1.6.1 MyDigital ID SSO Keycloak Client Configuration

When configuring a Keycloak client, you usually specify the following settings:

1. **Client ID**: A unique identifier for the client within Keycloak. This is how Keycloak knows which client is making a request.
2. **Client Secret**: A secret key used for secure communication between the client and Keycloak (in the case of confidential clients).
3. **Redirect URI**: The URL to which Keycloak will redirect the user after successful authentication. This is typically the URL of the application that the user is trying to access.
4. **Protocol**: The authentication protocol used by the client. Common protocols include:
    - **OpenID Connect** (OIDC) – A modern protocol based on OAuth 2.0, commonly used for web and mobile applications.
    - **OAuth 2.0** – A framework for access delegation, widely used for authorization.
5. **Access Type**:
    - **Confidential**: Clients that can securely store credentials (e.g., server-side applications). These clients authenticate themselves to Keycloak using client secrets.
    - **Public**: Clients that cannot securely store credentials (e.g., single-page applications, mobile apps).
    - **Bearer-only**: Clients that only accept access tokens and cannot initiate authentication themselves. Common for APIs or resource servers.
6. **Roles and Scopes**: The permissions or access levels that the client can request, often used to limit or specify access to certain resources or actions.