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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2010 (29.12.2010)

PCT

(10) International Publication Number
WO 2010/149222 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) International Application Number:
PCT/EP2009/058060

(22) International Filing Date:
26 June 2009 (26.06.2009)

(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)*: **BAUER-HERMANN, Markus** [DE/DE]; Hofmarkstrasse 37, 94529 Aicha v.W. (DE). **SEIDL, Robert** [DE/DE]; Laurenziweg 5, 82549 Königsdorf (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, 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: ATTRIBUTE MANAGEMENT

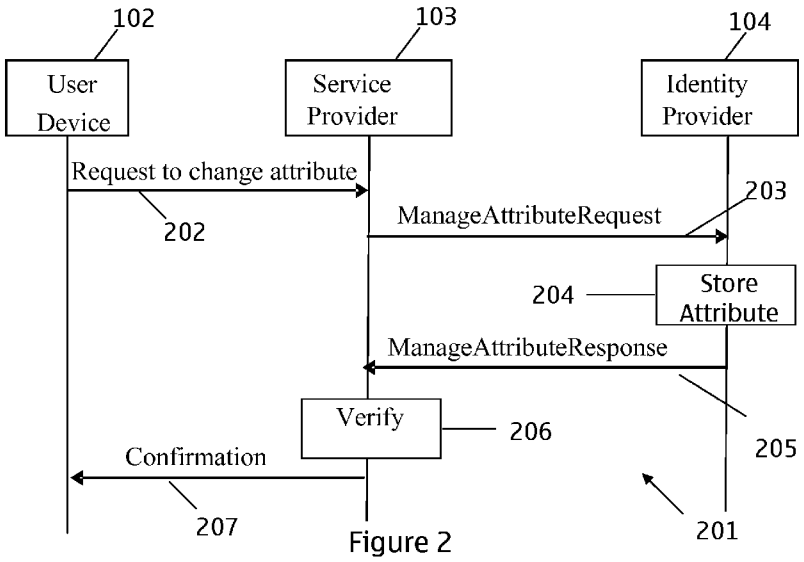


Figure 2

(57) Abstract: Methods and apparatus are described which enable user attributes to be stored and managed at an identity provider (104). A service provider (103) may pass (203) a manage attribute request which includes attribute values of at least one attribute to the identity provider (104). The identity provider (104) stores (204) the attribute values and returns (205) a manage attribute response message to the service provider (103).

WO 2010/149222 A1

Attribute Management

The present invention relates to attribute management in an identity management system.

More and more services and applications are becoming available on the Internet, and many of these services and applications require authentication. One approach that has been developed to assist users to access multiple services and 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.

Security Assertion Markup Language (SAML) is an XML (eXtensible Markup Language) standard for exchanging authentication and authorisation 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).

The SAML protocol currently provides two methods that enable a service provider to retrieve attributes relating to a user that has been authenticated by an identity provider.

The first method is an Attribute-Push-Method in which the identity provider can send attribute information within the SAML assertion provided in response to the service provider's user authentication request.

The second method is an Attribute-Pull-Method in which the service provider can use an AttributeAuthority message or an AttributeQuery message to retrieve information regarding user attributes from the identity provider once the user has been authenticated by the identity provider.

In both methods described hereinabove, the service provider can only obtain information relating to the attributes of the user logged into the service provider. There currently exists no mechanism to enable a service provider to transmit user attributes to be stored at the identity provider.

However, a problem with the conventional systems and methods is that there currently exists no mechanism to enable a service provider to transmit user attributes to be stored at the identity provider. This is particularly disadvantageous as the user cannot reuse a single profile containing user attributes, such as layout, preferred e-mail address etc, for different service providers. In current systems and methods the user will only be able to store attributes and change those attributes locally at each service provider meaning that the user will have to enter and change the same attributes multiple times in order to ensure they are consistent for each of the different service providers the user has an account with.

However, a further problem can arise when storing attributes at the service provider. If a user creates a temporary or transient account with a service provider then the user cannot reuse the attributes relating to the temporary or transient account when the user next logs on to the service provider. This is because by the very nature of a temporary or transient account the next time the user logs on to the service provider the user will have a different username and so the service provider will not be able to link the attributes for a user's temporary account with the user's permanent account.

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

According to a first aspect of the present invention there is provided a method comprising the steps of: transmitting a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and receiving a manage attribute response from said identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute, and wherein said at least one attribute relates to a user's profile.

Thus, many of the embodiments of the present invention provide a new mechanism that enables attribute values for one or more attributes to be transmitted to an identity provider where the identity provider may store the attribute values for the attributes. A service provider may transmit the attribute values to the identity provider in a manage attribute

request which requests the identity provider stores the attribute values for the at least one attribute. A response will be received from the identity provider that includes the stored attribute values for the attributes. An advantage of many embodiments of the present invention is that by storing the attribute values at the identity provider then the attribute values may be used for several different service providers without the user having to enter or change those attributes at each service provider.

The method may further comprise the step of: receiving a request from a user to store at the identity provider the attribute value for at least one attribute. Thus, a user can initiate the process of storing specific attribute values at the identity provider. A user may, for example, fill in a form via a web browser on a user device identifying the attributes and the corresponding attribute value that the user wishes to change or store at the identity provider.

The method may further comprise the step of: determining if the stored attribute value for the at least one attribute included in the manage attribute response matches the attribute value for the at least one attribute included in the manage attribute request. Thus, as the manage attribute response from the identity provider includes the attribute values that have been stored then it can be determined whether the attribute values for the attributes have been stored correctly or successfully. For example, if the stored attribute values do not match the attribute values that were included in the manage attribute request then it may be determined that an error has occurred in storing the attribute values at the identity provider.

Once it has been determined whether or not the attribute values for the attributes have been successfully stored then the method may further comprise transmitting a message to a user device where the message informs the user whether or not attributes were successfully stored.

A user of a service provider may have a profile that includes several attributes. The profile will include attributes relating to the user and attributes relating to the service provider that the user has an account with. User related attributes may define aspects relating to the user, for example, given name, family name, nickname, telephone number, e-mail address, postal address, hair colour, eye colour, height and so on. Service provider related attributes may define aspects that are specific to a particular service provider or general to all service provider accounts that a user may have, for example, the attributes may include preferred language, preferred layout, preferred means of communication and so on.

The manage attribute request may be compatible with, or in accordance with, the Security Assertion Markup Language protocol; and the manage attribute response may be compatible with, or in accordance with, the Security Assertion Markup Language protocol.

According to a second aspect of the present invention there is provided an appratus comprising: an output adapted to transmit a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and a first input adapted to receive a manage attribute response from said

identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute, and wherein said at least one attribute relates to a user's profile.

According to a third aspect of the present invention there is provided an apparatus adapted to transmit a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and receive a manage attribute response from said identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute, and wherein said at least one attribute relates to a user's profile.

The apparatus may be further adapted, for example, by comprising a second input, to receive a request from a user to store at the identity provider the attribute value for at least one attribute. The apparatus may be further adapted, for example, by comprising a processor, to determine if the stored attribute value for the at least one attribute included in the manage attribute response matches the attribute value for the at least one attribute included in the manage attribute request. The apparatus may be further adapted, for example, by comprising a second output, to transmit a message to the user where the message indicates whether or not the attribute values were successfully or correctly stored at the identity provider. The apparatus may be a server or a computing device. The apparatus may be operated by a service provider.

The first input and the second input may be the same input or different inputs to the apparatus. Similarly, the first output and the second output may be the same output or different outputs of the apparatus

As a skilled person in the art will appreciate, the apparatus may be adapted to perform the functions in many different ways. For example, the apparatus may be adapted by installing and executing on the apparatus the appropriate and corresponding computer readable executable code in order to enable the apparatus to perform the necessary functions and tasks.

According to a fourth aspect of the present invention there is provided a computer program or a computer program product comprising computer readable executable code for: transmitting a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and receiving a manage attribute response from said identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute, and wherein said at least one attribute relates to a user's profile.

The computer program product may further comprise computer readable executable code for: receiving a request from a user to store at the identity provider the attribute value for at least one attribute.

The computer program product may further comprise computer readable executable code for: determining if the stored attribute value for the at least one attribute included in the manage attribute response matches the attribute value for the

at least one attribute included in the manage attribute request.

The computer program product may further comprise computer readable executable code for performing any or all of the functions in accordance with the aspects of the invention.

According to a fifth aspect of the present invention there is provided a method comprising the steps of: receiving a manage attribute request from a service provider wherein the manage attribute request includes an attribute value for at least one attribute; storing the attribute value for the at least one attribute in a database; and transmitting a manage attribute response to the service provider wherein the manage attribute response includes the stored attribute value for the at least one attribute, and wherein the at least one attribute relates to a user's profile.

Thus, many of the embodiments of the present invention provide a new mechanism that enables attribute values for one or more attributes to be received from a service provider which are then stored in a database. Once the attribute values have been stored in the database a manage attribute response may be generated and transmitted to the service provider where the response includes the stored attribute values. This may enable the service provider to verify and check that the stored attribute values match the attribute values in the manage attribute request. An identity provider may receive the manage attribute request from the service provider, the database may be located at the identity provider and the identity provider may generate and transmit the manage attribute response.

The manage attribute request may be in accordance with Security Assertion Markup Language protocol; and the manage attribute response may be in accordance with Security Assertion Markup Language protocol.

According to a sixth aspect of the present invention there is provided an apparatus comprising an input adapted to receive a manage attribute request from a service provider wherein said manage attribute request includes an attribute value for at least one attribute; a processor adapted to store said attribute value for said at least one attribute in a database; and an output adapted to transmit a manage attribute response to said service provider wherein said manage attribute response includes said stored attribute value for said at least one attribute, and wherein said at least one attribute relates to a user's profile.

According to a seventh aspect of the present invention there is provided an apparatus adapted to: receive a manage attribute request from a service provider wherein the manage attribute request includes an attribute value for at least one attribute; store the attribute value for the at least one attribute in a database; and transmit a manage attribute response to the service provider wherein the manage attribute response includes the stored attribute value for the at least one attribute, and wherein the at least one attribute relates to a user's profile.

The apparatus may be a server or a computing device. The apparatus may be operated by an identity provider.

As a skilled person in the art will appreciate, the apparatus may be adapted to perform the functions in many different ways. For example, the apparatus may be adapted by install-

ing and executing on the apparatus the appropriate and corresponding computer readable executable code in order to enable the apparatus to perform the necessary functions and tasks.

According to an eighth aspect of the present invention there is provided a computer program or computer program product comprising computer readable executable code for: receiving a manage attribute request from a service provider wherein the manage attribute request includes an attribute value for at least one attribute; storing the attribute value for the at least one attribute in a database; and transmitting a manage attribute response to the service provider wherein the manage attribute response includes the stored attribute value for the at least one attribute, and wherein the at least one attribute relates to a user's profile.

The computer program product may further comprise computer readable executable code for performing any or all of the functions in accordance with the aspects of the invention.

An advantage of many embodiments of the present invention is that a new mechanism is provided which enables user attributes to be stored in a database of the identity provider where the process is initiated by a service provider. A further advantage of many embodiments of the present invention is that by storing user attributes in a database of the identity provider then the user can reuse the attributes for several different service providers without having to enter and provide the user attributes to each service provider independently. Furthermore, by providing the capability for the user attributes stored in a database of the identity provider to be changed then the user does not have to manually change the same attribute for each of the service providers with which the user has an account as the changed attribute values

at the identity provider may be used by all service providers.

Embodiments of the present invention will now be described, by way of example only, and with reference to the accompanying drawings in which:

Figure 1 is a block diagram of an identity management system in accordance with the aspects of the present invention.

Figure 2 shows a message sequence in accordance with aspects of the present invention.

Figure 1 shows a system, indicated generally by the reference numeral 101, comprising an end user 105, a user device 102, a service provider 103 and an identity provider 104. When the end user 105 of the system 101 wants to access a secure resource, service or application at the service provider 103, and the service provider 103 requires the user's identity to be authenticated, the identity provider 104 can be used to provide the required authentication information to the service provider 103.

The user device may comprise an inputs and outputs 106 in order to receive and transmit messages and data. The user device may be a computing device, such as a computer or a mobile device, such as a mobile phone, personal digital assistant. The service provider 103 may include a server or computing device that may comprise inputs and outputs 107 and processors 108. The identity provider 104 may include a server or computing device that may comprise inputs and outputs 109 and processors 110.

In an exemplary use of the system 101, SAML assumes that the user 105 has enrolled with at least one identity provider (such as the identity provider 104). The identity provider 104 is expected to provide local authentication services to the user 105. The service provider 103 relies on the identity provider 104 to identify the user 105. When a user 105 wants to access a service that is provided by a service provider 103 who has a contract with the identity provider 104 (i.e. the service provider 103 and the identity provider 104 form at least part of a circle of trust), the service provider 103 requests a user authentication from the identity provider 104. In response to the service provider's request, the identity provider 104 passes a SAML assertion to the service provider 103. On the basis of this assertion, the service provider 103 can make decisions, for example, the service provider 103 can decide whether to grant access to the resources, services or applications requested by the user 105.

If the user 105 has been authenticated then the user 105 is logged in to the service provider 103 and can access the services, resources and/or applications that the user 105 wishes to use.

Once a user 105 has logged in to the service provider 103 then the embodiments of the present invention provide a new mechanism to enable the user 105 to store and/or change user specific attributes and user's service provider attributes in an identity provider's database via the service provider.

A user 105 will have a profile that includes several attributes. The profile will include attributes relating to the user and attributes relating to each of the service providers that the user has an account with. User related attributes

may define aspects relating to the user, for example, given name, family name, nickname, telephone number, e-mail address, postal address, hair colour, eye colour, height and so on. Service provider related attributes may define aspects that are specific to a particular service provider or general to all service provider accounts that a user may have, for example, the attributes may include preferred language, preferred layout, preferred means of communication and so on.

The attributes defining a user profile may be stored in a database at the identity provider. If an attribute value does not exist in the database for a particular attribute then this can be created by storing an attribute value for the particular attribute. If an attribute doesn't exist then an attribute can be created by storing the attribute along with a corresponding attribute value in the database. If an attribute value for a particular attribute exits and a user wishes to change the attribute value then this can be performed by storing the new attribute value in place of the previous attribute value for a particular attribute in a database. In other words, the user may add or change any attribute relating to the user or to the user's account with a service provider by storing the appropriate attribute value in a database at the identity provider.

Figure 2 shows an exemplary message sequence, indicated generally by the reference numeral 201, demonstrating the process of storing attribute values relating to a user's profile at the identity provider in accordance with the embodiments.

The message sequence 201 starts with the end user 105 sending a message 202 to the service provider 103 via a user device 102 (for example using a web browser) requesting to add or change an attribute of the user's profile.

The user 105 may request to change or add attributes by, for example, entering data into a form on the service provider 103. The service provider 103 will then generate a new message called ManageAttributeRequest which will include an AttributeStatement block which includes at least one attribute value for one or more attributes that the user 105 wishes to change or store at the identity provider 104.

For example, if a user requests to change their given name to "Tom" and to change their e-mail address to "trscavo@gmail.com" then an example ManageAttributeRequest message is given below. The message given below is only an example of the format and content of a ManageAttributeRequest message. As a person skilled in the art will appreciate the message may include different, fewer or more blocks. Similarly, the message may also include different, fewer or more tags.

```
<samlp:ManageAttributeRequest
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   ID="aaf23196-1773-2113-474a-fe114412ab72"
   Version="2.0"
   IssueInstant="2006-07-17T20:31:40Z">
  <saml:Issuer
    Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
    C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
```

```
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameID>
    </saml:Subject>

    <saml:AttributeStatement>
      <saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
        x500:Encoding="LDAP"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:2.5.4.42"
        FriendlyName="givenName">
        <saml:AttributeValue
          xsi:type="xs:string">Tom</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
        x500:Encoding="LDAP"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
        FriendlyName="mail">
        <saml:AttributeValue

xsi:type="xs:string">trscavo@gmail.com</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
</samlp:ManageAttributeRequest>
```

The service provider passes 203 the ManageAttributeRequest to the identity provider 104. The ManageAttributeRequest may be passed to the identity provider as an HTTP redirect via the user device 102. The identity provider 104 on receipt of the ManageAttributeRequest will process 204 the request and store the identified attribute values for the identified user attributes in a database of the identity provider 104. An attribute value may be changed by storing the new attribute value in place of the previous attribute value for the particular attribute.

Once the identity provider 104 has stored the identified attributes in a database the identity provider 104 will generate a ManageAttributeResponse message that includes an AttributeStatement block. The AttributeStatement block will include the attribute values of the attributes that have been stored in the database of the identity provider 104. An example ManageAttributeResponse message is given below. The message given below is only an example of the format and content of a ManageAttributeResponse message. As a person skilled in the art will appreciate the message may include different, fewer or more blocks. Similarly, the message may also include different, fewer or more tags.

```
<samlp:ManageAttributeResponse
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   ID="aaf23196-1773-2113-474a-fe114412ab72"
   Version="2.0"
   IssueInstant="2006-07-17T20:31:40Z">

  <saml:Assertion
  MajorVersion="1" MinorVersion="0"
  AssertionID="128.9.167.32.12345678"
```

```
  Issuer="Smith Corporation">
    <saml:Issuer
    Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">
      http://idm.nsn.com
    </saml:Issuer>
    <saml:Subject>
      <saml:NameID
        Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameID>
    </saml:Subject>
    <saml:AttributeStatement>
      <saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X5
00"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
      Name="urn:oid:2.5.4.42"
      FriendlyName="givenName">
      <saml:AttributeValue
        xsi:type="xs:string">Tom</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X5
00"
      x500:Encoding="LDAP"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
      Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.26"
```

```
        FriendlyName="mail">
        <saml:AttributeValue

    xsi:type="xs:string">trscavo@gmail.com</saml:AttributeValue>
      </saml:Attribute>
      </saml:AttributeStatement>
    </saml:Assertion>
    <samlp:Status
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
      <samlp:StatusCode
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Value="urn:oasis:names:tc:SAML:2.0:status:Success">
      </samlp:StatusCode>
    </samlp:Status>
  </samlp:ManageAttributeResponse>
```

The identity provider 104 passes 205 the ManageAttributeResponse to the service provider 103. The ManageAttributeResponse may be passed to the service provider 103 as an HTTP redirect via the user device 102. The service provider 103 on receipt of the ManageAttributeResponse can check and verify 206 that the attributes have been correctly stored in the database of the identity provider 104. The attribute values for the user attributes included in the ManageAttributeResponse from the identity provider 104 were retrieved from the database of the identity provider after the attribute values were stored in the database. Thus, by comparing the attribute values included in the ManageAttributeResponse with the attribute values included in the ManageAttributeRequest that was originally passed from the service provider to the identity manager, the service provider can determine that the correct attribute values were stored in the identity provider's database.

The service provider 103 may then send 207 a message to the user device 102 to inform the user 105 that the attribute values of the user attributes the user requested to change or store were successfully (or not) stored at the identity provider 104.

Accordingly, the embodiments of the present invention provide a new mechanism that enables user attributes to be stored in a database of the identity provider rather than stored by the service provider. The embodiments also provide a new mechanism for editing or changing specific attributes stored in a database of the identity provider.

Thus, the embodiments of the present invention provide several advantages over the conventional systems which, as discussed hereinabove, do not enable a user of a service provider to store attributes directly to the identity provider's database or enable a user to change specific attributes stored in the identity provider's database via a service provider.

One advantage is that by storing user attributes in a database of the identity provider then the user can reuse the attributes for several different service providers without having to enter and provide the user attributes to each service provider independently. Furthermore, by providing the capability for a user to change attributes stored in a database of the identity provider then the user does not have to manually change the same attribute for each of the service providers with which the user has an account.

While preferred embodiments of the invention have been shown and described, it will be understood that such embodiments are described by way of example only. Numerous variations,

changes and substitutions will occur to those skilled in the art without departing from the scope of the present invention as defined by the appended claims. For example, although the invention has been described with reference to the SAML standard, other implementations are possible. Accordingly, it is intended that the following claims cover all such variations or equivalents as fall within the spirit and the scope of the invention.

Claims

1. A method comprising the steps of:

transmitting a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and

receiving a manage attribute response from said identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute,

wherein said at least one attribute relates to a user's profile.

2. The method as claimed in claim 1 further comprising the step of:

receiving a request from a user to store at said identity provider said attribute value for at least one attribute.

3. The method as claimed in claim 1 or 2 further comprising the step of:

determining if said stored attribute value for said at least one attribute included in said manage attribute response matches said attribute value for said at least one attribute included in said manage attribute request.

4. The method as claimed in any one of the preceding claims in which said manage attribute request is compatible with Security Assertion Markup Language protocol; and said manage attribute response is compatible with Security Assertion Markup Language protocol.

5. An apparatus comprising:

an output adapted to transmit a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and

a first input adapted to receive a manage attribute response from said identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute,

wherein said at least one attribute relates to a user's profile.

6. The apparatus as claimed in claim 5 further comprising:

a second input adapted to receive a request from a user to store at said identity provider said attribute value for at least one attribute.

7. The apparatus as claimed in claim 5 or 6 further comprising:

a processor adapted to determine if said stored attribute value for said at least one attribute included in said manage attribute response matches said attribute value for said at least one attribute included in said manage attribute request.

8. A computer program product comprising computer readable executable code for:

transmitting a manage attribute request to an identity provider, wherein said manage attribute request includes an attribute value for at least one attribute and said manage attribute request requests said identity provider to store said attribute value for said at least one attribute; and

receiving a manage attribute response from said identity provider wherein said manage attribute response includes a stored attribute value for said at least one attribute,

wherein said at least one attribute relates to a user's profile.

9. The computer program product as claimed in claim 8 further comprising computer readable executable code for:

receiving a request from a user to store at said identity provider said attribute value for at least one attribute.

10. The computer program product as claimed in claim 8 or 9 further comprising computer readable executable code for:

determining if said stored attribute value for said at least one attribute included in said manage attribute response matches said attribute value for said at least one attribute included in said manage attribute request.

11. A method comprising the steps of:

receiving a manage attribute request from a service provider wherein said manage attribute request includes an attribute value for at least one attribute;

storing said attribute value for said at least one attribute in a database; and

transmitting a manage attribute response to said service provider wherein said manage attribute response includes said stored attribute value for said at least one attribute,

wherein said at least one attribute relates to a user's profile.

12. The method as claimed in claim 11 in which said manage attribute request is compatible with Security Assertion Mar-

kup Language protocol; and said manage attribute response is compatible with Security Assertion Markup Language protocol.

13. An apparatus comprising:

an input adapted to receive a manage attribute request from a service provider wherein said manage attribute request includes an attribute value for at least one attribute;

a processor adapted to store said attribute value for said at least one attribute in a database; and

an output adapted to transmit a manage attribute response to said service provider wherein said manage attribute response includes said stored attribute value for said at least one attribute,

wherein said at least one attribute relates to a user's profile.

14. A computer program product comprising computer readable executable code for:

receiving a manage attribute request from a service provider wherein said manage attribute request includes an attribute value for at least one attribute;

storing said attribute value for said at least one attribute in a database; and

transmitting a manage attribute response to said service provider wherein said manage attribute response includes said stored attribute value for said at least one attribute,

wherein said at least one attribute relates to a user's profile.

1/1

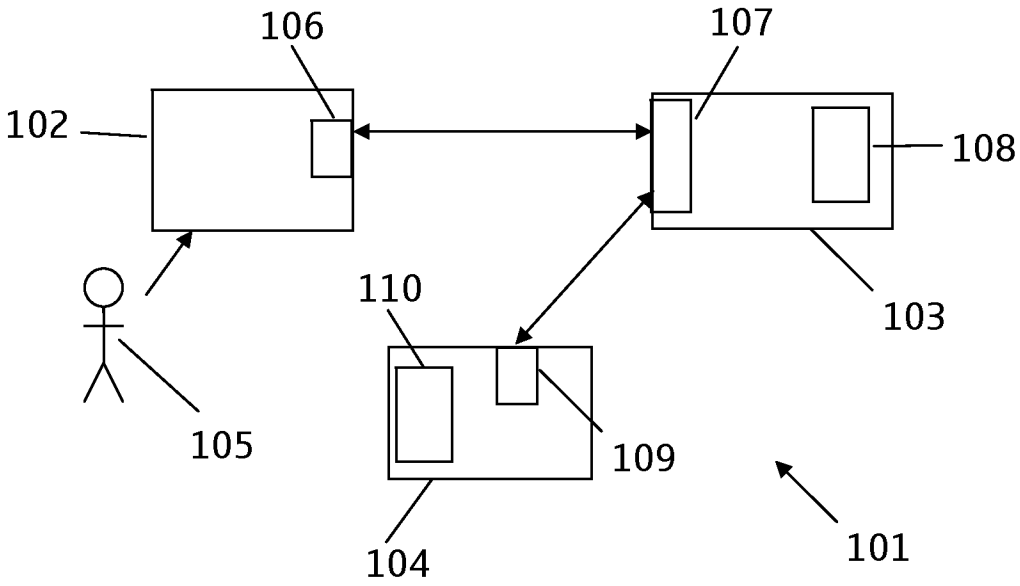


Figure 1

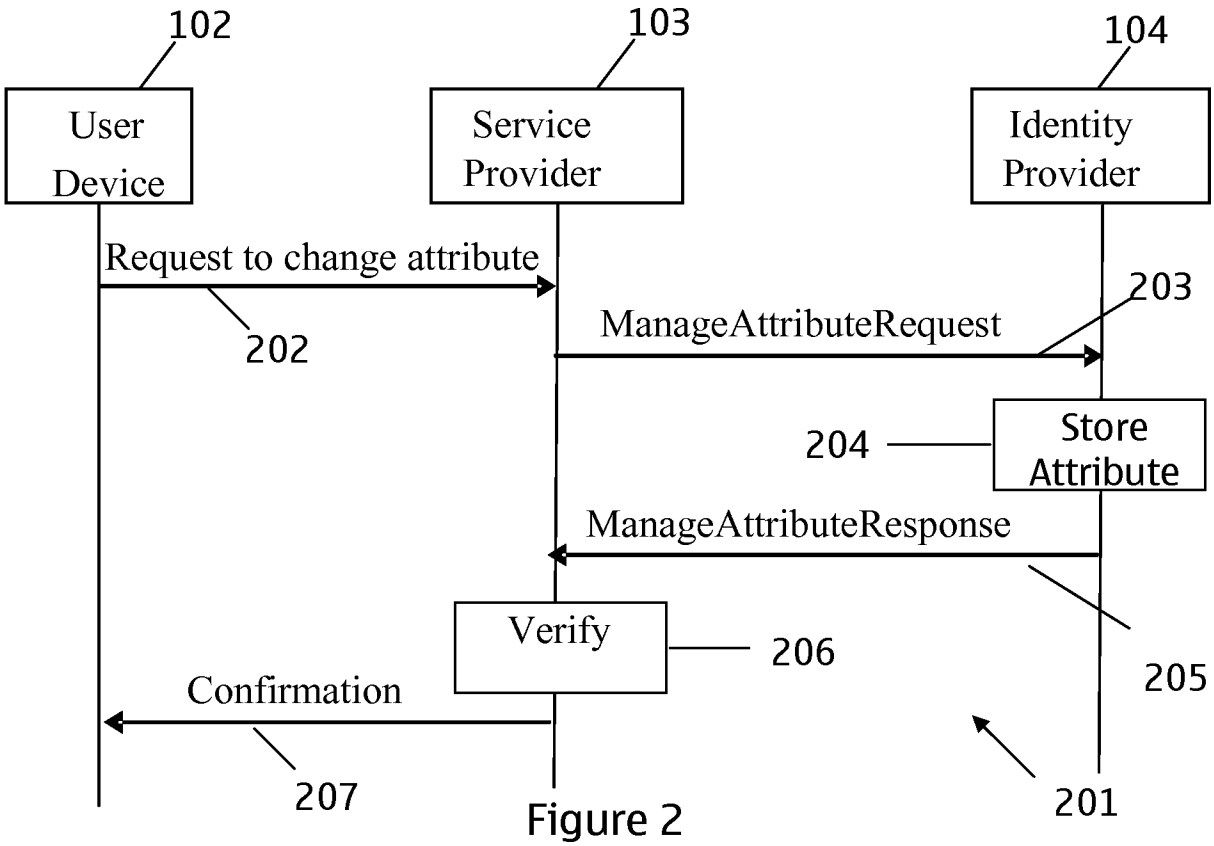


Figure 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/058060

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L29/08
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

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 2004/128378 A1 (BLAKLEY GEORGE ROBERT [US] ET AL) 1 July 2004 (2004-07-01) paragraph [0057] paragraph [0067] - paragraph [0074] paragraph [0082] paragraph [0085] paragraph [0090] paragraph [0097] paragraph [0149] - paragraph [0152] paragraph [0153] paragraph [0171] - paragraph [0174] paragraph [0175] claims 1-3 paragraph [0088] - paragraph [0089] paragraph [0147] ----- -/--	1-14

[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
20 April 2010	29/04/2010

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	Buhleier, Rainer

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/058060

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	OASIS: "Security Assertion Markup Language(SAML) V2.0 Technical Overview" vol. Committee Draft 02, 25 March 2008 (2008-03-25), XP002578461 http://www.oasis-open.org/ Retrieved from the Internet: URL:http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf> [retrieved on 2010-04-14] abstract sections 3.1, 3.2, 3.3, 4.4.2, 4.4.3, 5.4.3, 5.5	1-14
X	US 2006/236382 A1 (HINTON HEATHER M [US] ET AL HINTON HEATHER MARIA [US] ET AL) 19 October 2006 (2006-10-19) paragraph [0059] paragraph [0177] - paragraph [0179] paragraph [0187] - paragraph [0188] paragraph [0189] paragraph [0194] paragraph [0213]	1-14
A	US 2003/149781 A1 (YARED PETER [US] ET AL) 7 August 2003 (2003-08-07) paragraph [0057] paragraph [0096] - paragraph [0097] paragraph [0108] - paragraph [0110] paragraph [0117] - paragraph [0119] paragraph [0162] - paragraph [0165] paragraph [0176]	1-14
A	SHOICHIROU FUJIWARA ET AL: "A Privacy Oriented Extension of Attribute Exchange in Shibboleth" APPLICATIONS AND THE INTERNET WORKSHOPS, 2007. SAINT WORKSHOPS 2007. I NTERNATIONAL SYMPOSIUM ON, IEEE, PI, 1 January 2007 (2007-01-01), pages 28-28, XP031044122 ISBN: 978-0-7695-2757-4 abstract sections 4., 4.1.; page 3; figures 3-6	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/058060

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004128378 A1	01-07-2004	AU 2003288465 A1	22-07-2004
		WO 2004059530 A1	15-07-2004
		TW 246005 B	21-12-2005
US 2006236382 A1	19-10-2006	CN 101133421 A	27-02-2008
		EP 1864240 A1	12-12-2007
		WO 2006103176 A1	05-10-2006
		JP 2008538247 T	16-10-2008
US 2003149781 A1	07-08-2003	AU 2002360465 A1	17-06-2003
		EP 1461718 A1	29-09-2004
		US 2008014931 A1	17-01-2008
		US 2008016232 A1	17-01-2008