SAML

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

The single most important problem that SAML is trying to solve is the Web Browser Single Sign-On (SSO) problem, a problem also addressed by the OpenID protocol. Single sign-on solutions are abundant at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies.

SAML assumes the principal (often a user) has enrolled with at least one identity provider. This identity provider is expected to provide local authentication services to the principal. However, SAML does not specify the implementation of these local services; indeed, SAML does not care how local authentication services are implemented (although individual service providers most certainly will).

Thus, a service provider relies on an identity provider to identify a principal. At the principal's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision.

Subject\NameID – Employee ID

Saml attributes:

GroupNumber – reference to the group

EnrolleeID – Employee’s ID (can be used if Subject\NameID is not provided)

Transmittal – custom Selerix’s format for census data upload.

ReturnUrl – URL to redirect after enrollment is done.

HeaderAndFooter – yes/no

TopMenu – yes/no

Sidebar – yes/no

PersonalInfo – yes/no

BenefitSnapshot – yes/no

Welcome – yes/no

Review – yes/no

KeepAliveUrl – URL to poll to keep partner’s system session alive.

KeepAliveTimeout – Keep alive timeout.

EnrolleeSignaturePIN – set employee’s signature pin for form signing.