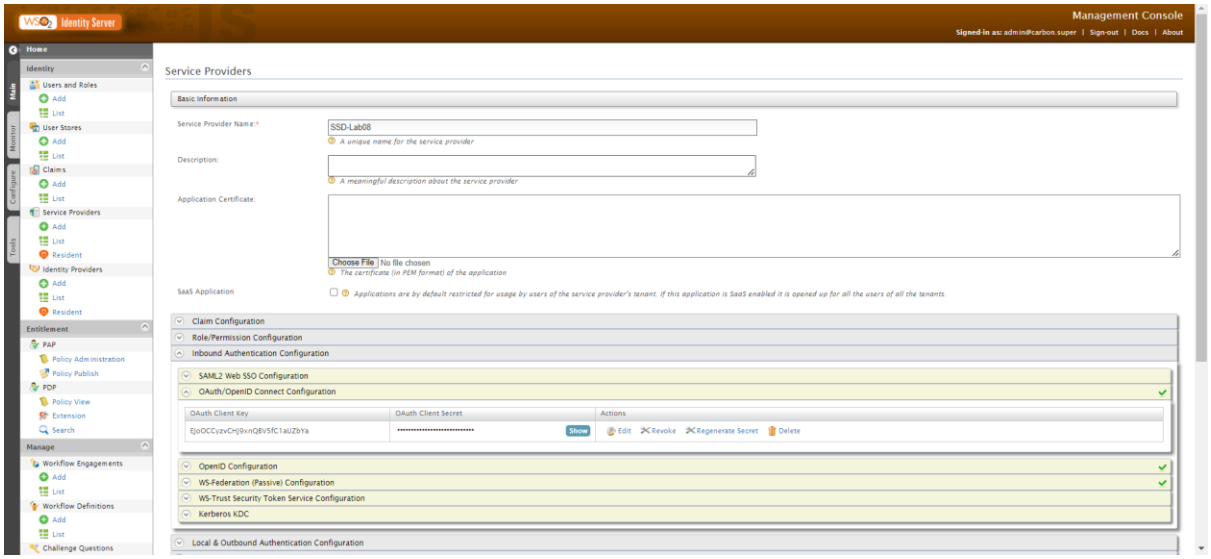
1)



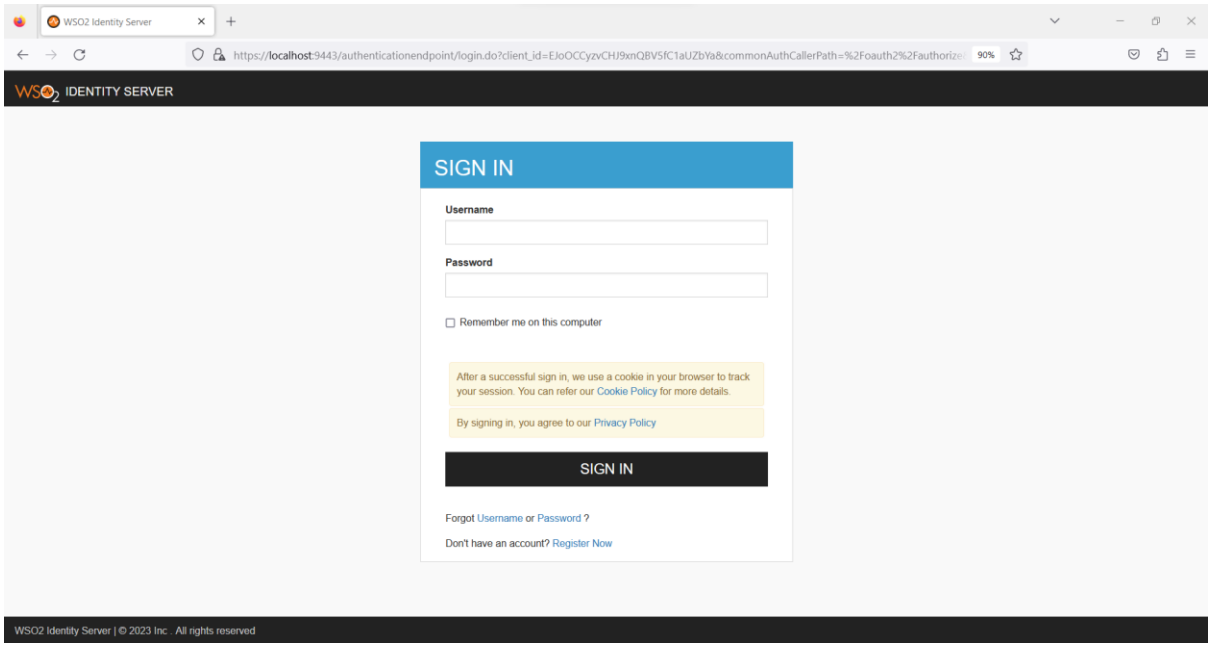
Client ID - EJoOCCyzvCHJ9xnQBV5fC1aUZbYa

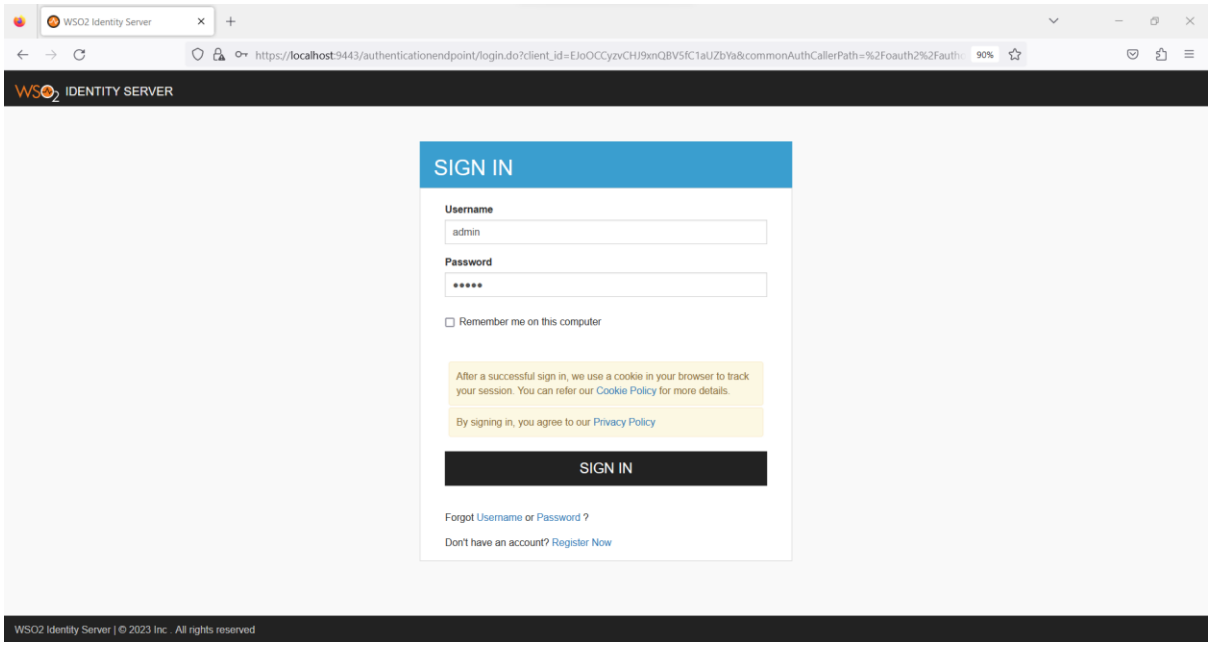
Client Secret - 4p1_ck8MsUAk0WTZxo6BJBbWMJEa

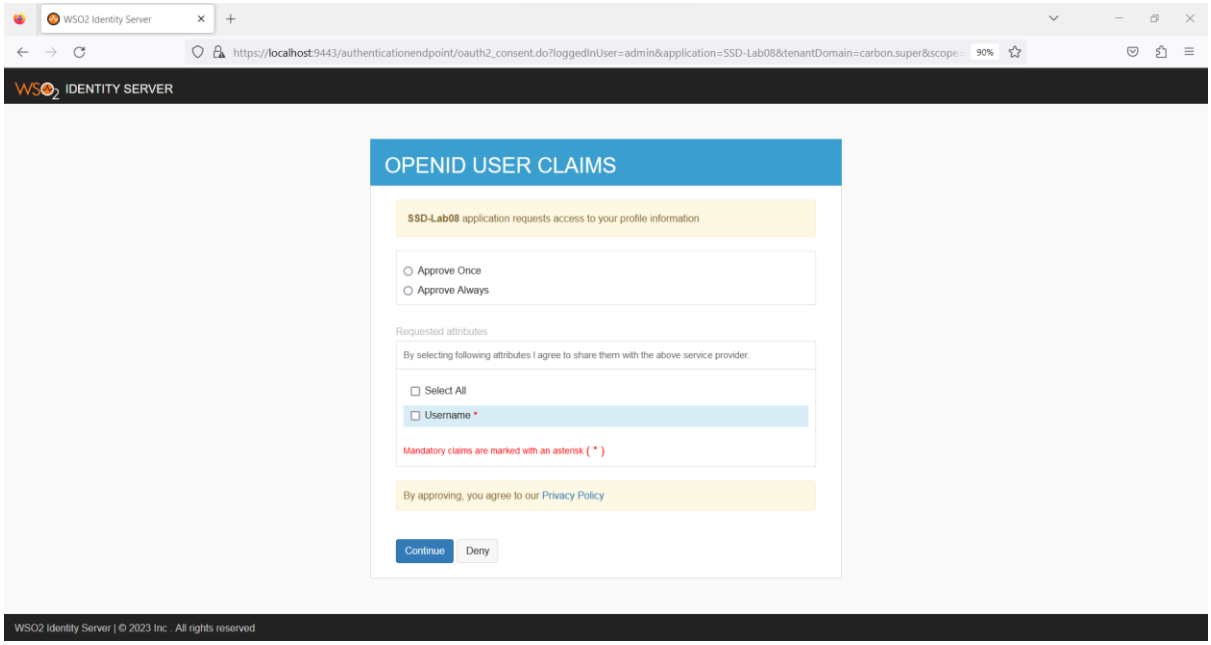
Redirect URL - https://localhost:8080/callback

2)

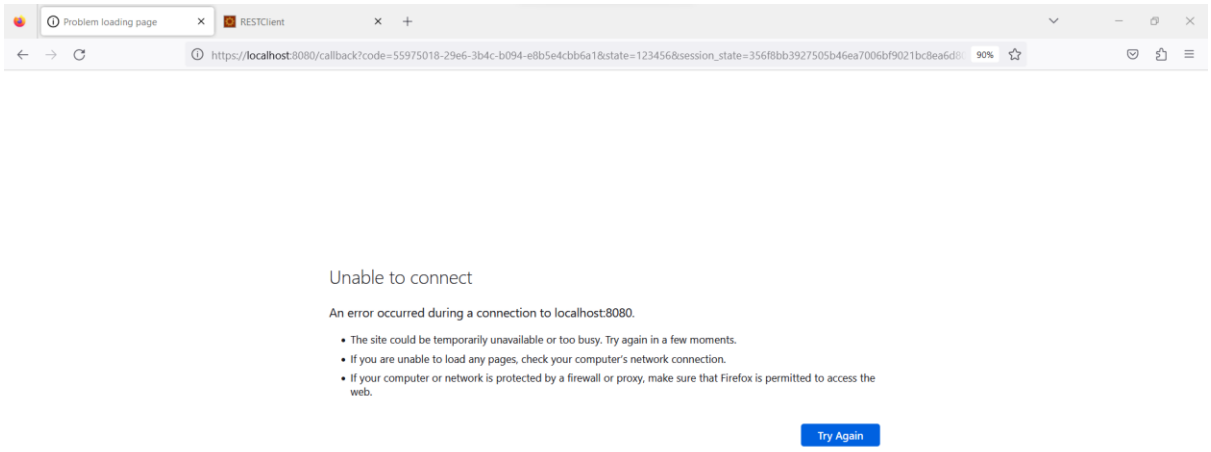
Request to get the access token - https://localhost:9443/oauth2/authorize?response_type=code&client_id=EJoOCCyzvCHJ9xnQBV5fC1aUZbYa&scope=openid&state=123456&redirect_uri=https%3A%2F%2Flocalhost%3A8080%2Fcallback







Response - https://localhost:8080/callback?code=55975018-29e6-3b4c-b094-e8b5e4cbb6a1&state=123456&session_state=356f8bb3927505b46ea7006bf9021bc8ea6d80b78811317b88f6222072e305c6.-u3_BdAfaRIciM9VlxMvyw



Request to get the Open ID token –

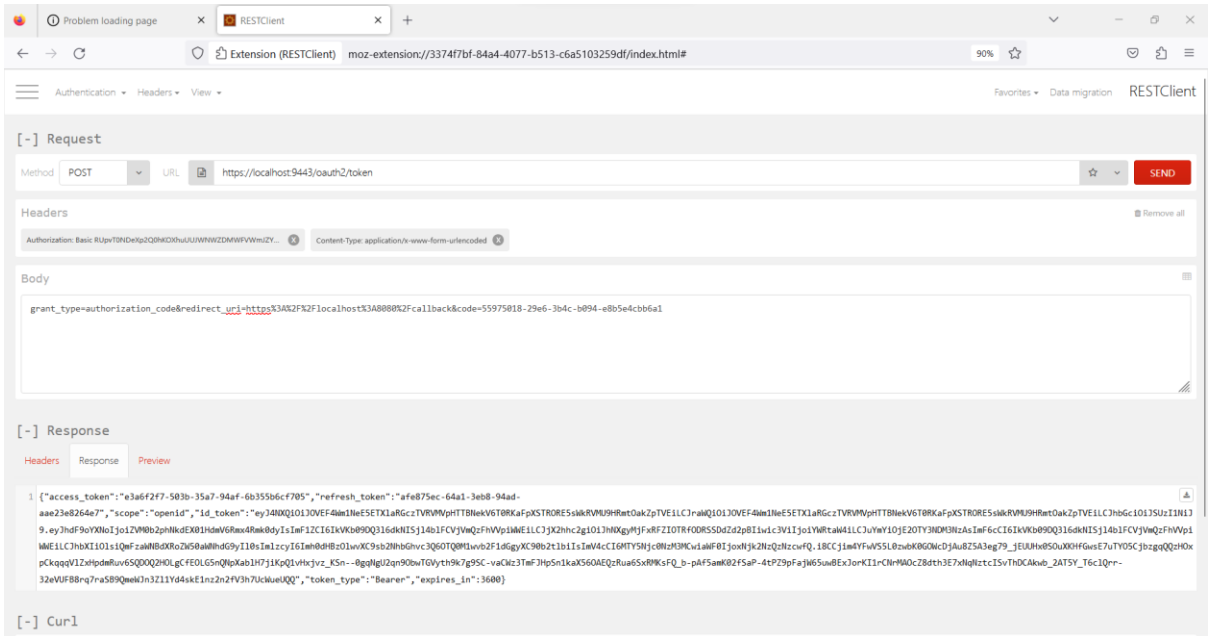
POST request - https://localhost:9443/oauth2/token

Headers –

Authorization -> Basic RUpvT0NDeXp2Q0hKOXhuUUJWNWZDMWFVWmJZYTo0cDFfY2s4TXNVQWswV1RaeG82QkpCYldNSkVh

Content-Type -> application/x-www-form-urlencoded

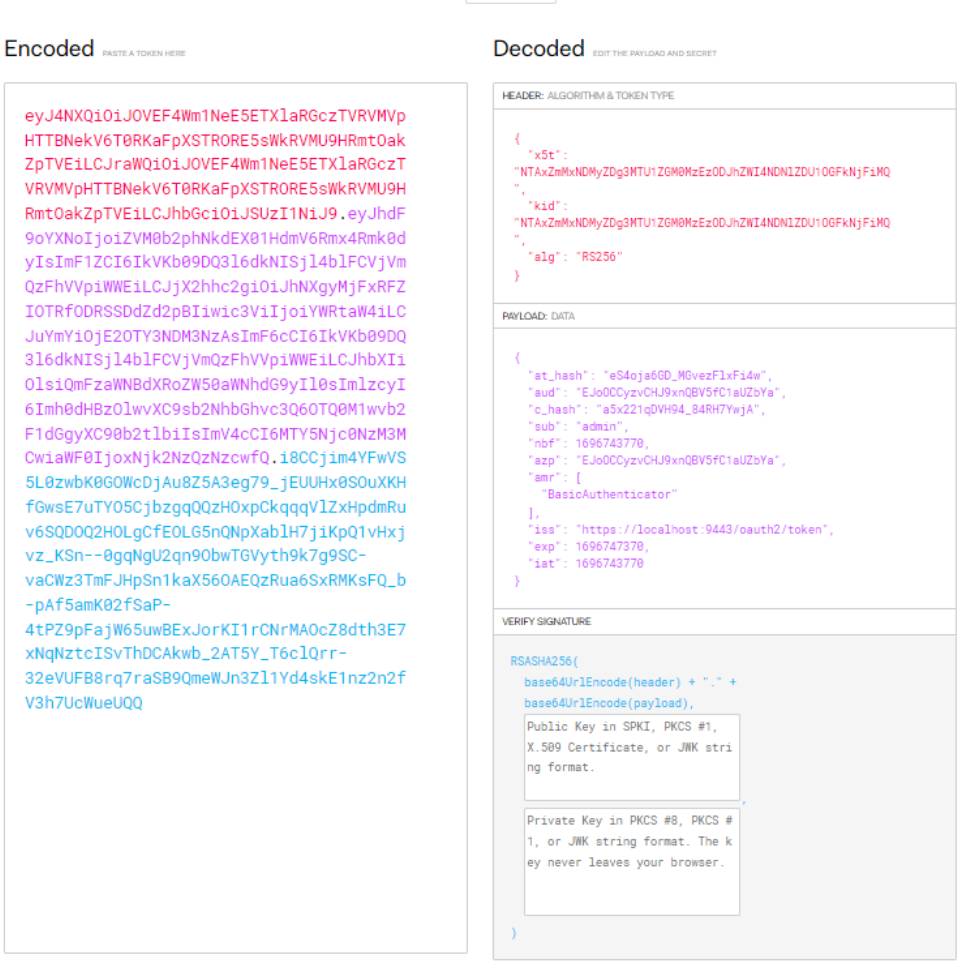
Body - grant_type=authorization_code&redirect_uri=https%3A%2F%2Flocalhost%3A8080%2Fcallback&code=55975018-29e6-3b4c-b094-e8b5e4cbb6a1



Response –

{"access_token":"e3a6f2f7-503b-35a7-94af-6b355b6cf705","refresh_token":"afe875ec-64a1-3eb8-94ad-aae23e8264e7","scope":"openid","id_token":"eyJ4NXQiOiJOVEF4Wm1NeE5ETXlaRGczTVRVMVpHTTBNekV6T0RKaFpXSTRORE5sWkRVMU9HRmtOakZpTVEiLCJraWQiOiJOVEF4Wm1NeE5ETXlaRGczTVRVMVpHTTBNekV6T0RKaFpXSTRORE5sWkRVMU9HRmtOakZpTVEiLCJhbGciOiJSUzI1NiJ9.eyJhdF9oYXNoIjoiZVM0b2phNkdEX01HdmV6Rmx4Rmk0dyIsImF1ZCI6IkVKb09DQ3l6dkNISjl4blFCVjVmQzFhVVpiWWEiLCJjX2hhc2giOiJhNXgyMjFxRFZIOTRfODRSSDdZd2pBIiwic3ViIjoiYWRtaW4iLCJuYmYiOjE2OTY3NDM3NzAsImF6cCI6IkVKb09DQ3l6dkNISjl4blFCVjVmQzFhVVpiWWEiLCJhbXIiOlsiQmFzaWNBdXRoZW50aWNhdG9yIl0sImlzcyI6Imh0dHBzOlwvXC9sb2NhbGhvc3Q6OTQ0M1wvb2F1dGgyXC90b2tlbiIsImV4cCI6MTY5Njc0NzM3MCwiaWF0IjoxNjk2NzQzNzcwfQ.i8CCjim4YFwVS5L0zwbK0GOWcDjAu8Z5A3eg79_jEUUHx0SOuXKHfGwsE7uTYO5CjbzgqQQzHOxpCkqqqVlZxHpdmRuv6SQDOQ2HOLgCfEOLG5nQNpXablH7jiKpQ1vHxjvz_KSn--0gqNgU2qn9ObwTGVyth9k7g9SC-vaCWz3TmFJHpSn1kaX56OAEQzRua6SxRMKsFQ_b-pAf5amK02fSaP-4tPZ9pFajW65uwBExJorKI1rCNrMAOcZ8dth3E7xNqNztcISvThDCAkwb_2AT5Y_T6clQrr-32eVUFB8rq7raSB9QmeWJn3Zl1Yd4skE1nz2n2fV3h7UcWueUQQ","token_type":"Bearer","expires_in":3600}

3)



OpenID tokens consist of 3 segments separated by two dots.

1) Header – Declaring the type as JWT, Hash or keyed hash algorithm
2) Payload – useful user-specific information (issuer, subject, expiry date etc)
3) Signature- encoded header and payload separated by a dot and encrypted with a hash algorithm afterwards

   As shown in above figure, x5t is the signature of the entire id token. When auth server has to deal with multiple id tokens, this x5t attribute is used to uniquely identify and search for each token. Algorithm is mentioned as RS256 which is asymmetric encryption. In the payload subject is the admin, because wso2 admin login was used for getting the token and the issuer is the token endpoint of the identity server. Signature is also available in an encrypted format.