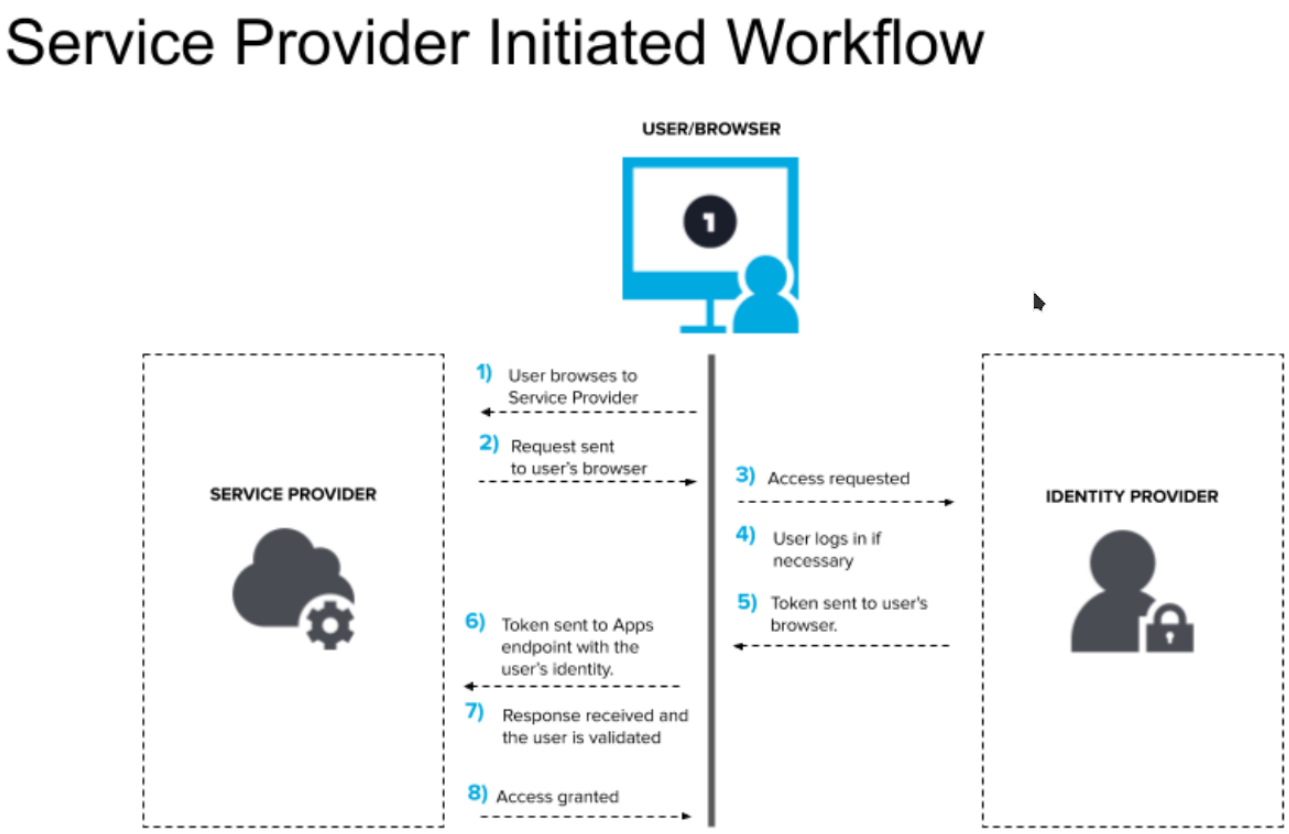
Single Sign-On



SSO is basically a trust relationship between an Application and a Identity Provider. This trust is based on certificates exchanged between the Service and the Identity providers. The certificates are then used to sign Identity documents whcih are then shared between the two providers. This certificate allows the Service Provider to validate that the information is being sent from a trusted source. The certificate is basically the digital signature which is exchanged during the initial configuration.

- User Requests the Service Provider, i.e. Web Application for the Service.
- The Service Provider requests the Identity Provider for the authentication and access.
- The Identity Provider checks if the user was previously authenticated, if yes then it sends the authentication token to the Service Provider via the users browser.
- If the user was not authenticated the user is prompted to enter the user credentials for authentication.
- Then a success token is created and sent to the Service Provider which then allows user the access to the Service.