SAML (Security Assertion Markup Language)

SAML(Security Assertion Markup Language) allows security credentials to be shared by multiple computers across a network. It describes a framework that allows one computer to perform some security functions on behalf of one or more other computers (Authentication, Authorization)

The Security Assertion Markup Language (SAML) standard defines how providers can offer both authentication and authorization services.

The Security Assertion Markup Language (SAML), is an open standard that allows security credentials to be shared by multiple computers across a network. It describes a framework that allows one computer to perform some security functions on behalf of one or more other computers:

- Authentication: Determining that the users are who they claim to be
- Authorization: Determining if users have the right to access certain systems or content

Strictly speaking, SAML refers to the XML variant language used to encode all this information, but the term can also cover various protocol messages and profiles that make up part of the standard.

What is a SAML provider?

In SAML lingo, a provider is an entity — generally, a server or other computer — within a system that helps the user access the services he or she wants. Systems that provide or consume SAML services are generically called service providers; the most important kind of service provider is an identity provider.

An identity provider is the entity within the system that makes sure the user really is who they claim to be — it provides authentication. It may also determine what services, if any, that user is authorized to access across various entities in the system. There are various implementations that can provide authentication services in line with the SAML standard — Salesforce can serve this role, for instance, and so can LDAP, RADIUS, or ActiveDirectory.

What is a SAML assertion?

A SAML assertion is the XML document by which all the information we've been discussing is transmitted from one computer to another. Once an identity provider has determined that you are who you say you are and have the right to access the content or services you're interested in, it sends a SAML assertion to the server that actually can actually provide those services to you. A SAML assertion may be encrypted for increased security.

Service flow example

Gliffy Macro Error

You do not have permission to view this diagram.

SAML vs. OAuth: What’s the difference?

OAuth is a somewhat newer standard than SAML, developed jointly by Google and Twitter beginning in 2006. It was developed in part to compensate for SAML's deficiencies on mobile platforms and is based on JSON rather than XML.

- SAML standard defines how providers can offer both authentication and authorization services.
- OAuth only deals with authorization. OpenID Connect is an even newer standard, developed in 2014, that provides authentication services, and is layered on top of OAuth.