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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/19018 A1

(51) International Patent Classification[7]: H04L 9/32, G06F 13/368

(21) International Application Number: PCT/NO00/00287

(22) International Filing Date:
4 September 2000 (04.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
19994334 6 September 1999 (06.09.1999) NO

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RÆSTAD, Atle** [NO/NO]; Nygaard, N-1798 Aremark (NO). **BACH CORNELIUSSEN, Knut, Snorre** [NO/NO]; Bygdøy Allé 117 A, N-0273 Oslo (NO). **AARVAAG, Dagfinn** [NO/NO]; Kampheimveien 19, N-0685 Oslo (NO). **IVELAND, Espen** [NO/NO]; Rings Gate 6, N-3045 Drammen (NO).

(74) Agent: **WESMANN, Johan, Fredrik**; Bryns Patentkontor A/S, P.O. Box 765, Sentrum, N-0106 Oslo (NO).

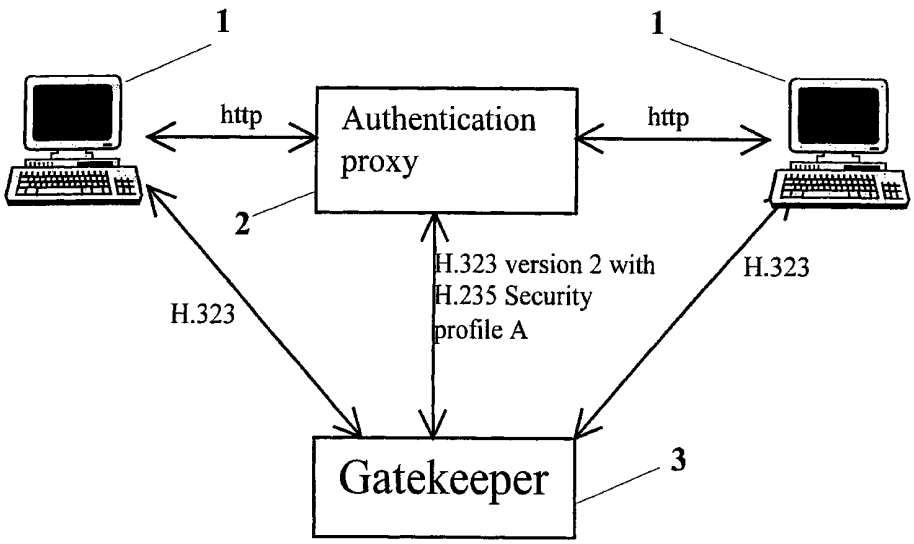
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

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.

(54) Title: SECURITY WITH AUTHENTICATION PROXY



(57) Abstract: An arrangement to accomplish authentication of end-users (1) and end-points (1) in a packet based network, which includes components that support all or parts of different versions of the H.323 recommended standard, be proposed. Authentication is accomplished by means of an authentication proxy (2), which will support security profiles supported by one or more associated gatekeepers (3). Provision of end-user (1) and end-point information for an authentication proxy (2) may be accomplished by means of standard non-proprietary communication and protocol such as http or https and a simple html form, an applet or a servlet respectively, and for a gatekeeper (3) by means of an RAS message such as gatekeeper request (GRQ).

WO 01/19018 A1

Security with authentication proxy

Field of invention.

The present invention relates to the field of audio, video and data communications across packet based networks, particularly to authentication of end-users and end-points in networks complying with the H.323 specification of the International Telecommunications Union.

The problem areas.

The ITU-T recommendation H.235 of the International Telecommunications Union recommends a standard for security and encryption for multimedia terminals complying with the H-Series recommendations (H.323 and other H.235-based) of International Telecommunications Union. H.235 is a new feature in version 2 (H.323v2) of the H.323 recommendation. It adds various security mechanisms like authentication and integrity checks to the recommended standard H.323. In version 1 (H.323v1) of the H.323 there were no security mechanisms, and the network had to trust that the end-users were who they claimed to be. This constitutes a problem when end-users have their own confidential profiles in the system including a set of supplementary services. End-user authentication is also a pre-requisite when billing the end-user for the H.323 traffic, and when building virtual private networks on the H.323 network.

Even though the use of H.235 looks promising, some major problems remain to be solved. One problem is that there is a wide use of H.323 version 1 end-points in use. As stated above, only end-points complying with H.323v2 can support H.235. Another problem is that very few of the end-points complying with H.323v2 that are on the marked today support H.235. Both of these problems need to be solved in an H.323 network which base its logic on authenticated end-users.

Another problem area is H.235 itself, since it is very generic and needs a security profile to be applied. In a network it is likely that many different security profiles will be in use by different end-points. When security profiles are different, conversion of one security profile to another security profile cannot be made since the security profiles generally will perform different hash function on different data. As a consequence it is not practical for the H.323 network components to support all security profiles.

An example to illustrate the problem with two clients with different security profiles is shown in fig 1. In this example the gatekeeper (3) needs to support both security profiles to be able to authenticate both end-users (1) using the two H.323 clients.

Known Solutions and problems with these.

One solution to the problems with H.235 is to not base the authentication on H.235 at all, and use a proprietary protocol for end-user (1) authentication. This in turn leads to two problems:

1) The end-user (1) has to start two programs, the authentication client, and the H.323 client when using the H.323 network even though the H.323 client is a version 2 client with H.235 support.

2) The H.323 network has to support a new proprietary protocol in addition to H.323.

Another known solution is to apply the IMTC Security Profile 1 (SP1) proposed by the International Multimedia Teleconferencing Consortium. It is however focused on message by message authentication and integrity, and has not made a clear distinction between user authentication and message integrity.

Objects of the invention

Accordingly, it is an object of the present invention to provide an arrangement in a H.323 network that will allow authentication of end-points that comply with H.323v1.

Another object of the present invention is to provide an arrangement in a H.323 network, which will allow authentication of end-points that comply with H.323v2 but do not support H.235.

A further object of the present invention is to provide an arrangement in a H.323 network, which will allow authentication of end-users (1) clients with different security profiles.

Brief description of the invention

The above objects are met in an arrangement provided by the present invention, wherein an authentication proxy is provided and a gatekeeper supports a security profile used by an authentication proxy.

Description of the drawings:

Fig 1 shows how the registration procedure is performed according to prior art when two end-points that supports either H.323v1 or H.323v2 without support for H.235 perform a registration towards a gatekeeper. In this scenario the Gatekeeper has to trust the end-points to be who they claim to be since no authentication actions are supported.

Fig. 2 shows an example of a prior art arrangement in which the gatekeeper (3) encounters different clients with different security profiles. The registration is following the same procedural flow as shown in Figure 1 (but now with H.235). In this arrangement the gatekeeper has to support all the different profiles used by the registering end-points. This constitutes a problem because the gatekeeper is a traffical node, and supporting several different profiles will slow down its normal operations.

Fig. 3 shows an example of signal flow of an arrangement according to the invention.

Fig 4 shows an example of a sequence of signal flow of an arrangement according to the invention including the messages sent between the different entities. In this sequence, a one-stage authentication scheme is shown.

Fig 5 shows an example of a sequence of signal flow of an arrangement according to the invention including the messages sent between the different entities. In this sequence, a two-stage authentication scheme is shown, this is called challenge/response scheme.

Fig 6 shows how an applet can be received from the authentication proxy. It is not necessary that the applet is received from the authentication proxy; it can be received from any other entity as long as it sends the http-request with username and password to the authentication proxy. Because the security aspects on the client becomes simpler (it is not an absolute requirement that the applet is signed) when the applet is received from the authentication proxy, this scenario will be used hereinafter.

Fig 7 shows a block diagram for the authentication proxy with a numbered signalling flow for a simple authentication scheme (no challenge/response). If a

challenge/response scheme is used, then the signalling flow must be extended between point 9 and 10 according to figure 5.

Fig. 8 shows a schematic representation of an embodiment example of a sequence of signal flow in an arrangement according to the invention.

Detailed description of embodiments.

In the following, by way of example the present invention will be described in more detail.

Referring to fig. 7, an example of an embodiment of the present invention is shown. All information the authentication proxy needs, will be requested from the end-user (1) through standard http communication or any other suitable protocol.

In the following, only for the purpose of explaining the present invention the protocol used will be http.

The end-user (1) could be presented a simple html form, an applet (that can be signed), a servlet or likewise for providing his/her user name and password. This is shown in step 1 and 2 in figure 7. If an applet is used it should be signed, so that the end-user can be sure of the origin of the applet. The applet must be signed if it is received from another entity than the authentication proxy. The reason is that most environments that execute applets do not allow applets to communicate with other entities than their origin unless they are signed.

The hashing described in the H.235 security profile should be done by the applet if an applet is used. If the hashing is not performed by the applet (e.g. according to fig 7.), or something else than an applet is used, the communication protocol should instead be SSL, i.e. https instead of http. The reason for adding a secure socket layer for http is that this will avoid the username and password to travel unsecured across the network. The hashing will then be performed in the authentication proxy, and the username and password will be secured all the way to the gatekeeper. In scenarios when end-point supports H.235 but with different security profiles (see fig 2) the authentication proxy can be used for converting between different security profiles (as shown in fig 3). This is beneficial because it keeps the complexity of understanding different security profiles away from the gatekeeper.

Referring to fig. 7, signal flow is explained in the following by way of example. When the authentication proxy (2) receives the information from the user over http, https or other standard protocols, it generates a standard RAS message such as a H.323v2 GRQ (gatekeeper Request), which holds the H.235 data. This is sent directly to a gatekeeper (3) according to H.323v2, where the actual authentication is done. The gatekeeper then checks the username and password, and sends back a GCF. A GRJ is sent back if the username and password does not match. When the authentication proxy receives the GCF, it will send an http-response to the client (step 12). If the authentication proxy receives a GRJ it will inform the end-point of the unsuccessful authentication attempt in the http-response. If challenge/response authentication is used, the authentication proxy will wait for an RRQ and a retrieval of an RCF before it sends the http response back to the user (see fig 7).

The H.323 client can now register with the gatekeeper (3) in a normal way by sending GRQ and RRQ. The gatekeeper (3) will know when it receives the GRQ and RRQ that the user/end-point (1) already is authenticated based on the user name, the Internet Protocol (IP)-address or both.

To avoid problems in the gatekeeper (3) when receiving two GRQ's (one from the proxy (2) and one from the end-point (1)), the authentication proxy can answer GRQ's sent from end-points (1) complying with H.323v1 and end-points (1) complying with H.323v2 without H.235 support directly (This is not shown in figure 8). Because the gatekeeper (3) will only receive H.323v2 GRQ's when this feature is added, the gatekeeper (3) can not, based on the GRQ, decide which version of the H.323 the various end-points (1) are complying with. The Gatekeeper (3) should instead base it decision on the received RRQs or other suitable RAS messages from endpoints. If this scenario is used together with challenge/response authentication. The RRQ must also be sent to the authentication proxy (see figure 7). Because of the nature of H.323, this scenario implies that all further RAS signalling has to go through the authentication proxy.

The authentication proxy can be placed anywhere in the network. In some networks where a firewall is present between the client and the gatekeeper, it can be wise to place the authentication proxy in De-Militarised Zone (DMZ). This misses because it is sometimes difficult to let an SSL stream pass through a firewall.

Patent claims

1.
An arrangement for audio, video, and data communications across packet based networks implementing the H.323 standard recommended by the International Telecommunications Union, the arrangement including one ore more gatekeepers (3), characterised in
that end-user (1) authentication is performed by means of an authentication proxy (2).

2.
An arrangement according to claim 1, characterised in
that a security profile used by an authentication proxy (2) is supported by a gatekeeper (3) associated with said authentication proxy (2).

3.
An arrangement according to claim 1 or 2, characterised in
that end-user information needed by an authentication proxy (2) is requested from the end-user (1) by means of a non-proprietary communications protocol.

4.
An arrangement according to claim 1, 2 or 3, characterised in
that an authentication proxy (2) communicates information to a gatekeeper (2) by means of a H.323 version 2 RAS message.

5.
An arrangement according to claim 3, characterised in
that a non-proprietary communications protocol is selected form a group of non-proprietary protocols comprising http and https.

6.
An arrangement according to claim 1 or 2, characterised in
that information for end-user (1) authentication is provided by the end-user (1) by means of a html form, an applet or a servlet.

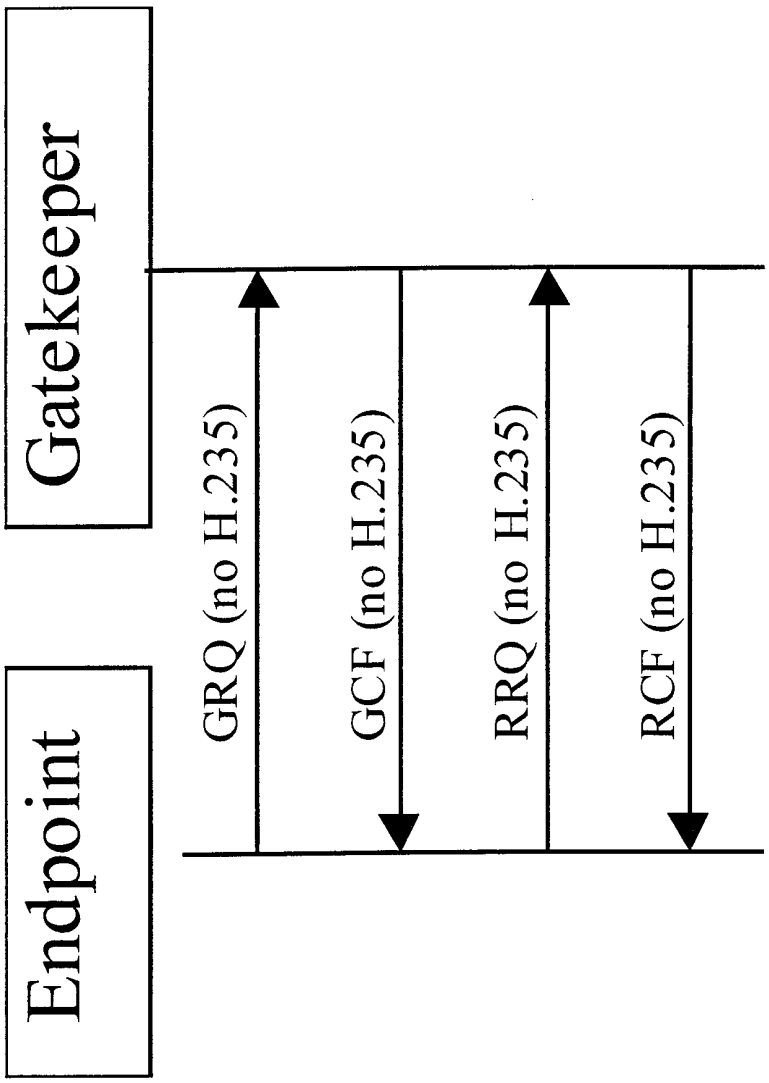
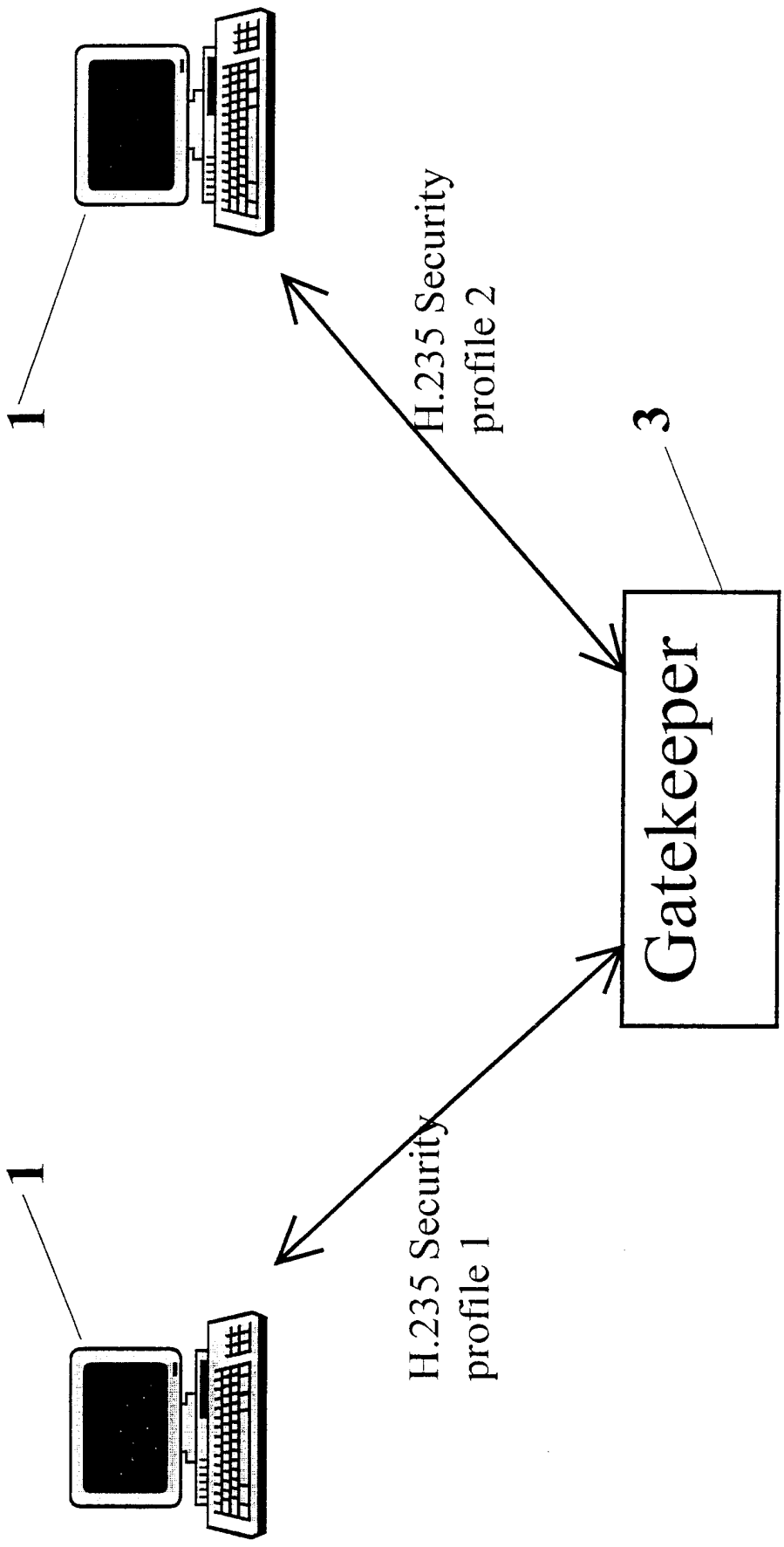

Endpoint
Gatekeeper
GRQ (no H.235)
GCF (no H.235)
RRQ (no H.235)
RCF (no H.235)

Fig. 1



PRIOR ART

Fig. 2

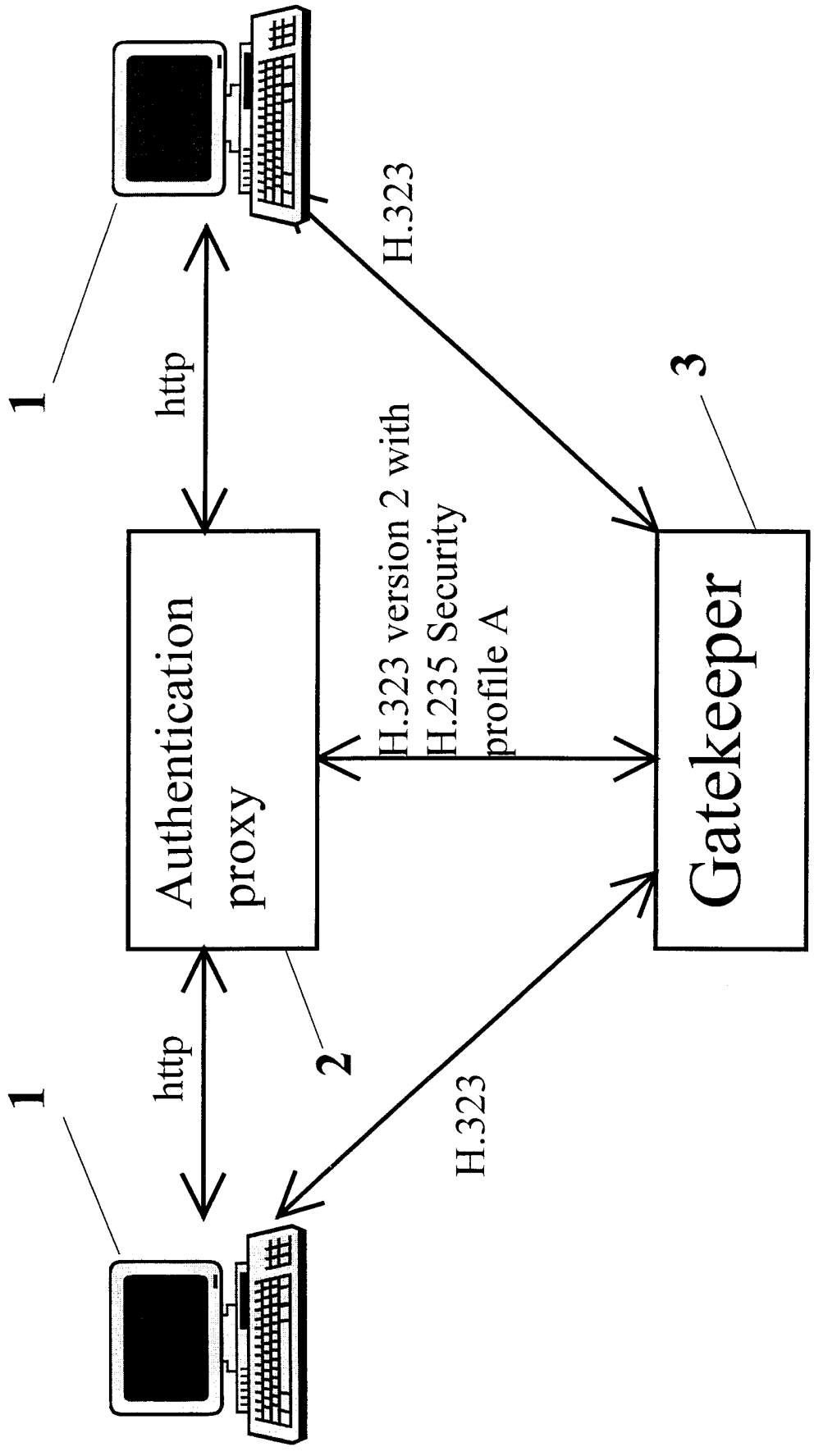

1
http
H.323
3
Authentication proxy
H.323 version 2 with H.235 Security profile A
Gatekeeper
1
http
2
H.323

Fig. 3

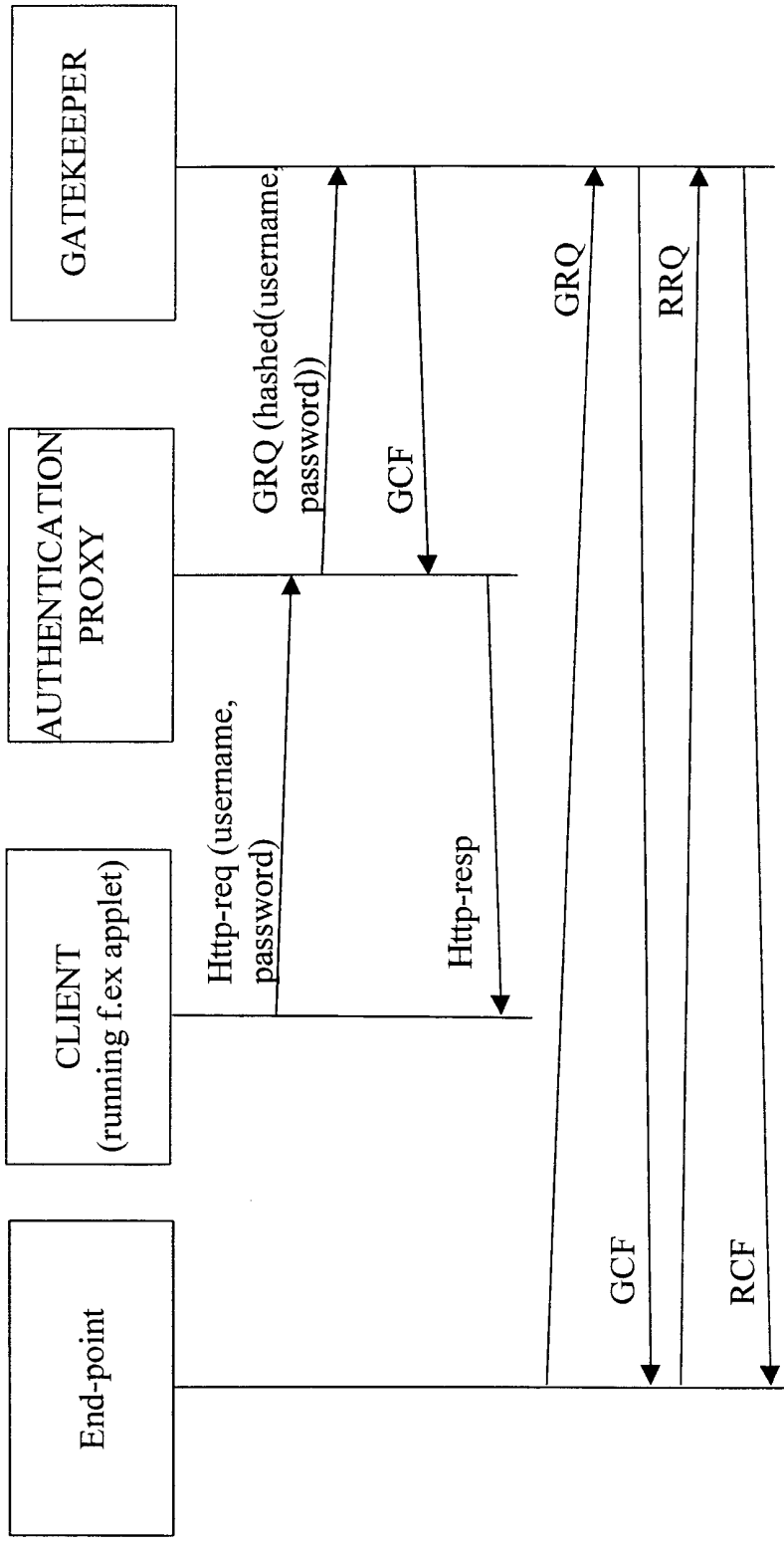

GATEKEEPER
AUTHENTICATION PROXY
CLIENT (running f.ex applet)
End-point
GRQ (hashed(username, password))
GCF
Http-req (username, password)
Http-resp
GRQ
RRQ
GCF
RCF

Fig. 4

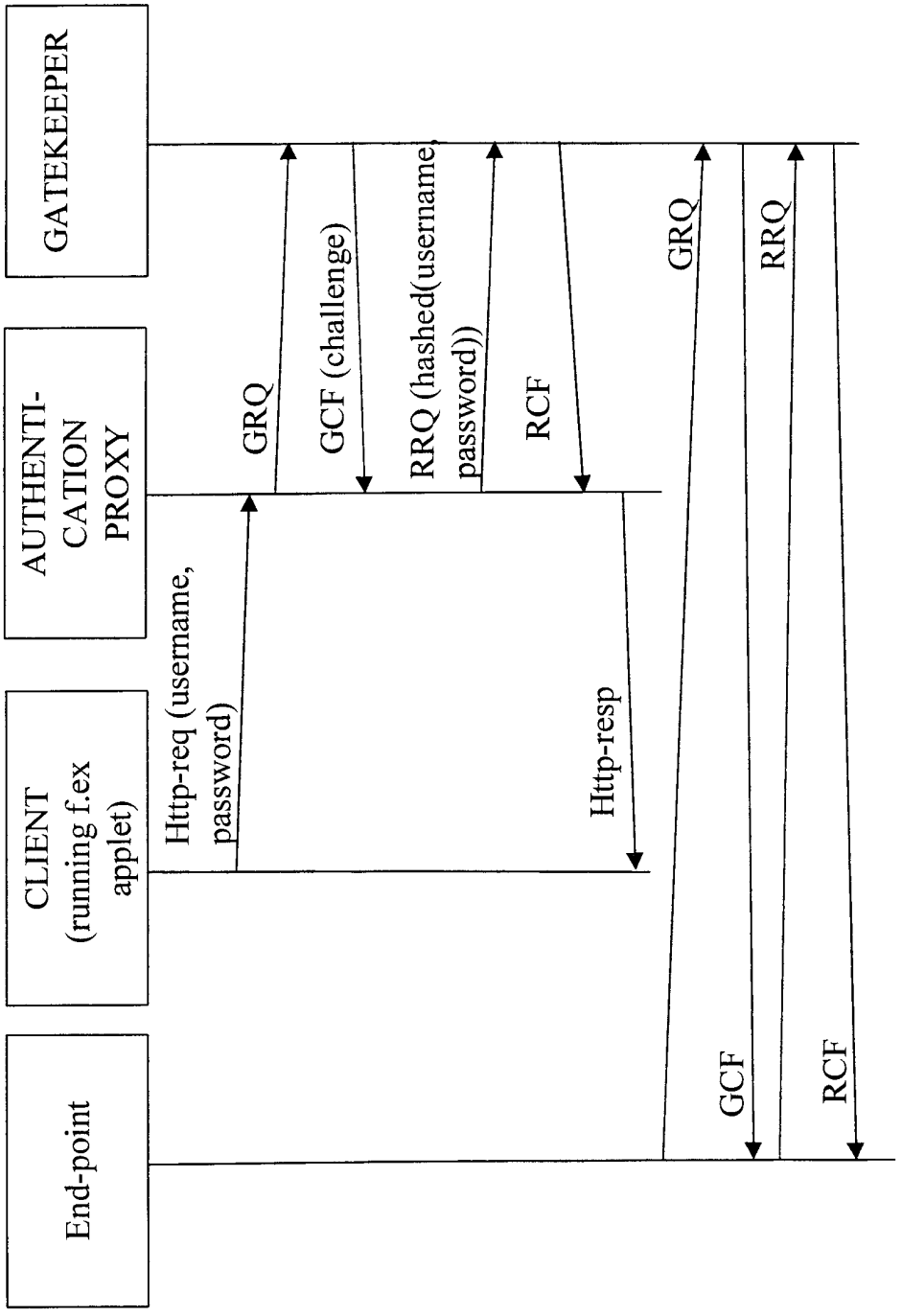

End-point
CLIENT (running f.ex applet)
AUTHENTI-CATION PROXY
GATEKEEPER
Http-req (username, password)
GRQ
GCF (challenge)
RRQ (hashed(username, password))
RCF
Http-resp
GRQ
RRQ
GCF
RCF

Fig. 5

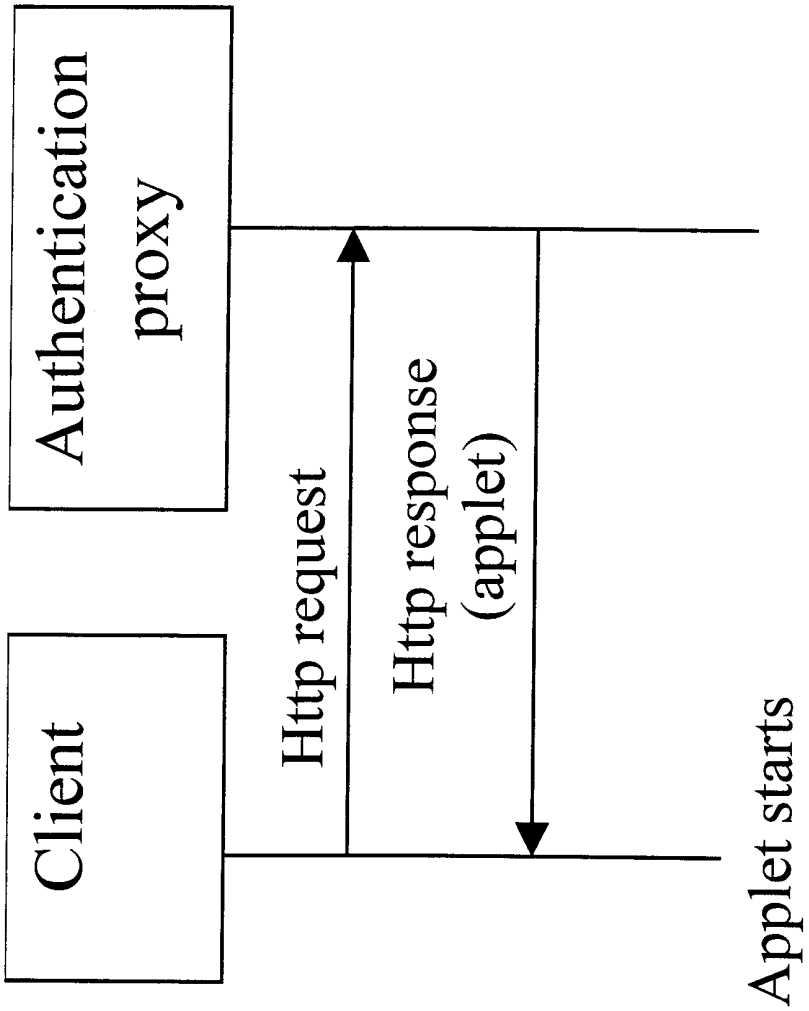

Client
Authentication proxy
Http request
Http response (applet)
Applet starts

Fig. 6

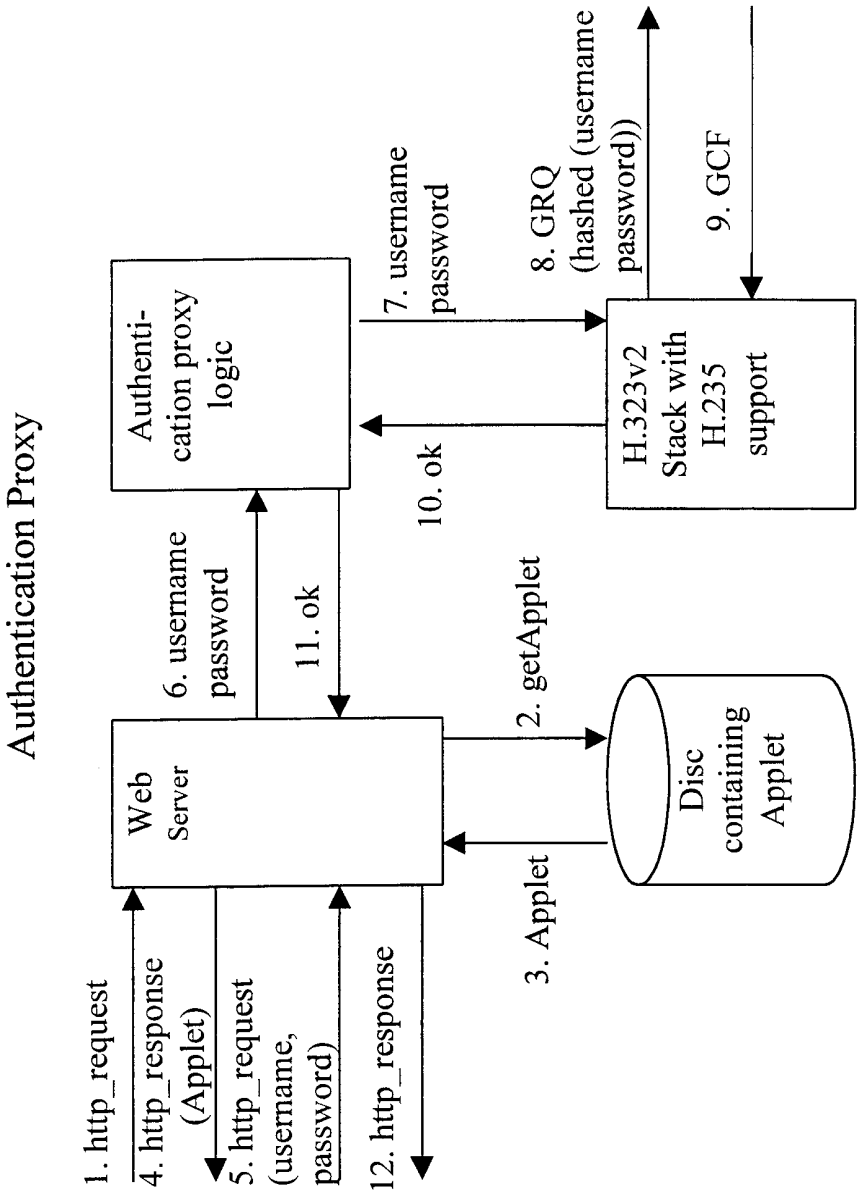

Authentication Proxy
Web Server
Authenti-cation proxy logic
H.323v2 Stack with H.235 support
Disc containing Applet
1. http_request
2. getApplet
3. Applet
4. http_response (Applet)
5. http_request (username, password)
6. username password
7. username password
8. GRQ (hashed (username password))
9. GCF
10. ok
11. ok
12. http_response

Fig. 7

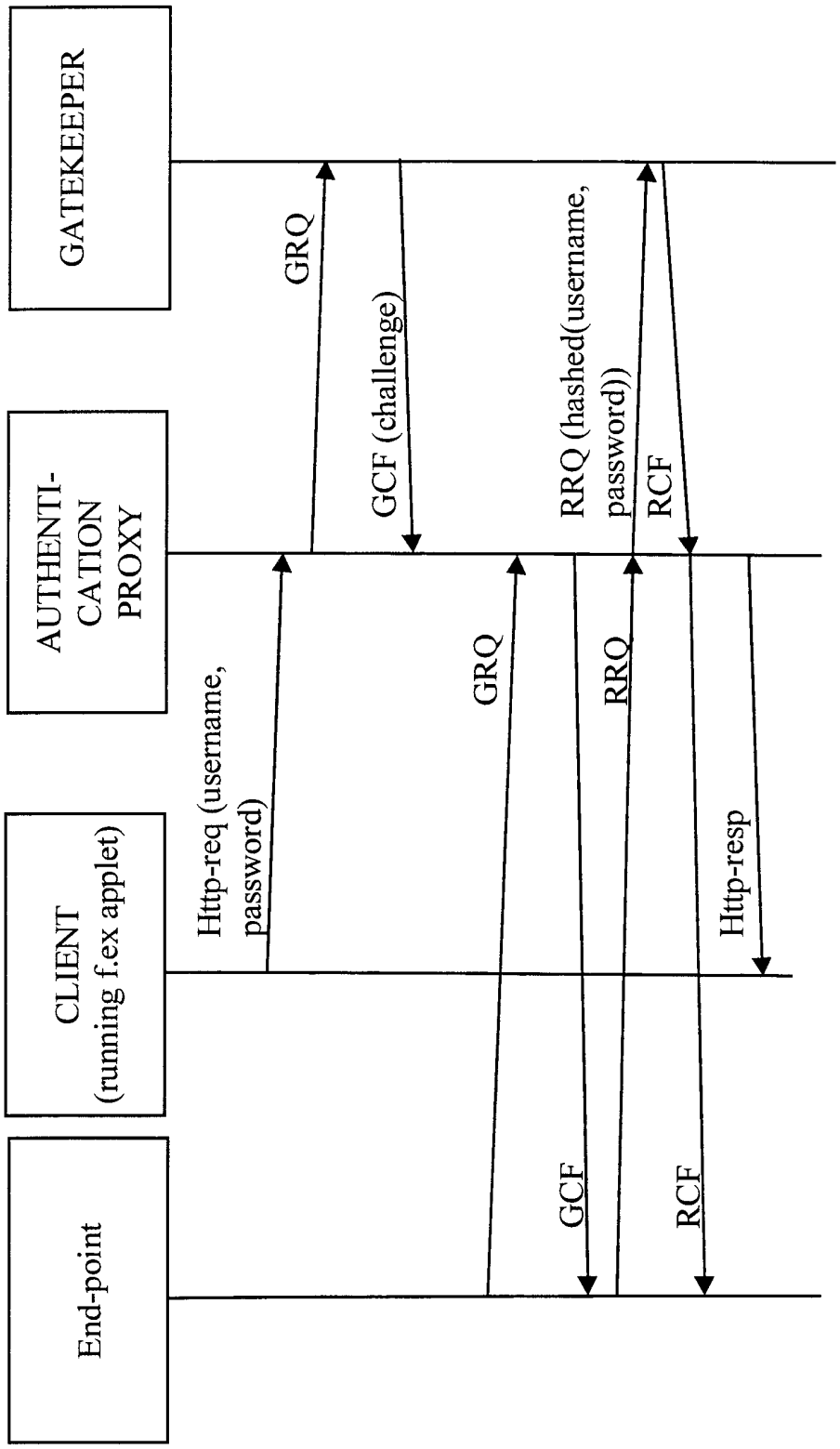

GATEKEEPER
AUTHENTI-CATION PROXY
CLIENT (running f.ex applet)
End-point
GRQ
GCF (challenge)
RRQ (hashed(username, password))
RCF
Http-req (username, password)
GRQ
RRQ
Http-resp
GCF
RCF

Fig. 8

Abbreviation / Term	Description
Hashing	Performing hashing means to code a text or data according to a specific algorithm. The hashed text or data can only de decoded by entities that knows the original hashing function
Proxy	By proxy is meant a function that is not taking active part (not an originating or terminating signalling or media entity) in any communication, the proxy is only helping out by doing small enhancements or other functions.
Endpoint	By endpoint is meant an entity that either originates or terminates signalling (H.323) and media (RTP/RTCP)
RTP	Real Time Protocol as described in RFC 1889
RTCP	Real Time Control Protocol, described in RFC 1889
End-user	The person that uses the End-point.
Authentication	The procedure to check the identity of end-users. Unlike a login procedure, which is combined with a logout, authentication is a one step function
SSL	Secure Socket Layer
RAS	Registration, Admission and Signalling
Security profile	A security profile defines which data should be hashed, and according to which function the data should be hashed.
Applet	An applet is a program that is transferred from a server to an end-user terminal (e.g a computer) and executed at the end-user terminal.
Http	Hyprt Text Transport Protocol
Firewall	An entity that is placed between a Local network and the outside network. The main object for the firewall is to prevent certain types of traffic to pass from the outside network to the inside.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00287

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32, G06F 13/368
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)

IPC7: H04L, G06F

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5586260 A (W-M HU), 17 December 1996 (17.12.96), abstract --	1-6
Y	International Telecommunication Union, ITU-T Recommendation H.323, "Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service", see page 31-32, chapter 7.2.1 --	1-6
P,A	US 5913025 A (DEEANNE BARKER HIGLEY ET AL.), 15 June 1999 (15.06.99), abstract --	

[X] Further documents are listed in the continuation of Box C. [X] 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 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	Date of mailing of the international search report
7 December 2000	12 -12- 2000
Name and mailing address of the ISA Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00287

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0503765 A2 (INTERNATIONAL COMPUTER LIMITED), 16 Sept 1992 (16.09.92), abstract -- --------	1-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/11/00

International application No.
PCT/NO 00/00287

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5586260 A	17/12/96	NONE	
US 5913025 A	15/06/99	NONE	
EP 0503765 A2	16/09/92	DE 69226386 D,T	25/03/99
		GB 9104909 D	00/00/00
		GB 9203166 D	00/00/00
		JP 5081204 A	02/04/93
		US 5220603 A	15/06/93
		ZA 9201425 A	25/11/92