**01) What is single sign on authentication?**

Single Sign-On (SSO) is an authentication process that allows users to access multiple applications or services with a single set of login credentials (such as username and password). Instead of requiring users to log in separately to each application, SSO enables them to authenticate once and then access all authorized resources without needing to re-enter their credentials

**The importance of implementing a SSO in my organization is that it helps to prevent boot force attacks these days. A lot of people are trying too much to boot force peoples credential but implementing SSO in my organization. It helps to reduce or prevent people from boot forcing user account.**

**06) What Is SAML?**

**SAML stands Security Assertion markup language it is XML based open standard and it is used to provide SSO to web based applications. This protocol can be used for exchanged the authentication and authorization data between the idp and sp.**

**What are some of the SSO protocol you used before??**

**Yes, I have used before SSO protocol is SAML . Before I setup the SAML integration with an application. The first thing that I did was that I want to in okta.Go to the okta admin console dashboard and click on applications tab go to brows catalog then go and search for the application if the application is already integrated with okta then search for application for ex Monday.com then select Monday.com and go to setup its going to ask you to which protocol do you want to use. If you want to SAML click on SAML and then its going to ask if you want to setup attributes like first name, last name, login, email. After that finalized okta is going to generate SAML assertion metadata. And going to copy those metadata and then have idp issues and idp login you have certificate and copy that and upload it in to the SP application.When you do that you will be able to get ACS url in to the okta to create the connection. After that you can go ahead and then activate the connection.**

**You have to setup custom integration??**

**Yes I have worked custom integration.Go to the okta admin console dashboard and click on applications tab. Go to create custom app click on that and then go and select SAML 2.o when you select SAML 2.o. it will ask you for the name of the app and logo of the app the enter name and put the logo there.After that it’s going to ask you for the url of the application. Then put in the url and then also ask you to audience url and ACS url. After that it’s going to ask you whether it is an internal app or external app you select the internal app. After that click on finish and save itIf application require that you have to also add attributes like first name, last name, login, email you can create an attributes and then save it.After that you can get a SAML metadata and then copy those metadata and send to application put those upload those metadata in to the application.After that you can get the login url and also ACS url then bring it to okta and do the integration after that activated.**

**07) What is IDP and explain IDP flow ?**

**IDP Initiated flow**

**IDP is the entity providing the identities, including the ability to authenticate a user.**

**IDP typically also contains the user profile and additional information like firstname, lastname,jobcode**

**In the flow user directly access to the idp SSO url , its redirects to the idp login page .**

**Where the user provides the credential .now the user credential will validated against the idp.**

**If the validation is success authentication is completed. idp will generated SAML assertion and send back to the sp or application through ACS Url.**

**Or**

* **User directly click on IDP SSO url**
* **Login page opens username and password**
* **User has provide credential**
* **The credential will be validated in IDp. If the credential which are given is correct authentication is success.**
* **Session will generate and checks for an authorization.**

**The SAML assertion will posted to ACS url upon successful of authentication and authorization**

**08) What is SP and explain SP flow ?**

**SP Initiated flow**

**SP is the entity. Providing the service**

**Sp stands for service provider it provides services to the end user**

**In the flow end user will access the application url**

**If there is no session on the browser, application will redirect the request to the idp, with the help of SAML authentication request.**

**its redirects to the idp login page .**

**Where the user provides the credential .now the user credential will validated against the idp.**

**If the validation is success authentication is completed. idp will generated SAML assertion and send back to the sp or application using the post message**

**The sp verifies the assertion maps it to user and then session can start.**

**Or**

* **User hits the SP url on the browser.**
* **SP will redirect to the idp by saml authentication request if session is not found**
* **IDP through login page to user through browser.**
* **Login page opens username and password**
* **User has provide credential**
* **The credential will be validated in IDp. If the credential which are given is correct authentication is success.**
* **Session will generate and checks for an authorization.**
* **The SAML assertion will posted to ACS url upon successful of authentication and authorization.**

**09)What are the components in SP metadata**

**Or what does SP meta data contains**

**A set of information supplies by the IDP to SP in XML format**

**Sp supplied metadata**

**ACS Url**

**EntityID(Audience Restriction)**

**Certificate**

**NameID format**

**10)What are the components in IDP metadata**

**Or what does IDP meta data contains**

**IDP Supplied matada**

**SSO Url**

**EntityID**

**Certificate**

**11) What is SAML request ? what does it contains?**

**It known as the authentication request ,is generated by the SP to request an authentication.**

**In the samal request is completed we will check to the saml tracer on request ulr in the flow we are checking the**

**1.issuer – Entity id of sp**

**2. Destination – the request where to sent location is IDP SSO location check the details**

**3.ACS location – check the both sp ACS url –endpoints of SP**

**4 – check The ID it wil generate Sp**

**12) what is SAML response ? wht does it contains?**

**Its generates by IDP. it Contains actual assertion of the authenticated user. In addition, a SAML response may contains additional information user profile information and group/rule, depending on what the SP can support**

**In the saml response we are checking the**

**1.issuer- entity id of IDP**

**2.Destination- ACS url of Sp (idp will send back to response on sp )**

**3.certificate**

**4 Responseto – here Id will check eith request id both are are matching response is good**

**5 subject :**

**If there is no subject in response the problem is idp Beacause username not properly prompted Authentication**

**Here seen the username and attributes.**

**Status: check the status Is success or not**

**13) What is entityID and ACS url?**

**A globally unique name for an IDP or SP . Unique okta entity id is generated for each application.**

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

**14) what is binding and types of bindings**

**Bingings**

**Binding is the explain how messages and assersion are sent between the sp and idp.**

**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** .

**The REDIRECT BINDING can be used for request for authentication messages sent from an sp to an idp.**

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

**15)How can you check the SAML response or Request?**

**By using the saml tracer will check the details of ACS url ,entity ID, attributes or claims, certificate**

**16) What are the prerequisites of SAML**

**Application type**

**SSO protocol**

**Env**

**Metadata**

**ACS url**

**Nameid format**

**MFA requirement**

**Target complession**

**Group info**

**User provisioning**

**Access**

17)What is Encryption in SAML?

In SAML (Security Assertion Markup Language), encryption plays a crucial role in ensuring the confidentiality and integrity of sensitive information exchanged between parties. Specifically, encryption in SAML involves securing assertions, which are XML documents containing information about a user's authentication and authorization.

When an assertion is encrypted in SAML, its contents are transformed into an unreadable format using cryptographic algorithms and keys. This ensures that even if the assertion is intercepted by unauthorized parties, they cannot decipher its contents without the appropriate decryption keys.

Encryption in SAML typically involves the following steps:

1. **Key Exchange**: Before encryption can occur, the parties involved must agree on encryption keys. This is often done through a process called key exchange, where cryptographic keys are securely shared between the identity provider (IdP) and the service provider (SP).
2. **Assertion Encryption**: Once the encryption keys are established, the sensitive parts of the SAML assertion (such as user attributes or authentication statements) are encrypted using these keys. This process ensures that the assertion remains confidential and cannot be tampered with while in transit.
3. **Transmission**: The encrypted assertion is then transmitted from the identity provider to the service provider or vice versa. During transmission, it remains in its encrypted form, protecting it from eavesdropping or tampering.
4. **Decryption**: Upon receiving the encrypted assertion, the receiving party uses its decryption keys to decrypt the assertion and access its contents. This allows the recipient to verify the authenticity of the assertion and make authorization decisions based on the decrypted information.