<https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language>

A SAML assertion query / request usually doesn't contain much private data, and the request itself is usually not persisted for use later, so there is little need to encrypt the SAML request itself. Signing it will allow the receiver to verify that the contents have not been altered in transit, and transimitting it via SSL will provide privacy during transmission. Encrypting the request in this situation is probably overkill.

A SAML assertion response, however, is a whole different animal. A SAML response that contains claims or assertions will likely contain private data. Depending on how these assertions are being used in your system, the assertions may be passed around between different parties, some which have the keys required keys to decrypt the content (because they have a trust relationship with the SAML provider) and some which do not. The SAML assertions could be stored in a cache or in a database, so you really don't know who will be poking through them in the future.

If the SAML response contains claims and assertions that contain private data, and the receiver of the response will be holding onto the SAML assertion for an indefinite period or passing the SAML assertions through intermediate parties you do not trust, then yes, the SAML assertions should be encrypted and the response signed, regardless of whether it is transmitted by SSL or not. Encryption is to protect the privacy of the data after it arrives at the other end of the SSL pipe.

<https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language>

<https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/ca-enterprise-software/layer7-identity-and-access-management/single-sign-on/12-7/using/administrative-ui/legacy-federation-reference/saml-2-0-service-provider-reference/saml-service-provider-encryption-and-signing-options.html>

<https://gravitational.com/blog/how-saml-authentication-works/>

            SAML: correct

Groups from: correct

            OIDC: correct

Grant Types: correct

Password Flow – doesn’t know

PKCE flow - incorrect

App Type in Okta: correct

            OAG: Correct

            Only SSO: Answered - Yes - Correct.

            On-prem SCIM connector provisioning:

Groups provision: doesn’t know

Configurations in Okta: Correct

            Behavior detection: concept is correct.

            Workflow Automations: Correct

            Inline & Event Hooks: Correct

            Self-service Reg: Correct

            Password Policy: inside the company’s network, perform SSPR, outside – No

Correct

            MFA for specific apps only - Correct

            AD Integration: Correct

            Create user from Okta to AD: correct

            Push Groups: correct

            Org 2 Org approach: correct

            Coding: Java

            API token validity: correct

            Okta APIs: good understanding

            Good understanding. Technically good.

            Listens well and answers to the point.

> Experience

> Brief Intro

> Their environment - AD, workday

> Custom sign-in widget

> IDP intg

* Okta to Okta integration

> I have a scenario where I want to bring in my AD users to Okta but I don’t want Okta to store my user’s credentials- how do u achieve this?

>What is Just in Time Prov?

If delegated authentication is enabled, you do not need to import users from AD first for JIT provisioning to create Okta accounts.

> I have a scenario where I want to map my AD email to Okta email but append the email with .in. How do you do this? – Using Okta expression language

**>Okta Username format** list, select one of these formats that you want AD-imported end users to use when logging in to Okta:

* Email address
* SAM Account Name
* User Principal Name (UPN)
* custom

>If the error message *The underlying connection was closed. Could not establish trust relationship for the SSL/TLS service channel*, appears you are likely installing a version of the Okta AD agent with SSL pinning enabled by default and this prevents communication with Okta. This is most likely to occur in environments that rely on SSL proxies. To complete the installation, Okta recommends adding the domain okta.com to a whitelist to bypass SSL proxy processing. You can also disable SSL certificate pinning.

>If I don’t want to schedule the import of users, but manually import it is there a way to do it?

>Types of import in okta

I see you have wrked on AD integration.

> Explain the Okta AD architecture.

> Okta service account?

## Required accounts

* [Okta admin account](https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-prerequisites.htm#Oktaadmin) — Used when you install the AD agent to allow the AD agent to connect to Okta. This account should be Okta-mastered, not AD-mastered. The minimum admin role required for this account is **Super admin**.
* [AD service account](https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-prerequisites.htm#ADuseraccount)— Required to install the Okta AD agent. It is important that the service account has permissions in all domains in that forest to read and access user data in all domains to which the agent connects.
* [Okta service account to run Okta AD Agent service](https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-prerequisites.htm#OktaService) — This is an AD domain service or user account. It can be created by the installer (called OktaService by default) or you can select an existing account.

> To provide high availability and failover protection, the installation of two or more Okta Active Directory (AD) agents on separate servers in each domain is recommended. If an Okta AD agent stops running or loses network connectivity, authentication requests are automatically routed to other Okta AD agents.

Change the Okta Active Directory agent user

>Change the Okta Active Directory agent user name when responsibility for managing the agent changes.

1. Sign in to the server running the Okta AD agent.
2. From the Start menu, type **run**, then type **services.msc**.
3. Locate the **Okta AD Agent Service**.
4. Right-click **Okta AD Agent Service** and select **Properties**.
5. Select the **Log On** tab and change the account credentials.
6. Restart the service.
7. Sign in to the Okta Admin Console, click **Dashboard**, and confirm that the circle next to the agent name is green.

>The AD user profile schema requires both the first and last name. You can create an Okta mastered user without a first or last name, but you cannot import an AD user into Okta without a first and last name.

> I have multiple agents, can i setup a Load balancing or failover mode of agent selection btw them?

              SSL Port for AD and SSL port for LDAP

              Okta Agent connections are Port 443 for AD (SSL Encrypted) and over Port 636 for LDAP

> You have setup an AD agent and the agent is running. You import users, users are imported. You push a user, you cant. The error is insufficient privileges, do you know how to resolve this?

> An Okta Administrator has installed the Okta Active Directory Agent but the Okta Active Directory Agent

is NOT connecting after startup.

Would you check the logs in Okta system logs or the AD agent logs on the server?

Transport Layer Security (TLS) 1.2 is NOT enabled.

> What is the agent log file location? C:\Program Files (x86)\Okta\Okta AD Agent\OktaAgentService.exe.config

1. On the system running the affected AD Agent, navigate to the "Logs" directory in the AD Agent install directory. By default, this is C:\Program Files (x86)\Okta\Okta AD Agent\logs

* ​The most recent log file will simply be called "Agent."  Older log files will have a number appended to the filename (i.e. Agent-1), with each successive number representing an older log file
* The log files are limited to 10 MB in size, and a new file will be created when this limit is reached
* the "InstallUtil" file provides both installation and update-related information
* the "Service" file details when the OktaADAgent Windows service stops and starts

>To synchronize passwords from Okta to AD, you enable Sync Password on the Okta Admin Console Provisioning page. To synchronize passwords from AD to Okta, you install the Okta Password Sync agent on all integrated domain controllers in your domain.

# >Update the Okta Active Directory agent

If you need to update an Okta AD agent, you don't need to uninstall it. The agent installer automatically updates existing Okta AD agents. Alternatively, you can uninstall and then reinstall the Okta AD agent to make sure that you have the most current features and functionality and are getting optimum performance.

If you have installed multiple Okta AD agents, make sure that they are all the same version. **Running different versions within a domain can cause all agents in that domain to function at the level of the oldest agent**. This does not affect other domains.

What are the agent related logfiles available on the server hosting the AD agent?

> Consider the scenario - I am Importing 1,00,000 users from AD to Okta.

              How many agents do you think i should have to perform this activity? What is the Okta recommendation here?How do you suggest i do this activity? Any Best practices?

1 ad agent can handle – 15k users

> Password Policies

              > Once a pswd is set for a user, i want to restrict the user from changin the pswd again in the next 5 days. How can i achieve that?

              > Do you know the feature Common password check?

                             Can i create a list of passwords my client does not want and use this feature to block those pswds?

              > Okta creates a password policy in Okta for AD when it is intgerated with AD. called the AD pswd policy.

                             What is it for?

# >Can you Register multiple domains to an Okta Active Directory agent-Yes

# <https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-register-multipledomains.htm>

>Version question:

https://help.okta.com/en/prod/Content/Topics/Settings/Version\_Histories/Ver\_History\_AD\_Agent.htm

>How to push users from Okta to AD: <https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-configure-provisioning.htm>

Enabling **Create Users** lets Okta create users in Active Directory (AD). This allows you, for example, to import users from an HR system, create the users in Okta, and then have Okta create the users in AD. The HR system is the master, with Okta and AD being updated based on changes in the HR master. Or, another use case may include Okta being the source of truth for all user information and pushing those updates into AD.

To implement this functionality, you first need to create a group in Okta and then assign that group to your AD instance. When users are added to the group, they are also created in AD. A common scenario is to use group rules in this kind of flow to add users to the AD provisioning group automatically.

In the **Activation email recipient** field, enter the email address of the Okta admin who receives activation emails with the Okta user's password. The admin is responsible for giving the end user their Okta password.

> Do you know the Group Push feature in Okta?

What does it do?

> There are Multiple profile masters in your environment but i want one of the attributes to be managed by Okta. How do I do that?

Attribute Level Mapping

> Which HRMS tool you said? Any knowledge on Workday?

> Workday

              Explain?

              Is the sync real time? If not, which features have a RTS?

              How does Immediate termination work btw Okta and Workday?

> Since we manually create Okta mastered users or either by CSVs, are there any other ways you create a user?

1. Through API’s

 2. Registrtion Self service: elaborate?

1. CSV
2. manuallu

> Explain user deactivation in Okta.

1. manually or through API

              Can i automate this w.r.t user inacivity? – Through Workflow automation we can give condition

> Where can you enforce MFA in Okta? Org Level or App Level

>Sign On policy takes precendence

>How do you restrict users from particular IP address to access any application?

>How do you kind of restrict a person from accessing from one location- dynamic zones(city,ASN) or through behavioral detection

>Device Trust: meant for trusting a device and accessing mobile app

> Inline Hooks?

              Can you give me an example of where i can use this? Inbound call to Okta

> How would you integrate a SAML/OIDC app?

              Explain the SAML flow between the Okta and a downstream app?

              What is the data you require from the SAML app to integrate it in Okta?

SAML FLOW: Idp idnitated and SP

How do you kind of troubleshhot Saml issues

              OIDC? Types of OIDC flow:

> What could be the possible reasons if the provisioning to an application is not working?

1. User is inactive

2. User is not assigned to application

> Bypass IDP discovery?

# Identity Provider Routing Rules

Identity Provider (IdP) routing rules enable you to direct end users to identity providers based on the user's location, device, email domain, attributes, or the app they are attempting to access. (This feature is also known as IdP Discovery, because these routing rules allow Okta to discover which identity provider to use based on this context.)

> Which admin can create an API token that CANNOT change configurations in Okta? API access administrator

> I am an Org admin, can i create another Admin user in Okta? No..only super admin

> What is the Behavior detection in Okta?

Can be done on what user request parameters?  --->

> API Token details:

Validity of a Token?

> API? --> What are the different APIs we have in Okta?

Have you used the APIs? In what cases?

Explain any API you have used?

Okta custom sign in widget- custom domain url

Custom email templates

New features of okta- ASA, OAG , Workflows,

Is this piece of information required the very first time a user launches Okta Mobile?

A. Company Name

B. Credentials (Username and Password)

[**With Agentless DSSO enabled, you browse to your Okta tenant and see the regular sign in page.**](https://help.okta.com/en/prod/Content/Topics/Directory/dsso-troubleshooting.htm)

You were not routed to the Agentless DSSO endpoint. Confirm your IP address is added to the correct zone and that zone is used for the Agentless DSSO.

[**Desktop SSO/IWA not working**](https://help.okta.com/en/prod/Content/Topics/Directory/dsso-troubleshooting.htm)

* Ensure the host name of the server is resolvable from within the client network.
* IWA must be turned on in both the IIS authentication configuration and in the client.