

performed because of the quality of the credential the user initially used to sign into the identity provider. For instance, a service provider performing banking transactions may require a stronger form of authentication (e.g., a certificate) to assure the integrity of the transaction.

[0010] In another embodiment, users create account linkages or federations among identity providers and service providers. An explicit trust chain is created when a user invokes account linking between a service provider and an identity provider. Accounts are linked using, for example, dynamically generated handles, which are shared by the service provider and identity provider being linked. When two elements of a trust chain communicate, they can differentiate a user by the shared secret or handle. The handle or handles are stored in user directories in each of the linked system entities. Users manage these links by setting user policies and privacy preferences. According to one embodiment, user policies are enforceable because a username is resolved within a limited namespace. That is, each link of a trust chain forms a namespace. Providers resolve the username and enforce the user's policies at each link in the trust chain and, therefore, cannot skip over each other in the trust chain because the account handle or handles are not resolvable in a global namespace.

[0011] In a further embodiment, system entities communicate using a web services architecture for back channel communications. Web services uses an application layer protocol, such as Hypertext Transport Protocol (HTTP) for communications. System entities exchange user profile data using Extensible Markup Language (XML) schemas. Simple Object Access Protocol (SOAP) encapsulates the XML data and provides interoperability among the numerous computing devices that can host service providers and identity providers.

[0012] In a still further embodiment, service delegation provides additional web services interactions. Service providers that are accessible to other service providers via an identity provider (i.e., a federated trust chain) can provide delegated services. For example, a user can specify in a primary identity provider a mobile phone serviced by a mobile operator. Service delegation embodiments include an identity provider functioning as a service gateway and as a service directory. An example service delegation is a merchant service provider that contacts an identity provider to send the user a Short Message Service (SMS) message using the user's mobile phone service provider. Service tickets can be used to authorize a service provider to perform the delegated service.

[0013] Further features of the invention, its nature and various advantages will be more apparent from the accompanying drawings and the following detailed description.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention and, together with the description, serve to explain the principles of the invention.

[0015] FIG. 1 is an illustration of a distributed identity system in accordance with the present invention.

[0016] FIG. 2 is an interaction flowchart illustrating a single sign-on embodiment including service provider initiated back channel communication.

[0017] FIG. 3 is an interaction flowchart illustrating a single sign-on embodiment including identity provider initiated back channel communication.

[0018] FIG. 4 is an interaction flowchart illustrating a single sign-on embodiment including common domain facilitation.

[0019] FIG. 5 is an interaction flowchart illustrating an identity federation process.

[0020] FIG. 6 illustrates further details of identity federation interactions according to one embodiment of the present invention.

[0021] FIG. 7 illustrates account linking for an identity provider and a service provider.

[0022] FIG. 8 illustrates account linking using handles.

[0023] FIG. 9 illustrates account linking for an identity provider and multiple service providers.

[0024] FIG. 10 illustrates account linking for multiple identity providers and a service provider.

[0025] FIG. 11 illustrates linking of multiple identity providers.

[0026] FIG. 12 illustrates a service provider user interface.

[0027] FIG. 13 illustrates an identity provider user interface.

[0028] FIG. 14 illustrates a user interface for account linking.

[0029] FIG. 15 is a message flow diagram of a single logout embodiment.

[0030] FIG. 16 is a message flow diagram of a further single logout embodiment.

[0031] FIG. 17 is an interaction flowchart illustrating a single sign-on embodiment including a user-signed ticket.

[0032] FIG. 18 is an interaction flowchart illustrating a single sign-on embodiment including a client-side certificate.

[0033] FIG. 19 is an interaction flowchart illustrating service delegation using an identity provider as a gateway.

[0034] FIG. 20 is an interaction flowchart illustrating service delegation using an identity provider as a directory.

[0035] FIG. 21 is an interaction flowchart illustrating a wallet service hosted by an identity provider.

[0036] FIG. 22 is an interaction flowchart illustrating a wallet service using an identity provider as a gateway.

[0037] FIG. 23 is an interaction flowchart illustrating a token-based wallet service.

[0038] FIG. 24 is an interaction flowchart illustrating user policy validation.

#### DETAILED DESCRIPTION OF THE EMBODIMENTS

[0039] The present invention is now described more fully with reference to the accompanying figures, in which several embodiments of the invention are shown. The present invention may be embodied in many different forms and should