**SAML**

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).

There are two primary types of SAML providers, **service** provider, and **identity** provider.

A service provider needs the authentication from the identity provider to grant authorization to the user.

An identity provider performs the authentication that the end user is who they say they are and sends that data to the service provider along with the user’s access rights for the service.

Microsoft Active Directory or Azure are common identity providers. Salesforce and other CRM solutions are usually service providers, in that they depend on an identity provider for user authentication.

* **SAML ASSERTION -**

A SAML Assertion is the XML document that the identity provider sends to the service provider that contains the user authorization.

* **How SAML works -**

SAML works by passing information about users, logins, and attributes between the identity provider and service providers. Each user logs in once to Single Sign On with the identify provider, and then the identify provider can pass SAML attributes to the service provider when the user attempts to access those services. The service provider requests the authorization and authentication from the identify provider. Since both of those systems speak the same language – SAML – the user only needs to log in once.

Each identity provider and service provider need to agree upon the configuration for SAML. Both ends need to have the exact configuration for the SAML authentication to work.

* **SAML vs OAUTH -**

SAML provides more control to enterprises to keep their SSO logins more secure, whereas OAuth is better on mobile and uses JSON.