Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2532083 C 2012/02/07

(11)(21) 2 532 083

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2004/07/30
(87) Date publication PCT/PCT Publication Date: 2005/02/17
(45) Date de délivrance/Issue Date: 2012/02/07
(85) Entrée phase nationale/National Entry: 2006/01/11
(86) N° demande PCT/PCT Application No.: EP 2004/008574
(87) N° publication PCT/PCT Publication No.: 2005/015875
(30) Priorité/Priority: 2003/07/31 (EP03017348.8)

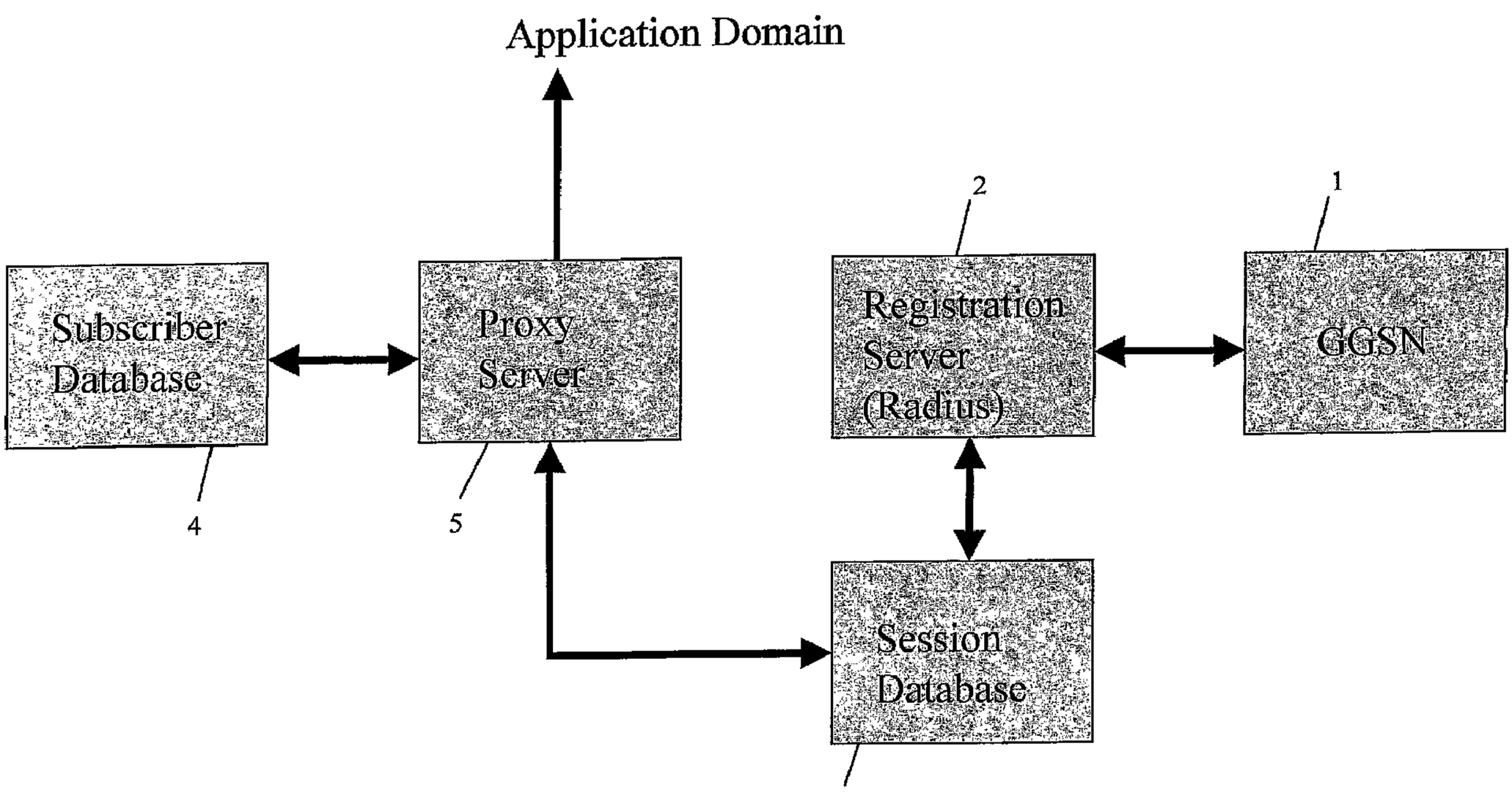
(51) Cl.Int./Int.Cl. *H04W 12/06* (2009.01), *H04W 80/04* (2009.01), *H04W 80/12* (2009.01), *H04L 29/06* (2006.01)

(72) Inventeurs/Inventors:
BLICKER, STEPHAN, DE;
BRITSCH, MATTHIAS, DE

(73) Propriétaire/Owner:
T-MOBILE DEUTSCHLAND GMBH, DE

(74) Agent: MARKS & CLERK

(54) Titre : AUTHENTIFICATION D'ACCES TRANSPARENTE DANS DES RESEAUX D'ACCES MOBILE 2GOU 2.5G
(54) Title: TRANSPARENT ACCESS AUTHENTICATION IN 2G AND 2.5G MOBILE ACCESS NETWORKS



(57) Abrégé/Abstract:
The present invention relates to a method for application layer authentication of subscribers connected to the authenticating network domain by a 2G or 2.5G GPRS core network or a 3G UMTS network, characterised by using data which are assembled by the network layer during establishment of a PDP context in GPRS networks. The invention comprises System of units in a mobile telecommunication network, including at least a first authentication unit which is connected via a data line to a second unit which assembles data according to the described method.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 February 2005 (17.02.2005)

PCT

(10) International Publication Number
WO 2005/015875 A1

(51) International Patent Classification[7]: H04L 29/06, H04Q 7/38

(21) International Application Number: PCT/EP2004/008574

(22) International Filing Date: 30 July 2004 (30.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03017348.8 31 July 2003 (31.07.2003) EP

(71) Applicant *(for all designated States except US)*: **T-MOBILE DEUTSCHLAND GMBH** [DE/DE]; Langrabenweg 151, 53227 Bonn (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BLICKER, Stephan** [DE/DE]; Auf dem Grevel 7, 53343 Wachtberg-Villip (DE). **BRITSCH, Matthias** [DE/DE]; Steinweg 4a, 53639 Königswinter (DE).

(74) Agent: **RIEBLING, Peter**; Postfach 31 60, 88113 Lindau/B. (DE).

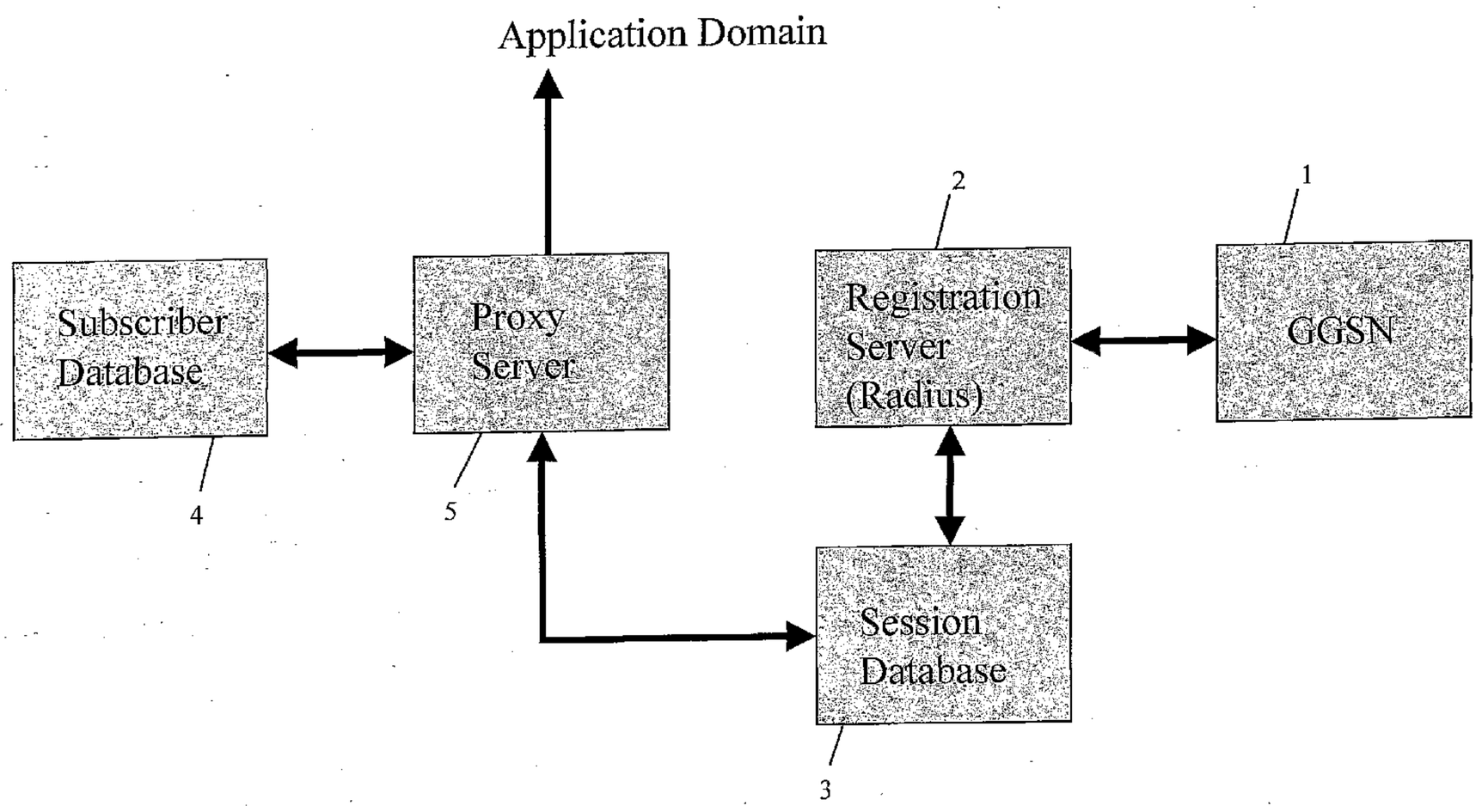
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

[Continued on next page]

(54) Title: TRANSPARENT ACCESS AUTHENTICATION IN GPRS CORE NETWORKS



(57) Abstract: The present invention relates to a method for application layer authentication of subscribers connected to the authenticating network domain by a 2G or 2.5G GPRS core network or a 3G UMTS network, characterised by using data which are assembled by the network layer during establishment of a PDP context in GPRS networks. The invention comprises System of units in a mobile telecommunication network, including at least a first authentication unit which is connected via a data line to a second unit which assembles data according to the described method.

WO 2005/015875 A1

WO 2005/015875 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Transparent Access Authentication in 2G and 2.5G Mobile Access Networks

The present invention relates to a method and system for transparent access authentication in 2G and 2.5G Mobile Access Networks. This includes communication networks of the GSM-, GPRS- and UMTS-standard well known to skilled persons.

In standardisation of Universal Mobile Telecommunication System (UMTS Rel.5) comprehensive means are foreseen to perform authentication on the application layer with no need to interwork with the underlying radio and transport networks. The mechanisms are based on the assumption that a specific environment is prepared for deployment of IP Multimedia Subsystem (IMS) services. It includes the use of IMS SIM (ISIM) application, which in turn requires Rel.99UICC's in the connected end devices to handle the authentication and key agreement (AKA).
In case of deployment of IMS and IMS based services in a network environment which is characterised by the use of SIM cards, the standardised authentication mechanism will not be applicable.

The Technical Specification 3GPP TS 33.203: "Access Security for IP-based Services", Release 5, V5.6.0, June 2003, XP-002264085, discloses a method for transparent access authentication of subscribers connected to an authenticating network domain by a GPRS core network or an UMTS network, the method using data which are assembled by a network layer during establishment of a PDP context in GPRS networks.

It is the object of the invention to provide method and system for transparent access authentication which allow it to run authentication transparently to the end device, without requiring proprietary extensions and functions on network or client side.

This object is achieved by providing a method and system as described in the independent claims.

Other features which are considered to be characteristic for the invention are set forth in the dependent claims.

The present invention describes a method for application layer authentication of subscribers, connected to the authenticating network domain by a 2G or 2.5G General Packet Radio Service (GPRS) core network or a 3G UMTS network. The authentication will be based on data which is assembled by the network layer during establishment of a PDP context in GPRS networks. This information is secured by standard SIM card application. As the same mechanisms are used for authentication in 3G networks, the further described mechanism is also applicable there. No standard would be touched in any way while using a 2G or 2.5G access network, because no authentication on application layer is foreseen in the standard. For UMTS Rel.5 standards and following, the standard foresees specific methods. The use of the further described method would be possible, although the standardised authentication mechanism needs to be switched off. Switching off the standardised authentication mechanism could be interpreted as standard sensitive, but subsequent use of the further described mechanism would be standard compliant again.

Further, a migration path to UMTS Rel.5 standardised authentication and the concept for parallel use of both mechanisms is described.

The invention will now be described in further detail with reference to the drawings.

Figure 1 depicts the general architecture of the system for carrying out the invention;

Figure 2 depicts an embodiment of the invention with migration to IMS compliant architecture.

With reference to Figure 1, during PDP context establishment the Serving GPRS Support Node (SGSN) is authenticating the subscriber using the A3/A8 algorithm based on the end devices SIM card in case of GSM and 2.5G GPRS and EDGE access network.

The Gateway GPRS Support Node 1 (GGSN) receives a context creation request and queries a Radius (Registration) server 2 (Remote Authentification Dial-In User Service) to get an IP address assigned for the particular PDP context. Within the context the Radius server 2 receives the MSISDN and/or the IMSI of the subscriber. So in the session database 3 of the Radius server 2 there is stored for each PDP context a pair of IP address and IMSI/MSISDN. Based on the tunnel endpoint ID (TEID) the GGSN 1 filters all packets running through the PDP context once established, for the correct IP source address. This means the GGSN 1 checks matching TEID/IP address pairs, thus preventing falsification of source addresses and so called "IP spoofing" for the complete lifecycle of the PDP context. The TEID unambiguously identifies a tunnel endpoint in the receiving GTP-U (GPRS Tunnelling Protocol - User) or GTP-C (GPRS Tunnelling Protocol - Control) protocol entity. The receiving side of a GTP tunnel locally assigns the TEID value for the transmitting side to use. The TEID values are exchanged between tunnel endpoints using GTP-C messages (or RANAP (Radio Access Network Application Part) in the UTRAN (UMTS terrestrial Radio Access Network

In the application domain a subscriber database 4 exists that stores all PubIDs the subscriber is using in the domain, referring it to his PrivID, which is unique in the respective

application domain. The PrivID is correlated with an MSISDN and/or IMSI.

In the request the user gives his PrivID for registration. Upon receiving the registration request, the registration proxy 5 queries the subscriber database 4 containing the subscribers IDs (both public and private) together with the MSISDN/IMSI. This data is stored in a table on the proxy server platform.

Subsequently the proxy server 5 queries the session database 3 of the Radius server 2 in order to get the assigned IP address of that session and the IMSI/MSISDN already authenticated by the network's Home Location Register (HLR). The authentication of the HLR guarantees further that the IP address can be considered to be authenticated as well. Also this information is stored in the table on the proxy server platform.

Now the proxy server 5 starts the authentication procedure according to the invention.

First, the proxy server 5 checks IMSI/MSISDN from Radius server 2 database 3 and application domain database 4 for match. If the pairs are not matching, the subscriber has tried to register with an incorrect PrivID, which is not correlated with his IMSI/MSISDN, if the pairs are matching the next step is performed.

Second step is checking the subscribers IP address in the IP network layer, meaning in the IP packet overhead field for source address for match with the IP address assigned by the Radius server 3. As the IP address was assigned to an IMSI/MSISDN-authenticated session, also the IP address can be considered as authenticated.

If the pairs are not matching, the subscriber used an incorrect IP address, if the pairs are matching the subsequent step is performed.

The proxy server 5 parses the application layer for IP addresses given in the headers of e.g. SIP registration message, SDP message bodies, etc and checks for match with the IP address in, which was already checked for match with the IP address assigned by the Radius server 2. If the pairs are not matching the subscriber used incorrect signalling information, e. g. response addresses, etc. If the pairs are matching, the session setup can be considered as authenticated.

In all subsequent messages arriving at the proxy server 5, it checks for match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifies the matching pairs against the IP address assigned by the Radius server 2. If PubIDs are used in the following session, the PubIDs are checked against the PrivID which was stored in a table on the proxy server platform after querying the application domains database 4.

The described functionality gives the network operator the opportunity to run authentication transparently to the end device, without requiring proprietary extensions and functions on network or client side. In case of SIP based signalling, the migration to fully standard compliant UMTS Rel.5 mechanisms and a strategy for parallel operation is necessary, this will be described now.

As the IMS domain as standardised for UMTS Rel.5 will include its own authentication mechanism, it is necessary to support a scenario where the subscribers are migrating to ISIM enabled end devices. To exploit the benefits of the standardised authentication mechanism, both mechanisms have to be supported in parallel.

This is done by an additional function that checks each incoming signalling message, first for the protocol, if itis any other protocol than SIP, the session is routed to the proxy server 5.

With reference to Figure 2,the same routing decision is taken if the message is based on SIP, but the client does not support standardised UMTS Rel.5 authentication. If the client does support standardised authentication method, e.g. is ISIM enabled, the message is routed to the standard compliant Proxy Call State Control Function (P-CSCF). First trigger for routing decisions is the protocol type, as described above. Further triggers could be the key exchange mechanism used for setting up the secured connection between UE and P-CSCF (if the end device is starting key agreement, it can be considered as standard compliant and the request is routed to the P-CSCF), or other elements included in the UMTS Rel.5 header as well as any private extension, which is, however, possible but not necessary. If trigger points available in signalling should be insufficient, also database lookups can be used to base routing decisions on.

The authentication procedure is as follows

First, a decision is required by which node P-CSCF 6 or proxy server 5 the register shall be routed

For this, a routing module 7 is provided which will be the standard entry point for all messages. The routing module 7

decides by evaluation of PrivID which node will handle the message. The routing module 7 refers to subdomains (e.g. user@gprs.tmo.de and user@tmo.umts.de) within the domain part of the Network Access Identifier (NAI), see 3GPP specification 23.228. This requires that NAIs for 3G subscribers have to provide subdomains.

The routing module 7 shall set a routing entry, by using only the PrivID, subsequent messages shall be identified by the IP source address listed in the routing table.
The routing module 7 identifies the responsible proxy function, i.e. proxy server 5 or P-CSCF 6, by evaluating the PrivID (URIs subdomains) This rises the request towards IMSI/MSISDN and URIs to be chosen according to this functionality.

In case other protocols shall be used beside SIP, such as e.g. SMTP, HTTP, SOAP (.NET), etc, the proxy server 5 must be extended, and authenticate the subscribers by use of the IP address, subsequently resolving the IMSI/MSISDN and matching of the particular identifier of the protocol, which is stored in the subscriber profile of the subscriber database 4. This requires the population of the subscriber profile with the required data elements and extension of the routing module to enable protocol dependent routing.

In case separate access networks are used, the application platform has to know which type of access network is used to adapt service delivery accordingly. This requires that a change request has to be stated against the SGSN to enable it to send the access type to the GGSN which includes it in the radius request, so the access network type will be available in the session database 3. This enables all applications to

request the access network type and use it, e.g. for Quality of Service (QoS) means.

Abbreviations

2.5G	second and half generation (e. g. GPRS, EDGE)
2G	second generation (e. g. GSM)
3G	third generation (e. g. UMTS)
AKA	authentication and key agreement
CC	Circuit Switched
IMS	IP multimedia subsystem
IMSI	International Mobile Subscriber Identity
ISIM	IMS SIM
MSISDN	Mobile Station ISDN Number
NAI	Network Access Identifier
P-CSCF	Proxy-Call-State-Control-Function
SIM (card)	(GSM) Subscriber Identity Module (card)
SIP	Session Initiation Protocol
TEID	Tunnel Endpoint ID
UE	User Equipment
UICC	UMTS IC Card
UMTS	Universal mobile telecommunication system
URI	Uniform Ressource Locator

T03018 PCT 10

26.04.2005

Claims

1. Method for transparent access authentication of subscribers connected to an authenticating network domain by a GPRS core network or an UMTS network, wherein the method using data which are assembled by a network layer during establishment of a PDP context in GPRS networks, characterised in
that when a Gateway GPRS Support Node (1) receives a context creation request it queries a registration server (2) to get an IP address assigned for the particular PDP context, and within the context the registration server (2) receives a Mobile Station ISDN Number, MSISDN, and/or an International Mobile Subscriber Identity, IMSI, of the subscriber and stores for each PDP context a pair of IP address and IMSI/MSISDN in a session database (3),
that a proxy server (5) is provided which checks IMSI/MSISDN from a registration server (2) session database (3) and IMSI/MSISDN from a application domain database (4) for match,
that if the IMSI/MSISDN pairs are matching, the proxy server (5) checks a subscribers IP address assigned in the IP network layer for match with the IP address assigned by the registration server (2), and
that the proxy server (5) parses the application layer for IP addresses given in the headers of registration messages and checks for match with the network layer IP address which was already checked for match with the IP address assigned by the radius server (2).

2. Method according to claim 1, comprising the step that during PDP context establishment a Serving GPRS Support

Node (SGSN) is authenticating the subscriber using the A3/A8 algorithm based on an end devices SIM card.

3. Method according to any preceding claim, comprising the step that in all subsequent messages arriving at the proxy server (5), it checks for match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifies the matching pairs against the IP address assigned by the Radius server (2).

4. Method according to any preceding claim, that a routing module (7) is provided which is a standard entry point for all messages and decides by evaluation of Private ID, PrivID, which network node will handle the message.

5. System of units in a mobile telecommunication network, characterised that at least a first authentication unit (2) is connected via a data line to a second unit (5; 6) which assembles data according to the method of claim 1.

6. System according to claim 5, wherein the first unit comprises a registration server (2).

7. System according to claim 5 or 6, wherein the first unit (2) is connected to a session database (3).

8. System according to any of claims 5 to 7, wherein the second unit comprises a proxy server (5).

9. System according to any of claims 5 to 8, wherein the second unit comprises a Proxy Call State Control Function (6).

10. System according to any of claims 5 to 9, wherein the second unit (5; 6) is connected to a subscriber database (4).

11. System according to any of claims 5 to 10, wherein a routing module (7) is provided which decides by evaluation of Private ID, PivID, which network node will handle the message.

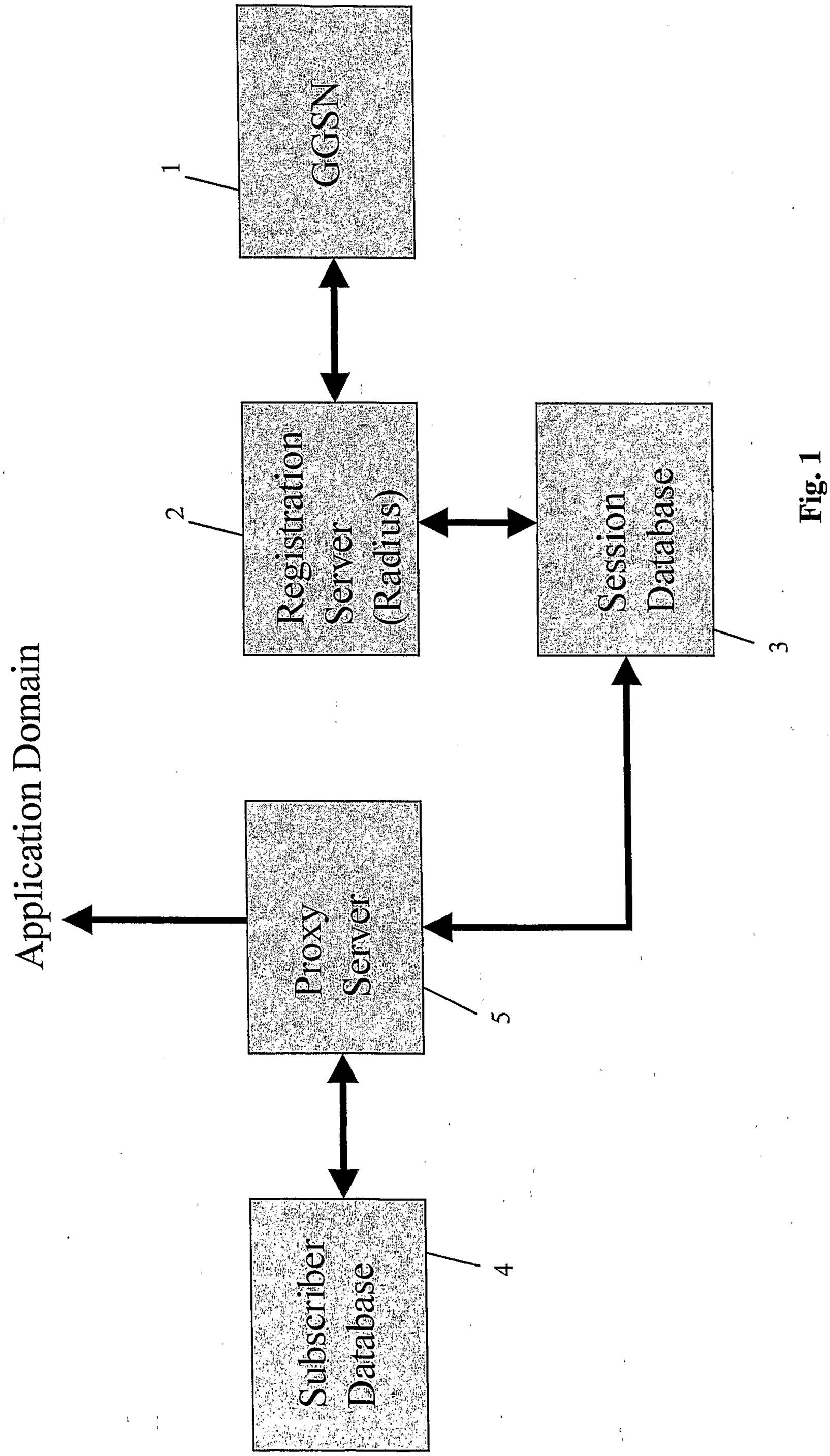

GGSN
1
Registration Server (Radius)
2
Session Database
3
Application Domain
Proxy Server
5
Subscriber Database
4

Fig. 1

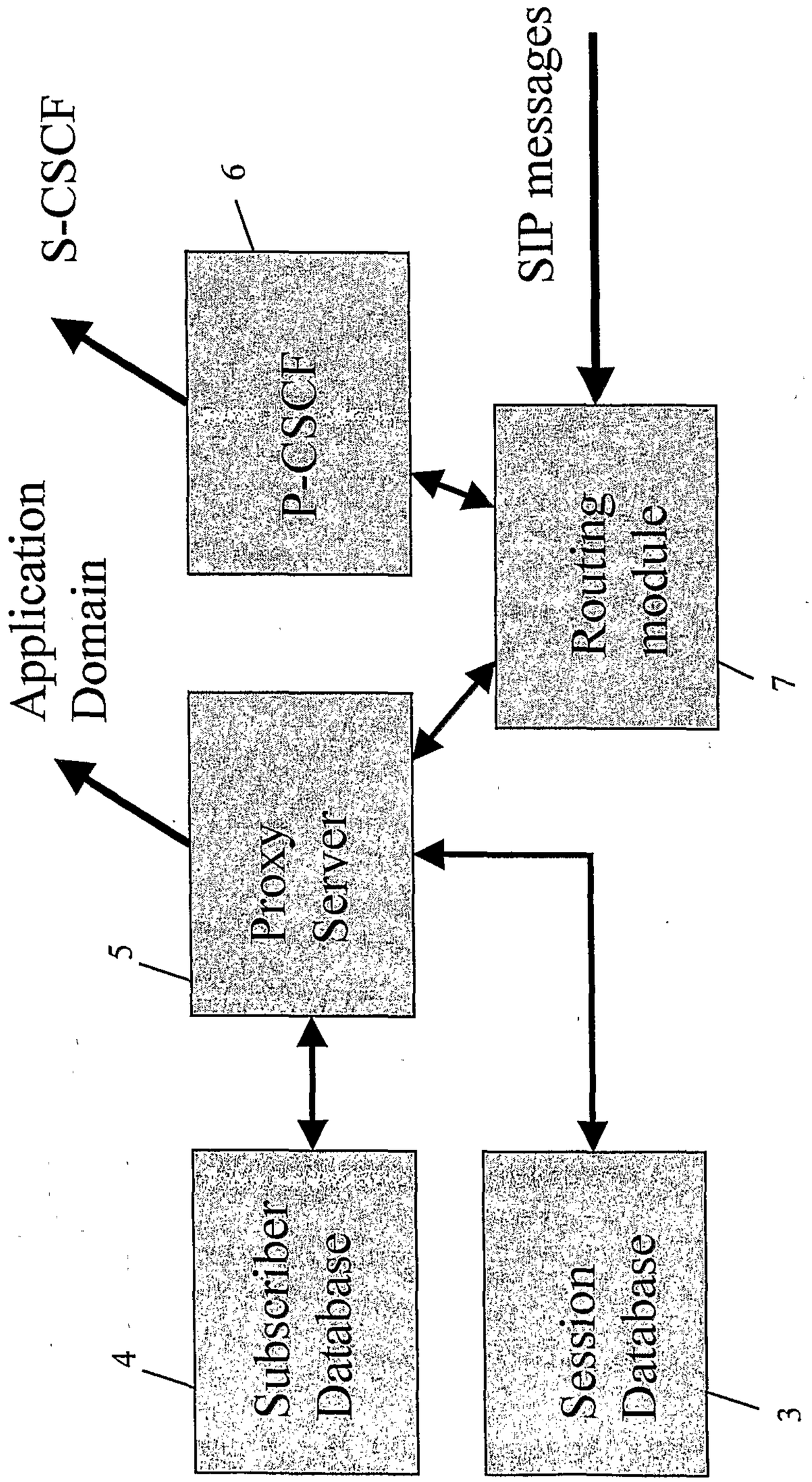
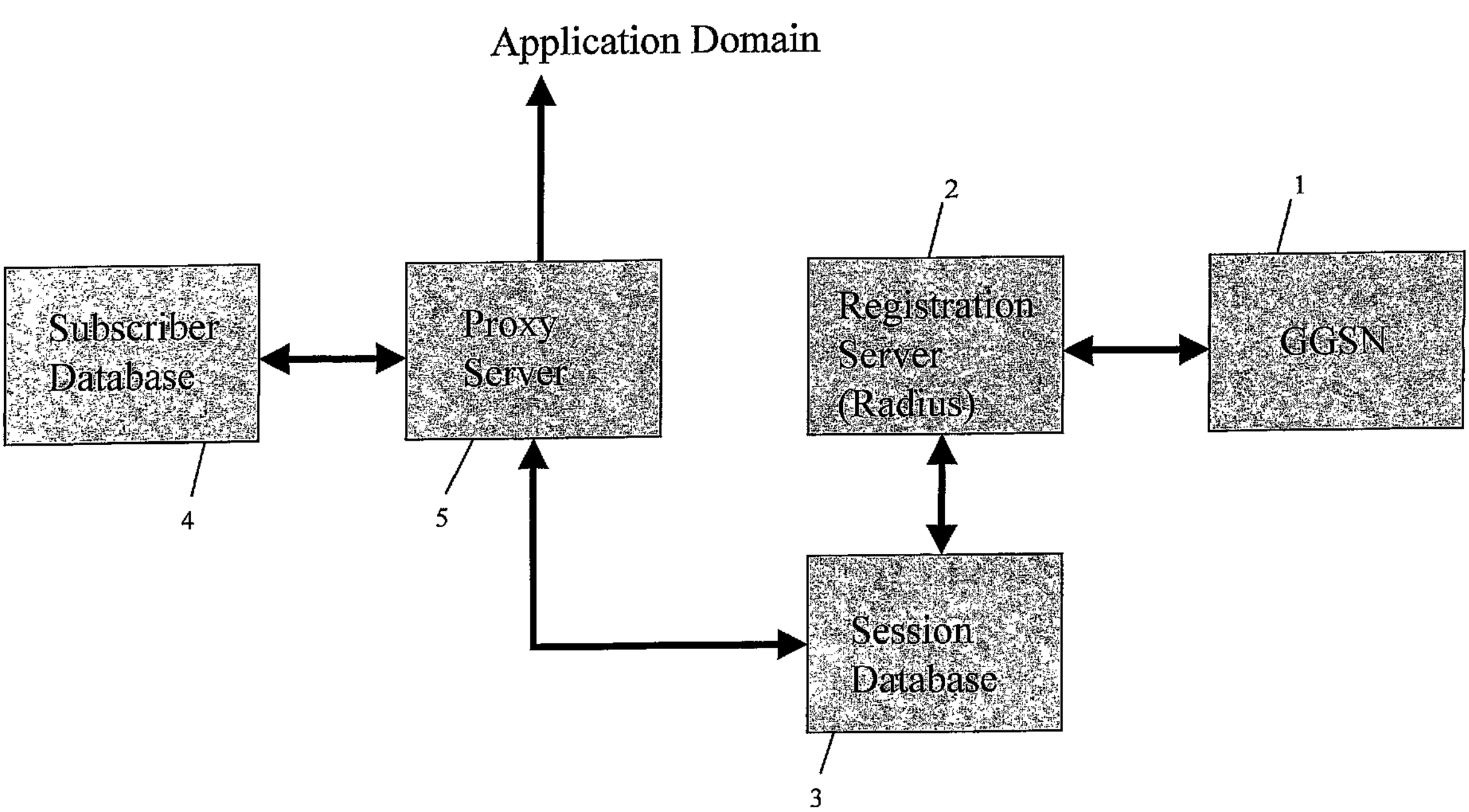

SIP message
S-CSCF
Application Domain
6
P-CSCF
Routing module
7
Proxy Server
5
Subscriber Database
4
Session Database
3

Fig. 2


Application Domain
Subscriber Database
Proxy Server
Registration Server (Radius)
GGSN
Session Database
1
2
3
4
5