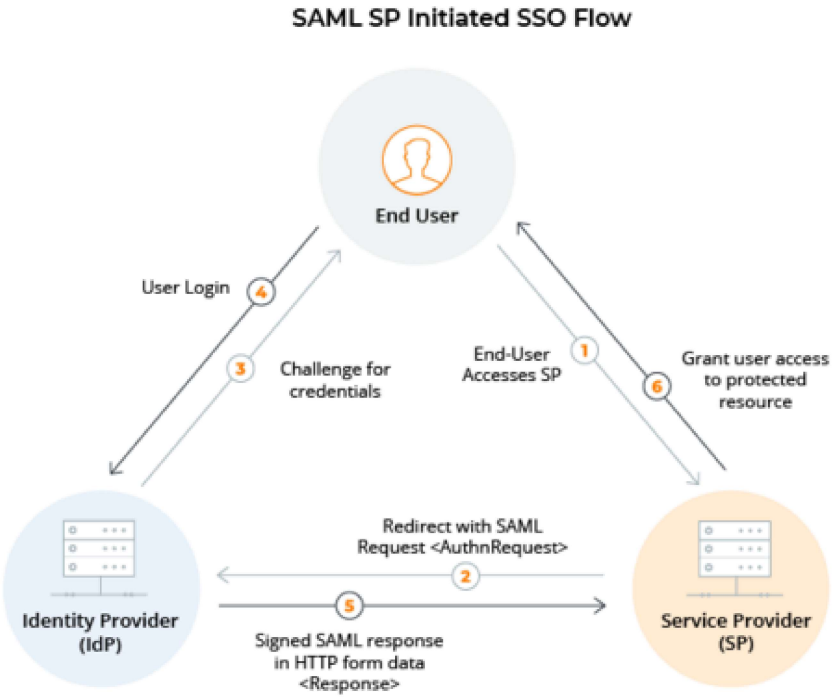
SecureAuth IAM SaaS

An Introduction to SAML (Security Assertion Markup Language)



Christine Mikolajczak

February 08, 2017

Jump to Section

What is SAML?

SAML is a standard that facilitates the exchange of security information. Developed developed by the Security Services Technical Committee of OASIS (Organization for the Advancement of Structured Information Standards), **SAML is an XML-based framework**. SAML enables different organizations (with

different security domains) to securely exchange authentication and authorization information.

How is SAML used with SaaS applications?

Due to the growing number of SaaS applications delivered to employees and consumers, a necessity grew for standards in underlying Single Sign On (SSO) and identity federation, such as **SAML** and **OpenID**. SAML caught on quickly with cloud-based providers, such as Google, Salesforce.com and WebEx. Using SAML, an organization can deliver information about user identities and access privileges to a service provider in a safe, secure and standardized way. This can include Business to Business (B2B) applications and Business to Consumer (B2C) Applications.

There are three main roles in this communication:

- End User
- Identity Provider (IdP) – for example SecureAuth
- Service Provider (SP) – for example Salesforce

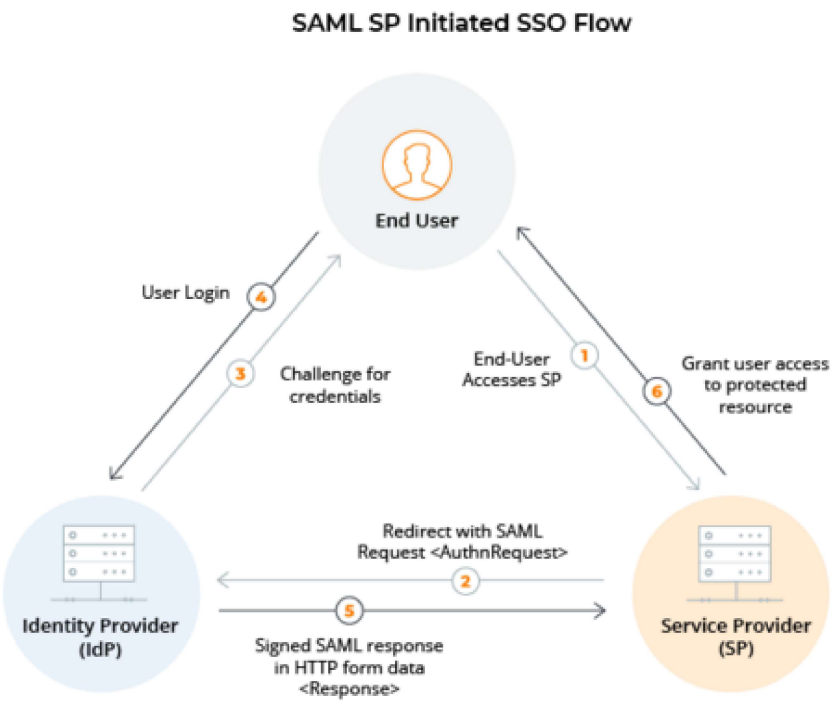
Identity Providers (IdP) provide online resources to give authentication to end users over the network. Sometimes these are also called an identity Service Provider or an Identity Assertion provider.

Service Providers (SP) provide resources to an end user for Single Sign On (SSO).

Here are some examples of SSO flows:

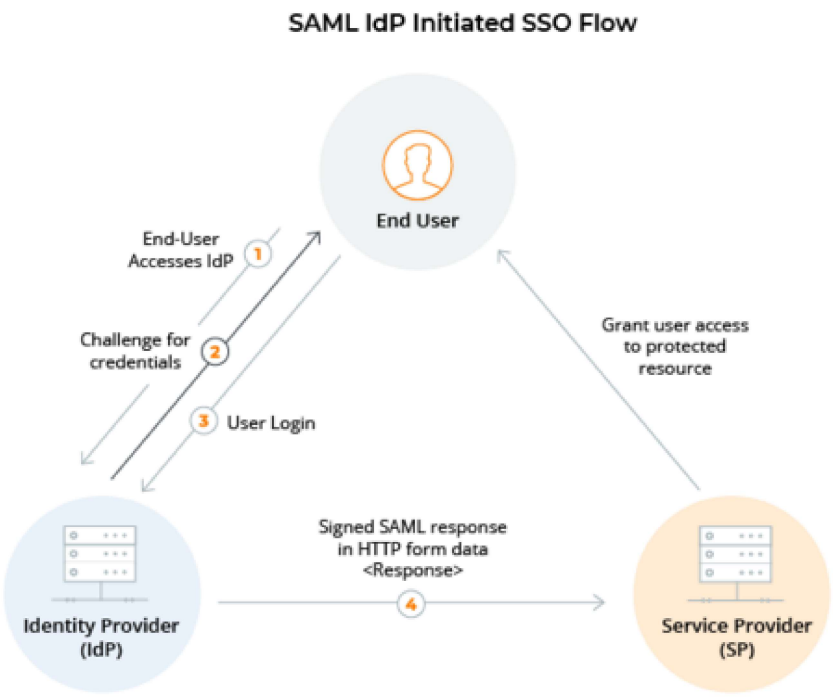
SAML Service Provider-Initiated SSO Flow

In this flow, the end-user initiates the login process at the SP. The SP will redirect the user to the IdP with a **SAML Request** (AuthnRequest). The SAML Request will contain the necessary information for the IdP to authenticate the end-user and reply to the SP with the correct **SAML Assertion** (SAMLResponse).

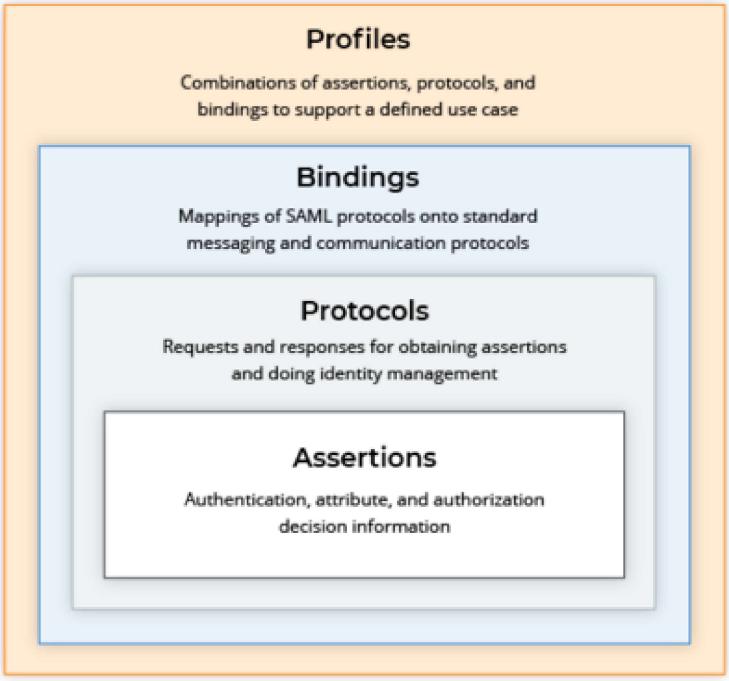


SAML Identity Provider-Initiated SSO Flow

In this flow, the end-user initiates the login process at the IdP. The IdP needs to be configured with the SP's SAML metadata information, such as Assertion Consumer URL, Issuer, and Audiences. The IdP will send a SAML Assertion (SAMLResponse) to the SP which the SP will validate based on the configured requirements.



SAML's standards provide a request/response for exchanging XML messages between these roles. The standard specifies four main components: profiles, assertions, protocol, and binding.



- **SAML Profile** describes in detail how SAML assertions, protocols, and bindings combine to support a defined use case.

- **SAML Binding** is a mapping of a SAML protocol message onto standard messaging formats and/or communications protocols.
- **SAML protocols** describe how the SAML elements are packaged.
- **SAML assertions** contain a packet of security information or decision information.

The bottom line is that to utilize SAML – in any form – your organization needs to become an IdP (Identity Provider). Just as individuals should never share sensitive personal information like their banking PIN, enterprises too should be wary of sharing critical data that could put them at risk if it fell into the wrong hands. Trusting user identities to third parties means that you will always have to keep your fingers crossed that those outside of your organization are following best practices and not degrading your organization's security.

Granted, becoming an IdP sounds like a serious burden, especially for organization with limited IT resources. The quickest way to become your own IdP is to implement SecureAuth. With SecureAuth your organization evolves from simply "holding" identities (AD, LDAP, SQL) to becoming a full, secure, guidance-compliant, highly available identity provider. With SecureAuth, you will be able to serve up secure identities to on- and off-premise applications in a standardized, automated and auditable fashion.

Next steps

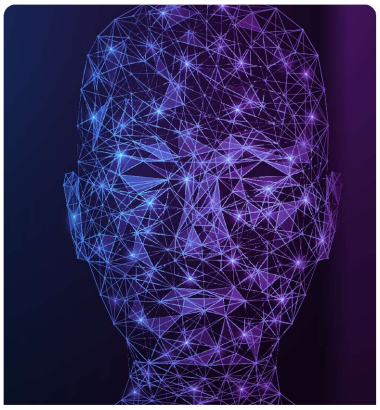
- Explore how SecureAuth Cloud IAM implements SAML SSO in workforce and CIAM use cases across enterprise systems.
- How to integrate a generic SAML application in SecureAuth

Related Stories

MAY 08, 2023

SecureAuth's Arculix Wins Next-Gen Passwordless Authentication and Identity & Access Management in...

Mandeep Khera



MAY 04, 2023

World Password Day 2023: Why Not Celebrate A Passwordless Continuous Authentication Day

Donovan Blaylock II

APRIL 21, 2023

Join SecureAuth at RSA Conference 2023 to Adopt Invisible MFA with Next-Gen...

Mandeep Khera

Get the latest stories from The SecureAuth Blog, every week.

Business Email

Subscribe

Privacy Policy

Privacy Shield Notice

Legal