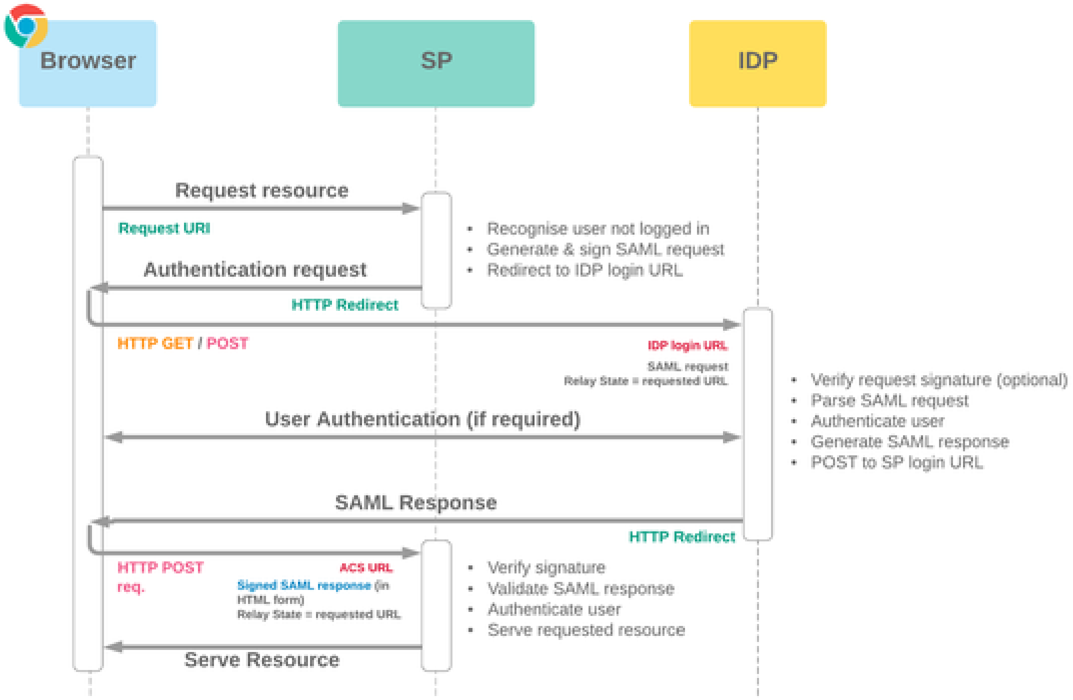
Cognito Low level Flow



If COGNITO acts as the Service Provider:

- COGNITO "Single-Sign On Settings" should be configured with values from the IDP
- Certificates from the IDP should be uploaded as the identity provider certificate in COGNITO. This is used for signature validation on incoming SAML responses
- Requests will be signed by COGNITO with the selected certificate, which can be validated by the IDP if necessary
- IDP-encrypted assertions are also supported, and decryption certificate uploaded and selected as Assertion Decryption Certificate
- SAML request bindings can be configured to be bound to HTTP Redirect or HTTP POST (determines whether initial SAML authentication request is GET or POST)
- Just In Time (JIT) user provisioning can be configured to enable automatic creation/update of users based on contents of incoming SAML assertions. COGNITO will attempt to match a user and will either update this record or create a new user in real time. Standard provisioning allows assertion attributes corresponding to standard field names to be used for matching and values for field contents, or custom logic can be defined in a class implementing the Auth.SamlJitHandler interface
- The IDP will need to be set up with the Authorisation Consumer Service (ACS) URL ("COGNITO Login URL") and Entity ID
- MyDomain required for SP-Initiated SSO, which enables deep linking (landing on requested URL) and OAuth with SAML

Reference : https://aws.amazon.com/premiumsupport/knowledge-center/cognito-okta-saml-identity-provider/

Entities Inside SAML Response

- **EntityDescriptor** - to identify the SP Metadata
- **entityID** - Unique ID to validate between IDP and SP
- **IDPSSODescriptor** - to check the Match between IDP's Metadata and SP's Metadata
- **SAML:2.0:protocol** - Communicates over HTTP Connection
- **KeyDescriptor** - Helps to exchange the Keys
- **X509Data** - Acts as a Authenticator by Exchanging Keys
- **Assertion Encryption** - Allows you to encrypt the Data flow between IDP and SP

TERMINOLOGY

SAML

- **Security Assertion Markup Language (SAML)** - Provides an open standard for XML-based confirmation of identity and transfer of identity attributes between an Identity Provider and Service Provider
- **Identity Provider (IDP)** - An application with the capability to authenticate a user's identity (i.e. allow the user to login), and confirm authentication and identity attributes to a Service Provider
- **Service Provider (SP)** - An application which defers to an Identity Provider for authentication of a user, and allows this user access to protected resources or capabilities based on this authentication

- **SAML Request** - The structured XML message sent by the Service Provider to an Identity Provider, identifying itself and requesting authentication of the user
- **SAML Response** - The XML message sent by the Identity Provider to the Service Provider identifying itself as the issuer, indicating the status of the authentication attempt, and including the SAML Assertion if this can be issued (typically signed with the Identity Provider's certificate)
- **SAML Assertion** - The portion of the SAML Response which confirms identity attributes of the authenticated user