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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 April 2011 (07.04.2011)

PCT

(10) International Publication Number
WO 2011/038752 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 17/30* (2006.01)
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/EP2009/062606

(22) International Filing Date:
29 September 2009 (29.09.2009)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SEIDL, Robert** [DE/DE]; Laurenziweg 5, 82549 Königsdorf (DE). **ABENDROTH, Joerg** [DE/DE]; Weidener Str. 3, 81737 München (DE). **MEYER, Gerald** [DE/DE]; Sandbergstr. 19 B, 82178 Puchheim-Bhf (DE). **BAUER-HERMANN, Markus** [DE/DE]; Hofmarkstrasse 37, 94529 Aicha v.W. (DE).

(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR/Patent administration, 80240 Munich (DE).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: AUTHENTICATION GATEWAY

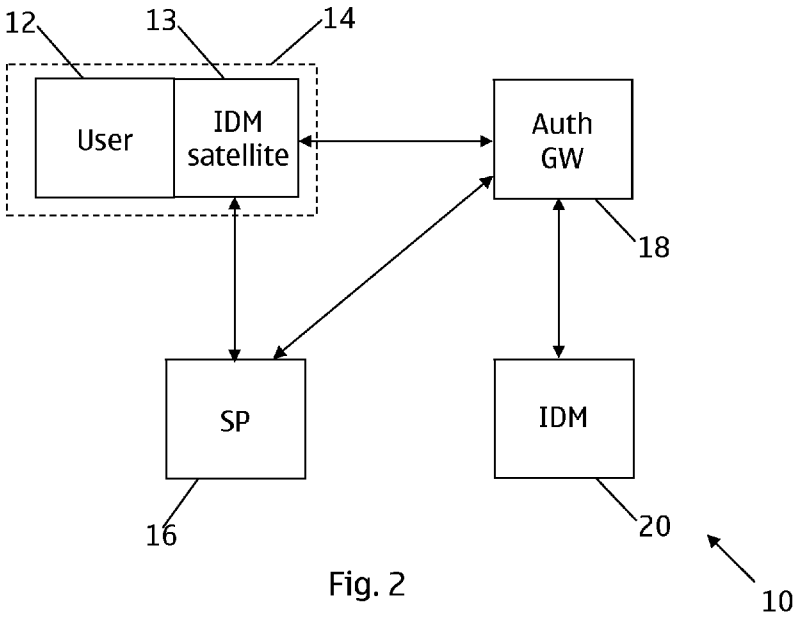


Fig. 2

(57) Abstract: An authentication gateway for providing authentication details to a service provider is described. The authentication gateway receives an authentication request, such as a log-in form, from a user, retrieves authentication details for the user (typically from an IDM), and responds to the authentication request. The response, which includes the authentication details, is sent directly to the service provider where the authentication request originated. Thus, the user device does not need to handle authentication details for the user, thereby improving the security of the system.

WO 2011/038752 A1

Published:

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

Description

Title

Authentication Gateway

This invention is related to the field of identity management in conjunction with service access control.

Figure 1 is a block diagram of a known system, indicated generally by the reference numeral 1, for providing user credentials to a service provider. The system 1 comprises a user 2, a service provider 4 and an identity provider or an identity management system (IDM) 6. The user 2 (typically in the form of a web browser) is in two-way communication with both the service provider 4 and the identity management system 6.

In use, the service provider 4 requires authentication information regarding the user 2 (such as user credentials) before the service provider will allow the user access to at least some services provided by the service provider. The service provider may, for example, present the user 2 with a log-in form. The requested user credentials are stored at the identity management system 6 and so the user 2 requests the user credentials from the IDM 6 and then completes the log-in form in order to gain access to the requested service(s).

It is known to provide web browsers with the ability to recognize log-in forms in web pages and to fill in the necessary content automatically according to certain rules, policies and/or security settings. These settings may be controlled by the user, by a network administrator and/or by a network provider and are intended to ensure an appropriate security level for the publication of log-in credentials. Example tools include the “password store” tool provided in

the Mozilla Firefox (RTM) browser and the password management tool called "Wand" provided as part of the Opera web browser.

Thus, the system 1 described above can be used to enable a browser at the user 2 to automatically recognize and complete a log-in form issued by the service provider 4 using user credentials stored at the identity management system 6. An advantage of such an arrangement is that the provision of user credentials on request by an IDM system avoids static storage of credentials within the browser extension. This can improve security since third parties may be able to access such statically stored credentials.

Nevertheless, although credentials are not statically stored at the user device, the credentials are temporarily available in the device's memory and might be vulnerable to attacks by viruses and other malicious software, such as Trojan horse applications. Additionally, it does not matter whether the credentials are temporarily visible in the device "as a whole" or just in sequential portions (e.g. as a sequence of keystrokes).

Thus, a browser at the user 2 cannot guarantee attack-free operation of the system 1 and thus cannot guarantee the authenticity of the user.

Particular problems exist in circumstances where the user browser is not owned and administered by the user. This may be the case, for example, where a shared computer is being used, for example in an Internet café, or as a community PC.

The system 1 is one example of a system in which passwords and other security-related information are stored away from the user device. Such arrangements, which are sometimes referred to as "password safes", generally suffer from the problem of temporary content exposure and thus can be attacked by malicious third parties.

The present invention seeks to address at least some of the problems outlined above.

According to an aspect of the present invention, there is provided a method comprising: receiving an authentication request from a user device, wherein the request originates at a service provider; retrieving authentication details for the user of the user device; preparing a response to the authentication request, the response including the retrieved authentication details; and sending the authentication response to the service provider. In a preferred embodiment of the invention, the authentication response is sent directly to the service provider. Thus, the authentication details are not (or at least need not) be provided to the user device. In any event, the authentication response is not sent to the service provider via the user device. The authentication request is typically received at an authentication gateway and the authentication response is typically prepared and sent by the authentication gateway.

According to an aspect of the invention, there is provided an apparatus (such as an authentication gateway) comprising: a first input adapted to receive an authentication request from a user device, wherein the request originates at a service provider; a second input adapted to receive authentication details for the user of the user device on request from the apparatus; a processor for preparing a response to the authentication request, the response including the retrieved authentication details; and a first output adapted to send the authentication response to the service provider. The authentication details are not (or at least need not be) provided to the user device. In particular, the authentication response is not sent from the apparatus (e.g. an authentication gateway) to the service provider via the user device.

The invention provides means for auto-completion of web forms and the like which are used for authentication of a user. In

contrast to existing solutions, the invention separates the detection of a log-in form in a web page or the like and the insertion of credentials. These steps can be performed in logically and spatially distinct entities.

In some forms of the invention, retrieving the authentication details comprises obtaining the authentication details from an identity provider or an identity management system.

The user device may comprise an IDM satellite. The authentication request may be received from the IDM satellite. Thus, the authentication request may be sent from the service provider to the apparatus of the present invention via the IDM satellite.

The said authentication request may be a log-in form originating at the service provider. Alternatively, the authentication request may be some other form that requires the inclusion of user credentials.

The invention may additionally require the identification of the user. In other words, the apparatus of the invention (e.g. an authentication gateway) may be required to identify the user. The authentication request received from the user device may include sufficient information to enable the user to be identified (e.g. by the authentication gateway). Thus, the authentication request may be received at the user device from the service provider, modified at the user device (e.g. by an IDM satellite) to include sufficient information to enable an IDM to identify the user, and then forwarded by the user device, e.g. to the apparatus of the invention. The information identifying the user may, for example, be provided by using trusted platform module (TPM) technology, chip card technology (e.g. a SIM card), shared secrets, certificates or keys.

The apparatus of the present invention may be physically and/or logically separated from the user device. In one form

of the invention, the apparatus is logically separated from the user device, but is not physically separated; for example, in one form of the invention, the apparatus is provided in a separated and protected domain to the user device and the IDM satellite.

In accordance with an aspect of the present invention, there is provided a method comprising: requesting access to a service provided by a service provider, wherein user credentials are required to access said service; and forwarding an authentication request originating at the service provider to an authentication gateway for completion by the authentication gateway, wherein the authentication gateway provides the requested user credentials to the service provider. Thus, the user credentials can be provided to the service provider without being provided to the user device. The method may further comprise sending authentication information to said authentication gateway sufficient to enable the authentication gateway to obtain the said user credentials.

In accordance with an aspect of the present invention, there is provided an apparatus comprising: a first output for requesting access to a service provided by a service provider, wherein user credentials are required to access said service; and a second output for forwarding an authentication request originating at the service provider to an authentication gateway for completion by the authentication gateway, wherein the authentication gateway provides the requested user credentials to the service provider without providing (or at least without needing to provide) the details to the user device. The apparatus may be a user device. The apparatus may be an IDM satellite and may, for example, be provided as a pluggable device, such as a USB memory stick or similar device.

The authentication request may be sent to the authentication gateway from an IDM satellite. Thus, the authentication

request may be sent from the service provider to the apparatus of the present invention via the IDM satellite.

The said authentication request may be a log-in form originating at the service provider. Alternatively, the authentication request may be some other form that requires the inclusion of user credentials.

The invention may additionally require the identification of the user. In other words, the authentication gateway may be required to identify the user. The authentication request sent to the authentication gateway may include sufficient information to enable the user to be identified (e.g. by the authentication gateway). Thus, the authentication request may be received at the user device from the service provider, modified at the user device (e.g. by an IDM satellite) to include sufficient information to enable an IDM to identify the user, and then forwarded by the user device, e.g. to the authentication gateway. The information identifying the user may, for example, be provided by using trusted platform module (TPM) technology, chip card technology (e.g. a SIM card), shared secrets, certificates or keys.

The apparatus of the present invention may be physically and/or logically separated from the user device. In one form of the invention, the apparatus is logically separated from the user device, but is not physically separated; for example, in one form of the invention, the apparatus is provided in a separated and protected domain to the user device and the IDM satellite.

In accordance with an aspect of the present invention, there is provided a computer program comprising: code (or some other means) for receiving an authentication request from a user device, wherein the request originates at a service provider; code (or some other means) for retrieving authentication details for the user of the user device; code (or some other means) for preparing a response to the

authentication request, the response including the retrieved authentication details; and code (or some other means) for sending the authentication response to the service provider, such that the authentication details are not provided to the user device. The computer program may be a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.

In accordance with an aspect of the present invention, there is provided a computer program comprising: code (or some other means) for requesting access to a service provided by a service provider, wherein user credentials are required to access said service; and code (or some other means) for forwarding an authentication request originating at the service provider to an authentication gateway for completion by the authentication gateway, wherein the authentication gateway provides the requested user credentials to the service provider. The requested user credentials may be proved directly to the service provider, i.e. without providing the details to the user device or IDM satellite. The computer program may be a computer program product comprising a computer-readable medium bearing computer program code embodied therein for use with a computer.

Exemplary embodiments of the invention are described below, by way of example only, with reference to the following numbered schematic drawings.

Figure 1 is a block diagram of a known system for providing authentication information to a service provider;

Figure 2 is a block diagram in accordance with an aspect of the present invention; and

Figure 3 shows a message sequence in accordance with an aspect of the present invention.

Figure 2 is a block diagram of a system, indicated generally by the reference numeral 10, in accordance with an aspect of

the present invention. The system 10 comprises a user 12, an identity management (IDM) satellite 13, a service provider 16, an authentication gateway 18 and an identity management system (IDM) 20. The user 12 and the IDM satellite 13 collectively form a user sub-system 14. The IDM satellite 13 is in two-way communication with both the service provider 16 and the authentication gateway 18. The authentication gateway 18 is also in two-way communication with the service provider 16 and the IDM 20.

In a similar manner to the system 1 described above, the service provider 16 requires the user 12 to provide user credentials (such as a user name and password pair) in order to access at least some services provided by the service provider. Those credentials are stored at the IDM 20.

The IDM satellite 13 typically resides at the user's premises, or forms part of a user device, and is used to recognize that a web page may contain a form requiring the user to fill-in some log-in credentials. As discussed below, the authentication gateway 18 is used to populate the log-in form with the required user credentials. Accordingly, there is a functional separation between login-in form detection (carried out by the IDM satellite 13) and login form completion (carried out by the authentication gateway 18).

The separation between the IDM satellite 13 and the authentication gateway 18 could be handled in a variety of ways. For example, a possible solution is as follows. Upon form submission (e.g. when a user clicks on a LOGIN-Button), the satellite 13 recognizes that a login step should occur and does not send the whole request back to the server 16 (as a proxy usually does) but sends it to the authentication gateway 18 (which is an external network element). Now the authentication gateway inserts the credentials, sends this all to the server 16, fetches the responses and sends the response back to the IDM satellite 13 who sends it back to the user browser 12.

Figure 3 shows a message sequence, indicated generally by the reference numeral 30, showing an exemplary use of the system 10. The message sequence 30 shows the interaction between the participating parties and explains the functional separation between log-in form detection and log-in form auto-completion. The message sequence 30 serves as an exemplary explanation of the principal functions of the present invention and does not describe the only possible implementation. For example, although the IDM satellite is described as being part of the user device 12, similar functionality could be provided by a proxy that forms part of an operator's network.

The message sequence 30 begins with the user 12 sending a message 32 to the IDM satellite 13 requesting access to a web page provided by the service provider 16. The message 32 may, for example, be a simple HTTP GET request. The IDM satellite sends a message 34 to the service provider 16 requesting access to that web page and the service provider responds by providing a web page as message 36. The message 34 may, for example, be also be a simple HTTP GET request. The response 36 may be the HTTP-Response 200 that includes an HTML payload.

The web page provided in the message 36 (the payload) includes a log-in form. The IDM satellite 13 recognizes that there is a log-in form. This may be achieved in a variety of ways. For example, in the payload of the message 36, password input fields may be marked as type "password" instead of type "input". Fields may also grouped together in a "form" which is submitted on a button click. By parsing the page for "type='password'" one can easily find these input fields and their names which are needed in the http-request.

On recognizing the log-in form, the IDM satellite delegates the form completion to the authentication gateway 18. In order to achieve this, the IDM satellite 13 has to send a

clear identification to the authentication gateway (i.e. it has to authenticate itself). Of course, there are security issues to consider. It should not be possible to compromise this authentication. This requires attack-resistant storage of the necessary keys, shared secrets, certificates or the like which might be achieved, for example, by using trusted platform module (TPM) technology or chip card technology (e.g. a SIM card). Various variants of authentication are possible here; the following non-exhaustive list contains three examples:

1. The IDM satellite 13 sends the necessary parameters to the authentication gateway 18 (e.g. the originator's address in order to determine which credentials are of interest) and signs them with a private key. The IDM satellite also forwards the corresponding public key which can later be inspected by the IDM 20 for validity. The public key identifies the IDM satellite 13 towards the authentication gateway 18.

2. A challenge-response procedure is used between authentication gateway 18 and IDM satellite 13. This means that there exists a shared secret between the IDM satellite 13 and the authentication gateway 18. First, the satellite 13 sends an authentication request (this could also contain the originator's address mentioned before). The authentication gateway 18 reacts by sending a "challenge". The satellite computes a response from the challenge and the shared secret and sends that response to the authentication gateway 18. The authentication gateway compares the result with the expected answer to determine whether or not the IDM satellite should be trusted.

3. A session binding exists between the IDM satellite 13 and the authentication gateway 18, e.g. by use of a non-compromisable identifier that is forwarded from the IDM satellite to the authentication gateway. The authentication gateway inspects the user's identifier to determine the

identity of the user. The binding can be reached by out of band means (e.g. the user's mobile communication device), a one-time password (like an RSA (Rivest, Shamir and Adleman) Token) or simple web login. If the non-compromisable identifier is used, it is stored on the IDM satellite by using cryptographic protection, e.g. on a SIM card or other chip card or using TPM (Trusted Platform Module) mechanisms.

In any event, the authentication gateway 18 receives the request 38 from the IDM satellite 13 and, in response, sends a message 40 to the IDM 20 requesting the user credentials required in order to complete the log-in form provided by the service provider 16. The message 38 may be an HTTP POST, including the payload discussed above. The message 40 may be a SAML attribute query, requesting the user credentials required to complete the login form provided by the service provider 16.

In response to the message 40, the IDM 20 provides the requested user credentials in a message 42. The message 42 may take the form of a SAML attribute response.

The authentication gateway is now able to modify the payload of the HTTP POST message 38 to include the user credentials for the user, as obtained from the IDM 20. Thus, the authentication gateway 18 completes the log-in form issued by the service provider 16 by including the requested user credentials and sends the completed form, as message 44, to the service provider 16. The message 44 may take the form of an HTTP POST message with the modified payload. The form itself is not generally shown to the user, since this is handled at protocol level. The authentication gateway 18 receives an HTTP Post containing the URL of the receiver and the form fields in the body. The authentication gateway replaces the values for the form fields (and maybe also the URL to protect against phishing)

The service provider 16 sends a response to the

authentication gateway 18, which gateway acts as a kind of second proxy for the user 12, as message 46. The message 46 may be an HTTP Response, with an HTML page as a payload. It should be noted that although the service provider sent the original log-in form to the IDM satellite 13, it is generally acceptable for the response to arrive from a different source (the authentication gateway 18 in this case). Typically the service provider is expecting to receive the requested credentials together with a cookie identifying the session. As the authentication gateway 18 can obtain both the cookie identifying the session and the requested credentials, the authentication gateway can provide all the information required to satisfy the service provider 16.

The authentication gateway 18 forwards the response to the IDM satellite 13, which is the first proxy for the user 12, as message 48. Finally, the IDM satellite 13 delivers the response to the user as message 50. The messages 48 and 50 may therefore be HTTP responses, with the payload referred to above.

Thus, the user 12 is authenticated at the service provider and can use the restricted services provided by the service provider without the user credentials being sent via the user device or the IDM satellite 13. Thus, using the system 10, it is not possible for malicious software at the user device to obtain the user credentials.

The IDM satellite 13 at the user client 12 may take the form of a pluggable device, such as a Universal Serial Bus (USB) memory stick or similar device. Thus, the IDM satellite can aid user mobility since it can be moved from one user device to another. For example, the user may use the IDM satellite at a user device at an Internet café. In such an environment, the IDM satellite can be used to instruct the authentication gateway 18 to provide log-in details to the service provider 16, with the user credentials not needing to pass through the machine at the Internet café. Since the

identity information that enables the IDM satellite 13 to log into the IDM 20 may be stored in a secure place (such as a SIM), malicious software on the actually used client (e.g. a personal computer at an Internet café) cannot access and misuse it.

The elements of the system 10 could be located in many different places. For example, the IDM satellite 13 may communicate with any one, two or all of the service provider 16, authentication gateway 18 and IDM 20 via the Internet. Alternatively, some of the elements of the system 10 may be located within an Intranet. For example, the user 12 and the IDM satellite 13 may be located outside an Intranet, but may be able to communicate with resources, such as the service provider 16 and/or the authentication gateway 18 that are located within the Intranet.

As described above, log-in forms and other web forms are sensitive to attacks by malicious software because the user credentials are handled in a non-encrypted way, at least for a short time. In the present invention, this function is handled by the authentication gateway 18 rather than the user device 12 or the IDM satellite 13. The authentication gateway 18 is functionally, and possibly also physically, separated from the IDM satellite 13 (and the user device 12). Accordingly, user credential data is no longer accessible to attacks by viruses or Trojan horses on the client device. The authentication gateway may be controlled by a network operator, which is not vulnerable to client-driven attacks.

In an alternative form of the invention, the authentication gateway 18 runs on the machine of the user (thereby forming part of the user sub-system 14), but in a separate and protected domain to the user 12 and the IDM satellite 13. This solution utilises virtualisation technology and may require the operator to verify the virtualisation host prior to deploying his authentication gateway. Such an arrangement

enables computation and availability demands to be distributed, although the added complexity of administration should not be neglected. In general terms, the idea here is to run a second "virtual machine" on the physical hardware and takes one step into so-called cloud computing. The second virtual machine runs in a protected environment and (maybe) also protects itself. So even if the outer machine is compromised, you still have the "secure and trusted second machine" which handles your user credentials and similar data.

The embodiments of the invention described above are illustrative rather than restrictive. It will be apparent to those skilled in the art that the above devices and methods may incorporate a number of modifications without departing from the general scope of the invention. It is intended to include all such modifications within the scope of the invention insofar as they fall within the scope of the appended claims.

CLAIMS:

1. A method comprising:

receiving an authentication request from a user device, wherein the request originates at a service provider;

retrieving authentication details for the user of the user device;

preparing a response to the authentication request, the response including the retrieved authentication details; and

sending the authentication response to the service provider, such that the authentication details are not provided to the user device.

2. A method as claimed in claim 1, wherein retrieving the authentication details comprises obtaining the authentication details from an identity provider.

3. A method as claimed in claim 1 or claim 2, wherein the user device includes an IDM satellite.

4. A method as claimed in any one of claims 1 to 3, wherein said authentication request is a log-in form.

5. A method as claimed in any preceding claim, further comprising identifying the user.

6. A method as claimed in any preceding claim, wherein said authentication request includes sufficient information to identify the user.

7. An apparatus comprising:

a first input adapted to receive an authentication request from a user device, wherein the request originates at a service provider;

a second input adapted to receive authentication details for the user of the user device on request from the apparatus;

a processor for preparing a response to the authentication request, the response including the retrieved authentication details; and

a first output adapted to send the authentication response to the service provider, wherein the authentication details are not provided to the user device.

8. An apparatus as claimed in claim 7, wherein the apparatus is physically separated from the user device.

9. An apparatus as claimed in claim 7 or claim 8, wherein the apparatus is logically separated from the user device.

10. An apparatus as claimed in any one of claims 7 to 9, wherein said authentication details are obtained from an identity provider.

11. An apparatus as claimed in any one of claims 7 to 10, wherein said authentication request identifies the said user.

12. A method comprising:

requesting access to a service provided by a service provider, wherein user credentials are required to access said service; and

forwarding an authentication request originating at the service provider to an authentication gateway for completion by the authentication gateway, wherein the authentication gateway provides the requested user credentials to the service provider without providing the details to the user device.

13. A method as claimed in claim 12, further comprising sending authentication information to said authentication gateway sufficient to enable the authentication gateway to obtain the said user credentials.

14. An apparatus comprising:

a first output for requesting access to a service provided by a service provider, wherein user credentials are required to access said service; and

a second output for forwarding an authentication request originating at the service provider to an authentication gateway for completion by the authentication gateway, wherein the authentication gateway provides the requested user credentials to the service provider.

15. A computer program product comprising:

means for receiving an authentication request from a user device, wherein the request originates at a service provider;

means for retrieving authentication details for the user of the user device;

means for preparing a response to the authentication request, the response including the retrieved authentication details; and

means for sending the authentication response to the service provider, such that the authentication details are not provided to the user device.

16. A computer program product comprising:

means for requesting access to a service provided by a service provider, wherein user credentials are required to access said service; and

means for forwarding an authentication request originating at the service provider to an authentication gateway for completion by the authentication gateway, wherein the authentication gateway provides the requested user credentials to the service provider.

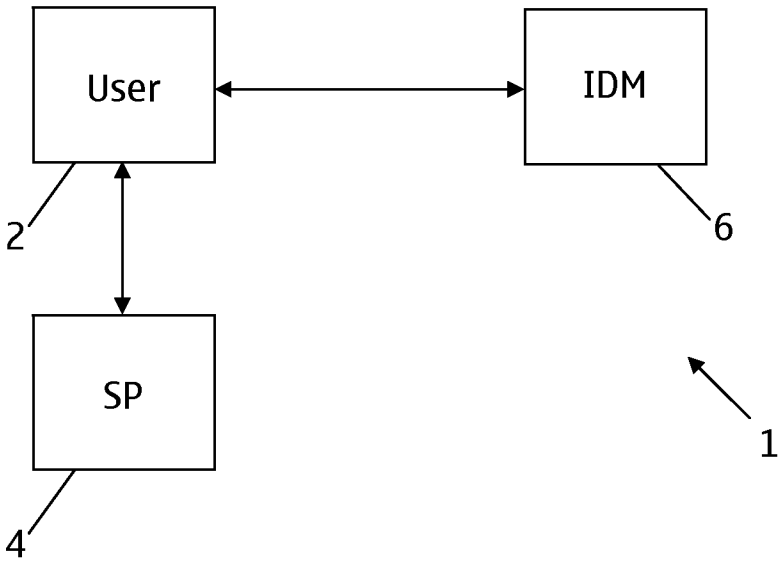

User
IDM
2
6
SP
1
4

Fig. 1

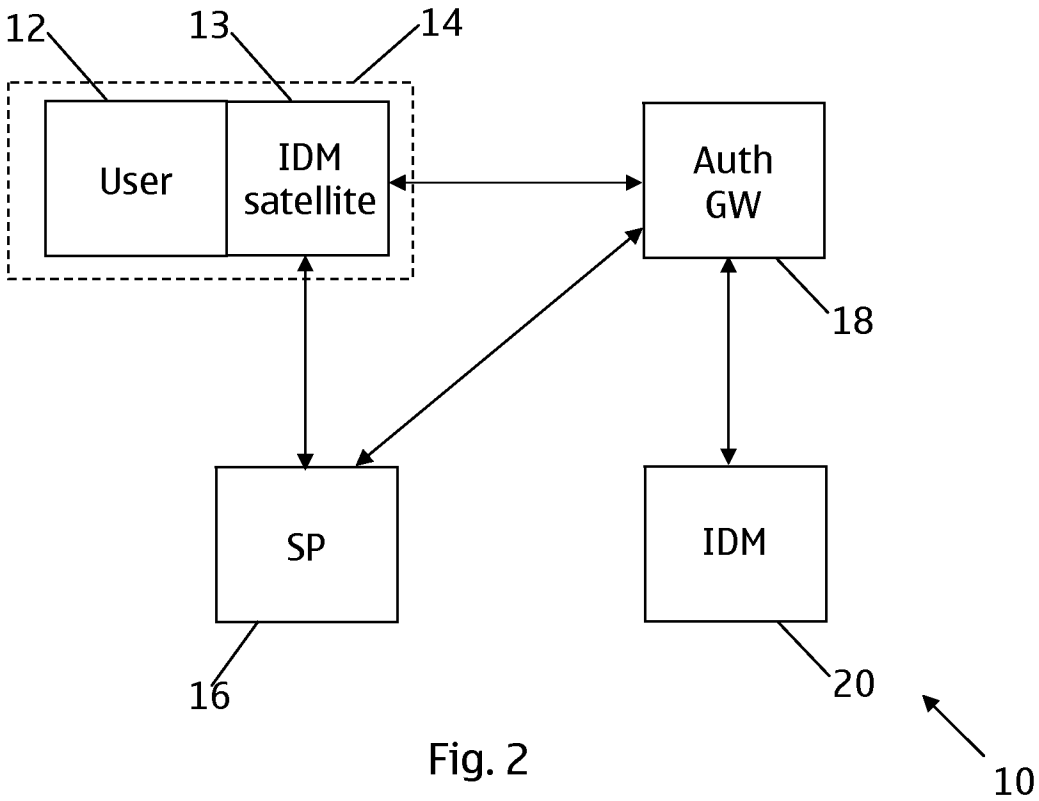

12
13
14
User
IDM satellite
Auth GW
18
SP
IDM
16
20
10

Fig. 2

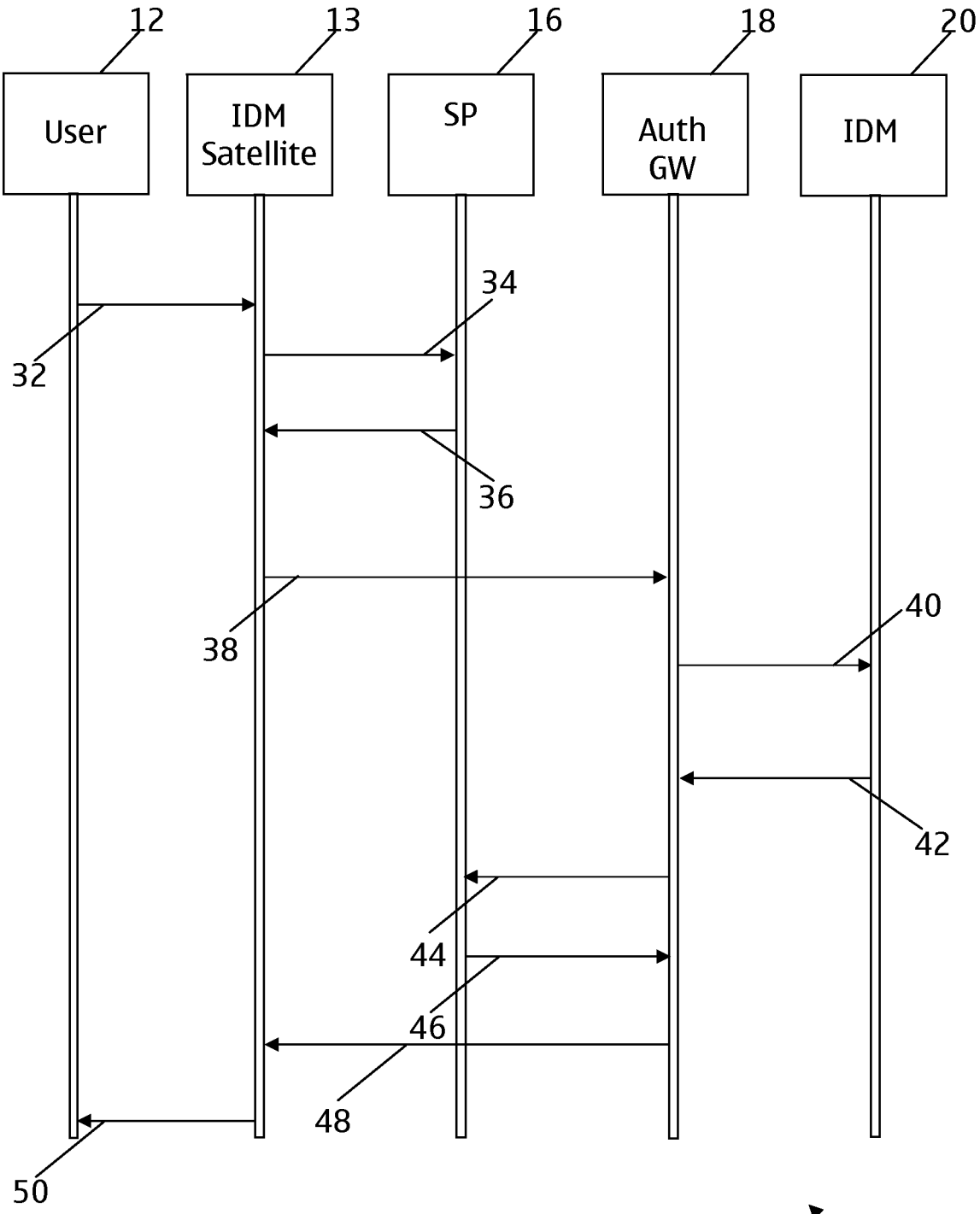

12
13
16
18
20
User
IDM Satellite
SP
Auth GW
IDM
34
32
36
38
40
42
44
46
48
50
30

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/062606

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/00 G06F17/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CA 2 484 487 A1 (IBM [US]) 6 November 2003 (2003-11-06) page 2, lines 9-13 page 13, lines 12-22 page 15, lines 2-17,28-31 page 16, lines 1-9 figures 1,2	1-16
X	WO 2005/125077 A1 (SXIP NETWORKS SRL [BB]; HARDT DICK C [CA]) 29 December 2005 (2005-12-29) page 17, line 31 - page 18, line 5 page 10, lines 5-15 figures 4,9,10	1-16
A	US 2008/071808 A1 (HARDT DICK C [CA] ET AL) 20 March 2008 (2008-03-20) paragraphs [0030], [0031], [0048]; figures 1,2	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 August 2010	11/08/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Pajatakis, Emmanouil

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/062606

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 2484487 A1	06-11-2003	AU 2003215813 A1	10-11-2003
		CN 1650246 A	03-08-2005
		WO 03091861 A2	06-11-2003
		JP 4143601 B2	03-09-2008
		JP 2005528679 T	22-09-2005
WO 2005125077 A1	29-12-2005	EP 1766840 A1	28-03-2007
		US 2006005020 A1	05-01-2006
US 2008071808 A1	20-03-2008	NONE	