Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Single sign on with SAML and its Implementation

Prashant Bansal

Keywords: SAML, SSO, IDP, SP, Single Sing ON

Abstract:
SAML is a technology that makes it easier to log in to multiple web applications. It acts as a bridge between your login credentials and the websites you want to access, ensuring your information is transmitted safely. It simplifies online access by allowing you to use the same login information for various websites. It works by securely exchanging authentication data between your login provider and the websites you visit. SAML-based SSO is often implemented in enterprises to streamline employee access. This type of setup eliminates employees having to create individual credentials for these other services. This increases security because employees don't have to remember passwords, and organization's IT department doesn't have to worry about their passwords being insecure. SAML was introduced to address the challenge of managing multiple logins for users accessing various websites. Before SAML, single sign-on was confined to websites within the same domain. SAML centralizes authentication with an identity provider, allowing users to access different websites using a single set of credentials. This simplifies the login process for users and improves security for service providers by reducing the risk of password-related vulnerabilities. In this article, I will demonstrate an overview of SSO (Single Sing On) and its working relation with SAML2. The literature will also establish the implementation guidelines for single sign on using SAML2 and its benefits.

1. INTRODUCTION:

SSO, or single sign-on, simplifies the login process by allowing users to access multiple online services with a single set of credentials. For example, you might use your Facebook account to log in to other apps, avoiding the need to create separate usernames and passwords for each service. SSO acts as a central authentication point in a federated identity system. Certain SSO systems also manage authorization, which defines a user's permissions within a service. Authentication establishes a user's identity, while authorization grants the user specific access rights. SSO offers a range of choices, including OpenID Connect, Facebook Connect, Microsoft Account, and SAML. Each option can be tailored to specific needs through various configurations. I am going to cover SAML as part of this article, and within that, going to explain one way to implement SSO with SAML. SAML is a valuable enterprise solution that offers significant benefits. It streamlines the login process by allowing users to access multiple web applications with a single set of credentials. This not only improves the user experience but also reduces the burden on IT departments by minimizing password-related help desk calls. SAML offers a dual benefit of enhanced user experience and heightened security. By centralizing login information with an identity provider, service providers can avoid storing sensitive user credentials. Identity providers, specializing in secure SAML authentication, have the expertise and resources to invest in robust security measures. For example, many identity providers offer comprehensive identity security solutions, including multi-factor authentication (MFA), to safeguard against common password attacks.

2. SAML WORKING MECHANISM.

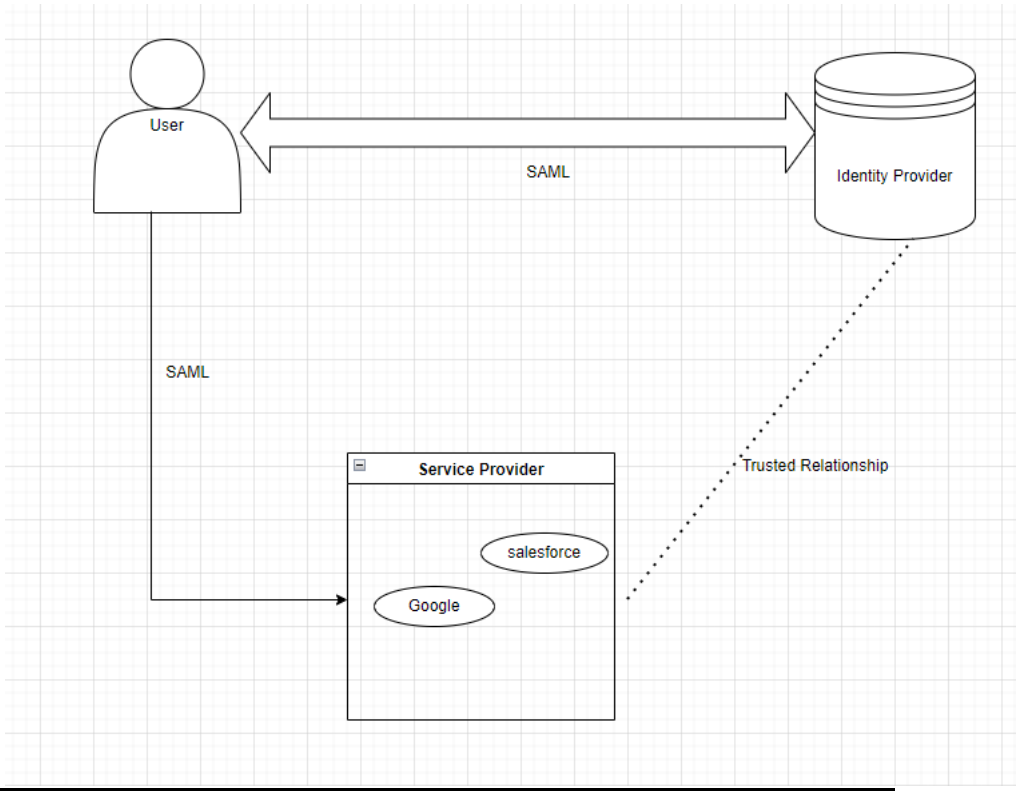
SAML acts as a bridge between the identity provider and the service provider, exchanging user information such as logins and authentication status. This streamlines the login process by requiring users to authenticate only once. When a user tries to access a service, the identity provider verifies their identity and authorizes access to the service provider. SAML Single Sign-On is a mechanism that leverages SAML allowing users to log on to multiple web applications after logging into the identity provider. As the user only must log in once, SAML SSO provides a faster, seamless user experience.

SAML Single Sign-On provides a seamless user experience by eliminating the need for multiple logins. Users can easily access various web applications with a single set of credentials, saving time and reducing frustration. This, in turn, benefits organizations by improving overall user satisfaction and reducing the burden on IT support teams. SAML Single Sign-On not only enhances user experience but also boosts productivity. Users save time by logging into multiple applications with a single set of credentials, reducing the need for frequent password resets and support requests

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Many organizations implement identity verification procedures to safeguard access. In the banking industry, verifying your identity is crucial for the safety of other passengers. This involves presenting a government-issued photo identification. If your identity matches the information on your bank account, you are granted permission to perform financial or non-financial transactions within bank.

In this example, the government acts as the identity provider, and the bank serves as the service provider. Your government-issued identification functions as the SAML assertion. When you obtain a government ID, you typically provide personal information, have your photo taken, and may also undergo fingerprint scanning. The government stores this identifying data and issues you a physical ID linked to your identity. At the bank, the teller verifies your ID (SAML assertion). If your ID is valid and contains your correct details, the teller grants you permission to perform tasks within bank.



3. OAUTH V/S SAML

OAuth and SAML are both protocols used to manage access, but they serve different purposes. SAML is used for authentication, verifying a user's identity. OAuth, on the other hand, is used for authorization, determining a user's access privileges. Think of it like boarding a plane: your ID (SAML) verifies your identity, while your ticket (OAuth) determines your seat and amenities.

SAML uses a claims-based authentication process. When a user tries to access a service, the service provider redirects them to the identity provider for authentication. The identity provider verifies the user's credentials and issues a SAML assertion. This assertion is then sent back to the service provider, which grants access if it's valid. Following are the steps followed in the process.

- User Access: A user tries to access a service provider's web application.
- SAML Request: The service provider sends a SAML request to the identity provider.
- Authentication: The identity provider authenticates the user, typically by requesting a username and password.
- SAML Assertion: If authentication is successful, the identity provider generates a SAML assertion and sends it to the user's browser.
- Access Grant: The user's browser sends the SAML assertion to the service provider, which verifies it and grants access.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

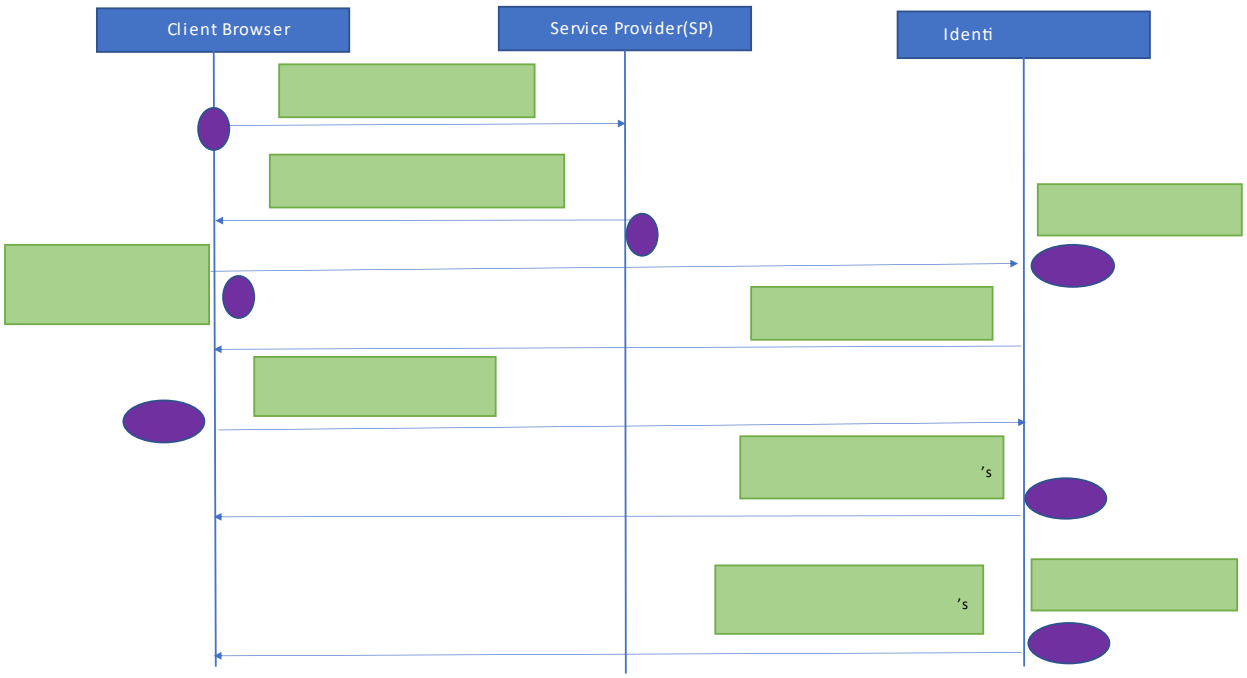
4. SAML IMPLEMENTATION METHODOLOGIES

There are two ways to implement SSO with SAML.

1. Service Provider Initiated- Users start by providing initial information to a service, which then determines the correct identity provider. If a user is accessing a company portal with their company email, the service will direct them to the identity provider linked to that company.
2. Identity provider Initiated- Users start at their identity provider, where they log in. Clicking a link then directs them to the service provider, along with their authentication details. The service provider verifies this information and grants the user access to their service.

1. Service Provider Initiated Steps

- User Access: The user accesses the service provider's application.
- SP-Initiated Request: The service provider sends an authentication request to the identity provider.
- Identity Provider Redirect: The identity provider redirects the user to its login page.
- User Authentication: The user enters their credentials and logs in to the identity provider.
- SAML Assertion: The identity provider generates a SAML assertion containing the user's authentication information.
- Assertion Redirect: The identity provider redirects the user back to the service provider, passing the SAML assertion as a query parameter or in the HTTP POST body.
- Assertion Verification: The service provider receives the SAML assertion and verifies its validity and authenticity.
- Access Grant: If the assertion is valid, the service provider grants the user access to the requested resource.



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

Steps Involved as per the above diagram.

1. Request target URL- User goes to the browser and hits the URL, the request to access the URL redirects user to a login page as configured at the service provider end. Following are the components involved in this transitioning.

   i. Certificate
   The service provider needs a public certificate from the identity provider to verify the authenticity of future messages. This certificate is stored by the service provider and used to validate SAML responses.

   ii. ACS Endpoint (Assertion Consumer Service URL)
   The ACS endpoint is the URL provided by the service provider where the identity provider can send a SAML response to confirm a user's authentication.

   iii. IdP Login URL
   The IdP login URL is the address the service provider directs users to when initiating the authentication process.

2. Redirect the URL to IDP- Service provider creates a SAML request and, if necessary, a relay state parameter, and then adds them to the identity provider's login URL. The browser is then redirected to the identity provider's single sign-on service. Following is the sample SAML request.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AttributeConsumingServiceIndex="1"
    Destination="https://yourdomain/broker/sp/saml/login" ForceAuthn="true"
    ID="_b6a016332e19a825bb42917c9870c93a" IssueInstant="2021-03-09T10:26:17.210Z"
    Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">

  </saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  </ds:Signature>
</saml2p:AuthnRequest>
```

3. SSO request to IDP- The user agent will send an HTTP GET request to IDP . The IDP will process the request and check the authentication request of the user.
   If user has a valid session, they will be redirected to SP dashboard, if not, they will be presented with a login page.

4. Send XHTML to Browser
   The identity provider will reply with an XML document containing a form. This form includes a SAML response parameter, which contains an assertion confirming the user's authentication. The assertion may also include attributes that define the user's roles or permissions. For example, an "Admin" attribute could grant full access, while a "Corporate User" attribute could restrict access to non admin related functions.

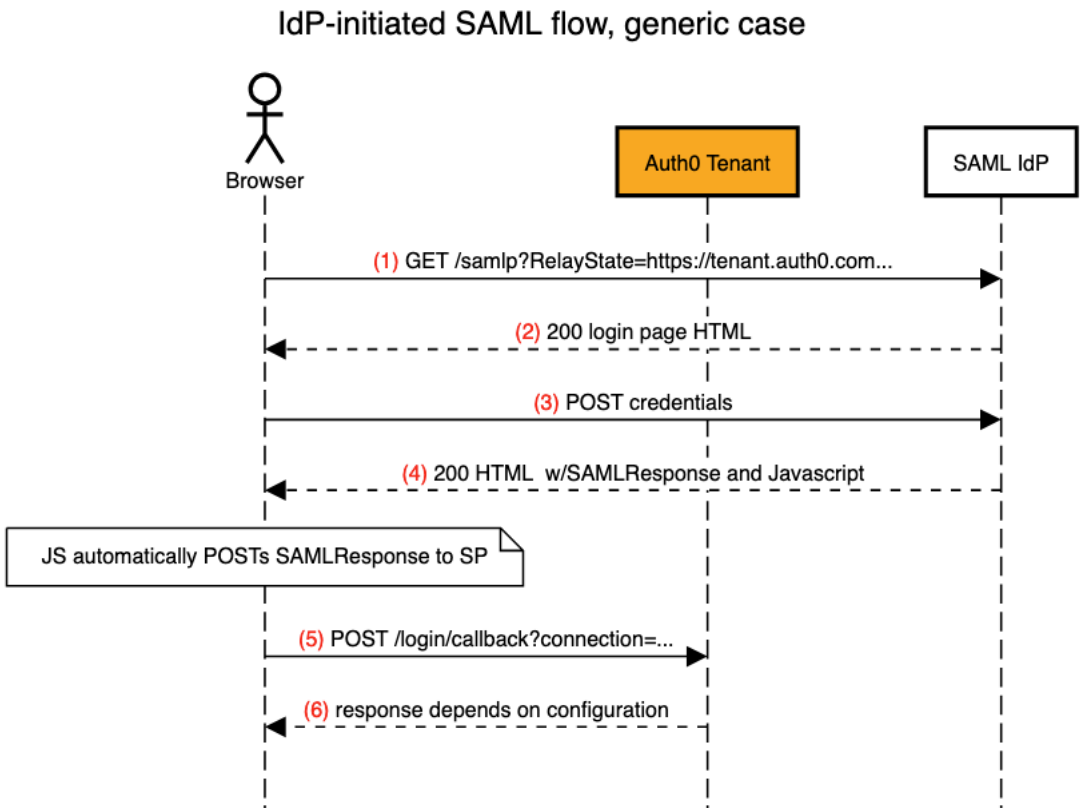
5. Request Assertion consumer
   The user's browser sends a POST request to the service provider's assertion consumer service URL. This is a specific endpoint where the service provider verifies authenticated users. The service provider can validate the incoming message by comparing the public certificate from the identity provider with the XML signature. If necessary, the service provider can also decrypt the XML document before verification.

6. Redirect to SP target URL.
   The service provider instructs the user's browser to navigate to the main application page for logged-in users. If a relay state parameter was included, the service provider would direct the browser to the specific page the user initially intended to access.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

2. Identity Provider Initiated Flow
   In IDP-Initiated SAML, the identity provider (IdP) initiates the authentication process. This flow is typically used when the user wants to access multiple applications at once or when the service provider (SP) is not known in advance.

- User Logs into IdP: The user logs into their identity provider's portal.
- Application Catalog: The IdP presents the user with a list of available applications that can be accessed via single sign-on.
- User Selects Application: The user chooses the desired application from the list.
- IdP Generates SAML Request: The IdP generates a SAML request containing the user's authentication information and the target service provider's details.
- Redirect to SP: The IdP redirects the user to the service provider's application, passing the SAML request as a query parameter or in the HTTP POST body.
- SP Receives SAML Request: The service provider receives the SAML request and verifies its validity.
- Access Grant: If the request is valid, the service provider grants the user access to the requested resource.



- User Logs into IdP: The user logs into their identity provider's portal.
- Application Catalog: The IdP presents a list of available applications.
- User Selects Application: The user chooses an application.
- IdP Generates SAML Request: The IdP creates a SAML request.
- Redirect to SP: The IdP redirects the user to the service provider.
- SP Receives SAML Request: The service provider receives the request.
- Access Grant: If the request is valid, the service provider grants access.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 9, September 2024

CONCLUSION:

SAML Single Sign-On (SSO) offers a robust solution for organizations seeking to improve security, streamline authentication processes, and enhance user experience. By centralizing authentication and authorization, SAML empowers users to access multiple web applications with a single set of credentials, reducing the risk of password-related breaches and improving overall productivity.

The implementation of both SP-initiated and IDP-initiated flows provides flexibility and adaptability to suit different organizational needs. SP-initiated flow is ideal for scenarios where the service provider is known in advance, while IDP-initiated flow is well-suited for providing users with a centralized view of available applications.

Key benefits of SAML SSO include:

- Enhanced security: Centralized authentication reduces the risk of password breaches and simplifies security management.
- Improved user experience: Users can access multiple applications with a single login, saving time and reducing frustration.
- Increased productivity: Streamlined authentication processes enhance efficiency and reduce the burden on IT support teams.
- Cost savings: Reduced password-related support requests and the potential to eliminate the need for custom authentication systems can lead to significant cost savings.

By carefully considering the specific requirements of their organization, organizations can effectively leverage SAML SSO to achieve a more secure, efficient, and user-friendly authentication environment.

REFERENCES:

[1] https://www.onelogin.com/learn/saml
[2] https://medium.com/the-mobile-mindset/how-does-sso-with-saml-2-0-work-33e025536e2e
[3] Zia, Nabeel. “SAML Authentication.” SAML Auth (2020): n. pag. Print.
[4] Wilson, Yvonne & Hingnikar, Abhishek. (2022). SAML 2. 10.1007/978-1-4842-8261-8_7.
[5] Wilson, Yvonne & Hingnikar, Abhishek. (2019). SAML 2.0. 10.1007/978-1-4842-5095-2_7.
[6] Rohatgi, Gaurav. (2024). Single Sign-On with Multifactor Auth Via SAML and Navigate Multiple Systems. International Journal of Computer Applications. 186. 1-2. 10.5120/ijca2024923472.
[7] Balatska, Valeriia & Poberezhnyk, Vasyl & Petriv, Petro & Opirskyy, Ivan. (2024). Blockchain Application Concept in SSO Technology Context. CEUR Workshop Proceedings. 525. 38–49.