request message together with the CSG ID or CSG information of the WFAP 210 to a Femto-GW 234. According to the embodiment described here the Femto-GW 234 acts as an Authenticator in  
25 charge for handling the network entry of the MS 220 over an R6 reference point (see Figure 1a). This can for example happen by extending the MS\_PreAttachment\_Req or AuthRelay\_EAP Transfer message from the WFAP 210 to the Authenticator 234. Also, the Authenticator 234 can be statically configured with  
30 the CSG ID or CSG information for each WFAP and can derive the correct CSG information based on the source identity of the WFAP entity which has sent respective message over the R6 interface.

35 Step 3: In a third step, the Access Request message is sent from the Femto-GW 234 to an AAA server 250. The corresponding message is for instance a Diameter DER message. Thereby, besides the EAP payload, the CSG ID is also attached, for in-

stance as a new RADIUS attribute or a Diameter attributed value pair (AVP).

Step 4: After receiving the Access Request message including  
5 CSG ID, in a fourth step the AAA server executes an admission control procedure for the MS 220. Thereby, the CSG\_ID or CSG information is matched against admission control data (allowed WFAP identities for this subscription or MS 220), which are stored as a part of the subscription data in the AAA  
10 server 250. Thereby, the AAA server 250 can perform this matching either based on the subscription ID (permanent ID or NAI) and/or based on the MS\_ID of the MS 220 used by the subscriber.

15 Step 5: If both Authentication and Admission Control succeed, in a fifth step the AAA server 250 returns a first Access message to the Femto-GW 234. This first message includes a CSG ID list or a CSG information of the subscription or this specific MS 220. Further, the first Access message may also  
20 include other femto-related policy information. This may allow an Access Service Network (ASN) being connected to the Femto-GW 234, after receiving such information to do handover (HO) decisions locally based on Femto specific policy of the subscription or MS 220. Such local HO decisions would not re-  
25 quire to contact the AAA server 250 for every handover decision.

Step 6: In a sixth step the Femto-GW 234 respectively the authenticator 234 caches the CSG ID list, the CSG information  
30 and/or other femto-related policy locally as part of the MS context for the specific session.

Step 7: In a seventh step the authenticator 234 returns the admission control result including the received data to the  
35 WFAP 210 in an AuthRelay\_EAP Transfer message or in a Key\_Change\_Directive message.

When a HO action or preparation takes place in the ASN or between different ASNs, the ASN (ASN-GW, Femto-GW, a Base Station or a WFAP) uses the CSG\_ID or CSG information and additional Femto-specific policy received by the above described  
5 method to assist any HO decision. The authenticator for the subscription respectively for the MS may assist the admission control through an Authentication Key (AK) context retrieve procedure. This might be realized by the following steps (a), (b), (c) and (d).

10

Step (a): The CSG ID or CSG information of a target point of attachment is included in the Context Request message as a sub RADIUS Type Length Value (TLV)

15 Step (b): an anchor authenticator, i.e. the authenticator being assigned to the first point of attachment (e.g. Femto GW) may carry out the HO admission control for the MS based on the cached CSG info and/or another femto-related policy.

20 Step (c): If admission control succeeds, an AK context is sent. By contrast, if the admission does not succeed, the authenticator rejects to feedback an AK context and the reject reason is given in a result code of the context response message.

25

Step (d): If the AK context retrieve procedure happens during a HO preparation phase and is triggered by the target point of attachment, the reject reason for admission control may be added into an HO response message (HO\_Rsp) from the target  
30 point of attachment to the source point of attachment.

Figure 2b shows a transactional flow diagram for updating a Closed Subscriber Group information with a resolution from a  
35 Network Access Identifier to a Mobile Station Identifier.

Step 1: In a first step the user will retrieve the information about the real username for the WiMAX subscription from

the friend or owner of the new MS to be added to the WFAP CSG. The WFAP owner enters the username or NAI for whom the MSID has to be added to the CSG information of the WFAP.

- 5 Step 2: In a subsequent second step the WFAP 210 triggers the NAI-to-MSID resolution by sending a message to the Femto-GW 234. Preferably, this is a new WiMAX R6 message, carrying at least the WFAP ID, CSG ID, and the username/NAI information to be resolved.

10

It is mentioned that if the WFAP 234 triggers this through a WFAP Management system instead of the Femto-GW, the procedure will be basically the same. However, in this case the corresponding message is preferably based on the TR-69 protocol  
15 for WFAP management.

- Step 3: In a subsequent third step the Femto-GW 234 will trigger a request to the AAA server 252 of the WFAP 210. This is preferably a RADIUS or Diameter request message that is a  
20 new message. Alternatively, the corresponding message may be based on an already existing exchange extended by one or more new RADIUS attributes, or Diameter AVPs. It will carry at least the WFAP ID, CSG ID, and the username/NAI information to be resolved.

25

- Step 4: In a subsequent optional fourth step in case the AAA server 252 for the WFAP 210 is not the same as the AAA server 254 for the MS, the AAA (WFAP) server 252 will send a request message to the AAA (MS) server 254. This request message will  
30 carry at least the WFAP ID, CSG ID, and the username/NAI information to be resolved.

- It is mentioned that if the AAA server 252 for the WFAP 210 is not the same as the AAA server 254 for the MS, in the  
35 above described third step the Femto-GW 234 can alternatively send the message directly to the AAA server 254 of the MS. The AAA server 254 for the MS can be discovered based on the realm information in the username respectively in the NAI.

Preferably also this message is based on the RADIUS or Diameter protocol.

Step 5: In a subsequent fifth step, which is associated with  
5 the optional request message of the fourth step, the AAA (MS) server 254 will respond to the request received in the fourth step with a response containing the MSID. It will resolve the received NAI or username information to the appropriate MSID using the subscription information stored in the AAA server  
10 (or backend) database.

It is mentioned that if there are several MSIDs configured for the subscription identified by the username or NAI, the AAA server 254 can return the whole list of MSIDs. It can  
15 also return only this MSID that has an active session.

Step 6: In a subsequent sixth step the AAA (WFAP) server 252 will respond to the request received in step 3, with a response containing the MSID. It will resolve the received NAI  
20 or username information to the appropriate MSID using the subscription information stored in the AAA server (or backend) database.

It is mentioned that if step 4 and step 5 are not performed  
25 and the functionality of the AAA (WFAP) server 252 and of the AAA (MS) server 254 are the same, the combined AAA server will also update the CSG information of the WFAP 210 with the new MSID(s).

30 It is further mentioned that if there are several MSIDs configured for the subscription identified by the username or NAI, the AAA server can return the whole list of MSIDs. However, the AAA server can also return only this MSID that has an active session.

35 The response message of step 6 may be a RADIUS or Diameter response message that is a new message. Alternatively, this message may be based on an already existing exchange message

extended by one or more new RADIUS attributes or Diameter AVPs.

Step 7: In a subsequent seventh step the Femto-GW will respond to the message received from the WFAP in step 2, by sending the requested MSID information. Preferably, this is a new WiMAX R6 message, carrying at least the WFAP ID, CSG ID, MSID and the username/NAI information.

It is mentioned that if the WFAP 210 has triggered this in above described step 2 through the WFAP Management system instead of the Femto-GW, the procedure will be the same. However, in this case the message may be preferably based on the TR-69 protocol for the WFAP management.

Step 8: In a subsequent eighth step the WFAP 210 updates its CSG information with the received MSID.

It is further mentioned that alternatively (but with the same message flow) the WFAP 210 can request an update of the CSG instead of just requesting resolution to a MSID. In this case the AAA server will receive a CSG update request from the WFAP with the NAI, will update the CSG (if allowed by operator policy) and will return the updated CSG information instead or in addition to the MSID.

As an alternative to the above described implementation, the WFAP owner can enter the username (see step 1 of Figure 2b) by using a self-administration portal 260 of the WFAP operator instead of entering the information directly in the WFAP 210. However, the basic concept is the same as in the message flow shown in Figure 2b (resolve NAI to MSID(s) via AAA server).

Figure 2c shows the related steps and message flows, which are considered to be self-explanatory and for the sake of conciseness will not be described in detail here.

It is noted that message 5 of Figure 2c can be realized for example with a RADIUS CoA (change-of-authorization) message that is carrying the CSG information, WFAP ID etc. Correspondingly, in this case message 9 would be a CoA\_Ack message.

It should be noted that the term "comprising" does not exclude other elements or steps and "a" or "an" does not exclude a plurality. Also elements described in association with different embodiments may be combined. It should also be noted that reference signs in the claims should not be construed as limiting the scope of the claims.

15

List of reference signs:

|    |     |                                                       |
|----|-----|-------------------------------------------------------|
|    | 100 | telecommunication network / femto system architecture |
| 5  | 110 | WiMAX Femto Access Point                              |
|    | 120 | Mobile Station                                        |
|    | 130 | network element implementing                          |
|    |     | (a) WiMAX Femto Access Point Management System and    |
|    |     | (b) Femto Gateway                                     |
| 10 | 132 | WiMAX Femto Access Point Management System            |
|    | 134 | Femto Gateway                                         |
|    | 140 | Connective Service Network                            |
|    | 150 | AAA server                                            |
|    | 152 | AAA (WFAP) server                                     |
| 15 | 154 | AAA (MS) server                                       |
|    | 210 | WiMAX Femto Access Point                              |
|    | 220 | Mobile Station                                        |
|    | 234 | Femto Gateway / Authenticator / WiMAX Femto Access    |
| 20 |     | Point Management System                               |
|    | 250 | AAA server                                            |
|    | 252 | AAA (WFAP) server                                     |
|    | 254 | AAA (MS) server                                       |
|    | 260 | Administration Portal                                 |
| 25 |     |                                                       |

CLAIMS:

1. A method for controlling an admission of a mobile station (120, 220) to a femto access point (110, 210) of a mobile telecommunication network (100), in particular to a WiMAX femto access point (110, 210) of a WiMAX telecommunication network (100), the method comprising
- receiving an access request message by an authentication, authorization and accounting server (150, 250),  
10     - wherein the access request message comprises a closed subscriber group information being assigned to the femto access point (110, 210) and  
      - wherein the access request message is indicative for an access request of the mobile station (120, 220) to the fem-  
15     to access point (110, 210), which is connected via a femto gateway (134, 234) and/or via a femto access point management system (132) to the authentication, authorization and accounting server (150, 250),
  - performing an admission control by the authentication, authorization and accounting server (150, 250), whereby the  
20     closed subscriber group information of the access request message is compared with admission control data being stored in the authentication, authorization and accounting server (150, 250),
  - 25     • returning a first access message from the authentication, authorization and accounting server (150, 250) to the femto gateway (134, 234) and/or to the femto access point management system (132), wherein the first access message is in-  
      dicative for a match or a missing match between the closed  
30     subscriber group information and the admission control data,  
      • transmitting a second access message from the femto gateway (134, 234) and/or from the femto access point management system (132) to the femto access point (110, 210) based on  
35     first access message, and  
      • granting or refusing the access request to the mobile station (120, 220) by the femto access point (110, 210) based on the second access message.

2. The method as set forth in the previous claim, further comprising

- performing an authentication procedure with respect to the  
5 mobile station (120, 220).

3. The method as set forth in any one of the previous claims, further comprising

- transferring the closed subscriber group information from  
10 the femto gateway (134, 234) and/or from the femto access point management system (132) to the authentication, authorization and accounting server (150, 250).

4. The method as set forth in the previous claim, further  
15 comprising

- transferring the closed subscriber group information from the femto access point (110, 210) to the femto gateway (134, 234) and/or to the femto access point management system (132).

20 5. The method as set forth in any one of the previous claims, further comprising

- using the closed subscriber group information by an Access Service Network for carrying out a handover decision for  
25 the mobile station (120, 220) between a source access point and a target access point.

6. The method as set forth in any one of the previous claims, further comprising

- sending a message from the authentication, authorization and accounting server (150, 250) to an access serving network being associated with the femto gateway (134, 234), wherein  
30 the message comprises the closed subscriber group information and/or policy information for admission control of the  
35 femto access point (110, 210).

7. The method as set forth in any one of the previous claims, further comprising

- receiving a user identification of the subscriber of the mobile station (120), which is requesting access to the femto access point (110, 210), by the authentication, authorization and accounting server (152, 154, 252, 254) from the femto access point (110, 210) and/or from the femto access point management system (132),
- looking up for subscription information of the mobile station (120) based on the user identification, wherein subscription data stored in the authentication, authorization and accounting server (152, 154, 252, 254) are taken into account,
- transferring the subscription information from the authentication, authorization and accounting server (152, 154, 252, 254) to the femto access point (110, 210).

8. The method as set forth in the previous claim, wherein the user identification is the username of the subscriber of the mobile station (120).

9. The method as set forth in any one of the previous claims 7 to 8, wherein

- the user identification is received by the authentication, authorization and accounting server (152, 154, 252, 254) from the femto access point (110, 210) via the femto gateway (134, 234) and/or via a femto access point management system (132) and/or
- the subscription information is transferred from the authentication, authorization and accounting server (152, 154, 252, 254) to the femto access point (110, 210) via the femto gateway (134, 234) and/or via the femto access point management system (132).

10. The method as set forth in any one of the previous claims 7 to 9, further comprising

- updating the closed subscriber group information being assigned to the femto access point (110, 210) by the authentication, authorization and accounting server (152, 252).

5 11. The method as set forth in any one of the previous claims 7 to 10, wherein the subscription information is an identification of the mobile station (120).

10 12. The method as set forth in any one of the previous claims 7 to 11, wherein the subscription information comprises a list of mobile station identifications that are valid for a specific user owning the subscription.

15 13. The method as set forth in any one of the previous claims 7 to 12, further comprising entering the user identification in an administration interface (260) of the femto access point (210).

20 14. An authentication, authorization and accounting server for controlling an admission of a mobile station (120, 220) to a femto access point (110, 210) of a mobile telecommunication network (100), in particular to a WiMAX femto access point (110, 210) of a WiMAX telecommunication network (100), the authentication, authorization and accounting server (150, 250) comprising

- a receiving unit for receiving an access request message,
    - wherein the access request message comprises a closed subscriber group information being assigned to the femto access point (110, 210) and
    - wherein the access request message is indicative for an access request of the mobile station (120, 220) to the femto access point (110, 210), which is connected via a femto gateway (134, 234) and/or via a femto access point management system (132) to the authentication, authorization and accounting server (150, 250),
  - a storage unit for storing admission control data,
- 30  
35

- a processor unit for performing an admission control, whereby the closed subscriber group information of the access request message is compared with the admission control data, and
- 5 • a transmitting unit for returning a first access message to the femto gateway (134, 234) and/or to the femto access point management system (132), wherein the first access message is indicative for a match or a missing match between the closed subscriber group information and the ad-  
mission control data.

15 15. A computer program for controlling an admission of a mobile station (120, 220) to a femto access point (110, 210) of a mobile telecommunication network (100), in particular to a WiMAX femto access point (110, 210) of a WiMAX telecommunication network (100), the computer program, when being executed by a data processor, is adapted for controlling the method as set forth in any one of the claims 1 to 13.

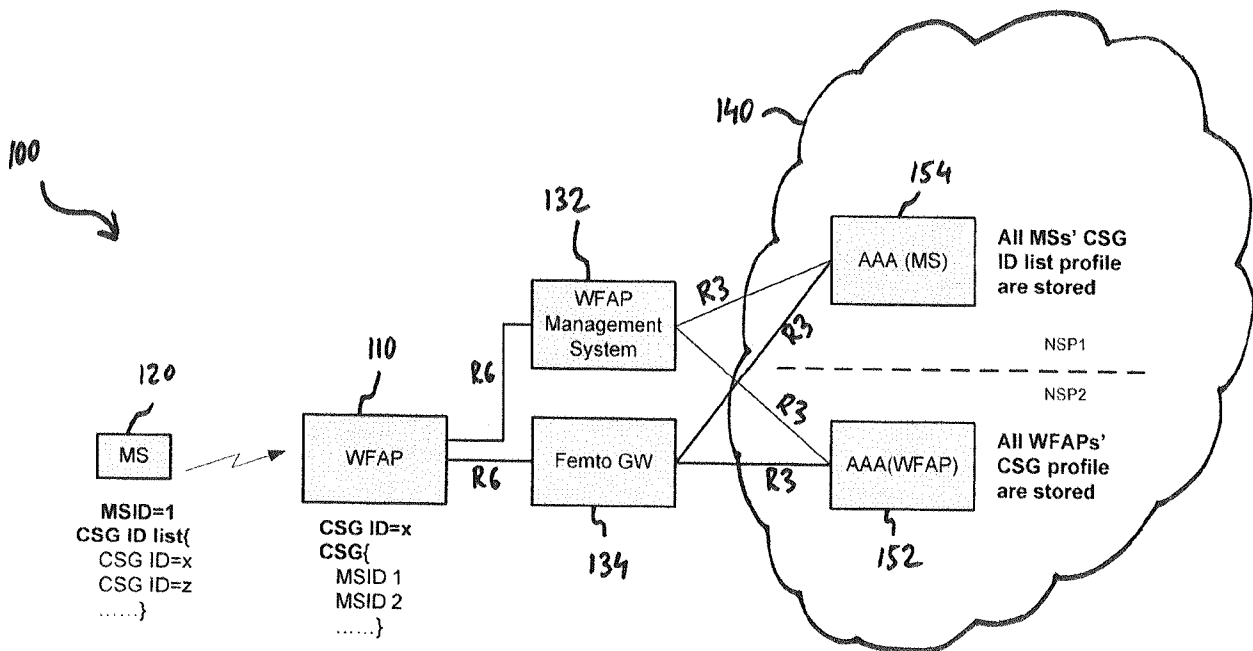


Fig. 1a

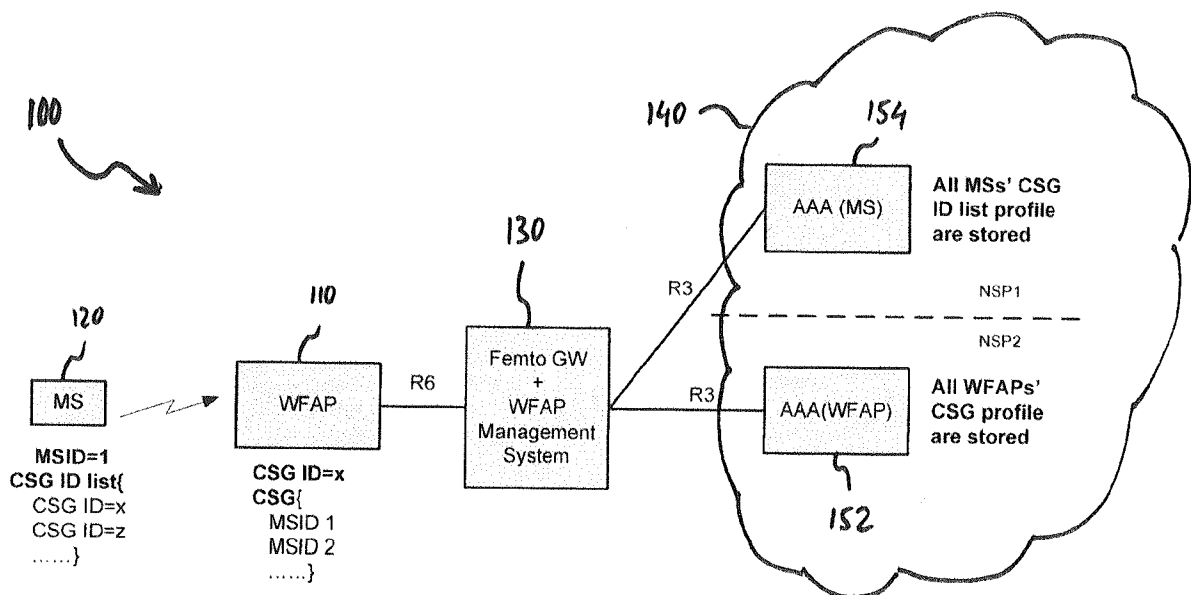
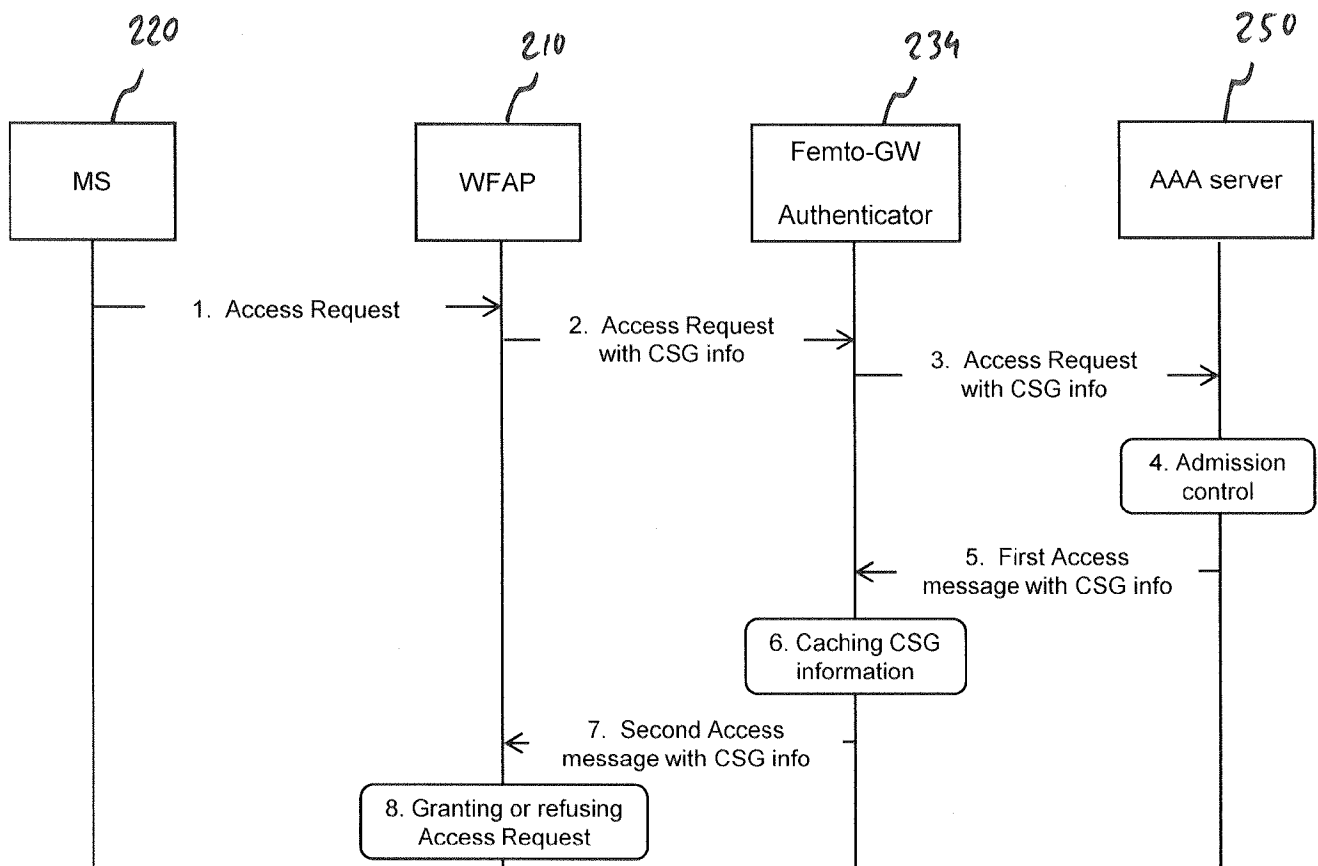


Fig. 1b

**Fig. 2a**

3/3

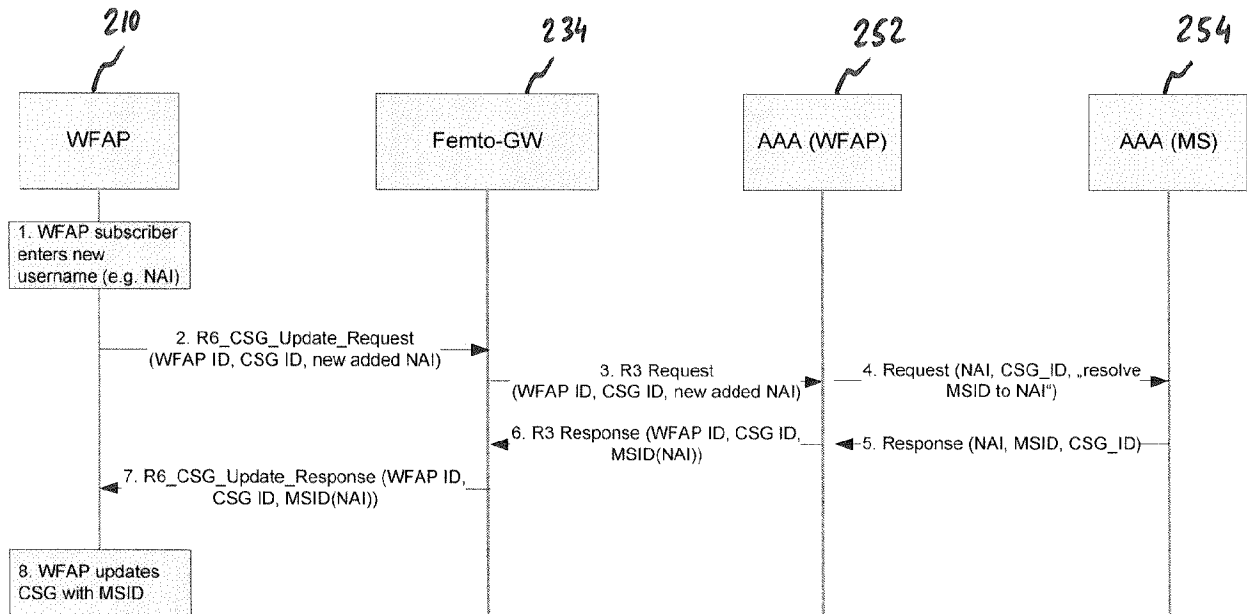


Fig. 2b

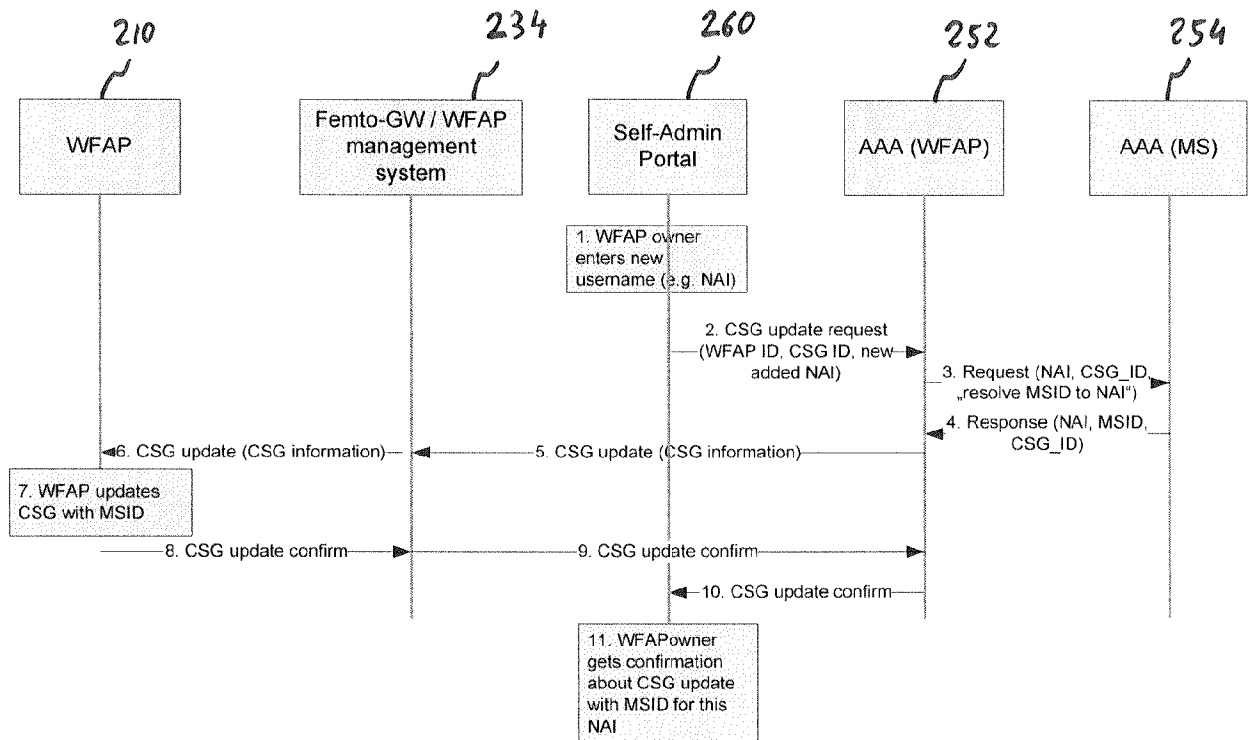


Fig. 2c

# INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/055494

## A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/08

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)

H04W H04L

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 practical, 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. |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | <p>SHU-PING YEH ET AL: "WiMAX femtocells: a perspective on network architecture, capacity, and coverage"</p> <p>IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US LNKD-DOI:10.1109/MCOM.2008.4644120, vol. 46, no. 10, 1 October 2008 (2008-10-01), pages 58-65, XP011236260</p> <p>ISSN: 0163-6804</p> <p>page 59, left-hand column, line 32 - page 60, right-hand column, line 8; figure 2</p> <p style="text-align: center;">-----<br/>-/--</p> | 1-15                  |



Further documents are listed in the continuation of Box C.



See patent family annex.

### \* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document 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

23 June 2010

Date of mailing of the international search report

08/07/2010

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

Ruiz Sanchez, J

# INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/055494

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                                                                                                                                                                                                                                                                                              | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | <p>US 2009/093232 A1 (GUPTA RAJARSHI [US] ET AL) 9 April 2009 (2009-04-09)<br/> paragraph [0042]<br/> paragraphs [0048] - [0051]<br/> paragraphs [0058] - [0060]<br/> paragraph [0083]<br/> paragraphs [0086] - [0091]<br/> paragraphs [0096] - [0099]<br/> paragraphs [0102] - [0106]<br/> paragraphs [0113] - [0121]<br/> paragraphs [0148] - [0152]<br/> paragraph [0159]<br/> paragraph [0195]</p>                                                                                                          | 1-15                  |
| A         | <p>-----<br/> "WiMAX Forum Network Architecture (Stage 3: Detailed Protocols and Procedures) Release 1.0 version 4"<br/> WiMAX Forum<br/> no. WMF-T33-001-R010v04,<br/> 3 February 2009 (2009-02-03), pages<br/> 146-158, 167, 168, XP002588322<br/> Retrieved from the Internet:<br/> URL: <a href="http://www.wimaxforum.org/resources/documents/technical/T33">http://www.wimaxforum.org/resources/documents/technical/T33</a><br/> [retrieved on 2009-06-22]<br/> section 5.1.1; figure 4-41<br/> -----</p> | 1-15                  |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/055494

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|-------------------------------------------|---------------------|----------------------------|---------------------|
| US 2009093232 A1                          | 09-04-2009          | AU 2008311002 A1           | 16-04-2009          |
|                                           |                     | AU 2008311003 A1           | 16-04-2009          |
|                                           |                     | AU 2008311004 A1           | 16-04-2009          |
|                                           |                     | CA 2701906 A1              | 16-04-2009          |
|                                           |                     | CA 2701924 A1              | 16-04-2009          |
|                                           |                     | CA 2701961 A1              | 16-04-2009          |
|                                           |                     | EP 2198653 A2              | 23-06-2010          |
|                                           |                     | EP 2198585 A2              | 23-06-2010          |
|                                           |                     | EP 2198586 A1              | 23-06-2010          |
|                                           |                     | US 2009094680 A1           | 09-04-2009          |
|                                           |                     | US 2009094351 A1           | 09-04-2009          |
|                                           |                     | WO 2009048887 A1           | 16-04-2009          |
|                                           |                     | WO 2009048888 A2           | 16-04-2009          |
|                                           |                     | WO 2009048889 A2           | 16-04-2009          |

---