**SAML**

SAML abbreviated as Security Assertion Markup Language is a protocol that gives certain set of rules for making authentication and authorisation process more secure. Using SAML protocol, service providers can authenticate user credentials from identity providers. It is also a framework that gives a predefined format of exchanging data between service and identity providers.

**SAML WORKING:-**

SAML working takes place in two ways:

1. IDP intiated flow: In this flow, the user who wants to sign in into the service provider must first authenticates into an IDP . After successful authentication, IDP post a XML document containing user credentials called as SAML assertion and attach system certificate as signature. This SAML assertion goes to the user, the user give it to the service provider. Service provider has its own SAML assertion, it validates it with the signature and then allow user to sign in.
2. SP intiated flow: In this flow, the service provider directs the user to the IDP for authentication, after authentication of the user the IDP generates a SAML assertion containing user credentials . This assertion is sent via user to the SP. SP validates it then user is allowed to sign in.

**SAML Benefits:**

1. It is widely used for enterprises because it has advantage of sign in once and access multiple web services.
2. Highly secured.
3. Provides a great user experience as user does not have to give user credentials to different service providers and can sign in to multiple sites by single set of credentials entered once.

**Authentication:**

Authentication is the process in which the identity of users are verified. It uses different processes like OTP verification, Multi factor authentication.

**Authorisation:**

Authorisation is the process which checks the user’s authority for assessing the resources. In layman language it determines what permissions do user have .