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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 August 2010 (26.08.2010)

PCT

(10) International Publication Number
WO 2010/094330 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *G06F 21/00* (2006.01)
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/EP2009/051944

(22) International Filing Date:
19 February 2009 (19.02.2009)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SUN, Shao Jun** [CN/CN]; 7-1501, No.2, Maliandao South Str. Xuanwu District, Beijing 100055 (CN).

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

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

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

Published:

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

(54) Title: WIRELESS IDENTITY TOKEN

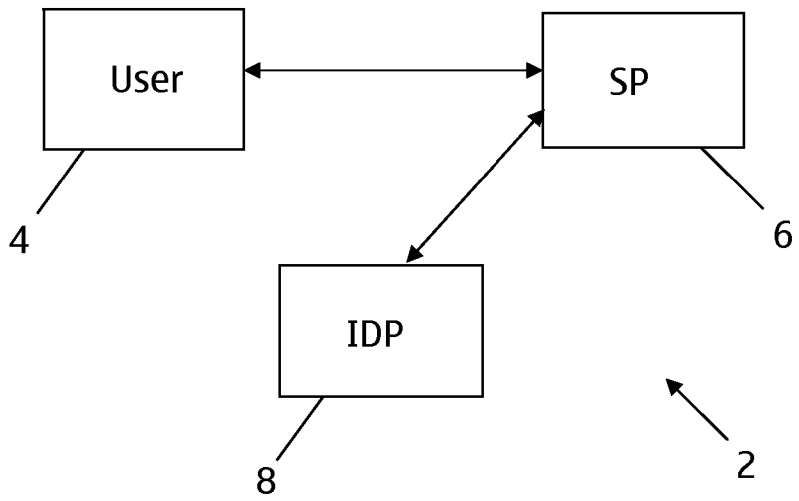

Fig. 1

(57) Abstract: A system is described comprising a user device, a wireless identity token, a service provider and an identity provider. In use, the user device requests access to a secure service provided the service provider. The service provider requests authentication and the user device passes the authentication request to the wireless identity token. The wireless identity token obtains user credentials for the secure service from the identity provider. The user credentials are passed from the wireless identity token to the user device and from the user device to the service provider. On receipt of the user credentials, the service provider grants the user device access to the requested secure service.

WO 2010/094330 A1

Wireless Identity Token

The present invention is related to identity and trust management.

More and more services are becoming available on the Internet, and many of these services require authentication. The most widespread solution for electronic authentication today is the use of a username and password pair, since this is easy to deploy and manage. However this kind of authentication method has a number of drawbacks. For example, it is vulnerable to security attacks such as man in the middle and replay, usernames and passwords are easily lost or forgotten, and usernames and passwords can often be easily stolen by third parties.

Furthermore, as the number of services grows so does the number of username and password pairs that users need to remember. Already many people are experiencing difficulties in remembering all of the combinations of usernames and passwords that they use. Some people are using the same pairs of usernames and passwords for some or all of the services that they use. Further, many users are choosing passwords that are easy to remember and that are often easy for third parties to guess. Such practices reduce the security of an already relatively weak authentication mechanism.

More secure solutions for user authentication exist, such as one-time passwords (OTP) or Smart Card PKI solutions. Such solutions address some of the problems identified above with username/password authentication schemes, but typically place an increased burden on the user. There is an ongoing need for an authentication scheme that is easy and convenient to

use from the user's perspective, and also offers a greater level of security than the use of a password.

One approach that has been developed to assist users to access multiple applications, each requiring separate authentication procedures, involves the use of identity federation.

Federated identity management, or the "federation" of identity, describes technologies that serve to enable the portability of identity information across otherwise autonomous security domains. A goal of identity federation is to enable users of one domain to access data or systems of another domain seamlessly and securely, and without the need for redundant user administration. Eliminating the need for repeated login procedures each time a new application or account is accessed can substantially improve the user experience.

Figure 1 is a block diagram demonstrating the concept of identity management. Figure 1 shows a system, indicated generally by the reference numeral 2, comprising an end user 4, a service provider 6 and an identity provider 8. When the end user 4 of the system 2 wants to access a secure resource at the service provider 6, and the service provider 6 requires the user's identity to be authenticated, the identity provider 8 can be used to provide the required authentication information to the service provider.

Security Assertion Markup Language (SAML) is an XML (eXtensible Markup Language) standard for exchanging authentication and authorization data between security domains. For example, SAML is used for exchanging assertion data between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a specification

defined by the OASIS (Organization for the Advancement of Structured Information standards).

In an exemplary use of the system 2, SAML assumes that the user 4 has enrolled with at least one identity provider (such as the identity provider 8). The identity provider 8 is expected to provide local authentication services to the user. The service provider 6 relies on the identity provider 8 to identify the user 4. When a user 4 wants to access a service that is provided by a service provider 6 who has a contract with the identity provider 8 (i.e. the service provider and the identity provider form at least part of a circle of trust), the service provider 6 requests a user authentication from the identity provider. In response to the service provider's request, the identity provider 8 passes a SAML assertion to the service provider 6. On the basis of this assertion, the service provider can make decisions; for example, the service provider can decide whether to grant access to the resources/services as requested by the user.

Figure 2 shows an exemplary message sequence, indicated generally by the reference numeral 10, demonstrating the algorithm described above.

The message sequence 10 starts with the end user 4 sending a message 12 to the service provider 6 (for example using a web browser) requesting access to a particular application provided by the service provider 6. The service provider requires user credentials, which credentials are not provided in the request 12.

In order to obtain user credentials, the service provider 6 sends a SAML authentication request 14 to the identity provider 8. Assuming that the user is known to the identity

provider 8, the identity provider returns a SAML assertion response 16 providing credentials for the user 4. In response to receiving the assertion response 16, the service provider 6 grants the user access to the requested service (message 18).

Identity federation offers assistance in accessing multiple applications, but the user is still required to provide a variety of information to the service provider, such as the location of the identity provider and user information required by the identity provider in order to identify and authenticate the user to the identity provider's satisfaction. Accordingly, the use of identity federation suffers from at least some of the problems outlined above.

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

According to an aspect of the invention, there is provided an apparatus (such as a wireless identity token) comprising: a first memory (such as an EEPROM) for storing user information; a first interface (such as a USB interface) adapted to couple the apparatus to a user device; and a second interface (such as a wireless interface) adapted to couple the apparatus to an identity provider, wherein the apparatus is adapted to register with the identity provider using said user information and to obtain user credentials for a first application from the identity provider on request from the user device. The first application may, for example, be provided by a service provider.

Accordingly to a further aspect of the invention, there is provided a method comprising: using a module (such as a wireless identity token) to register a user at an identity pro-

vider, using user information stored at said module; receiving, at said module, a request from a user device to obtain user credentials for an application; using said module to obtain said user credentials for said application from the identity provider; and forwarding said user credentials from said module to said user device. The order in which the steps of the method may differ in different embodiments of the invention. For example, in some embodiments of the invention, the module may register at an identity provider before receiving the request from the user device to obtain user credentials for a particular application. In other embodiments of the invention, the order of those steps may be reversed, so that the module registers at the identity provider in response to receiving the request from the user device to obtain credentials for a particular application.

According to another aspect of the invention, there is provided a system comprising a first module (such as a wireless identity token) and a user device, wherein the first module comprises: a first memory (such as an EEPROM) for storing user information; a first interface (such as a USB interface) adapted to couple the first module to the user device; and a second interface (such as a wireless interface) adapted to couple the first module to an identity provider, wherein the first module is adapted to register with the identity provider using said user information and to obtain user credentials for a first application from the identity provider on request from the user device. The first application may, for example, be provided by a service provider.

According to another aspect of the invention, there is provided a computer program product comprising: means for storing user information; means for registering the user at an identity provider, using said user information to identify

the user at the identity provider; means for receiving a request from a user device to obtain user credentials for a particular application; means for obtaining said user credentials for said application from the identity provider; and means for forwarding said user credentials to said user device.

According to a further aspect of the invention, there is provided a computer program comprising: code for storing user information; code for registering the user at an identity provider, using said user information to identify the user at the identity provider; code for receiving a request from a user device to obtain user credentials for a particular application; code for obtaining said user credentials for said application from the identity provider; and code for forwarding said user credentials to said 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.

Some forms of the invention make use of the SAML standard for providing identity assertions. Thus, in use, an application or a service provider providing an application may request an identity assertion via a SAML authentication request. The SAML authentication request may be forwarded by the user device to the apparatus of the invention (e.g. a wireless identity token) that is, for example, attached to the user device (for example, via a USB connection). The apparatus of the invention (e.g. a wireless identity token) may retrieve the required SAML assertion from the identity provider (for example, via a wireless link between the apparatus and the identity provider). The SAML assertion may be returned to the user device and, from there, to the application being accessed.

In many forms of the invention, the application being accessed does not need to communicate with the identity provider that is providing the user credentials. This is convenient since it means that the application (or a service provider providing the application) does not need to know details of the identity provider (such as the location and/or the identity of the identity provider).

An advantage of many embodiments of the present invention is that the user does not need to remember details such as a username and password in order to gain access to the identity provider. Thus, convenience for the user is improved.

An advantage of many embodiments of the present invention is that the user does not need to enter identification information. Thus, it is more difficult for third parties to obtain such information (for example, by phishing), thereby improving security.

The apparatus of the present invention may be removably connectable to the user device. By way of example, the apparatus may be connectable to the user device via a USB connection. The apparatus may obtain power from the user device by means of a USB port of the user device.

The use of a USB connection is not essential to all embodiments of the invention. Other forms of wired, or indeed wireless, connections could be provided.

In some forms of the invention, the interface between the apparatus of the invention and the identity provider is a wireless interface. By way of example, the wireless interface may be a mobile communication network, such as a 3G network.

In some forms of the invention, the user credentials for the first application obtained from the identity provider are forwarded to the user device. Furthermore, in some forms of the invention, the user credentials for the first application are forwarded from the user device to the application (or to the service provider providing the application), for example, using the Internet or some other network.

The apparatus of the present invention may include a second memory (such as a ROM) for storing an application for controlling communications between the apparatus and the identity provider. The application may be an embedded web application. In some forms of the invention including first and second memories, the first and second memories of the apparatus are provided as separate memory modules: in other forms of the invention, the first and second memories are provided as a single module.

In some forms of the invention, the request to obtain user credentials for the application is originally issued by the application (or by a service provider providing the application). The request to obtain user credentials for the application may be issued by the application or service provider in response to a request from the user device for access to the application.

The connection with the identity provider used in the present invention may make use of an existing mobile telephone connection. As a result, the present invention can taken advantage of many of the security features that have been developed for mobile telephone applications, such as 3G AKA and GBA security.

The identity provider used in the present invention may be provided by a telecommunications provider, which provider may also provide a wireless link with the identity provider. The user account can be maintained in the telecommunication provider's identity provider based on a user's mobile phone, which may be more secure than that of other internet applications. Furthermore, the application (or a service provider providing the application) may be more willing to trust an identity provider provided by a telecommunications service provider than some other identity providers.

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 demonstrating the use of identity management in the prior art;

Figure 2 shows a message sequence demonstrating a use of the system of Figure 1;

Figure 3 is a block diagram of a system in accordance with an aspect of the invention;

Figure 4 is a flow chart showing an algorithm in accordance with an aspect of the invention;

Figure 5 is a block diagram of a module in accordance with an aspect of the invention; and

Figure 6 shows a message sequence in accordance with a further aspect of the invention.

Figure 3 is a block diagram of a system, indicated generally by the reference numeral 20, in accordance with an aspect of the present invention. The system 20 comprises a user device 22, a wireless identity token 24, an identity provider 26 and a service provider 28. The wireless identity token 24 is connected to the user device, for example using a physical

connection such as a USB connection. The wireless identity token 24 is also connected to the identity provider 26 via a wireless network 30. The user device 22 is connected to the service provider 28 via the Internet 32.

The user device 22 may, for example, be a computer. Alternatively, the user device may be an Internet Protocol (IP) communication device, such as an IP telephone.

The wireless network 30 may be a mobile communications network, such as a 3G network.

In the system 20, the user device 22 can communicate with the service provider 28 via the Internet 32. However, the service provider 28 requires the user to be authenticated before access is granted to a service provided by the service provider. The identity provider 26 can be used to provide user authentication.

The service provider 28 is configured to establish trust between itself and the identity provider 26 according to the SAML standard. The identity provider 26 is built to provide federated identities for service providers, including the service provider 28. SAML is used as the protocol between the identity provider 26 and service providers.

In the system 20, the wireless identity token 24 is used to assist in the authentication of the user device at the service provider 28. The wireless identity token 24 has the wireless access ability to communicate with the wireless network 30. Further, the wireless identity token 24 uses smart card technology to store user credentials like a Mobile Subscriber Integrated Service Digital Network (MSISDN) number, and cipher keys which are required to access wireless network

30, in a similar manner to a Subscriber Identity Module (SIM) or a User Subscriber Identity Module (USIM). The wireless identity token also stores identity information used by the identity provider 26 to identify the selected user identity, as discussed further below.

Figure 4 is a flow chart showing an algorithm, indicated generally by the reference numeral 40, showing, in broad terms, the functionality of the wireless identity token 24.

The algorithm 40 starts at step 42 with the service provider 28 issuing a SAML authentication request message to the user device 22, thereby requesting an identity assertion. The user device 22 forwards the SAML authentication request to the wireless identity token 24 (step 44). Next, at step 46, the wireless identity token delivers the request to the identity provider 26 together with the identity information stored by the identity token. The identity provider 26 authenticates the wireless token's identity and generates the required SAML assertion (step 48). The SAML assertion is sent from the identity provider 26 to the service provider 28 via the wireless identity token 24 and the user device 22 (step 50). Finally, the service provider 28 validates the SAML assertion to authenticate the user identity and grants the user access to the requested service (step 52).

In this way, the user device 22 is authenticated to the satisfaction of the service provider 28, without the service provider needing to communicate directly with the identity provider 26.

Figure 5 is a block diagram showing an exemplary implementation of the wireless identity token 24. As shown in Figure 5, the wireless identity token includes a central processing

unit (CPU) 60, read-only memory (ROM) 62, electrically erasable programmable read-only memory (EEPROM) 64, random access memory (RAM) 66, Universal Serial Bus (USB) interface module 67 and wireless interface module 68.

User credentials are stored in the EEPROM 64. An embedded web application is stored in the ROM 62 and is launched when the wireless identity token 24 is powered on and connected to the wireless network 30. The web application stored in the ROM 62 is used to communicate with user devices (such as the user device 22 described above) and should be able to handle HTTP POST and REDIRECT requests.

The Universal Serial Bus (USB) interface 67 is able to provide required power to the wireless identity token 24 and transmit data between the wireless identity token and user device 22.

The driver for the wireless identity token can be a normal USB network interface card (NIC) driver with additional configuration for the TCP/IP to enable the user device to send transmission control protocol (TCP) data packages to the embedded web application of the wireless identity token 24.

The following steps are carried out when the wireless identity token 24 is attached to the user device 22:

1. The wireless identity token 24 receives power from the user device 22 via the USB module 67 and is turned on.
2. The wireless identity token registers with the wireless network 30.
3. The web application stored in the ROM 62 is initiated.

4. The user credentials stored in the EEPROM 64 are used to authenticate the user at the identity provider 26, under the control of the web application stored in the ROM 62.
5. The identity provider 26 returns the requested user credentials to the wireless identity token 24.
6. The wireless identity token 24 waits for a request for user credentials to be received from the user device 22.
7. The user device 22 determines that it has connected to a new NIC device and activates the additional drivers with pre-configured TCP/IP properties.

As noted above, the user credentials stored in the EEPROM 64 are used to authenticate the user at the identity provider 26, under the control of the web application stored in the ROM 62.

In one form of the invention, Generic Bootstrapping Architecture (GBA) bootstrapping (an authentication method standardised by the 3GPP (see www.3gpp.org)) is used to authenticate the wireless identity token 24 at the identity provider 26. A bootstrapping transaction identifier (B-TID) and a session key are generated as part of the GBA procedure and are used in the message sequence 80 discussed below. After the GBA procedure has been carried out, the wireless identity token 24 maintains an authenticated session (for example, an HTTP session) with the identity provider 26.

Figure 6 shows a message sequence, indicated generally by the reference numeral 80, demonstrating the accessing of a secure service at the service provider 28 by the user device 22, in accordance with an aspect of the present invention.

The message sequence 80 begins with the user device 22 issuing a service access request 82 to the service provider 28.

The service access request 82 takes the form of an HTTP GET Request. The request 82 requests access to a secure service, but does not include the required user credentials. Accordingly, the service provider 28 responds to the request 82 by issuing an authentication request 84. The authentication request takes the form of an HTTP redirect request, in accordance with the SAML protocol.

The authentication request 84 is passed from the user device 22 to the wireless identity token 24. The user device 22 then waits for a SAML authentication response to be returned from the wireless identity token.

The wireless identity token 24 recognizes the SAML authentication request and forwards the authentication request and the session data obtained during the GBA bootstrapping process (such as an HTTP cookie) to the identity provider 26 via the wireless network 30 as message 88.

The identity provider 26 recognises the wireless identity token 24 by means of the session information (e.g. HTTP cookie) received from the wireless identity token and prepares a SAML assertion, including user credentials for the service being accessed. The identity provider 26 signs the assertion with its private key (the paired certificate is known to the service provider 28 as suggested in the SAML standards). The signed SAML assertion is then returned to the wireless identity token 24 in message 90.

When the wireless identity token 24 receives the SAML assertion 90 from the identity provider, the assertion is returned to the user device in message 92. Thus, the wireless identity token 24 is used to obtain SAML assertion data from the identity provider 26 and to provide that data to the user de-

vice 22. The user device can, in turn, provide this data to the relevant service provider 28. In this way, the wireless identity token 24 bridges the identity communication between the user device 22, the identity provider 26 and the service provider 28.

The SAML assertion is redirected to the service provider 28 as message 94. The service provider 28 then validates the SAML assertion and grants the user device access to the requested secure resource. This is confirmed in message 96 sent from the service provider 28 to the user device 22.

In the message sequence 80 described above, the authentication request 84 takes the form of an HTTP redirect request. Typically the redirect request includes an indication of where the request should be redirected. In the present case, the redirect request could specify that request should be redirected to a "local stick" or to the "wireless identity token". In such an example, the wireless identity token 24 would appear to the service provider to act as the identity provider. In reality, the wireless identity token would route the request on to the real identity provider 26, with the wireless identity token acting as an IDP delegate. Such an arrangement is not, however, an essential feature of the present invention.

The skilled person would be aware of a variety of different methods to enable the user browser to redirect the authentication request to the wireless identity token. The following are provided by way of example only:

1. The authentication request may omit a location indication of the identity provider, leaving the user browser free to redirect the request where it wishes (i.e. to the wireless

identity token 24).

2. The authentication request may provide the address of the identity provider 26, with the user browser interpreting that address as being the address of the wireless identity token, since the wireless identity token will forward the request on to the identity provider 26.

3. An HTTP proxy may be provided between the user device 22 and the service provider 28 to intercept SAML authentication requests and to request SAML assertion data from the wireless identity token 24.

4. The service provider may ask the user to provide an address for an identity provider. In response to this, the user can provide the address of the wireless identity token.

The embodiments of the invention described above make use of the SAML standard. This is not essential. The skilled person would be aware of a number of other authentication procedures, such as OpenID and Windows® CardSpace, that could make use of features of the present invention.

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. An apparatus comprising:

a first memory device for storing user information;

a first interface adapted to couple the apparatus to a user device; and

a second interface adapted to couple the apparatus to an identity provider,

wherein the apparatus is adapted to register with the identity provider using said user information and to obtain user credentials for a first application from the identity provider on request from the user device.

2. An apparatus as claimed in claim 1, wherein the apparatus is removably connectable to the user device by means of the first interface.

3. An apparatus as claimed in claim 1 or claim 2, wherein the first interface is a USB interface.

4. An apparatus as claimed in any one of claims 1 to 3, wherein the second interface is a wireless interface.

5. An apparatus as claimed in any preceding claim, further comprising forwarding the user credentials for the first application to the user device.

6. An apparatus as claimed in any preceding claim, further comprising a second memory for storing an application for controlling communications between the apparatus and the identity provider.

7. An apparatus as claimed in claim 6, wherein the application for controlling the communications between the apparatus

and the identity provider is an embedded web application.

8. A method comprising:

using a module to register a user at an identity provider, using user information stored at said module;

receiving, at said module, a request from a user device to obtain user credentials for an application;

using said module to obtain said user credentials for said application from the identity provider;

forwarding said user credentials from said module to said user device.

9. A method as claimed in claim 8, further comprising forwarding said user credentials from the user device to a service provider providing the application.

10. A method as claimed in claim 9, wherein the user device communicates with the service provider via the Internet.

11. A method as claimed in claim 9 or claim 10, wherein the request to obtain user credentials for the application is originally issued by the service provider.

12. A method as claimed in claim 11, wherein the request to obtain user credentials for the application is issued by the service provider in response to a request from the user device for access to the application.

13. A method as claimed in any one of claims 8 to 12, wherein the module communicates with the identity provider via a wireless link.

14. A system comprising a first module and a user device, wherein the first module comprises:

a first memory device for storing user information;

a first interface adapted to couple the first module to the user device; and

a second interface adapted to couple the first module to an identity provider, wherein the first module is adapted to register with the identity provider using said user information and to obtain user credentials for a first application from the identity provider on request from the user device.

15. A system as claimed in claim 14, wherein said user device is adapted to forward the user credentials to a service provider providing the first application.

16. A system as claimed in claim 15, wherein the user device communicates with the service provider via the Internet.

17. A computer program product comprising:

means for storing user information;

means for registering the user at an identity provider, using said user information to identify the user at the identity provider;

means for receiving a request from a user device to obtain user credentials for a particular application;

means for obtaining said user credentials for said application from the identity provider; and

means for forwarding said user credentials to said user device.

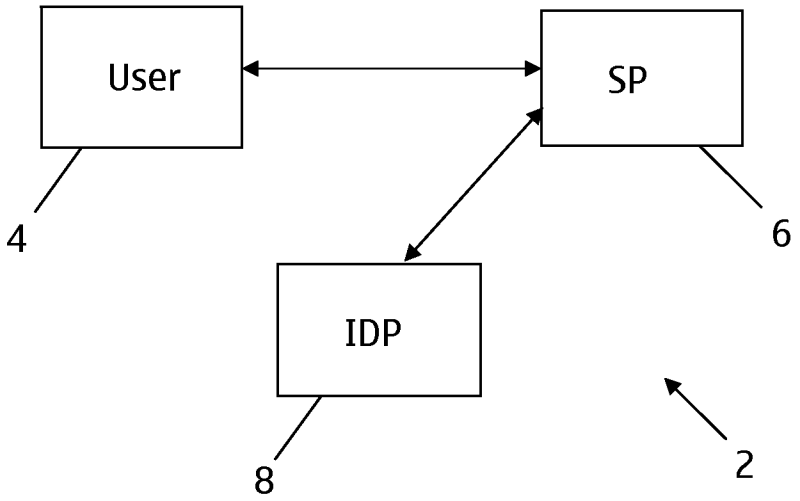
User
SP
IDP
4
6
8
2

Fig. 1

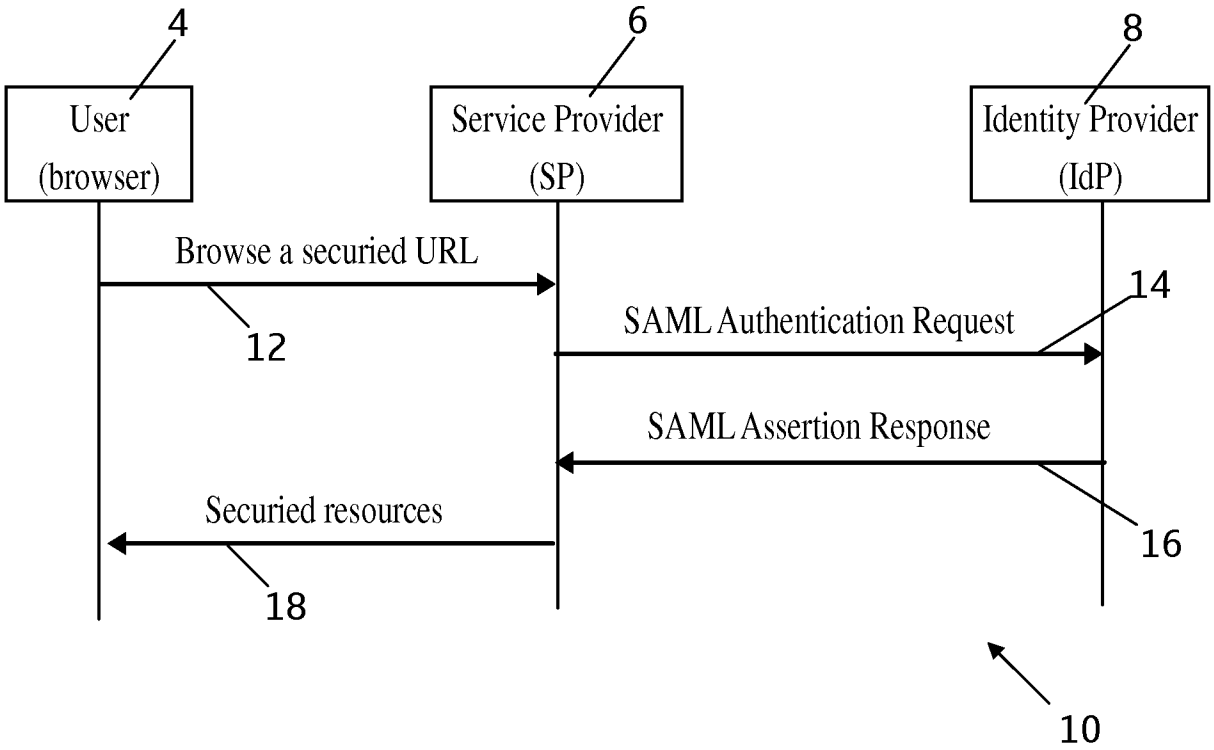
4
6
8
User
(browser)
Service Provider
(SP)
Identity Provider
(IdP)
Browse a securied URL
12
SAML Authentication Request
14
SAML Assertion Response
Securied resources
16
18
10

Fig. 2

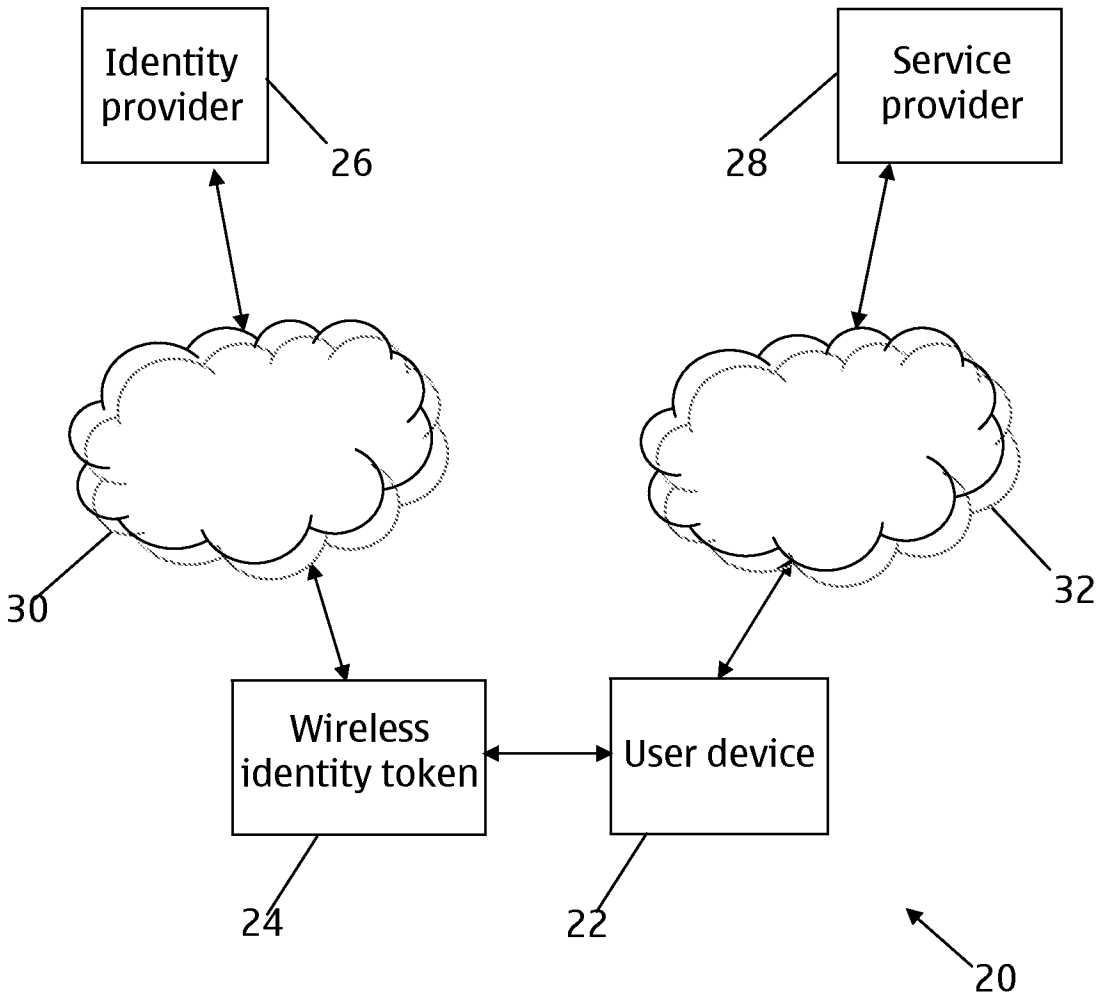
Identity provider
26
Service provider
28
30
32
Wireless identity token
User device
24
22
20

Fig. 3

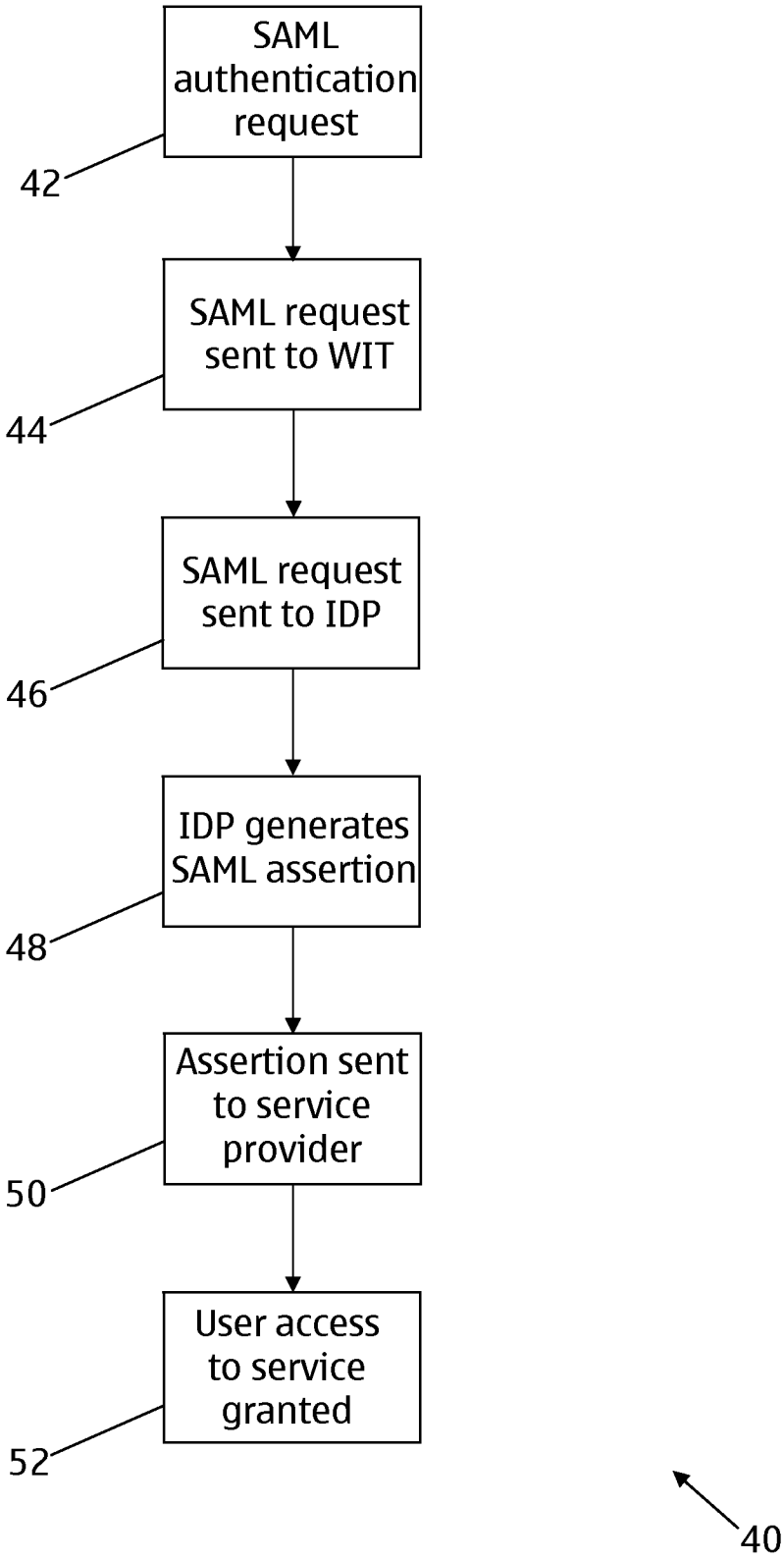
SAML authentication request
42
SAML request sent to WIT
44
SAML request sent to IDP
46
IDP generates SAML assertion
48
Assertion sent to service provider
50
User access to service granted
52
40

Fig. 4

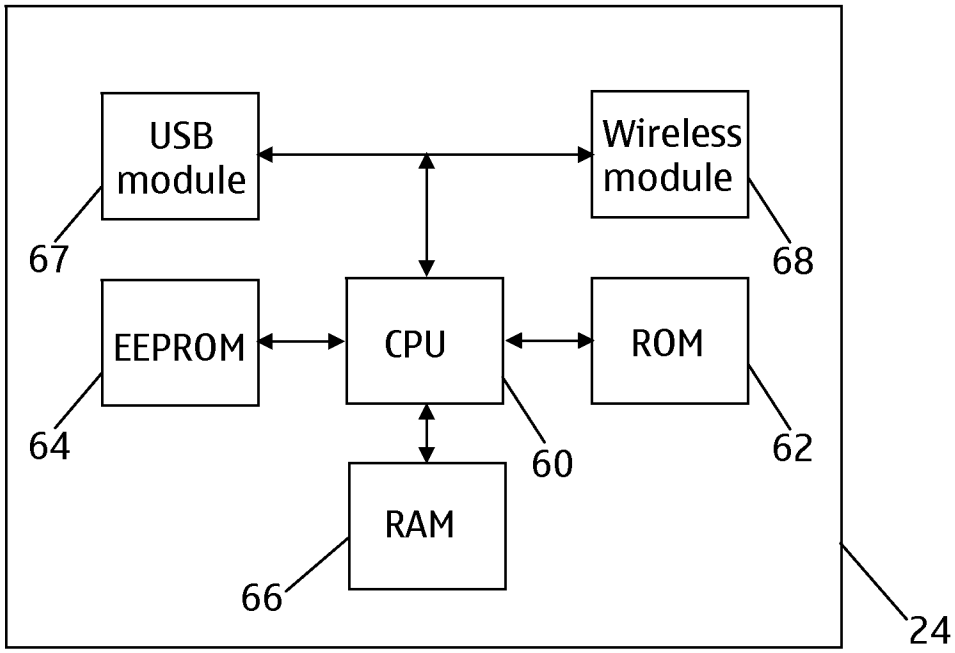
USB module
Wireless module
67
68
EEPROM
CPU
ROM
64
60
62
RAM
66
24

Fig. 5

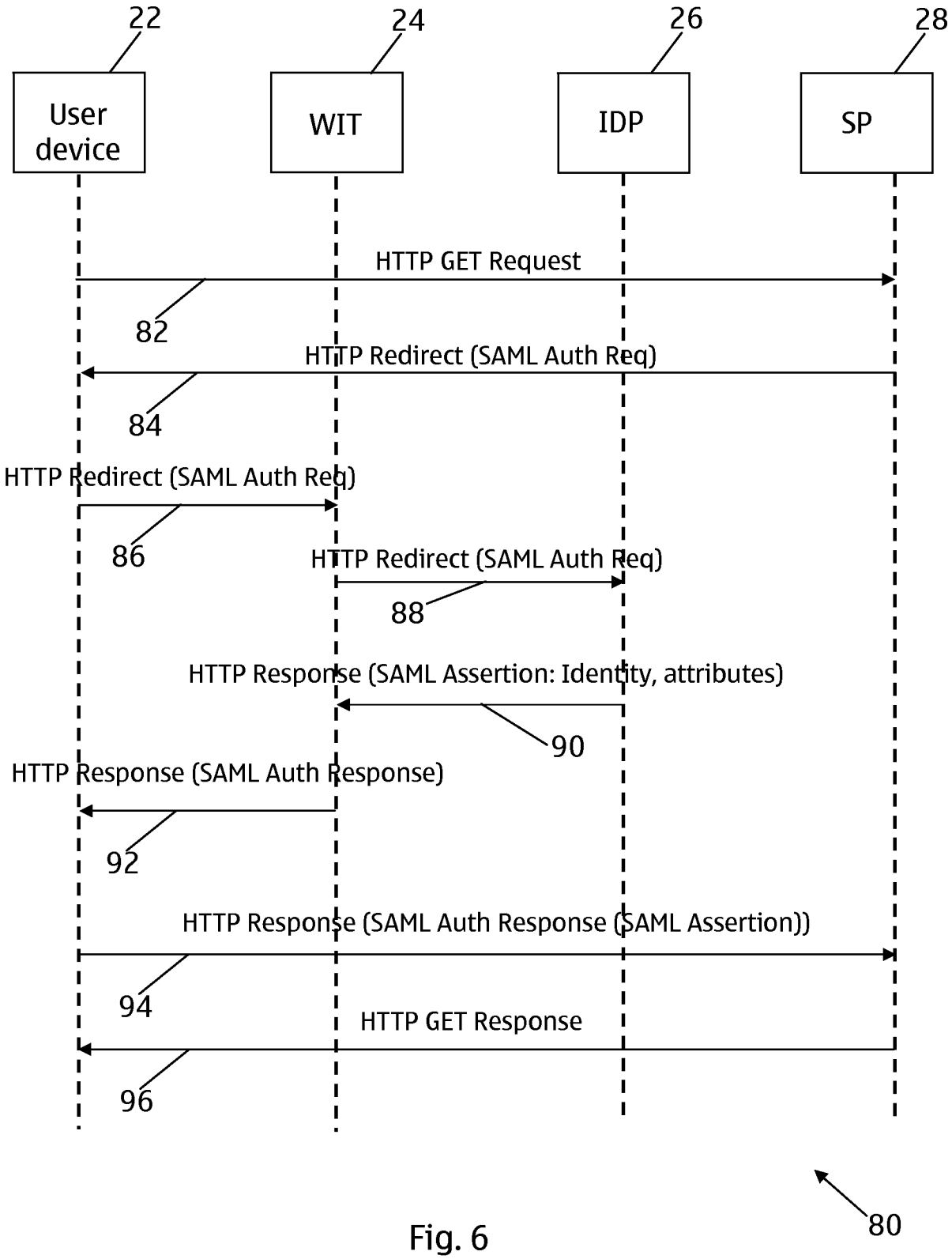
22
24
26
28
User device
WIT
IDP
SP
HTTP GET Request
82
HTTP Redirect (SAML Auth Req)
84
HTTP Redirect (SAML Auth Req)
86
HTTP Redirect (SAML Auth Req)
88
HTTP Response (SAML Assertion: Identity, attributes)
90
HTTP Response (SAML Auth Response)
92
HTTP Response (SAML Auth Response (SAML Assertion))
94
HTTP GET Response
96
80

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/051944

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06 G06F21/00

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 H04W 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	US 2005/278547 A1 (HYNDMAN ARN [CA] ET AL) 15 December 2005 (2005-12-15) abstract figures 1,2,4 paragraph [0001] paragraph [0009] paragraph [0016] - paragraph [0017] paragraph [0029] paragraph [0032] - paragraph [0034] paragraph [0049] paragraph [0058] paragraph [0063] ----- -/--	1-12, 14-17

[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 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
18 January 2010	28/01/2010

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	Oliveira, Joel

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Pat Patterson et al: "Federated Identity: Single Sign-On Among Enterprises" 14 October 2004 (2004-10-14), XP002563689 Retrieved from the Internet: URL:developers.sun.com/identity/reference/techart/federated.html> [retrieved on 2010-01-13] figure 1 page 2	1-17
A	OASIS: "Security Assertion Markup Language (SAML) V2.0 Technical Overview" 25 March 2008 (2008-03-25), XP002563690 Retrieved from the Internet: URL:www.oasis-open.org> [retrieved on 2010-01-13] the whole document	1-17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/051944

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005278547 A1	15-12-2005	NONE	