ShibOnedotThree

Shibboleth 1.3 is the final major release aligned with SAML 1.1, and includes the additions required for SAML 1.1 interoperability.

Major New Features

- Shibboleth now supports all of the required features of the SAML v1.1 specification. Support has been added to both the IdentityProvider and ServiceProvider components for the BrowserArtifact Profile and AttributePush.
- A pluggable extension accompanies the release that can function in the CredentialService role defined in the US Federal E-Authentication Initiative (http://www.cio.gov/eauthentication/\). It should soon be certified by the E-Authn labs for use by campuses along with the Shibboleth v1.3 release when interacting with applications offered by US federal agencies.
- SAML interoperability has been successfully tested with a number of commercial vendor implementations of the SAML 1.1 specificaton.
- Trust validation support has been revamped and extended. The !IdP component no longer relies on the Apache web server to validate certificates accompanying Attribute Queries. Instead, the !IdP uses the new metadata format to validate the provided certificate via PKIX and ensure that the requesting SP is authorized to use the provided certificate. Certificate authorities can be specified as applying to a group of sites or a single site. Certificates can also be exchanged directly via metadata with no PKIX validation required at all. These changes allow an instance of an !IdP or SP to successfully operate within multiple Federations, and greatly simplifies the management of certificates and trust.
- This release will support the use of two different schema to specify Federation !MetaData: the proprietary schema used in the previous Shibboleth release, and the schema specified in the SAML v2.0 specification. In the future, the older proprietary Shibboleth site and trust metadata schema will likely be deprecated. The IdentityProvider component included with this release requires the newer SAML v2.0 format metadata in order for trust validation to function. We expect Federations to be making their metadata available in this format in the near future.
- The IdentityProvider component contains an extension mechanism that should greatly simplify the process of adding features and functionality to the !IdP component. The E-Authn extension uses this mechanism; other projects (eg !GridShib, !LionShare, etc) are also planning to use this.
- The Shibboleth Deploy Guides for both the !IdP and SP componenets have been revised and expanded. They have been refocused toward containing an installation checklist and conceptual information needed to manage a Shibboleth installation. In addition, we are now publishing a significant amount of information via the Shibboleth !Wiki, and are encouraging the Shibboleth community to participate in growing the content on the !Wiki.
- The build process for the IdentityProvider component has been restructured to simplify the management of the configuration files and any custom extensions that are being used (eg. the configuration files can be stored outside the deployed directories.). The new build process supports upgrading and patch application while preserving configuration files.
- The ServiceProvider component is now available in easy-to-install packages. RPMs are available for Fedora 3 (Fedora 4 will be available soon); Solaris/SunCC packages are available for use with Solaris 8+; a new Windows Installer package is available that significantly improves the installation process and upgrade process. Some sites may still wish to compile the ServiceProvider implementation that they use in production, and README files are included that describe this process. However, using the packages should greatly simplify the evaluation and "learn about Shibboleth" stages. In addition, this release has been tested successfully with Debian 3.0 and 3.1.
- A beta version of a native java implementation of the ServiceProvider component will be available soon. This will be tested with Sun Java 1.4 and 1.5, for use with the Tomcat 5.0 and 5.5 servlet containers.
- This release does NOT support any of the SAML 2.0 protocols. The next major Shibboleth will begin to support SAML v 2.0.

Minor Changes

- The Shibboleth !IdP can be configured to only use and accept certain NameIdentifier formats with specific !RelyingParties.
- The !IdP attribute query handler is now metadata-driven when dealing with Shibboleth v1.1 or pure SAML SPs; it no longer uses a Shibboleth HTTP header for compatibility.
- Added support for authenticating artifact requesters via digital signature (but not attribute queries, so the original comments about 1.3 not fully supporting signing still stand)
- SP now fully supports digital signing of artifact or attribute queries for IdPs that support it. If https is not used, response signing from the !IdP is mandated (but encryption would then be missing).
- SP now supports user-specified signature and digest algorithms, although OpenSSL 0.9.8 is needed to enable anything other than SHA-1.
- SP now supports HTTP basic, digest, ntlm, and gss-nego SOAP authn for IdPs that support it (i.e. not Shibboleth's)
- Upgraded and tested new XML-Security-C library, fixes signatures that include non-line-wrapped base64 content
- Revamped TARGET handling in accordance with RelayState proposal
- Better handling of missing TARGET parameter
- SP now supports auto-detection of key and certificte formats
- Handles NameIdentifiers without a Format attribute as "unspecified" in accordance with SAML spec.