

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
6 November 2003 (06.11.2003)

PCT

(10) International Publication Number  
**WO 03/091891 A1**

(51) International Patent Classification<sup>7</sup>: **G06F 15/16**,  
15/173

(21) International Application Number: PCT/IB03/01174

(22) International Filing Date: 31 March 2003 (31.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
10/132,226 26 April 2002 (26.04.2002) US

(71) Applicant: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant (for LC only): **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: **ISOMAKI, Markus**; Ajurinkatu 3B 43, FIN-02600 Espoo (FI). **COSTA-REQUENA, Jose**; Karjalankatu 11 A 11, FIN-00520 Helsinki (FI). **LAN-SISALMI, Atte**; Koukkuniementie 16 A 2, FIN-02230 Espoo (FI). **NIEMI, Valtteri**; Tallberginkatu 3 as 43, FIN-00180 Helsinki (FI). **NIEMI, Aki**; Messeniuksenkatu 9 A 33, FIN-00250 Helsinki (FI). **HAUKKA, Tao**; Taskilantie 18, FIN-90580 Oulu (FI). **BAJKO, Gabor**; Rezeda

u. 8A, H-1214 Budapest (HU). **VIITANEN, Tommi**; Hussankatu 21 H 40, FIN-33730 Tampere (FI).

(74) Agent: **STOUT, Donald, E.**; Antonelli, Terry, Stout & Kraus, LLP, Suite 1800, 1300 North Seventeenth Street, Arlington, VA 22209 (US).

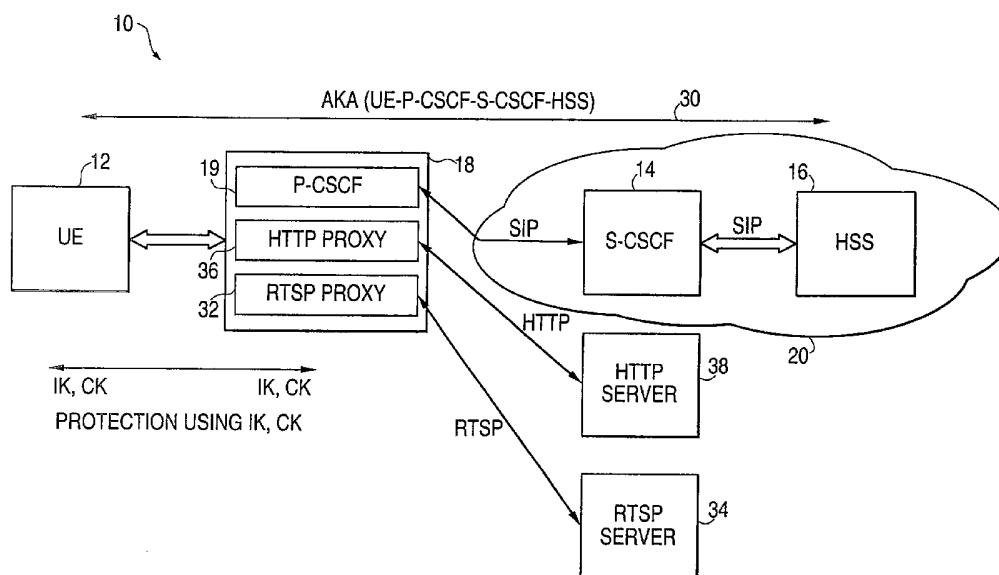
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (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: AUTHENTICATION AND PROTECTION FOR IP APPLICATION PROTOCOLS BASED ON 3GPP IMS PROCEDURES



(57) Abstract: The present invention is a system and method which provides authentication for data services for at least one UE (12) using common authentication information based upon information stored in a HSS (16) of a home network (20) of the at least one UE for multiple protocols. At least one proxy server (18) stores authentication information for each of the protocols which may be used to provide data services to the at least one UE. Authentication of the protocols available to the at least one UE uses the authentication information stored at the at least one proxy server obtained from the protocol used in the home network of the at least one UE.



WO 03/091891 A1



---

*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.*

0172.41180A00  
NC 16507 PCT

## **AUTHENTICATION AND PROTECTION FOR IP APPLICATION PROTOCOLS BASED ON 3GPP IMS PROCEDURES**

5

### TECHNICAL FIELD

The present invention relates to systems and methods for authenticating requests for data services from at least one user equipment using multiple protocols.

10

### BACKGROUND ART

The 3GPP Technical Specification TS 33.203 v1.0.0 (2001-12), which is incorporated herein by reference in its entirety, authenticates IP multimedia core network subsystem (IMS) customers by running the Authentication and Key Agreement (AKA) protocol during a SIP register transaction. See Section 6.1 for a discussion of the AKA. After authentication using AKA is completed, the created integrity key (IK) and Cipher Key (CK) are shared between the User Equipment (UE) and the Proxy Call State Control Function (PCSCF) which is the first entity in a SIP network receiving a request for a session from UE. The P-CSCF may be resident in either a home network or a visited network. SIP requests for services are protected by the IK and CK keys until the keys are renewed by another register transaction. The IK and CK keys are securely distributed by any well known technique, such as IP Sec or EPS.

The main SIP entities used for registration of the UE are: UE, P-CSCF, the serving call state control function (S-CSCF) and a home subscriber server (HSS). The UE communicates with the P-CSCF, which communicates with the S-CSCF which communicates with the HSS. A detailed description of authentication and registration is found in Sections 4 and 5-5.2 of the aforementioned specification.

30

With the advent of IP multimedia services (IM), it is desirable for UE using SIP to have access to data services using additional protocols, such as the Hyper Text Transport Protocol (HTTP) and the Real-Time Streaming Protocol (RTSP)

protocol. A description of the RTSP is found in RFC 2326 dated 1998 which is incorporated herein by reference in its entirety.

Basic to the access of UE to network services involving any protocol, such as SIP, HTTP, and RTSP, is the need for authentication of the UE and security. The state of the art presently is that each protocol utilizes its own security and authentication measures when a request by UE is made for a session of data services. When a UE is a requester of data services involving multiple protocols, individual protocol specific network entities are necessary in the form of a proxy server or otherwise to perform authentication for each protocol. The multiple entities required currently for authentication of UE to obtain sessions involving multiple protocols, which may have different network addresses, involve a duplication of processing by each proxy to obtain the authentication information.

#### DISCLOSURE OF THE INVENTION

The present invention is a system, method, and at least one proxy server which provides authentication for UE sessions of data services requiring multiple protocols which use common authentication information for each of the multiple protocols. At least one proxy server is used to authenticate requests for sessions of data services from UE for the multiple protocols. While the simplest architecture which may be used to practice the invention is a single proxy server, it should be understood that more than one proxy server may be used to perform authentication for data services for UE for the multiple protocols using the common authentication information.

The at least one proxy server stores authentication information from a subscriber data server of a home network for at least one UE required for a first protocol. The at least one proxy server authenticates requests for sessions of data services received from at least one UE for protocols other than the first protocol by using the authentication information obtained from the subscriber data server for the first protocol. Authentication of sessions involving IMS transactions is readily

performed by the at least one proxy server for protocols other than the first protocol.

5 The at least one proxy server provides access to users of IMS services with a protocol (for example, HTTP) different from SIP (as normally is used in IMS). The IMS services include different data structures (XML, SOAP, ACAP, etc) for performing service management tasks like authorization policy manipulation, member list management, etc. This is necessary for data management requiring a reliable protocol like HTTP while still applying IMS specific security mechanisms.

10 The at least one proxy server authenticates the message according to the IMS specifications and algorithms and passes the content to the correct application server using another protocol different from SIP, like HTTP (for example, Presence, Messaging or a Conferencing Server applications) that implements the service itself.

15

The at least one proxy server also adds information, preferably in the form of a shared secret key pair or other security mechanism, that the at least one application server, for example, a HTTP or RTSP server, can use to ensure the identity of the user is authenticated that issued the request for services using the particular protocol. The at least one application server has the final responsibility

20 of authorizing the user and/or action to be performed by the application server for the user.

In a preferred embodiment, the first protocol is SIP and the at least one additional

25 protocol is one or both of HTTP and RTSP. Requests for sessions of data services using SIP are transmitted from the P-CSCF resident in the at least one proxy server to a S-CSCF server of the home network and then to the HSS. Requests for sessions of data services using the HTTP protocol use the SIP authentication information and are transmitted from a Hyper Text Transport

30 Protocol (HTTP) proxy of the at least one proxy server to a HTTP server. Requests for sessions of data services using the RTSP protocol use the SIP

authentication information and are transmitted from a Real-Time Streaming Protocol (RTSP) proxy of the proxy server to a RTSP server.

5 The preferred authentication information transmitted from the HSS to the at least one proxy server comprises an integrity key (IK) and a cipher key (CK). The authentication information transmission from the at least one UE to the at least one proxy server also comprises the integrity key (IK) and the cipher key (CK). The keys are processed by the at least one proxy server to determine if the at least one UE is authentic.

10

The invention eliminates the need for unique authentication information for each protocol to authenticate data sessions for UE. In a preferred embodiment a single proxy server includes all of the proxies for the protocols resident therein. The authentication information for the additional protocols, for example, HTTP and  
15 RTSP, is obtained from SIP authentication information of the at least one UE.

The invention is a system including a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to  
20 authenticate the at least one user of the data services when a request for data services is made using a first protocol; at least one user equipment which requests data services using the first protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to  
25 authenticate the at least one user; at least one proxy server including resident therein a first proxy for the first network protocol and at least one additional proxy for the at least one additional protocol; and wherein the first proxy and the at least one additional proxy of the one proxy server authenticates requests for data services received from the at least one user equipment for the protocols by using  
30 the authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user

equipment to the at least one proxy server. The subscriber data server may be a home subscriber server (HSS); and the first protocol may be the Session Initiation Protocol (SIP) and a request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a  
5 Serving Call State Control Function (S-CSCF) server of the home network. The subscriber data server may be a home subscriber server (HSS); the first protocol may be the Session Initiation Protocol (SIP) and a request for data data services using SIP is transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF)  
10 server of the home network; and the at least one additional protocol may be the Hyper Text Transport Protocol (HTTP) and a request for data services using HTTP may be transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP server. The subscriber data server may be a home subscriber server (HSS); the first protocol may be the Session Initiation  
15 Protocol (SIP) and a request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server; and the at least one additional protocol may be the Real-Time Streaming Protocol (RTSP) and a request for data services may be transmitted from a Real-Time Streaming  
20 Protocol (RSTP) proxy of the at least one proxy server to a RTSP server. The subscriber data server may be a home subscriber server (HSS); the first protocol may be the Session Initiation Protocol (SIP) and a request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF)  
25 server of the home network; and the at least one additional protocol may be the Hyper Text Transport Protocol (HTTP) and the Real-Time Streaming Protocol (RTSP) and a request for data services using HTTP may be transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP server and a request for data services using RTSP may be transmitted from  
30 a Real-Time Streaming Protocol (RTSP) proxy of the at least one proxy server to a RTSP server. The authentication information transmitted from the subscriber data server to the at least one proxy server may comprise an integrity key IK and

a cipher key CK and the authentication information transmitted from the at least one user equipment to the at least one proxy sever may comprise an integrity key IK and a cipher key CK which keys are processed by the at least one proxy server to determine if the at least one user is authentic. The authentication information  
5 transmitted from the subscriber data server and the at least one user equipment may be generated using the Authentication and Key Agreement (AKA) protocol.

In a system comprising a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one  
10 user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol and at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication  
15 information which is used when a request for data services is made to authenticate the at least one user; at least one proxy server including resident therein a first proxy for the first network protocol and at least one additional proxy for the at least one additional protocol, a method of authentication of the at least one user equipment includes the first proxy and the at least one additional proxy  
20 of the at least one proxy server authenticates requests for data services received from the at least one user equipment for the protocols by using the authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at  
25 least one proxy server. The subscriber data server may be a home subscriber server (HSS); the first protocol may be the Session Initiation Protocol (SIP) and a request for data data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network; and the at least one  
30 additional network protocol may be the Hyper Text Transport Protocol (HTTP) and a request for data services using HTTP may be transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP



server. The subscriber data server may be a home subscriber server (HSS); the first protocol may be the Session Initiation Protocol (SIP) and a request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server; and the at least one additional protocol may be the Real-Time Streaming Protocol (RTSP) and a request for data services may be transmitted from a Real-Time Streaming Protocol (RTSP) proxy of the at least one proxy server to a RTSP server. The subscriber data server may be a home subscriber server (HSS); the first protocol may be the Session Initiation Protocol (SIP) and a request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network; and the at least one additional protocol may be the Hyper Text Transport Protocol (HTTP) and the Real-Time Streaming Protocol (RTSP) and a request for data services using HTTP may be transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP server and a request for data services using RTSP may be transmitted from a Real-Time Streaming Protocol (RTSP) proxy of the at least one proxy server to a RTSP server. The authentication information transmitted from the subscriber data server to the at least one proxy server may comprise an integrity key IK and a cipher key CK and the authentication information transmitted from the at least one user equipment to the at least one proxy sever may comprise an integrity key IK and a cipher key CK which keys may be processed by the at least one proxy server to determine if the at least one user is authentic. The authentication information transmitted from the subscriber data server and the at least one user equipment may be generated using the Authentication and Key Agreement (AKA) protocol.

In a system comprising a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol and at least one user equipment which

requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user, at least one proxy server in accordance with

5 the invention includes a first proxy for the first network protocol and at least one additional proxy for the at least one additional protocol which are resident in the at least one proxy server; and wherein the first proxy and the at least one additional proxy of the at least one proxy server authenticates requests for data services received from the at least one user equipment for the protocols by using the

10 authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server. The subscriber data server may be a home subscriber server (HSS); and the first protocol may be the Session Initiation

15 Protocol (SIP) and any request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network. The subscriber data server may be a home subscriber server (HSS); and the first protocol may be the Session Initiation Protocol (SIP) and a request

20 for data data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network; and the at least one additional network protocol may be the Hyper Text Transport Protocol (HTTP) and a request for data services using HTTP may be transmitted from a Hyper Text

25 Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP server. The subscriber data server may be a home subscriber server (HSS); and the first protocol may be the Session Initiation Protocol (SIP) and a request for data services using SIP may be transmitted from the at least one proxy server to a Serving Call State Control Function (S-CSCF) server, and the at least one

30 additional protocol may be the Real-Time Streaming Protocol (RTSP) and a request for data services may be transmitted from a Real-Time Streaming Protocol (RSTP) proxy of the at least one proxy server to a RTSP server. The

- subscriber data server may be a home subscriber server (HSS); and the first protocol may be the Session Initiation Protocol (SIP) and a request for data services using SIP may be transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network, and the at least one additional protocol may be the Hyper Text Transport Protocol (HTTP) and the Real-Time Streaming Protocol (RTSP) and a request for data services using HTTP may be transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP server and a request for data services using RTSP may be transmitted from the at least one proxy server to a RTSP server. The authentication information may be transmitted from the subscriber data server to the at least one proxy server may comprise an integrity key IK and a cipher key CK and the authentication information transmitted from the at least one user equipment to the at least one proxy sever may comprise an integrity key IK and a cipher key CK which keys may be processed by the at least one proxy server to determine if the at least one user is authentic. The authentication information transmitted from the subscriber data server and the at least one user equipment may be generated using the Authentication and Key Agreement (AKA) protocol.
- A system in accordance with the invention includes a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol; at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user; at least one proxy server, including resident therein a first proxy for the first protocol and at least one additional proxy for the at least one additional protocol; at least one application server coupled to the at least one proxy server, each application server providing data services to the at least one user using at least one of the at least one additional protocols

through the at least one proxy server; the first proxy and the at least one additional proxy of the at least one proxy server authenticating requests for data services received from the at least one user equipment for the protocols by using the authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server and provides information to the at least one application server permitting the at least one application server to provide final authorization of the at least one user to access the at least one application server or to provide final authorization of an action to be performed for the at least one user by the at least one application server. The at least one proxy server may process the authentication information to provide the information to the at least one application server to permit the at least one application server to provide the final authorization including guaranteeing the identity of the at least one user. The processing of the authentication information to provide the information to the at least one application server may comprise a shared secret known to the at least one proxy server and the at least one application server which guarantees the identity of the at least one user at the at least one application server. The shared secret may be a shared key pair which is processed by the at least one application server to verify the identity of the user who is to receive access to the at least one application server or for whom the at least one application server is to take action. The coupling of the at least one proxy server to the at least one application server may be via a secure medium. The at least one application server may register data services with the at least one proxy server which the at least one application server may provide to the at least one user through the at least one proxy server; and the at least one proxy server may store an address of each application server that provides data services for selection by the at least one user which is used to connect the at least one user to the at least one application server to obtain selected data services. The at least one proxy server may be an access point in the system for the transmission of data services between the at least one user and the at least one proxy server.

In a system comprising a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol and at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user, at least one proxy server including resident therein a first proxy for the first network protocol and at least one additional proxy for the at least one additional protocol, and at least one application server coupled to the at least one proxy server, each application server providing data services to the at least one user using at least one of the at least one additional protocols through the at least one proxy server, a method of authentication of the at least one user equipment in accordance with the invention includes the first proxy and the at least one additional proxy of the at least one proxy server authenticating requests for data services received from the at least one user equipment for the protocols by using the authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server and providing information to the at least one application server permitting the at least one user to provide final authorization of the at least one user to access the at least one application server or to provide final authorization of an action to be performed for the at least one user by the at least one application server. The at least one proxy server may process the authentication information to provide the information to the at least one application server to permit the at least one application server to provide the final authorization including guaranteeing the identity of the at least one user. The processing of the authentication information to provide the information to the at least one application server may comprise a shared secret known to the at least one proxy server and the at least one application server which guarantees the identity of the at least one user at the at least one application server. The shared

secret may be a shared key pair which is processed by the at least one application server to verify the identity of the user who is to receive access to the at least one application server or for whom the at least one application server is to take action. The coupling of the at least one proxy server to the at least one application server may be via a secure medium. The at least one application server may register data services with the at least one proxy server which the at least one application server may provide to the at least one user through the at least one proxy server; and the at least one proxy server may store an address of each application server that provides data services for selection by the at least one user which is used to connect the at least one user to the at least one application server to obtain selected data services. The at least one proxy server may be an access point in the system for the transmission of data services between the at least one user and the at least one proxy server.

#### 15 BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a block diagram of a system in accordance with the present invention.

#### BEST MODE FOR CARRYING OUT THE INVENTION

20 Fig. 1 illustrates a system 10 which includes conventional SIP entities. The entities include at least one UE 12, S-CSCF 14 and HSS 16. At least one proxy server 18 has resident therein the SIP P-CSCF 19, which is contacted by the UE 12, during sessions requesting data services using the SIP protocol. While a single proxy server 18 is illustrated, it should be understood that the invention may be practiced with more than one proxy server 18, including proxies using authentication information transmitted from the subscriber data server to authenticate sessions for multiple protocols. Authentication of the at least one UE 12 for SIP and additional protocols uses the HSS 16 of the home network 20 which stores at least one user profile of the users of the at least one UE regarding providing sessions of data services. It should be understood that use of SIP in the home network 20 as the source of the authentication information for the other protocols is not required in the practice of the invention with the invention being

applicable to protocols other than SIP. The at least one user profile stored in the HSS 16 includes authentication information. The same stored authentication information is used to authenticate the at least one UE 12 for a session of data services when a request for data services is made using a first protocol, e.g.,  
5 without limitation, the SIP protocol and at least one additional protocol.

The at least one UE 12 requests sessions for data services using the first network protocol e.g. SIP and sessions for data services using at least one additional protocol. The at least one UE 12 stores authentication information for the first  
10 protocol which is transmitted to the at least one proxy server 18 to authenticate the at least one UE 12 for all of the protocols. The HSS 16, without limitation, may utilize the AKA protocol to provide the authentication information in the form of the IK and CK keys as indicated by arrow 30 from the HSS 16 to the P-CSCF 19 and the UE 12 where the authentication information is stored and from the UE to the  
15 P-CSCF as indicated by arrow 40.

The present invention differs from the prior art in that the at least one proxy server 18 includes P-CSCF 19 and RSTP and HTTP proxies 32 and 36 respectively for authenticating the at least one UE 12 to use at least one protocol  
20 in addition to the protocol used by the home network, e.g. SIP, e.g. RTSP and HTTP. In a preferred architecture, a single proxy server 18 is used, but the invention is not limited thereto. In a preferred embodiment, the additional proxies are a RTSP proxy 32 and a HTTP proxy 36 all of which are resident in the at least one proxy server 18. The SIP generated authentication information used by the at  
25 least one UE 12 for the RTSP proxy 32 and HTTP proxy 36 is the same as that used by the P-CSCF 19.

In accordance with the invention, when the at least one UE 12 requests a session of data services, such as IMS, using any protocol other than protocol of the home  
30 network 20, the request is authenticated by using the authentication information provided by the home network, e.g. SIP authentication information IK and CK from the HSS 16. It should be understood that the invention is not limited to the use of

the IK and CK authentication information. Therefore, if the at least one UE 12 requests a session of data services using a protocol other than the protocol used by the home network 20, the authentication information obtained from a subscriber data server and specifically, the HSS 16 of the SIP protocol is used for at least one other protocol. Requests for data services for the at least one additional protocol, for example, RTSP and HTTP protocols are authenticated using the authentication information of the home network 20 stored in the subscriber data server of the home network, e.g. HSS 16.

10 The use of at least one proxy server 18 to provide authentication for at least one UE 12 requesting sessions using multiple protocols by using the authentication information of only one protocol used in the home network 20 saves performing authentication with unique information for each of the protocols as in the prior art. As a result, the prior art requirement of providing distinct authentication  
15 information to authenticate each request for a session of data services by the at least one UE 12 for each additional protocol is simplified since authentication of the UE to use the additional protocols requires use of only the authentication information already provided from the HSS 16 of the home network 20 for the first protocol.

20 A request for a session of data services from the at least one UE 12 is transmitted to the RTSP proxy 32 of the proxy server 18 where the at least one UE12 is authenticated and thereafter is transmitted to RTSP server 34. Similarly, a request for a session of data services from the at least one UE 12 is transmitted to  
25 the HTTP proxy 36 of the proxy server 18 where the at least one UE 12 is authenticated and thereafter is transmitted to the HTTP server 38.

The RTSP and HTTP servers 34 and 38 are connected to the RTSP proxy 32 and the HTTP proxy 36 respectively of the at least one proxy server 18 which  
30 connections are preferably secure. The secure connections avoid message integrity problems and man in the middle attacks. The at least one proxy server 18 and specifically, the RTSP proxy 32 and the HTTP proxy 36 store the



address of each associated application server which are generically represented by the RTSP server 34 and the HTTP server 38 respectively. The routing may be based on the addressing that may embed hierarchical address information in a URL such as http.www.nokia.com/presence/user1 or adding extra functionality to the at least one proxy server 18 that is based on content or proprietary databases containing the addresses of the applications bound to the proxy server. This may be implemented so that the at least one proxy server 18 acts as an entry point for a group of application servers such as, but not limited to the RTSP and HTTP servers 34 and 38 respectively. The at least one proxy server 18 may process the data packets destined for the at least one application server 34 and 38 to strip off the payload and forward the payload over the aforementioned connections. Examples of application servers represented by the generically identified HTTP server 38 without limitation are Presence, Messaging and Conferencing servers used, for example, to perform service management tasks like authorization policy manipulation and member list management which operate in accordance with the HTTP protocol. Examples of application servers represented by the generically identified RTSP server 34 without limitation are real time audio and video streaming applications.

The at least one proxy server 18 provides information to the at least one application server 34 and 38 permitting the at least one application server to provide final authorization of the at least one user of the UE 12 to access the at least one application server or to provide final authorization of an action to be performed for the at least one user by the at least one application server.

In a IMS application, the application server performs most of the authorization of the user of the UE 12 to obtain access to or have a service performed for the UE. The at least one proxy server 18 authenticates the message according to existing IMS specifications and algorithms and passes the result of the authorization to the at least one additional server 34 and 38. The at least one additional server 34 and 38 has the ultimate knowledge of service specific details which are available therefrom to the user of the UE 12 and the final responsibility of authorizing the

user and/or the action to be performed in the specific server. The at least one additional server 34 and 38 has the totality of knowledge of service specific information and other information to process the content received from the at least one proxy 18 over the preferably secure link to authorize the attempted action.

- 5 The ultimate authorization process performed by the at least one additional server 34 and 38 is preferably based upon secret knowledge exchange which may be without limitation the use of shared key pairs.

- 10 While the invention has been described in terms of its preferred embodiments, it should be understood that numerous modifications may be made thereto without departing from the spirit and scope of the present invention. It is intended that all such modifications fall within the scope of the appended claims.

CLAIMS

What is claimed is:

1. A system comprising:
  - 5 a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol;
  - 10 at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user;
  - at least one proxy server, including resident therein a first proxy for  
15 the first protocol and at least one additional proxy for the at least one additional protocol; and wherein  
the first proxy and the at least one additional proxy of the at least one proxy server authenticates requests for data services received from the at least one user equipment for the protocols by using the authentication information  
20 of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server.
- 25 2. A system in accordance with claim 1 wherein;  
the subscriber data server is a home subscriber server (HSS); and  
the first protocol is the Session Initiation Protocol (SIP) and a  
request for data services using SIP is transmitted from a Proxy Call State Control  
Function (P-CSCF) of the at least one proxy server to a Serving Call State Control  
30 Function (S-CSCF) server of the home network.

3. A system in accordance with claim 1 wherein:  
the subscriber data server is a home subscriber server (HSS);  
the first protocol is the Session Initiation Protocol (SIP) and  
5 a request for data data services using SIP is transmitted from a Proxy Call State  
Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server of the home network; and  
the at least one additional network protocol is the Hyper Text  
Transport Protocol (HTTP) and a request for data services using HTTP is  
10 transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one  
proxy server to a HTTP server.
4. A system in accordance with claim 1 wherein:  
the subscriber data server is a home subscriber server (HSS);  
15 the first protocol is the Session Initiation Protocol (SIP) and  
a request for data services using SIP is transmitted from a Proxy Call State  
Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server; and  
the at least one additional protocol is the Real-Time Streaming  
20 Protocol (RTSP) and a request for data services is transmitted from a Hyper Text  
Transport Protocol (HTTP) proxy of the at least one proxy server to a RTSP  
server.
5. A system in accordance with claim 1 wherein:  
25 the subscriber data server is a home subscriber server (HSS);  
the first protocol is the Session Initiation Protocol (SIP) and  
a request for data services using SIP is transmitted from a Proxy Call State  
Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server of the home network; and  
30 the at least one additional protocol is the Hyper Text Transport  
Protocol (HTTP) and the Real-Time Streaming Protocol (RTSP) and a request for  
data services using HTTP is transmitted from a Hyper Text Transport Protocol

(HTTP) proxy of the at least one proxy server to a HTTP server and a request for data services using RTSP is transmitted from a Real-Time Streaming Protocol (RTSP) proxy of the at least one proxy server to a RTSP server.

5           6.       A system in accordance with claims 1-5 wherein:

                  the authentication information transmitted from the subscriber data server to the at least one proxy server comprises an integrity key IK and a cipher key CK and the authentication information transmitted from the at least one user equipment to the at least one proxy sever comprises an integrity key IK and a  
10       cipher key CK which keys are processed by the at least one proxy server to determine if the at least one user is authentic.

                  7.       A system in accordance with claim 6 wherein:

                  the authentication information transmitted from the subscriber data  
15       server and the at least one user equipment is generated using the Authentication and Key Agreement (AKA) protocol.

                  8.       In a system comprising a home network including a subscriber data server which stores at least one user profile regarding providing of data services  
20       to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol and at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing  
25       authentication information which is used when a request for data services is made to authenticate the at least one user, at least one proxy server including resident therein a first proxy for the first network protocol and at least one additional proxy for the at least one additional protocol, a method of authentication of the at least one user equipment comprising:

30               the first proxy and the at least one additional proxy of the at least one proxy server authenticates requests for data services received from the at least one user equipment for the protocols by using the authentication information

of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server.

5

9. A method in accordance with claim 8 wherein:  
the subscriber data server is a home subscriber server (HSS); and  
the first protocol is the Session Initiation Protocol (SIP) and  
any request for data services using SIP is transmitted from a Proxy Call State  
10 Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server of the home network.

10. A method in accordance with claim 8 wherein:  
the subscriber data server is a home subscriber server (HSS);  
15 the first protocol is the Session Initiation Protocol (SIP) and  
a request for data data services using SIP is transmitted from a Proxy Call State  
Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server of the home network; and  
the at least one additional network protocol is the Hyper Text  
20 Transport Protocol (HTTP) and a request for data services using HTTP is  
transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least  
one proxy server to a HTTP server.

11. A method in accordance with claim 8 wherein:  
25 the subscriber data server is a home subscriber server (HSS);  
the first protocol is the Session Initiation Protocol (SIP) and  
a request for data services using SIP is transmitted from a Proxy Call State  
Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server; and  
30 the at least one additional protocol is the Real-Time Streaming  
Protocol (RTSP) and a request for data services is transmitted from a Hyper Text

Transport Protocol (HTTP) proxy of the at least one proxy server to a RTSP server.

12. A method in accordance with claim 8 wherein:
- 5 the subscriber data server is a home subscriber server (HSS);  
the first protocol is the Session Initiation Protocol (SIP) and  
a request for data services using SIP is transmitted from a Proxy Call State  
Control Function (P-CSCF) of the at least one proxy server to a Serving Call State  
Control Function (S-CSCF) server of the home network; and
- 10 the at least one additional protocol is the Hyper Text Transport  
Protocol (HTTP) and the Real-Time Streaming Protocol (RTSP) and a request for  
data services using HTTP is transmitted from a Hyper Text Transport Protocol  
(HTTP) proxy of the at least one proxy server to a HTTP server and a request for  
data services using RTSP is transmitted from a Real-Time Streaming Protocol
- 15 (RTSP) proxy of the at least one proxy server to a RTSP server.

13. A method in accordance with claims 8-12 wherein:
- the authentication information transmitted from the subscriber data  
server to the at least one proxy server comprises an integrity key IK and a cipher
- 20 key CK and the authentication information transmitted from the at least one user  
equipment to the at least one proxy sever comprises an integrity key IK and a  
cipher key CK which keys are processed by the at least one proxy server to  
determine if the at least one user is authentic.

- 25 14. A method in accordance with claim 13 wherein:
- the authentication information transmitted from the subscriber data  
server and the at least one user equipment is generated using the Authentication  
and Key Agreement (AKA) protocol.

15. In a system comprising a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol and at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user, at least one proxy server comprising:
- 10 a first proxy for the first protocol and at least one additional proxy for the at least one additional protocol which are resident therein; and wherein
- the at least one proxy server authenticates requests for data services received from the at least one user equipment for the protocols by using the authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server.
- 15
16. A proxy server in accordance with claim 15 wherein;
- the subscriber data server is a home subscriber server (HSS); and
- the first protocol is the Session Initiation Protocol (SIP) and any request for data services using SIP is transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network.
- 20
17. A proxy server in accordance with claim 15 wherein;
- the subscriber data server is a home subscriber server (HSS); and
- the first protocol is the Session Initiation Protocol (SIP) and a request for data data services using SIP is transmitted from a Proxy Call State Control Function (P-CSCF) of the at least one proxy server to a Serving Call State Control Function (S-CSCF) server of the home network; and the at least one
- 25
- 30



additional network protocol is the Hyper Text Transport Protocol (HTTP) and a request for data services using HTTP is transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one proxy server to a HTTP server.

5           18.    A proxy server in accordance with claim 15 wherein:  
                  the subscriber data server is a home subscriber server (HSS); and  
                  the first protocol is the Session Initiation Protocol (SIP) and a  
request for data services using SIP is transmitted from the at least one proxy  
server to a Serving Call State Control Function (S-CSCF) server, and the at least  
10   one additional protocol is the Real-Time Streaming Protocol (RTSP) and a request  
for data services is transmitted from a Real-Time Streaming Protocol (RTSP)  
proxy of the at least one proxy server to a RTSP server.

              19.    A proxy server in accordance with claim 15 wherein:  
15                   the subscriber data server is a home subscriber server (HSS); and  
                  the first protocol is the Session Initiation Protocol (SIP) and a  
request for data services using SIP is transmitted from a Proxy Call State Control  
Function (P-CSCF) of the at least one proxy server to a Serving Call State Control  
Function (S-CSCF) server of the home network, and the at least one additional  
20   protocol is the Hyper Text Transport Protocol (HTTP) and the Real-Time  
Streaming Protocol (RTSP) and a request for data services using HTTP is  
transmitted from a Hyper Text Transport Protocol (HTTP) proxy of the at least one  
proxy server to a HTTP server and a request for data services using RTSP is  
transmitted from a Real-Time Streaming Protocol (RTSP proxy of the at least one  
25   proxy server to a RTSP server.

              20.    A proxy server in accordance with claims 15-19 wherein:  
                  the authentication information transmitted from the subscriber data  
server to the at least one proxy server comprises an integrity key IK and a cipher  
30   key CK and the authentication information transmitted from the at least one user  
equipment to the at least one proxy sever comprises an integrity key IK and a

cipher key CK which keys are processed by the at least one proxy server to determine if the at least one user is authentic.

21. A proxy server in accordance with claim 20 wherein:  
5 the authentication information transmitted from the subscriber data server and the at least one user equipment is generated using the Authentication and Key Agreement (AKA) protocol.
22. A system comprising:  
10 a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol;  
15 at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user;  
at least one proxy server, including resident therein a first proxy for  
20 the first protocol and at least one additional proxy for the at least one additional protocol;  
at least one application server coupled to the at least one proxy server, each application server providing data services to the at least one user using at least one of the at least one additional protocols through the at least one  
25 proxy server;  
the first proxy and the at least one additional proxy of the at least one proxy server authenticating requests for data services received from the at least one user equipment for the protocols by using the authentication information of the at least one profile which is transmitted from the subscriber data server to  
30 the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server and provides information to the at least one application server permitting

the at least one application server to provide final authorization of the at least one user to access the at least one application server or to provide final authorization of an action to be performed for the at least one user by the at least one application server.

5

23. A system in accordance with claim 22 wherein:  
the at least one proxy server processes the authentication information to provide the information to the at least one application server to permit the at least one application server to provide the final authorization  
10 including guaranteeing the identity of the at least one user.

24. A system in accordance with claim 23 wherein:  
the processing of the authentication information to provide the information to the at least one application server comprises a shared secret  
15 known to the at least one proxy server and to the at least one application server which guarantees the identity of the at least one user at the at least one application server.

25. A system in accordance with claim 24 wherein:  
20 the shared secret is a shared key pair which is processed by the at least one application server to verify the identity of the user who is to receive access to the at least one application server or for whom the at least one application server is to take action.

25 26. A system in accordance with claim 22 wherein:  
coupling of the at least one proxy server to the at least one application server is via a secure medium.

27. A system in accordance with claim 22 wherein:  
30 the at least one application server registers data services with the at least one proxy server which the at least one application server may provide to the at least one user through the at least one proxy server; and

the at least one proxy server stores an address of each application server that provides data services for selection by the at least one user which is used to connect the at least one user to the at least one application server to obtain selected data services.

5

28. A system in accordance with claim 22 wherein:

the at least one proxy server is an access point in the system for the transmission of data services between the at least one user and the at least one proxy server.

10

29. In a system comprising a home network including a subscriber data server which stores at least one user profile regarding providing of data services to at least one user with the profile including authentication information used to authenticate the at least one user of the data services when a request for data services is made using a first protocol and at least one user equipment which requests data services using the first network protocol and data services using at least one additional protocol, the at least one user equipment storing authentication information which is used when a request for data services is made to authenticate the at least one user, at least one proxy server including resident therein a first proxy for the first network protocol and at least one additional proxy for the at least one additional protocol, and at least one application server coupled to the at least one proxy server, each application server providing data services to the at one user using at least one of the at least one additional protocols through the at least one proxy server, a method of authentication of the at least one user equipment comprising:

25

the first proxy and the at least one additional proxy of the at least one proxy server authenticating requests for data services received from the at least one user equipment for the protocols by using the authentication information of the at least one profile which is transmitted from the subscriber data server to the at least one proxy server and the authentication information of the at least one user transmitted from the at least one user equipment to the at least one proxy server and providing information to the at least one application server permitting

30

the at least one user to provide final authorization of the at least one user to access the at least one application server or to provide final authorization of an action to be performed for the at least one user by the at least one application server.

5.

30. A method in accordance with claim 29 wherein:

the at least one proxy server processes the authentication information to provide the information to the at least one application server to permit the at least one application server to provide the final authorization including guaranteeing the identity of the at least one user.

10

31. A method in accordance with claim 30 wherein:

the processing of the authentication information to provide the information to the at least one application server comprises a shared secret known the at least one proxy server and the at least one application server which guarantees the identity of the at least one user at the at least one application server.

15

32. A method in accordance with claim 31 wherein:

the shared secret is a shared key pair which is processed by the at least one application server to verify the identity of the user who is to receive access to the at least one application server or for whom the at least one application server is to take action.

20

33. A method in accordance with claim 29 wherein:

coupling of the at least one proxy server to the at least one application server is via a secure medium.

25

34. A method in accordance with claim 39 wherein:

the at least one application server registers data services with the at least one proxy server which the at least one application server may provide to the at least one user through the at least one proxy server; and

30

the at least one proxy server stores an address of each application server that provides data services for selection by the at least one user which is used to connect the at least one user to the at least one application server to obtain selected data services.

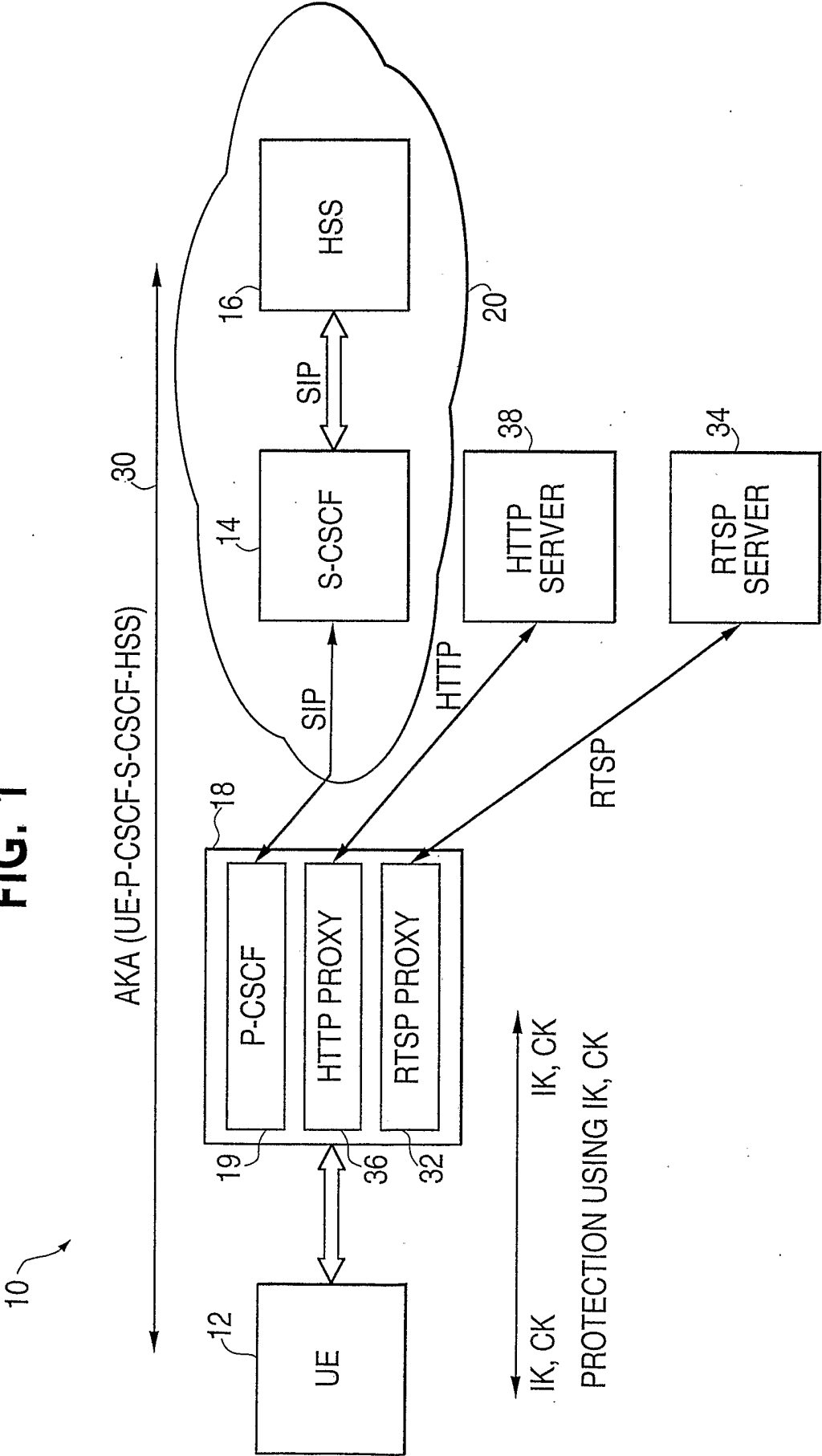
5

35. A method in accordance with claim 29 wherein:

the at least one proxy server is an access point in the system for the transmission of data services between the at least one user and the at least one proxy server.

10

FIG. 1



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB03/01174

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(7) : G06F 15/16, 15/173

US CL : 709/201, 203, 219, 225, 230

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)

U.S. : 709/201, 203, 219, 225, 230

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
Please See Continuation Sheet**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,958,016 A (CHANG et al) 28 September 1999, column 4, line 45 - column 6, line 37.	1-35
Y,P	US 2002/0151312 A1 (ROSEMARIJN BOS et al), OCTOBER 17, 2002 page 1 and pages 4-5.	1-35
Y,P	US 2002/0147845 A1 (SANCHEZ-HERRERO et al), pages 1-2. OCTOBER 10, 2002	1-35



Further documents are listed in the continuation of Box C.



See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent 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

"&amp;"

document member of the same patent family

Date of the actual completion of the international search

28 July 2003 (28.07.2003)

Date of mailing of the international search report

19 AUG 2003

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Paul H Kang

Telephone No. (703) 305-3900



# INTERNATIONAL SEARCH REPORT

PCT/IB03/01174

**Continuation of B. FIELDS SEARCHED Item 3:**  
EAST  
search terms: subscriber, server, SIP, HSS, CSCF