



Your Guide to Interoperability & Conformance Test Services

April 2007

DGI Commentary—Understanding Identity Federation and SAML

Globally, one of the most common and effective forms of government is federalism. Federalism employs a central or federal government which unites partially self-governing states. The United States is an example of a federal government. The individual states have some autonomy in the creation of tax and laws within its state, but the states are united under federal laws. A governmental federation allows for cooperation among individual and semi-autonomous states.

Much like governmental federation, identity federation utilizes a decentralized approach. Companies and organizations have their internal identity databases and authorization procedures. As their employees or users come to their websites and use their software applications, they are required to provide some kind of identification before they are authorized to continue or access certain information. Logins are most commonly password-related, but could be other forms such as personal digital certifications. The autonomy of the company allows it to select its authorization framework and manage its users.

However, if companies and organizations are to work with their trading partners, they must have some centralized approach to identity management. Authorized users with one company must be able to gain access to certain applications or files controlled by their trading partners. One approach is to require the user to sign on at each site and retain the necessary authorization information (e.g. password) at each site. As the number of trading partners grow, this becomes troublesome. A better solution is identity federation. Like its governmental namesake, identity federation allows companies to control their own users and authorization, but allows for their authorization to be shared with other companies. The result is less login authorizations to remember for the users and easier integration of the companies' trading partners.

Security Assertion Markup Language (SAML) is the open standard which enables federation for identity management. SAML allows for authorization-related information to be shared between trading partners who have agreed to trust each other's identity management. This trust between trading partners is called a Circle of Trust. Assertions are the statements made identifying the user, the method which the user was authorized and what authorization permissions the user has been granted. While hidden from the user, trading partners exchange these assertions with each other through various bindings and protocols. The user is able to use a single sign-on



Your Guide to Interoperability & Conformance Test Services

April 2007

login with an identity provider and then is granted necessary access with the other trusted service providers.

Given the critical nature of identity management and the obvious interoperability required, certification to ensure interoperability among SAML providers is critical. As the sole certification agent of Liberty Alliance, Drummond Group offers interoperability certification for SAML 2.0. The next SAML certification event begins later this year.

For additional information, see Liberty Alliance and Federation at:
http://www.projectliberty.org/index.php/liberty/strategic_initiatives/federation