**01) What is SAML 2.O ? Why it is Using?**

Ans) SAML is a security Assersion markup language it is a XML based open standard for transferring/ exchanging the identity (Authentication/Autherization) data between service provider and an identity provider.

SAML defines how user identity information is exchanged in the form of SAML assertions, which are digitally signed and can include user attributes and other relevant data. SAML is commonly used to establish trust between different web applications and services,it possible for users to access multiple resources with a single set of credentials.

IDP : Identity provider performs the authentication and passes the users identity like username and password and autherization level for the service provider

1. **Identity Provider** (IDP): The Identity Provider is a crucial component in the SAML framework. It acts as the trusted entity responsible for authenticating users. When a user attempts to access a service or application, the IDP verifies their identity through various authentication methods. Once authenticated, the IDP issues a SAML assertion, which is a digitally signed statement confirming the user’s identity and attributes. This assertion is sent to the Service Provider (SP) to grant or deny access.

SP: Trusts the identity provider and it will authorizes the given user to access.

**Service Provider** (SP): The Service Provider hosts the online service or application that users want to access. It relies on the assertions provided by the IDP to make access decisions. When the SP receives a SAML assertion, it validates the digital signature, extracts user information, and uses this data to determine whether to grant or deny access to the requested resource. The SP plays a pivotal role in ensuring the security and integrity of the service

Okta can act as both the Identity Provider (IdP) or as the Service Provider (SP), depending on use cases

Application

Okta

When using Saml we have 2 methods in starting for saml SSO

1. Identity provider initiated SSO
2. Service provider initiated SSO

Single Sign-On (SSO) is a user authentication process that allows individuals to access multiple applications or services with a single login.

**02) what are the saml sso flows?**

**Service provider initiated flow**

**End user /client Sp IDP**

**1**

In the Service provider flow End user/client will access the the sp login url. if there is no session on the browser sp will redirect the requent to identity provider with the help of saml authentication requent, now idp challenge for login page to the ur. In the login page user provide the credential now user credential will validated again the idp if the validation is success authentication is completed and then saml assersion generate idp and sends back to the service provider or application

**IDP flow**

1. In the IDP flow End user/client directly a access identity provider initiated sso url .
2. The IdP presents an authentication page to the user, prompting them to enter their credentials.
3. The user enters their credentials, and the IdP verifies the user’s identity.
4. After successful authentication, the IdP generates a SAML Assertion and sends it to the User browser and then user browser passes it to SP.
5. The SP validates the SAML Assertion, ensuring it is signed and trusted.
6. If the SAML Assertion is valid, the SP authorize the user request.

**03) what is Binding and types?**

Bindings are the format in which data is transferred between service providers and identity providers. The two most popular are HTTP Redirect Binding and HTTP POST Binding .

HTTP Redirect Bindings transfer data using HTTP redirects and query parameters; this type of binding is typically used in authentication requests.

HTTP POST binding is used for an identity provider response to a request from a service provider

SAML bindings are mechanisms that define how SAML messages are exchanged between different entities in a Security Assertion Markup Language (SAML) based authentication and authorization system. In SAML, there are several standard bindings that specify how SAML messages are transmitted, where they are sent, and how they are formatted. These bindings are crucial for establishing communication between identity providers (IdPs) and service providers (SPs) and ensuring the security and integrity of SAML exchanges. Here are some common SAML bindings:

* HTTP Redirect Binding: SAML messages, such as authentication requests or responses, are sent as URL query parameters in an HTTP redirect. This is useful for carrying SAML messages through a user’s browser.
* HTTP POST Binding: SAML messages are embedded in the body of an HTTP POST request. This binding is often used when sending larger or sensitive SAML messages that shouldn’t be exposed in the URL.
* HTTP Artifact Binding: Instead of sending the entire SAML message, a reference (artifact) to the message is sent over HTTP. The recipient can then retrieve the actual SAML message using the artifact.
* SOAP Binding: SAML messages can be encapsulated within SOAP (Simple Object Access Protocol) messages when integrating with web services and SOAP-based systems.

**04) how can you check saml response ?**

Ans) by using the saml tracer will check the details of ACS url ,entity ID, attributesor claims, certifications

**05) in idp meta data which elements you can check ?**

Ans) entity id , certification, ACS url

**06) what sis ACS url ?**

Ans) The ACS url directs your idp where to send its SAML response after authentication user

**07)What is entity ID?**

Ans) Entity Id is Unique name of the service provider

**Assertion consumer service (ACS) URL—The URL where the identity provider sends SAML responses.**

**Entity ID—The unique identifier of the service provider.**