

DISTRIBUTED NETWORK IDENTITY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a divisional of U.S. patent application Ser. No. 10/309,773, filed Dec. 3, 2002, which claims priority to U.S. provisional patent application Ser. No. 60/337,234, filed on Dec. 4, 2001, entitled "Identity solution for a network," U.S. provisional patent application Ser. No. 60/339,536, filed on Dec. 10, 2001, entitled "Identity solution for a network," and U.S. provisional patent application Ser. No. 60/365,943, filed on Mar. 19, 2002, entitled "Federated Identity," from which priority is claimed under 35 U.S.C. §119(e) and which applications are incorporated by reference herein in their entireties.

TECHNICAL FIELD

[0002] This invention relates generally to network computing and, more particularly, to a distributed network identity architecture including single sign-on authentication, federation, and delegation among system entities.

BACKGROUND

[0003] Network-based services are becoming increasingly pervasive. For example, electronic commerce services are widely available and appealing for both individual consumers and businesses. From a consumer perspective, an abundance of services offers flexibility and economic benefits. Internet-based businesses or service providers routinely maintain an account relationship with their customers. Customer databases that include identity information facilitate and increase the integrity of transactions. Identity information helps a service provider deliver value to its consumer. Further, customer directories and data are important business assets. From the service provider viewpoint, a well-developed customer database creates revenue. A customer database enables targeted marketing and extended functionality that increases customer loyalty and generates business goodwill.

[0004] In a typical service provider framework, each service provider maintains a distinct user account database. For a user or consumer, this often means that the user must create a unique account with the service provider to access the services. One difficulty with this conventional identity framework is that it hinders service provider usability. For example, the user is required to enter repetitively similar identity information for each service provider, such as name, mailing address, and telephone number. Because user accounts are distinct for each service provider, the user must be singularly authenticated (e.g., a password-based login) for each service provider. The user also must remember or securely store the account name and password used for each service provider, which further frustrates and inconveniences the user. Because each service provider requires a unique account name, a user may have many different account names and identity profiles for various service providers by necessity. Alternatively, in the conventional context, a user may desire many different account names to reduce the likelihood that service providers will be able to engage in the unauthorized sharing of a customer's personal information. Thus, because of these complications, users may be highly selective of service providers or prefer to restrict their usage of network-based service providers.

[0005] Centralized identity methods address some of the limitations of the conventional identity framework. Centralized technologies can reduce the amount of repetitive data entry required when users access various service providers. However, the privacy and security of centralized identity data are paramount user concerns. Centralized identity technologies typically create a global name that is used for multiple affiliated service providers. A central authority stores the identity data and disseminates it to the service providers. The central authority may permit some user control over the information that is available to the service providers. The service providers could, however, collude to violate the user's privacy preferences because of the common visibility of the global user name. Further, a physical or an electronic breach of security at the central authority could expose large amounts of identity data to theft or to tampering.

[0006] From a service provider perspective, an additional problem with typical centralized identity methods is the control or ownership of the customer database. The central authority could impose restrictions on the service provider's use of its customer directory. This could have the undesirable consequence of restricting the service provider's ability to generate revenue from a valuable business asset.

[0007] Additionally, other identity approaches have been network- or application-specific implementations. One disadvantage of these approaches is that they are often limited to homogeneous networks or operate only with specific computing devices. For example, a network- or application-specific single sign-on architecture may enable a user to access the resources of a local or a closely administered service provider, but not resources offered by other service providers. Therefore, network- or application-specific approaches are often limited in scope to local or closely administered environments and offer a user few convenience benefits outside of these environments.

[0008] What is therefore needed is an identity architecture that is decentralized or distributed for user authentication and storage of identity information, that provides single sign-on and single logout convenience for users, that permits users to link accounts and to set enforceable privacy controls, and that provides for delegation of services among service providers.

SUMMARY OF THE INVENTION

[0009] An embodiment of the present invention provides a distributed network identity. Users store portions of their identity information with one or more identity providers. Identity information includes attributes such as the user's name, mailing address, e-mail, telephone number, and credit card number. An identity provider is an entity that creates, manages, and stores identity information for a plurality of users. A service provider is an entity that provides a service to a user and makes use of the aspects of the user's identity it has been authorized to access. A single sign-on architecture is provided to facilitate user interactions with service providers. A user can authenticate with an identity provider using, for example, a password-based credential or any other authentication mechanism. Service providers can then rely upon that authentication to provide access to authorized resources without requiring additional authentication. In some embodiments, however, additional authentication is