3/24/2022

Self-Learning Document

on

**SAML**

Chirag Gaur

Deloitte

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **S. No** | **Topic** | **Page No.** |
| 1. | What is SAML? | 2 |
| 2. | How SAML works? | 2-3 |
| 3. | Role of Metadata file in SAML | 3 |
| 4. | Types of SSO Initiation   1. IdP Initiated SSO 2. SP Initiated SSO | 4 |
| 5. | SAML Bindings | 5 |
| 6. | SAML Assertion Components | 5-6 |

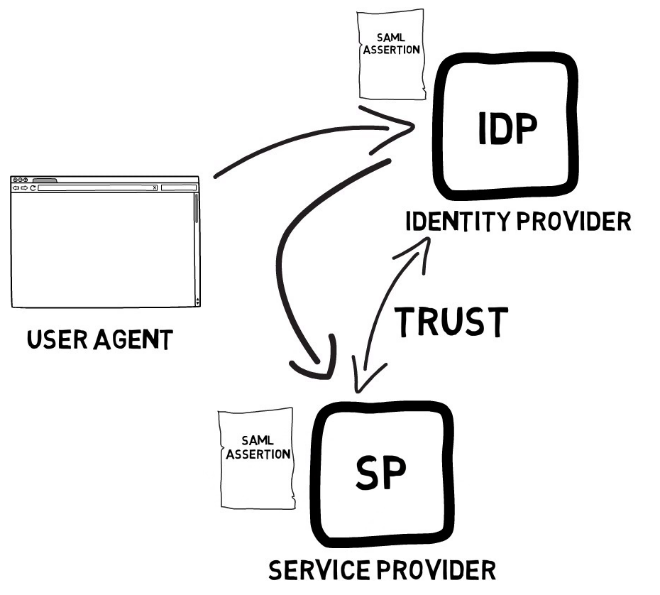
1. **What is SAML?**

* SAML stands for Security Assertion Markup Language. It is an XML based standard which allows users to log into multiple applications using single sign on option.
* As the user’s identity is stored in directory so it would make more sense to fetch those identities from the directory and log users into different applications.
* Ex: In Deloitte username and password remains stored in the directory and the target applications such as Skype, outlook, teams etc. will be logged in automatically using the same credentials for all of them.

1. **How SAML works?**

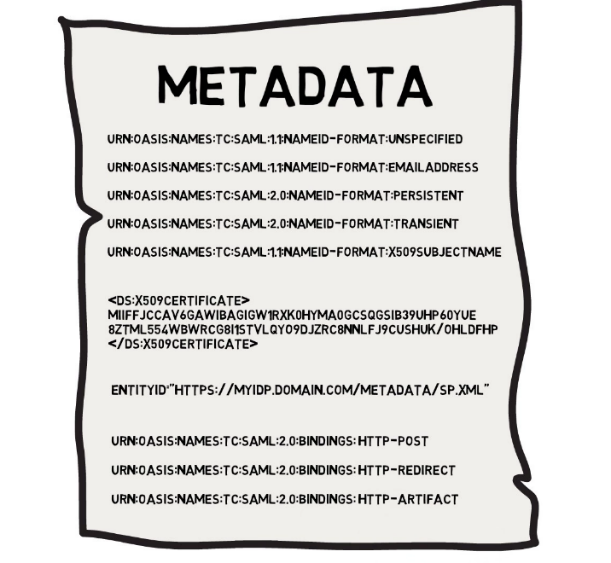
* SAML protocol has three primary components:

1. User Agent: Generally, it is user’s browser.
2. IdP: Identity provider is a centralized system where user credentials are stored. It is a system which authenticates user credentials. It authenticates the user's identity and authorizes to the service provider.
3. SP: Service provider provides services to end user. It authorizes the given user to access the requested resource. Service providers do not authenticate users but instead request authentication decisions from an identity provider.



* When configuring SAML federation we establish a trust relationship between IdP and SP.
* A user who wants to access the service provider must first authenticate into IdP and if the user successfully authenticates to IdP then IdP generates a SAML assertion. This SAML assertion is sent to the application (SP) and then the user is allowed access to the application.
* Since the user is already authenticated to IdP so the user can SSO in multiple applications.

1. **Role of Metadata file in SAML:**



* The configuration or rule are very essential to configure SAML federation between both IdP and SP.
* Metadata file contains the configuration and certificates in XML format. These metadata files can be exchanged between IdP and SP to configure the federation.
* Metadata file comprises of

1. User Identifier: IdP knows about the user and its attributes. When IdP generates the SAML assertion, it is sent along with user identifier. SP reads the user identifier and maps it to the user in its own user store.

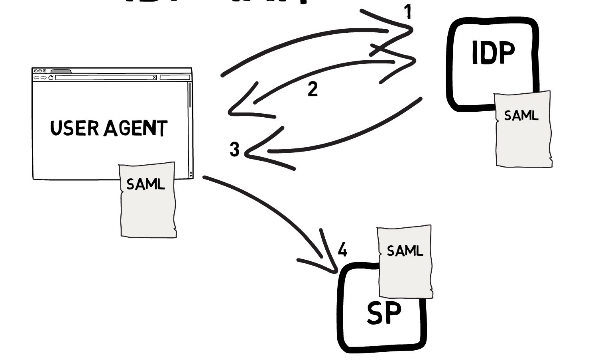
* For ex: SP may request the IdP that the user identifier should be email address and responding to the request IdP will send the SAML assertion with user identifier as email address.

1. NameId-format: It is the format of user identifier.
2. Certificate: Metadata file also contains the sender’s certificate so that receiver end can validate the sender and establish a connection.
3. **Types of SSO Initiation**

Two ways of initiating the flow of Authentication:

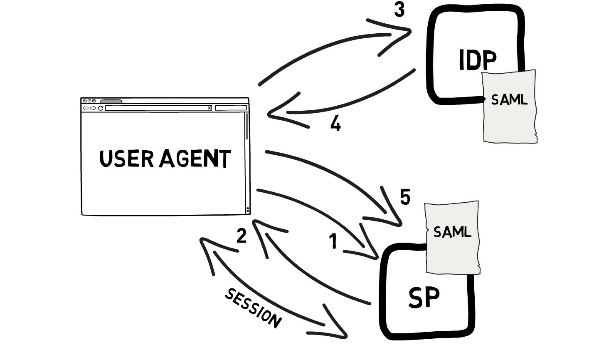
1. IdP initiated SSO
2. SP initiated SSO
   1. **IdP Initiated SSO**

In this flow user starts by accessing the IdP and then the user is prompted for authentication. Once it is done the user can request a service. If the user is authorized, then IdP generates a SAML assertion. This assertion is sent to the SP through user agent using post message. User agent acts a transport mechanism for this assertion. SP verifies the assertion and maps to local user and then the session can start.



* 1. **SP initiated SSO**

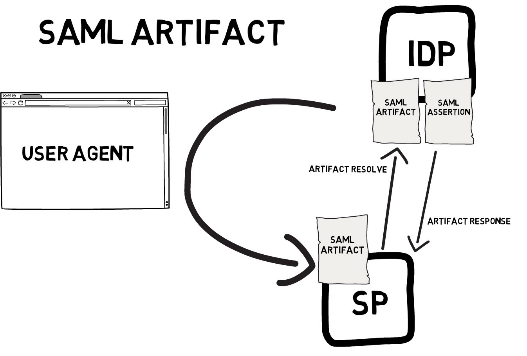
Here the user starts by reaching out to Service provider. Since the user is not authenticated so SP redirects the user to IdP using a request for authentication message. Once the user is validated the IdP generates the SAML assertion. The assertion is sent to the SP via user agent and session can start.



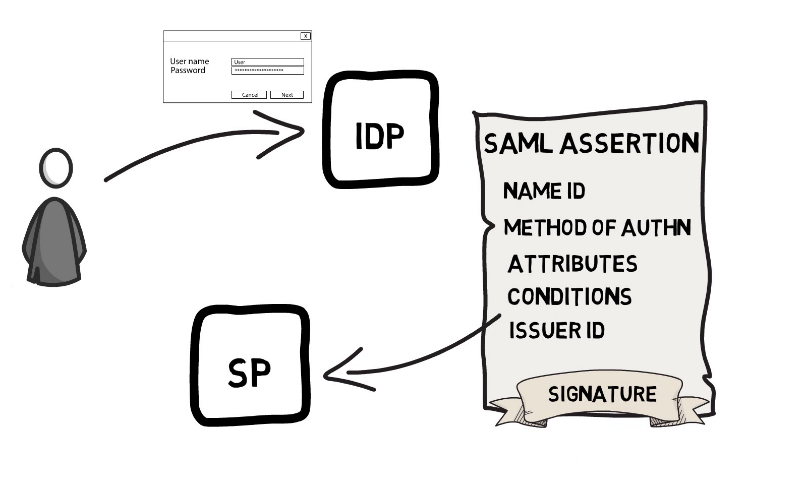
1. **SAML Bindings**

* Bindings explains how messages and assertions are technically sent between the IdP and SP.
* Three common types of Binding used in SAML Assertion are

1. HTTP Redirect binding: It can be used for authentication requests messages sent from SP to IdP
2. HTTP Post Binding: It can be used for both transporting the assertion and request messages.
3. SAML Artifact Binding: IdP generates SAML assertion and SAML artifact. SAML artifact is a small message containing unique identifier. The artifact is sent to the SP via user agent. Then the SP sends an artifact resolve message to IdP in order to retrieve the assertion.

****

1. **SAML Assertion Components:**



* SAML Assertion consists of

1. Name-Id
2. Method of Authentication
3. Attributes
4. Conditions
5. Issuer Id
6. Signature

* Name-Id: Assertion includes name-id with correct format for user identification.
* Name-id format is the unique id of the user trying to authenticate to Sp and it would be mapped to user in local storage of SP
* Method of Authentication: The method used to authenticate the user into IdP is of great importance. The identification of authentication methods is known as SAML context classes.
* Attributes: A user object have attributes associated with it. Attributes are added in assertion providing more details about the user. Attribute’s format must be specified in both IdP and SP.
* Conditions: Conditions such as Valid time of assertion.
* Issuer ID: Issuer id helps the SP to know about the issuer of assertion.
* Issure: person Initiates the flow. Initetes the user request
* Signature: The whole assertion needs to be hashed and signed to provide protection from being tampered.

<https://sptest.iamshowcase.com/ixs?idp=8a1eac0c8a36a1872410059d5939f8e998dc90d1>

<https://sptest.iamshowcase.com/ixs?idp=8a1eac0c8a36a1872410059d5939f8e998dc90d1>

Idp cert : to sign the idp response to SP

SP cert: to plceaes

Used tp identify ki SP se aa rha h yeah nhi

Used to identity the request from SP to IdP.

Used to encrypt.

Assertion includes the authentication is successful, attributes

Servvice now is uses a private key to decrypt the assertion.