1.5.1 MyDigital ID SSO Protocol Sequence Components

Components:

1. **User**: The end-user requesting access to resources.
2. **3rd-Party Application (App)**: The client application consists of a mobile application or web application that the user interacts with.
3. **MyDigitalID App**: An app responsible for verifying users and generating tokens.
4. **Keycloak/MyDOW Cluster (OIDC Provider)**: The OpenID Connect (OIDC) provider for handling authentication.
5. **WebSocket Cluster (WSS)**: Manages WebSocket connections for real-time communication.
6. **Signet Cluster**: Handles secure token verification and status updates.
7. **Flow Explanation:**

   1. User Request

   - The user makes a request to the application for a resource, but there is no prior authentication.

   2. Redirect to Keycloak

   - The application redirects the user to Keycloak for authentication.
   - Keycloak detects the Mydigital ID Identity Provider as the IDP stated in the authentication flow of the client.
   - Keycloak redirects requests to MyDigital MyDOW IDP which then produces the unique nonce and generates the MyDigital ID QR code to be scanned and application url link to Signet server if the QR is clicked.

   3. Action and Token Generation

   - The user performs an action by scanning using MyDigital ID app (Desktop web app) or click on the QR code (Mobile app or Mobile PWA)
   - MyDigitalID commence the MyDigital ID authentication protocol (3way handshaking)

4. WebSocket Initiation

- While the MyDigital ID app is bound to the websocket server, the 3rd party application is also connected with the Websocket Connections. The connections from the 3rd party application will join a channel determined by the nonce.
- The Two apps, 3rd party login and my Digital ID websocket login are bound by the nonce websocket channel.

5. Final Token Generation and Authentication

- Once the 3-way handshaking process is accomplished (includes the password verification), a JWT Token is responded to Keycloak.
- The JWT Token responded by MyDOW OIDC to Keycloak will consist of full name and IC Number.
- Once Keycloak receives the JWT Token, Keycloak will take the claims (fullname and IC Number) and incorporate the info into a newly generated JWT token to be returned to the initiator client.

6. Resource Access

- The user accesses the application with the JWT token.
- The application validates the token with Keycloak.
- Upon successful validation, Keycloak informs the application, and the application provides access to the requested resources.