



WWW.SSOJET.COM

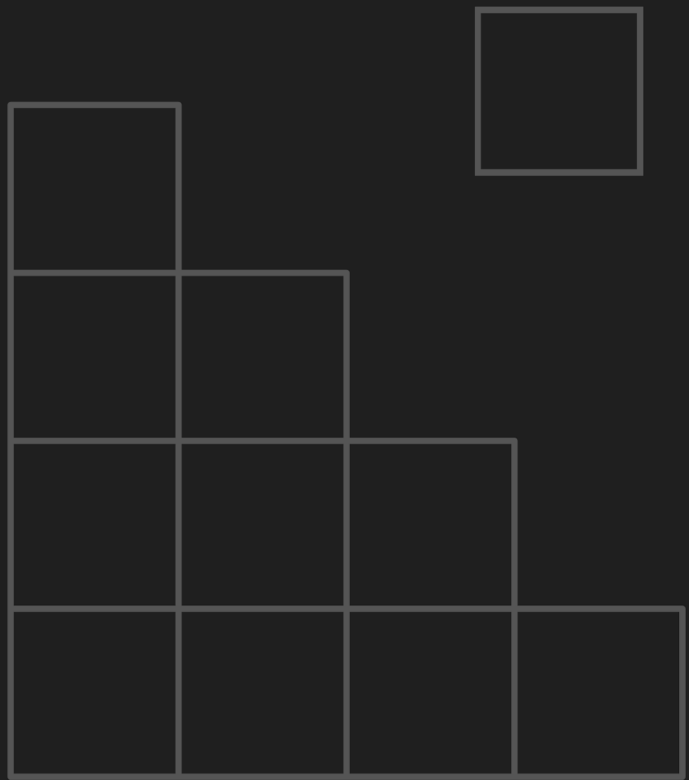


WHITEPAPER
SAML 101

SAML Authentication, Explained. What it is, how it works, and how you can configure a SAML identity provider

Table of Contents

Introduction	1
What is SAML?	2
Benefits of SAML	2
SAML terminology	4
SAML flows	5
SAML Use cases	10
Conclusion	12
We can help	13



Introduction

Marketing is about telling a compelling story that resonates with your audience and conversion is about turning that story into action.

What is SAML ?

Security Assertion Markup Language (SAML) is an XML-based standard protocol for exchanging authentication data between two parties. SAML is designed to enable Single Sign-On (SSO) across different applications and systems that belong to the same organization or consortium.

SAML allows a user to log in once and then access multiple applications or services without having to log in again for each application or service, this is exactly SSO.

SAML is based on the concept of a trust relationship between the identity provider (IdP) and the service provider (SP). The IdP is responsible for authenticating the user and providing the necessary identity information in the form of SAML assertions to the SP. SP uses the SAML assertions to grant or deny access to resources.

SAML is famous in enterprise environments, online service providers and government agencies. It is most popular SSO protocols. The SAML standard is maintained by the Organization for the Advancement of Structured Information Standards (OASIS), and it is continually evolving to meet the changing security and privacy requirements of modern internet-based applications.

Benefits of SAML

Secure: SAML allows for the secure transfer of authentication and authorization data between parties and makes sure that user identity and access information are confidential. SAML is designed by keeping in mind the security requirement of enterprises and regulated industries, that's why it's a highly secure protocol.

SSO: Using SAML organizations can implement SSO for their multiple applications means users can access multiple web applications and services without login multiple times. it solves the problem of multiple credentials for multiple applications which belongs to one organization.

Scalability: SAML supports a wide range of authentication and authorization scenarios and use cases. This makes SAML highly scalable and adaptable to a variety of business requirements. It can fit in most of the industry with it's flexibility and security.

Interoperability: SAML is a popular SSO Protocol which means it can be used with different vendors' applications and systems. It's specifications are well-defined and give great flexibility without doing customization to it, which makes sure that cross-organization applications are compatible with each other.

Save cost: SAML reduces the cost of managing users' authentication and access to multiple applications and services, Login once reduces the processing of the number of authentications on multiple applications.

Enhanced User Experience: SSO always make the user experience better, if the organization have multiple applications and if the user doesn't require to sign up as well log in multiple time.

Compliance: SAML is well designed for enterprises' requirements, it has all security and privacy scenarios which make it's compliant protocol.

SAML terminology

Identity Provider (IdP): Identity Provider is to authenticate users and generate SAML assertions that contain data about user identity and related access.

Service Provider (SP): The service provider is an application that users want to access after successful authentication by Identity Provider. Service Provider accepts SAML assertion sent by Identity Provider.

SAML Assertion: A SAML assertion is an XML document that contains data of the user's identity (ID and Attributes) and access, also metadata of the assertion itself, such as its validity period, the public key, and the IdP that issued it.

SAML Protocol: A set of rules and methods for exchanging SAML assertions between the Identity provider and the Service Provider. In January 2001, OASIS Security Services Technical Committee (SSTC) convened for the first time with the mandate of creating an XML framework to facilitate the exchange of authentication and authorization information.

Attribute: An attribute is a user profile-related field, such as name, email address, or group. It is part of a SAML assertion. Attributes are used by the SP to identify users and provide access according to them.

NameID: A NameID is a unique identifier that is assigned to a user by the IdP and included in a SAML assertion. NameID is used by the SP to identify the user across different applications.

Subject: Subject refers to the user on whose behalf the SAML assertion has been generated, it contains the NameID XML tag also.

Metadata: Metadata is information about an identity Provider or Service Provider, SP requires IdP's metadata and IdP require SP's metadata to establish trust between both. Metadata includes information about the SP or IdP's endpoints (assertion consumer service URL, SLO URL, etc.), certificate, audience, and other relevant details.

Single Logout (SLO): A process that enables a user to log out of all web applications or services that use SAML authentication with a single action.

Binding: Method for transmitting SAML messages between an IdP and an SP, such as HTTP Redirect, HTTP POST, or SOAP.

SAML flows

Here are The general steps of creating a SAML assertion and consumption involve the following steps:

- **User Attempt to Access Restricted Resources:** The user attempts to access a service provider (SP) application that requires authentication. SP redirects the user to the Identity Provider (IDP) for authentication.
- **IdP Authentication:** IdP authenticates the user in this step if the user's session doesn't exist. IdP can authenticate using various methods example username and password, two-factor authentication, or smart card authentication.
- **Assertion Creation:** Once the user is authenticated, IdP creates a SAML assertion that contains data about the user and authentication status. IdP Sign the assertion using IdP Private key to ensure its authenticity and integrity.

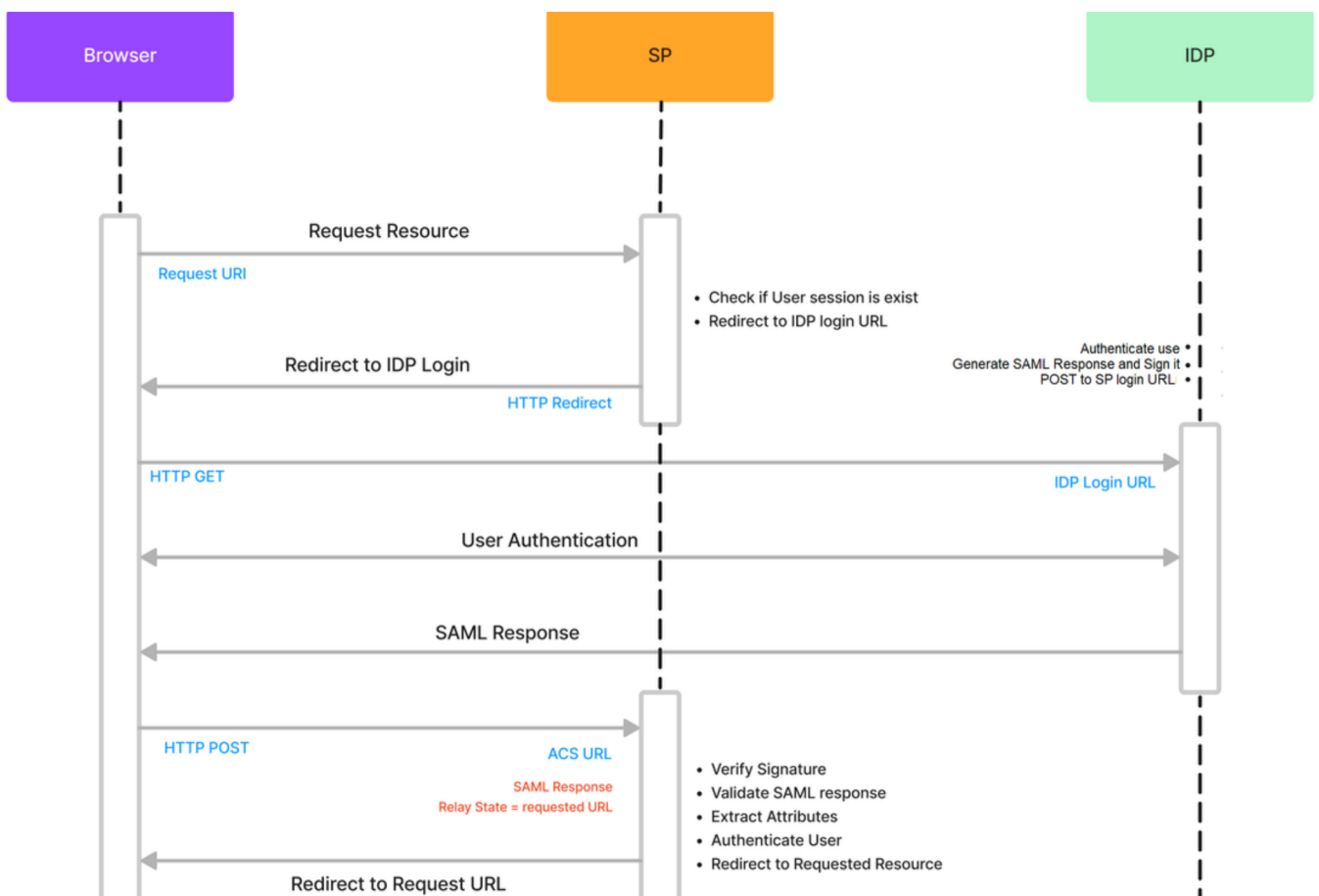
- **Assertion Delivery:** IdP sends the SAML assertion to the SP via the user's browser, using either the HTTP POST or HTTP Redirect binding. IdP Sends assertions in XML format.
- **Assertion Validation:** SP receives the SAML assertion and validates it by verifying the signature, checking the expiration date, and verifying that the assertion is intended for the SP.
- **Attribute Extraction:** Once the SAML assertion is validated, SP extracts user attributes such as name, email, and group.
- **Session Creation:** SP creates a session for the user, allowing the user to access the SP application. There are two types of flows in SAML, these are IdP-Initiated and SP-Initiated flows.

IdP initiated

SAML IdP-initiated flow is a scenario where the user is first authenticated by the Identity Provider (IDP) and then redirected to a Service Provider (SP) application without the user having to initiate the request. The process involves the following steps:

- **IdP Authentication:** The user tries to access the specific SP application, IdP authenticates the user in this step if the user's session doesn't exist. IdP can authenticate using various methods example username and password, two-factor authentication, or smart card authentication.
- **Assertion Creation:** Once the user is authenticated, IdP creates a SAML assertion that contains data about the user and authentication status. IdP Sign the assertion using the IdP Private key to ensure its authenticity and integrity.

- **Assertion Delivery:** IdP sends the SAML assertion to the SP via the user's browser, using either the HTTP POST or HTTP Redirect binding. IdP Sends assertions in XML format.
- **Assertion Validation:** SP receives the SAML assertion and validates it by verifying the signature, checking the expiration date, and verifying that the assertion is intended for the SP.
- **Attribute Extraction:** Once the SAML assertion is validated, SP extracts user attributes such as name, email, and group.
- **Session Creation:** SP creates a session for the user, allowing the user to access SP application. In the IdP-initiated flow, the user is first authenticated by IdP, and the request is initiated by the IdP, which then sends SAML assertion to SP. This flow is typically used in situations where user is on IdP portal and use want to access SP directly.

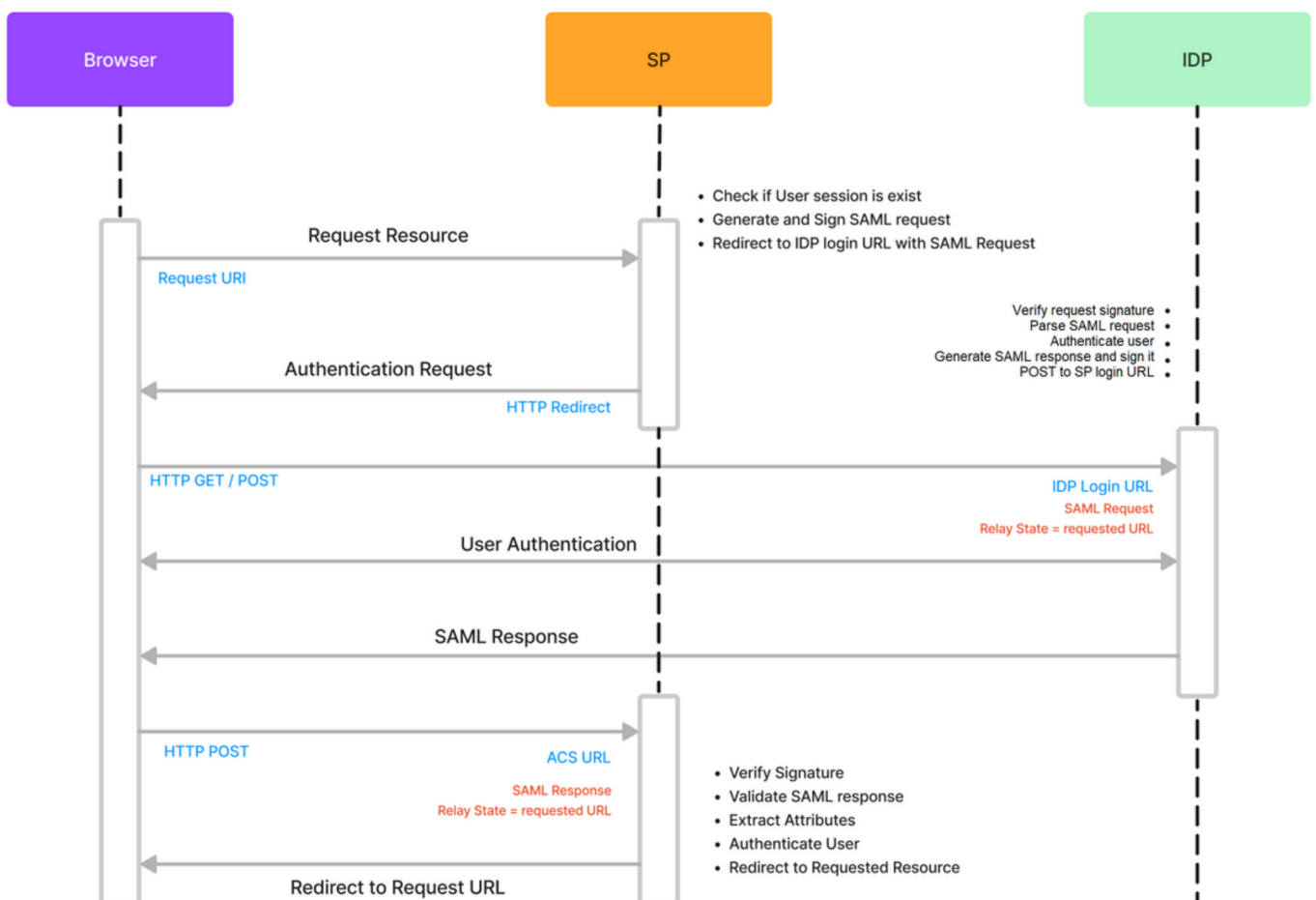


SP-Initiated

SAML SP-initiated flow is a scenario where the user initiates the request to access a Service Provider (SP) application and is then redirected to the Identity Provider (IDP) for authentication. The process involves the following steps:

- **User Attempt to Access Restricted Resources:** User attempts to access a service provider (SP) application that requires authentication.
- **SP Request:** The SP determines that the user needs to be authenticated and sends a SAML request to the IdP, requesting the user's authentication and authorization information,.
- **SP Request validation:** IdP receives the SAML request and validates and verifies it by signature.
- **IdP Authentication:** IdP authenticates the user in this step if the user's session doesn't exist. IdP can authenticate using various methods example username and password, two-factor authentication, or smart card authentication.
- **Assertion Creation:** Once the user is authenticated, IdP creates a SAML assertion that contains data about the user and authentication status. IdP Sign the assertion using IdP Private key to ensure its authenticity and integrity.
- **Assertion Delivery:** IdP sends the SAML assertion to the SP via the user's browser, using either the HTTP POST or HTTP Redirect binding. IdP Sends assertions in XML format.

- **Assertion Validation:** SP receives the SAML assertion and validates it by verifying the signature, checking the expiration date, and verifying that the assertion is intended for the SP.
- **Attribute Extraction:** Once the SAML assertion is validated, SP extracts user attributes such as name, email, and group.
- **Session Creation:** SP creates a session for user, allowing user to access SP application. In the SP-initiated flow, the user initiates the request to access the SP application, and the SP sends a SAML request to the IDP for authentication and authorization. This flow is typically used in situations where the user needs to access a specific resource or application directly.



SAML Use cases

SAML is commonly used in Single Sign-On (SSO) scenarios, where a user can authenticate once with an identity provider and then access multiple service providers without having to authenticate again.

Workforce SSO

SAML is very popular in Workforce SSO, All the Workforce SSO providers support SAML so it can be integrated with internal tools either SaaS or on-prem. Using Workforce SSO companies can control their employee's accesses from a single dashboard, onboarding, management, and offboarding.

As SAML is a well-defined protocol so it's highly secure and flexible which fits in the enterprise ecosystem for the identity use case. All enterprises and mid-sized businesses use Workforce SSO.

B2B SaaS SSO

When we say that all the Enterprise and mid-sized use Workforce SSO means all B2B SaaS solutions that deal or want to deal in this segment means they require to integrate SAML so their customer's Workforce SSO can be integrated with their system.

All the B2B SaaS platform these days supports the integration of Workforce SSO.

Cloud-based SSO

SAML can also be used to provide single sign-on access to cloud-based services, such as Software-as-a-Service (SaaS) applications. Users can authenticate once with the identity provider and then access any cloud-based service that accepts SAML authentication.

Enterprise SSO

SAML can be used to provide single sign-on access to multiple web applications within an enterprise. Users can authenticate once with the identity provider and then access any service provider that accepts SAML authentication.

Partner SSO

SAML can be used to provide single sign-on access to services provided by partner organizations. For example, a company might use SAML to allow its employees to access a partner's services without having to create separate accounts and credentials.

Federation

SAML can be used for federated identity management, where multiple organizations agree to trust each other's identity providers. This allows users to access services provided by other organizations without having to create separate accounts and credentials.

Mobile Device Management

SAML can be used to provide authentication and authorization for mobile devices accessing enterprise resources. This allows mobile devices to access enterprise resources without requiring the user to authenticate separately for each resource.

Conclusion

SAML solves the Security and User experience problems with greater flexibility, it is a defacto solution when we think about the identity exchange between two parties. SAML's strength is it's well-defined specification which makes this fir for most of the use cases of Identity Federation and SSO. SAML is not that popular in B2C applications, JWT, OAuth, and OIDC are well-known protocols into B2C.

Conclusion

In conclusion, SAML (Security Assertion Markup Language) is a widely adopted standard for exchanging authentication and authorization data between parties. SAML enables Single Sign-On (SSO) scenarios, where a user can authenticate once with an identity provider and then access multiple service providers without having to authenticate again.

Through this book, we have covered the basics of SAML, including its components, message flow, and various SAML profiles. We have also discussed some common use cases for SAML, including enterprise SSO, cloud-based SSO, partner SSO, federation, and mobile device management.

SAML is a flexible and powerful technology that can help organizations streamline their authentication and authorization processes, reduce the risk of data breaches, and improve user experience. However, implementing SAML can be complex and requires a good understanding of the technology and its underlying concepts.

We hope that SAML 101 has provided you with a solid foundation in SAML and helped you understand how SAML can be used to improve the security and usability of your applications. If you have any further questions or want to learn more about SAML, there are many resources available online, including the official SAML specification and various online communities and forums.

We Can Help

SSOJet offers Identity as a Service (IDaaS) to B2B SaaS companies, providing them with a platform that can help increase sales conversion rates, shorten sales cycles, reduce engineering time, and sell their products to enterprise customers at a premium while ensuring compliance with enterprise security standards. Compared to homegrown identity management solutions or labor-intensive options like Azure Active Directory and ADFS, SSOJet's total cost of ownership can be significantly less. SSOJet's IDaaS platform provides a range of powerful features, including single sign-on, multifactor authentication, anomaly detection, customizable access and profile enrichment rules, and more.

-
- SSOJet is a trusted identity management solution designed with state-of-the-art security in mind.
- The platform offers enterprise customers the ability to configure and implement enterprise federation and single sign-on in just a few lines of code.
- SSOJet supports social connections with all major providers, such as LinkedIn, Facebook, Twitter, and Google, in addition to traditional username/password authentication with enhanced security features like multifactor authentication and anomaly detection.
- The platform offers a painless user migration process, allowing companies to audit and view identity-based analytics for compliance and upsell opportunities.
- SSOJet also provides fine-grained permissions and powerful custom rules for companies to manage trial features and user access, along with delegated administration to administer granular access, visibility, and control to customers.
- With SSOJet, a developer can set up a robust and customizable identity management system for any technology stack in less than thirty minutes.