SOLUTIONS OVERVIEW: SAML 2.0 SINGLE SIGN ON

Overview

We aim to minimize barriers when it comes to learning and use of our applications. When a user has to remember security credentials for multiple systems, it can create a barrier and reduce utilization.

To help with this challenge, we can be configured as a SAML 2.0 service provider (sP). This requires clients to have an existing SAML 2.0 identity provider (idP).

Each SAML identity provider configuration will be handled as a professional service project. We will engage the client's IT staff directly to configure and test the authentication flow to verify that systems are correctly working.

Goals

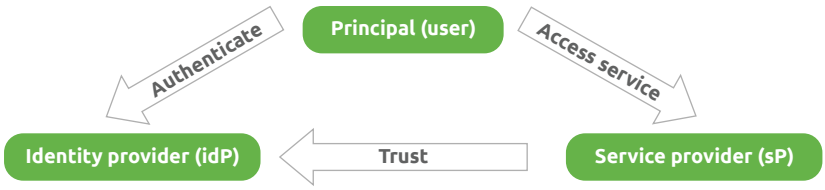
- Reduce barriers for users
- Keep the client's internal systems as the controlling entity for authentication
- Implement a solution that utilizes industry accepted best practices

Solution

BizLibrary assumes the role of the service provider in the SAML SSO implementation.

Example Flow

1. User A goes to BizLibrary.
2. User A is redirected to the identity provider for authentication.
3. After successfully authenticating, the identity provider interacts over HTTPS and then a series of steps are taken as part of the SAML 2.0 flow.



Dependencies & Impacts

- The client must have an existing SAML 2.0 identity provider setup and working.
- The client must provide appropriate IT support staff that will work with BizLibrary during the configuration process.
- Once configured for SAML, a targeted branded site can support both SAML and non-SAML authentication.

The BizLibrary service provider supports several configurations, depending on your identity provider. If your identity provider makes use of service provider metadata, and SAML has been configured by BizLibrary you can view the XML metadata at the following, publicly available URL: https://{yourorganization}.bizlibrary.com/SAML/Metadata

Signatures and Certificates

- Requests may or may not be signed.
- Assertions may or may not be encrypted.
- All Assertion ans response combinations may or may not be signed.

	Unsigned Response	Signed Response
Unsigned Assertion	Supported	Supported
Signed Assertion	Supported	Supported

- Signatures may be verified from a public key that the client delivers or via the provider XML metadata.
- Signing requests may be done with a private key that you provide or via the public key that we indicate in our service provider XML metadata.
- We support AES-128, AES-192, AES-256, and Triple-DES encryption algorithms.

Best Practices | Single Log-Out

The BizLibrary service provider fully implements the SAML single logout specification. We support logout when it's being initiated by the client identity provider, as well as logout when it's initiated by the BizLibrary service provider (via user clicking on a logout link).