What is SAML?

Security Assertion Markup Language

Security Assertion Markup Language, or SAML, is a way of simplifying confidential authentication for users between an identity provider (IDP) and service provider (SP). SAML is an XML (Extensive Markup Language) that centralizes the user management so that the user's authorization is dependent on the identity provider instead of the service.

During the transfer of authentication between the identity provider and service provider, the SAML Assertion (the XML document that the IDP sends to the SP which contains the user's authorization) takes one of three steps:

- Authentication: where the report provides the information of the user and the time the user logged in.
- Attribution: where the document passes the SAML attributes to the service provider.
- Authorization decision: which contains the information of whether the user can or cannot use the service for a reason (i.e., wrong password)

Through the use of SAML, users will no longer have to enter credentials to log into an individual application, which simplifies the process while increasing security.

SAML can keep the retention rate for users logging in at a high level, which makes it appealing to use for many businesses. In a scenario featuring two similar services, it's clear that most users would prefer the service using this protocol to "save" their credentials for access over a service that would require you to log in each time that you go to use the application.

How does it work?

Once a service becomes SAML compliant, users will not have to use their username and password (for the application) to log in. Instead, there is an exchange of authentication between the service and the identity provider which will either grant or deny the service to the user. An example of SAML is using your Google account to log into third-party services.

SAML enables Single Sign-On (SSO) which allows users only to have to log in once, and those same credentials are stored and can be reused to log into other service providers. Using Google as an example, if you log in to a third-party service using Google, you can log into other services using Google (if provided the option).

SAML Adoption

Businesses adopt SAML for two main reasons:

- It is standardized. Its format is designed to operate with any system independent of implementation. This means that this can be compliant with any SP.
- It has a high-security profile. SAML is used to provide a single point of authentication of IDP. This is because credentials never pass through the identity provider's firewall.

Advantages of SAML

- Platform neutrality: this means that the service does not have to provide user security because the identity provider incorporates information protection. Therefore, the service's security is entirely independent of the service.
- Improved online experience: this is because SAML utilizes SSO which makes it easier for users to log in. Logging in once provides a much better experience than having to log in multiple times.
- Reduced administration costs: with SAML, the identity provider controls the account information, which means that the service saves money by reducing the cost of maintaining account information. With SSO, the service does not have to worry about misplaced account information.

“SAML benefits a diverse group. It allows security systems and application software to be developed and evolve independently.” – saml.xml

How ID Director for SAML incorporates biometric authentication

For organizations that are currently using SAML and want biometric sign-in options, BIO-key has introduced ID Director for SAML.

During the onboarding and credentialing of a new employee or when adding ID Director to an existing SAML platform, the system administrator will ask the under to enroll their fingerprints into the credentialing system. We recommend enrolling several fingerers from both hands. Upon enrollment, the user then has the option of using their fingerprint to authenticate or they can still select the SAML assertion link. Adding ID Director enhances security across the entire organization while complimenting a static free workflow environment.

Links for SAML:
What is SAML
Advantages of SAML
Three Benefits of Using SAML