Understanding federated identity

By William Stallings, special to Network World
August 30, 2007 05:50 PM ET
This vendor-written tech primer has been edited by Network World to eliminate product promotion, but readers should note it will likely favor the submitter's approach.

Network World - Federated identity management is a relatively new concept that is an extension of identity management, which is a centralized, automated approach to regulating access to enterprise resources by employees and other authorized individuals.

The focus of identity management is defining an identity for each user (human or process), associating attributes with the identity and enforcing a means by which a user can verify identity. Once implemented, identity-management systems support single sign-on (SSO), the ability of a user to access all network resources after a single authentication.
Federated identity management refers to the agreements, standards and technologies that enable the portability of identities, identity attributes and entitlements across multiple enterprises and numerous applications, supporting thousands, even millions, of users.

When multiple organizations implement interoperable federated identity schemes, an employee in one organization can use SSO to access services across the federation with trust relationships associated with the identity.

Beyond SSO, federated identity management provides other capabilities. One is a standardized means of representing attributes. Increasingly, digital identities incorporate attributes other than an identifier and authentication information (such as passwords and biometric information). Attributes can include account numbers, organizational roles, physical location and file ownership. And a user may have multiple identifiers associated with multiple roles, each with its own access permissions.

Another key function of federated identity management is identity mapping. Security domains may represent identities and attributes differently. Further, the amount of information associated with an individual in one domain may be more than is necessary in another domain. The federated identity-management protocols map identities and attributes of a user in one domain to the requirements of another domain.

A generic federated identity-management architecture includes identity providers and service providers. The identity provider acquires attribute information through dialog and protocol exchanges with users and administrators.

Service providers are entities that obtain and employ data maintained and provided by identity providers, often to support authorization decisions and to collect audit information. For example, a database server or file server is a data consumer that needs a client's credentials to know what access to provide to that client. A service
provider can be in the same domain as the user and the identity provider or in a different domain.

The goal is to share digital identities so a user can be authenticated once and access applications and resources across multiple domains. The cooperating organizations form a federation based on agreed-upon standards and mutual levels of trust.

Federated identity management uses a number of standards as the building blocks for secure identity exchange. In essence, organizations issue some form of security tickets for their users that can be processed by cooperating partners. Identity federation standards are thus concerned with defining these tickets, in terms of content and format, providing protocols for exchanging them and performing a number of management tasks. These tasks include configuring systems to perform attribute transfers and identity mapping, and performing logging and auditing functions.

The principal standard for federated identity is the Security Assertion Markup Language (SAML), which defines the exchange of security information between online business partners.

SAML is part of a broader collection of standards being issued by the Organization for the Advancement of Structured Information Standards for federated identity management. For example, WS-Federation enables browser-based federation; it relies on a security token service to broker trust of identities, attributes and authentication between participating Web services.

The challenge with federated identity management is to integrate multiple technologies, standards and services to provide a secure, user-friendly utility. The key is the reliance on a few mature standards widely accepted by industry. Federated identity management seems to have reached this level of maturity.

Stallings is coauthor of the new book, Computer Security: Principles and Practice. Contact him at ws@shore.net.

Read more about security in Network World's Security section.