**Authentication and Non-Authenticated Flow**

**1.Introduction**

This document outlines the authentication and non-authenticated flows for the server-side application, which uses Spring Cloud Azure Starter Directory and

Spring Boot Starter OAuth Client for authentication. The application is designed to serve an Android/iOS app, enabling secure access via OAuth 2.0 authentication

with Azure Active Directory (AAD).

**2. Authentication Flow (Authenticated Requests)**

The authentication flow ensures secure access to the application's protected resources using OAuth 2.0.

**2.1 Flow Overview**

1. **User Initiates Login**: The Android/iOS app redirects users to Azure AD login.

2. **Azure AD Authentication:** Users provide credentials (email/password, multi-factor authentication if enabled).

3. **Access Token Issuance**: Upon successful authentication, Azure AD issues an \*\*OAuth 2.0 access token\*\* to the client (Android/iOS app).

4. **Client Sends Token to Server**: The Android/iOS app includes the \*\*Bearer token\*\* in the `Authorization` header of API requests.

5. **Server Validates Token:** The Spring Boot application:

- Extracts the token from the request.

- Validates the token signature using Azure AD public keys.

- Decodes the claims (roles, permissions, expiration).

6. **Access Granted**: If the token is valid, the server processes the request and returns the requested data.

7. **Token Expiry & Refresh**: When the token expires, the Android/iOS app refreshes it using the refresh token from Azure AD.

**2.2 Sequence Diagram**

Android/iOS App -> Azure AD: User login request

Azure AD -> Android/iOS App: Access token issued

Android/iOS App -> Server: API request with Bearer token

Server -> Azure AD: Validate token

Azure AD -> Server: Token valid

Server -> Android/iOS App: Response with requested data

**3. Non-Authenticated Flow (Unauthenticated Requests)**

The non-authenticated flow applies to endpoints that do not require authentication, such as public resources or login requests.

**3.1 Flow Overview**

1. **User Initiates Request:** The Android/iOS app makes a request to a public API endpoint.

2. **No Token Required**: Since the endpoint does not require authentication, the request proceeds.

3. **Server Processes Request**: The server processes the request and returns the appropriate response.