WEB TECHNOLOGIES

Federated Identity Management

Simon S.Y. Shim, San Jose State University
Geetanjali Bhalla, Force10networks
Vishnu Pendyala, Synopsys

The Liberty Alliance is developing a framework for identity-based Web services.

Most confidential, valuable resources on the World Wide Web are protected by some form of authentication technology. To access these resources, either via the public Internet or private intranets, users must verify their digital identity. This can range from a simple username-password combination to biometric data such as fingerprints to physical objects like hardware tokens and smart cards.

Today a typical enterprise has numerous online resources for its employees, business partners, contractors, and customers. As businesses have become more distributed to meet e-commerce demands, so too have user identities. To effectively manage these identities across different domains, there is a need for a federated identity infrastructure that links attributes in users' service provider accounts—names, addresses, phone numbers, credit information, Social Security numbers, medical data, and so on—without centrally storing personal information.

Federated identity management would enable individuals to interact with various service providers or Web sites with trust relationships by signing in just once. For example, employees could log into their company's intranet to review their healthcare information and then use the Internet to access their online bank account from the same screen without having to reauthenticate. Users could also have more control of their personal data by determining when and how service providers share their attributes across domains.

EXISTING STANDARDS

Companies have well-defined business agreements and policies for securely sharing information; they must also comply with federal laws regarding the exchange of personal data. Numerous well-established standards based on the Extensible Markup Language currently define identity information exchange across different domains or heterogeneous systems.

XML is a hardware- and software-independent data format that uses tags to describe information. XML Digital Signature adds authentication, data integrity, and nonrepudiation support for signed data. XML Encryption defines the processing rules for applying confidentiality to a wide variety of content.

SOAP is a lightweight protocol that exchanges information in a decentralized, distributed environment. The SOAP messaging framework defines a suite of XML elements for packaging arbitrary XML messages for transport between systems.

WS-Security is a set of SOAP extensions, developed by the Organization for the Advancement of Structured Information Standards (Oasis; www-open.org), for implementing message integrity and confidentiality in Web services. To ensure the secure exchange of SOAP messages among applications, the standard assigns security tokens to each message to authenticate users who can be in different domains.

The Security Assertion Markup Language is an XML-based language created by Oasis for the exchange of security-related information between online business partners. The key underlying standard for federated identity management, SAML conveys authentication information in the form of assertions about subjects. *Assertions* are statements about the subject issued by the authoritative entity. A *subject* can be any entity recognized by an identity in some security domain—for example, an individual identified by a username-password pair.

LIBERTY ALLIANCE PROJECT

Since September 2001, the Liberty Alliance (www.projectliberty.org), a global consortium of more than 150 companies and nonprofit organizations, has been developing open standards for federated identity and identity-based Web services. The consortium aims to create an infrastructure that supports all current and emerging network access devices and has defined interoperability requirements for those products—of which there are already more than 20—that meet its specifications.

The alliance establishes privacy and security best practices as well as implementation guidelines. It also collaborates with other standards bodies with an eye toward adopting or extending other specifications. For example, it has analyzed WS-Federation—a federated identity standard being jointly developed by Microsoft, IBM, RSA Security, VeriSign, and BEA—to assess the potential for converging overlapping functions. WS-Federation relies on a security token service to broker trust of identities, attributes, and authentication between participating Web services.

The Liberty Alliance framework architecture, shown in Figure 1, consists of three major components: the Identity Federation Framework (ID-FF), the Identity Web Services Framework (ID-WSF), and the Identity Services Interface Specifications (ID-SIS).

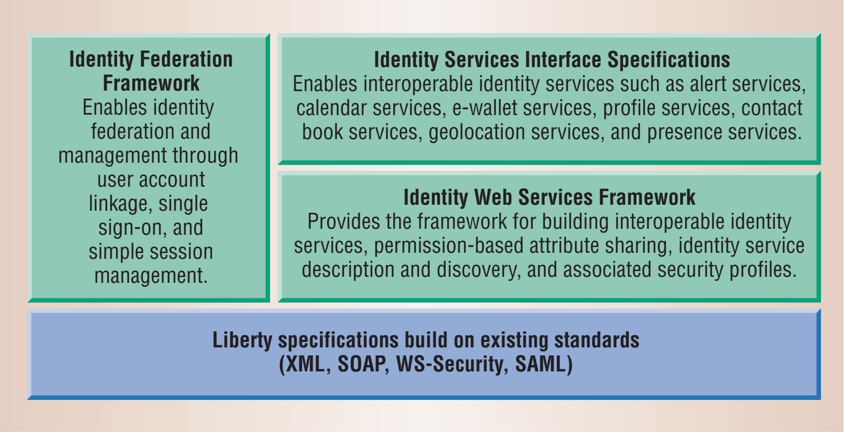
Identity Federation Framework
Enables identity federation and management through user account linkage, single sign-on, and simple session management.
Identity Services Interface Specifications
Enables interoperable identity services such as alert services, calendar services, e-wallet services, profile services, contact book services, geolocation services, and presence services.
Identity Web Services Framework
Provides the framework for building interoperable identity services, permission-based attribute sharing, identity service description and discovery, and associated security profiles.
Liberty specifications build on existing standards (XML, SOAP, WS-Security, SAML)

Figure 1. The Liberty Alliance federated identity management architecture is built on top of existing XML-based standards.

Identity Federation Framework

The completed ID-FF is built on top of existing XML-based standards and enables identity federation and management through single sign-on, user account linking, and simple session management. Various Web-based *service providers* form a federated network with an *identity provider*—an entity responsible for creating, maintaining, and authenticating all user identities—that enables users to securely operate among network members. Users need only sign on once with any member to access Web sites in the *circle of trust*.

The framework links user's service provider and identity provider accounts through pseudonyms—arbitrarily assigned names that have meaning only in the context of a given exchange. This eliminates the need for global identification and prevents collisions between different service providers. The framework also guarantees anonymity by allowing service providers to request certain attributes without knowing the user's identity.

The ID-FF consists of three main components. *Web redirection* allows Liberty-enabled entities to provide services via agents using HTTP- and SOAP-based redirection. *Web services* are protocol profiles that let Liberty-enabled entities communicate with one another.

Metadata consist of various subclasses of information exchanged between service providers and the identity provider. This includes account/identity (the name providers use while communicating), authentication content (which allows multiple authentication contexts), and provider metadata. Service and identity providers must obtain metadata regarding one another to communicate.

Identity Web Services Framework

The ID-WSF, which is nearly complete, leverages services in the ID-FF to provide a framework for building interoperable identity services, permission-based attribute sharing, identity service description and discovery, and associated security profiles. Identity services are deployed using a SOAP-based service invocation framework with a layered architecture. The framework includes a number of key features.

Permission-based attribute sharing enables companies to provide personalized Web services based on attributes that users elect to share.

Service providers can offer more efficient Web services to users by gaining access to portions of their distributed identity. A *discovery service* dynamically and securely provides the location of a user's identity service to the requesting service provider.

An *interaction service* offers an identity provider the means to obtain permission from the user to share attributes among service providers. It allows entities to interact with the owner of a resource exposed by the Web service provider.

Security profiles specify the ways for securely discovering and using identity services. They ensure that messages exchanged between service providers are secure by protecting their integrity and confidentiality.

SOAP binding defines the SOAP-based invocation of the identity service via SOAP requests and responses.

Extended client support lets devices host Liberty-enabled identity-based services, even without requiring HTTP servers or being IP addressable.

Identity services templates are building blocks for implementing identity services—for example, a personal profile service. They specify how to modify or query an identity service.

Identity Services Interface Specifications

The ID-SIS extends ID-FF and ID-WSF to support a diverse range of identity-enabled application services such as alert services, calendar services, e-wallet services, profile services, location-specific services, and presence services. It will also address emerging industry requirements for identity federation through mobile technology.

The Liberty Alliance is helping other standards groups extend their identity schemas to enable using core Liberty features including user account linking, single sign-on, simple session management, and global logout. Thus far it has published ID-SIS specifications for a personal profile service, an employee profile service, a contact book service, a geolocation service, and a presence service. These specifications define a set of protocols for providing effective, interoperable Web services.

Federated identity management standards will likely proliferate as current adopters influence their business partners to embrace them as well. However, despite the tangible advantages the technology offers—especially with respect to business mergers, acquisitions, and spin-offs—it is still in its infancy.

For federated identity management to reach critical mass in the marketplace, adopters must purchase, configure, and integrate Web access management products with existing applications or incorporate federated identity standards into their existing applications. They should also watch for emerging identity standards such as SAML 2.0 as well as forthcoming Liberty Alliance and WS-Federation specifications. ■

Simon S.Y. Shim is an associate professor in the Department of Computer Engineering at San Jose State University. Contact him at sishim@email.sjsu.edu.

Geetanjali Bhalla is a technical support engineer at Force10networks, Inc. Contact her at geet_b@hotmail.com.

Vishnu Pendyala is a R&D senior engineer at Synopsys, Inc. Contact him at vishnupendyala@hotmail.com.

Editor: Simon S.Y. Shim, Department of Computer Engineering, San Jose State University; sishim@email.sjsu.edu