Authenticate With JWT

1. Generate Digital Certificate and Key
   1. Create a certification folder where you want to keep your digital certificate and key.
   2. From within the certificate folder, generate an RSA private key:

openssl genrsa -des3 -passout pass:SomePassword -out server.pass.key 2048

* 1. Create a key file from the server.pass.key file:

openssl rsa -passin pass:SomePassword -in server.pass.key -out server.key

* 1. Delete the server.pass.key:
  2. Request and generate the certificate:

openssl req -new -key server.key -out server.csr

* 1. Enter all requested information.
  2. Press Enter when prompted for the challenge password.
  3. The Certificate Authorities use this password to authenticate the certificate owner when they want to revoke their certificate. Because it’s a self-signed certificate, there’s no way to revoke it via CRL (Certificate Revocation List).
  4. Enter a period (.) to skip entering an optional company name.
  5. Generate the SSL certificate:

openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt

* 1. The self-signed SSL certificate is generated from the server.key private key and server.csr files.
  2. Your certificate folder should have below three files.
     1. server.crt
     2. server.csr
     3. server.key

1. Create connected app in Salesforce
   1. API (Enable OAuth Settings)
      1. Enable OAuth Settings
      2. Callback URL : <http://localhost:1717/OauthRedirect>
      3. Use digital signatures and upload digital certificate from step #1.
   2. Add these OAuth scopes:
      1. Access and manage your data (API)
      2. Perform requests on your behalf at any time (refresh\_token, offline\_access)
      3. Provide access to your data via the Web (web)
   3. Rest Keep Default.
2. Create a Permission set and deployment user.
   1. *Create a Permission set*
   2. *Add permission to the above connected app*
   3. *Assign this permission set to the deployment user (who wants to do JWT authentication)*
3. Change connected app OAuth policy
   1. *Go to manage connected app*
   2. *Edit policy and change OAuth policy >> Permitted Users to*
      1. Admin approved users are pre-authorized
   3. Verify in the Permission set section of the connected app is having the permission set added in step 2.
4. Authenticate with JWT
   1. Copy clientid from connected app step 1
   2. Copy directory path to the private key with file name generated at step 4.f.iii
   3. Copy user name of the deployment user (which has permission set assigned from step 2)
   4. Execute the below command for JWT Authentication where instance url is the target salesforce url.
   5. sfdx force:auth:jwt:grant --clientid <clientid> --jwtkeyfile <private key file including path> --username <deployment username> --instanceurl <salesforce instance>

Example: sfdx force:auth:jwt:grant --clientid 3MVG95jctIhbyCpopqU.7KUooKvfZk36BosqlB3NlrNkDKbaMc5Xl8DbAs0W9UPuIN4Bn5KvQg1HmMj.hjHzl --jwtkeyfile "C:\Users\GOYALDEV\Documents\Docs\Projects\CI CD\JWT Key\Development-POC\ server.key" --username development@poc.com --instanceurl https://login.salesforce.com

* 1. This should return you following successfully message

Successfully authorized development@poc.com with org ID 00D5w000002sC27