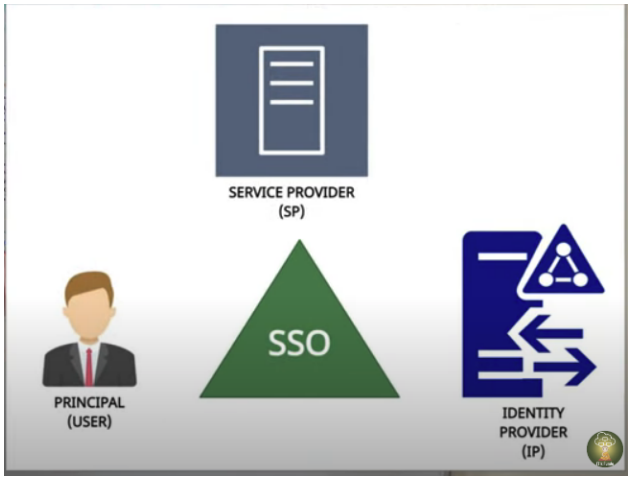
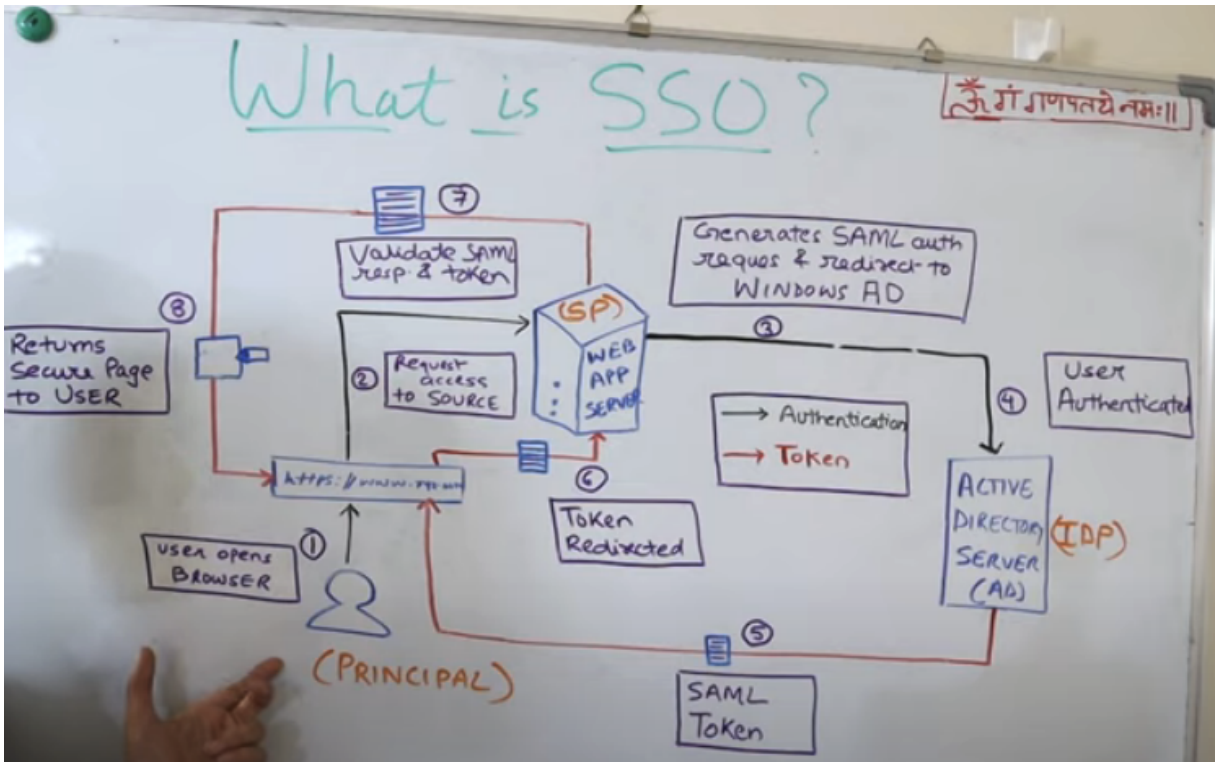


SP stands service provider (passport office)
IDP - identity provider (eg: aadhar card)
User who enters credentials is PRINCIPAL.
SSO - single sign on
SAML - Security Assertion Markup Language
SAML Request and Response happens are in xml format

It is something like once you show your identity and invitation at the gate to the security in a marriage. They tag you. So that you can enjoy food and drink and marriage.



Black arrow is authentication workflow and red arrow is token workflow

1. User open the browser and enter url of service provider
2. Browser redirects to web app server (request access to service)
3. Web app generates SAML auth request and passes it to Identity provider (it can be Active Directory server or Azure). This is because the web app server wants to know if a request is coming from a legitimate user or not.
4. User is authenticated
5. SAML token Generated and sent to browser by identity provider
6. Browser redirects token to Service provider
7. Service provider validate SAML token
8. Service provider grants access to page (for certain period - Token contain how much time)