भारतीय खाद्य निगम

FOOD CORPORATION OF INDIA

SSO Integration

with

ANNA DARPAN

Development Object Title	**:**	**AnnaDarpan_SSO_Integration_v0.1**
Development Object Title	**:**	**SSO Integration**
Version	**:**	**0.1**
Document Status	**:**	**Draft/Final Version**

Table of Contents

1 Introduction

In Anna Darpan, the Single Sign-On (SSO) process will be implemented & managed by Keycloak, an open-source identity and access management solution, designed to enable seamless and secure user authentication across different FCI internal applications.

Anna Darpan leverages LDAP as the central user identity repository, integrated with Keycloak, to provide a unified authentication layer across all integrated applications.

Anna Darpan serves as the centralized authentication platform, implemented using Keycloak, allowing users to log in once and access various FCI internal applications, such as HRMS, without needing to log in again for each one.

2 Scope:

The integration of external applications with Anna Darpan for user authentication, the technical approach leverages a **simplified authorisation code grant flow**. This process involves a series of redirects and exchanges between the external application, the user's browser, and Anna Darpan (Keycloak).

Additionally, LDAP acts as the backbone, ensuring user identity consistency and centralized management. User credentials are created once in LDAP and reused across all connected applications.

i. **Integration with Applications**:

   Client applications such as HRMS rely on Anna Darpan for centralized authentication. Users log in once through Anna Darpan SSO, and the same session is reused across all connected applications, eliminating the need for multiple logins. Each application validates user identity using tokens issued by Keycloak.

ii. **Technical Approach**:

   In this integration, each application is registered as a client in Keycloak, which enables Anna Darpan to manage authentication centrally. The Authorization Code Grant flow (OIDC) is used, where users authenticate through Anna Darpan and applications receive an authorization code that is exchanged for tokens.

The SSO integration enables Anna Darpan to serve as the central authentication hub, allowing users to log in once and access multiple applications seamlessly. This unified approach improves transparency, reduces the need for repeated logins, and ensures secure, real-time session management, thereby empowering stakeholders with a simplified and efficient user experience.

3 End-to-End Flow (Step-by-Step)

i. The user tries to log in to another FCI internal application that is integrated with Anna Darpan SSO (e.g., HRMS).

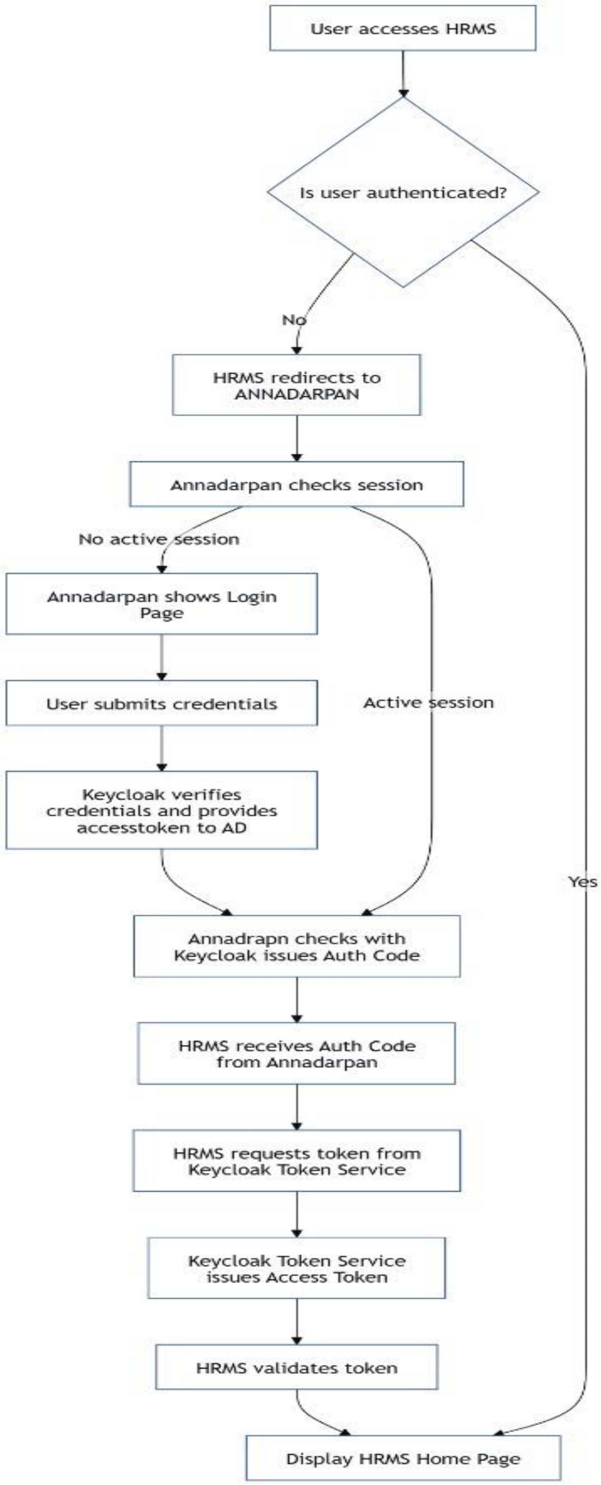
ii. The application shall redirect unauthenticated users to the Anna Darpan Single Sign-On (SSO) URL, appending the client_id & redirect_uri as a query parameter for authentication.

iii. Upon entering their credentials, the user is authenticated by Keycloak. If the verification is successful, Keycloak redirects the user back to the application, providing an authorization code. (Credentials are verified against LDAP through Keycloak).

iv. The application will exchange the authorization code and its client credentials with Keycloak, which validates the request and returns an access token along with a refresh token.

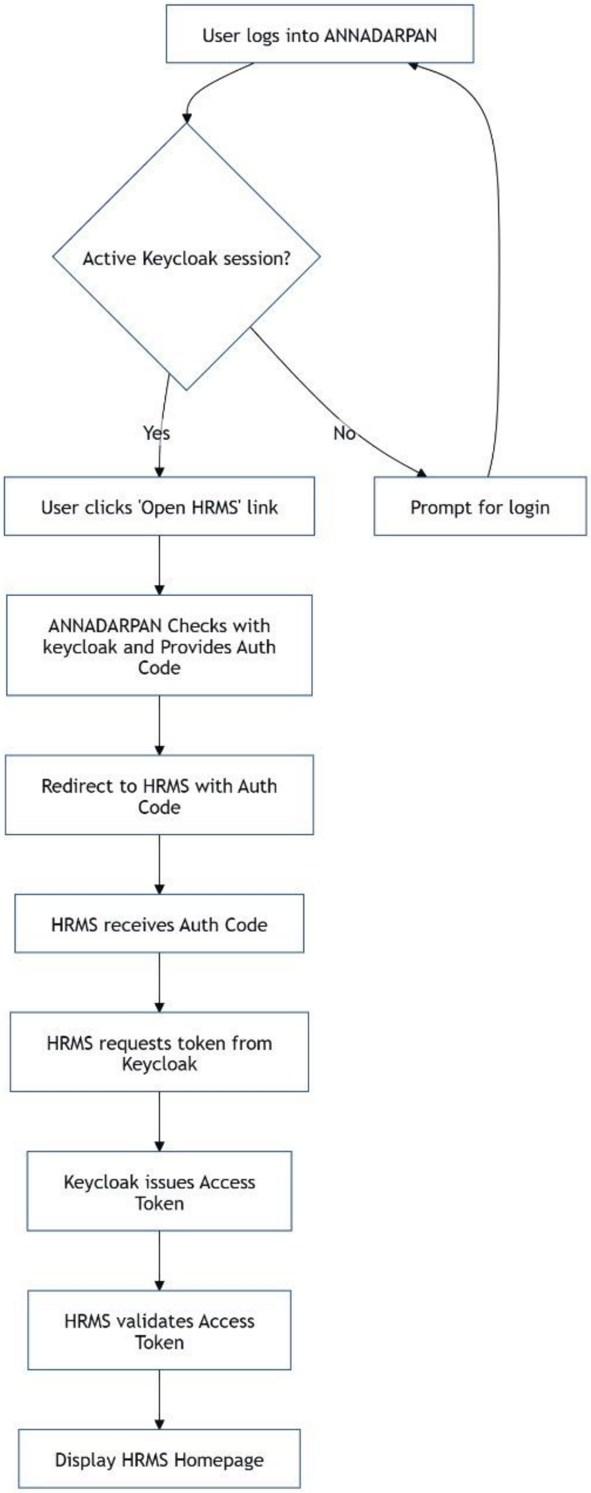
v. The application backend validates the tokens, establishes a session, and grants the user secure access without requiring further logins.

4 Flow Diagram



User accesses HRMS
Is user authenticated?
No
HRMS redirects to ANNADARPAN
Annadarpan checks session
No active session
Annadarpan shows Login Page
User submits credentials
Keycloak verifies credentials and provides accesstoken to AD
Active session
Yes
Annadrapn checks with Keycloak issues Auth Code
HRMS receives Auth Code from Annadarpan
HRMS requests token from Keycloak Token Service
Keycloak Token Service issues Access Token
HRMS validates token
Display HRMS Home Page

Figure 1: Direct access to HRMS



User logs into ANNADARPAN
Active Keycloak session?
Yes
No
User clicks 'Open HRMS' link
Prompt for login
ANNADARPAN Checks with keycloak and Provides Auth Code
Redirect to HRMS with Auth Code
HRMS receives Auth Code
HRMS requests token from Keycloak
Keycloak issues Access Token
HRMS validates Access Token
Display HRMS Homepage

Figure 2: Access HRMS from AnnaDarpan

5 External Application Setup for SSO Integration

5.1 External Application Calls Anna Darpan (Login Request / Redirection)

The external application initiates the SSO process by redirecting the user to Anna Darpan's Keycloak Authorization Endpoint. This is the first step in the OIDC Authorization Code Flow.

Note: During registration of new applications in Keycloak, users of that application are required to be synced with Anna Darpan LDAP using the common attribute, i.e., HRMS Employee ID. While authentication will be handled by Keycloak, each application needs to manage its own authorization logic based on the user roles and permissions. Applications should map user roles and permissions based on their internal role management systems.

i. The external application constructs a URL pointing to Anna Darpan's authorization endpoint with the required parameters.
ii. The user's browser is redirected to this URL. If the user is not already authenticated, Anna Darpan prompts them with a login page.

Endpoint - `http://dev.annadarpan.in/annadarpan/authorize`

Parameters

client_id → Unique identifier of the external application registered in Keycloak (e.g., APP3-CLIENT).

redirect_uri → Callback URL where Anna Darpan will redirect after authentication (e.g., http://hrms /callback).

response_type → Must be set to code for the Authorization Code Flow. (e.g.,response_type=code)

scope → Typically includes openid (required for OIDC), and may optionally include additional scopes such as profile or email.

URL :
https://dev.annadarpan.in/annadarpan/authorize?clientId=<clientId>&redirectUri=<redirectUri>

The external application will redirect the user's browser to this URL. If the user is not authenticated, Anna Darpan will display a login page. After successful authentication, Anna Darpan processes the request and redirects back.

5.2 Anna Darpan Redirects to the External Application

After successful authentication, Anna Darpan (Keycloak) redirects the user's browser back to the external application's redirect_uri with an authorization code and other parameters.

i. Anna Darpan authenticates the user (via login or an existing session).
ii. Keycloak generates an authorization code and redirects the user to the external application's callback URL.

Redirect URL: The redirect_uri provided in the initial request (e.g., https://hrms/callback).

Parameters (appended as query parameters):

iii. code: The authorization code (e.g., xyz789), a short-lived token to be exchanged for an access token.
iv. username: The authenticated user's username (e.g., johndoe), as specified in the document.
v. clientId: The external application's client ID (e.g., APP3-CLIENT).
vi. state: The same state value sent in the initial request (e.g., xyz123), if provided.

Redirect URL :

<redirectURI>?authCode=<authCode>&username=<username>&clientId=<clientId>

Anna Darpan redirects the user's browser to this URL. The external application's frontend receives these parameters and forwards them to its backend for token exchange

5.3 External Application Calls Its Keycloak API to Get Access Token

The external application's frontend receives the authorization code and forwards it to its backend, which exchanges the code for an access token by calling Keycloak's api.

i. The frontend sends the authorization code and other parameters to the backend.
ii. The backend makes a secure POST request to Keycloak's token endpoint to exchange the code for an access token.

5.3.1 Handling Authorization Code in the External Application

i. The frontend extracts the code, username, clientId, and state from the redirect URL.
ii. It sends a POST request to the external application's backend API with these parameters.

```
{
  "authCode": "<authCode>",
  "username": "<username>",
  "clientId": "<clientId>"
}
```

5.3.2 Backend to Keycloak Custom Token Endpoint

i. The frontend extracts the code, username, clientId, and state from the redirect URL.

ii. It sends a POST request to the external application's backend API with these parameters.

cURL Example:

```
curl -X POST
"https://devkeycloak.annadarpan.in/realms/AnnaDarpan/getExternalApplicationToken" \

  -H "Content-Type: application/x-www-form-urlencoded" \

  --data-urlencode "grant_type=authorization_code" \

  --data-urlencode "client_id=<client_id>" \

  --data-urlencode "client_secret=<client_secret>" \

  --data-urlencode "code=<auth_code>" \
```

Backend to Keycloak Token Endpoint:

i. The backend constructs a POST request to Keycloak's token endpoint, including the client secret for authentication.

ii. **Parameters** (in the request body, application/x-www-form-urlencoded):
grant_type: authorization_code

<authCode>
<username>
<clientId>
<clientSecret>

```
curl -X POST "https://devkeycloak.annadarpan.in/realms/AnnaDarpan/protocol/openid-
connect/token" \

  -H "Content-Type: application/x-www-form-urlencoded" \

  --data-urlencode "grant_type=authorization_code" \

  --data-urlencode "client_id=<clientId>" \

  --data-urlencode "client_secret=<clientSecret>" \

  --data-urlencode "code=<authCode>" \
  --data-urlencode "username=<username>" \

  --data-urlencode "redirect_uri=<redirectURI>"
```

6 SSO Integration flow using sample HRMS API Endpoints

To simulate the integration steps, let's consider the sample **HRMS App** (https://qa.anndarpan.in/ad-hrms/) that needs to be integrated with **Anna Darpan** (https://dev.annadarpan.in/annadarpan/) for **Single Sign-On (SSO)** using **OpenID Connect (OIDC)**.

To log users in, the HRMS backend calls the **/getHrmsAccessToken** endpoint to fetch an access token.

6.1 User Accesses HRMS Directly (Not Logged In)

A user tries to access HRMS but is not logged in. HRMS redirects them to Anna Darpan to log in, then back to HRMS with an authorization code. HRMS uses this code to get an access token.

Steps:

i. **User visits HRMS**:

   a. URL: https://qa.anndarpan.in/ad-hrms/

   b. HRMS sees that the user is not logged in and redirects to ANNADARPAN.

ii. **Redirect to ANNADARPAN for login**:

   a. URL: https://dev.annadarpan.in/annadarpan/authorize?client_id=ad-hrms&redirect_uri=https://qa.anndarpan.in/ad-hrms/callback/

   b. User logs in with username (administrator) and password.

iii. **ANNADARPAN redirects back to HRMS**:

   a. URL: https://qa.anndarpan.in/ad-hrms/callback?authCode=FKRAZTU4UDQCA4VCH2ZTQXZKIXAYUTQZCO52XJQ%3D&username=administrator&clientId=ad-hrms

iv. **HRMS gets access token**:

   a. HRMS sends the code to its backend:

```
POST /getHrmsAccessToken HTTP/1.1

Host: qa.anndarpan.in

Content-Type: application/json

{

  "authCode": "FKRAZTU4UDQCA4VCH2ZTQXZKIXAYUTQZCO52XJQ%3D",

  "username": "administrator",
  "clientId": "ad-hrms"
}
```

b. Backend gets an access token from Anna Darpan and logs the user in.

Result: User is logged into HRMS and sees the dashboard.

6.2 User Accesses HRMS from Anna Darpan (Already Logged In)

A user, already logged into Anna Darpan, clicks an icon to HRMS. Since they are authenticated, Anna Darpan sends an authorization code to HRMS without asking for login again. HRMS uses the code to get an access token.

Steps:

i. **User is on Anna Darpan dashboard**:
   a. URL: https://dev.annadarpan.in/annadarpan/dashboard

ii. **User clicks HRMS link**:
   a. Anna Darpan will redirect to its authorization endpoint:
   https://dev.annadarpan.in/annadarpan/authorize?client_id=ad-hrms&redirect_uri=https://qa.anndarpan.in/ad-hrms/callback&response_type=code&scope=openid%20profile&state=pqr789
   b. No login needed (user is already authenticated).

iii. **Anna Darpan redirects to HRMS**:
   a. URL:https://qa.anndarpan.in/ad-hrms/callback?authCode=FKRAZTU4UDQCA4VCH2ZTQXZKIXAYUTQZCO52XJQ%3D&username=administrator&clientId=ad-hrms

iv. **HRMS gets access token**:
   a. HRMS sends to backend:

```
POST /getHrmsAccessToken HTTP/1.1
Host: qa.anndarpan.in
Content-Type: application/json
{
  "authCode": "FKRAZTU4UDQCA4VCH2ZTQXZKIXAYUTQZCO52XJQ%3D",
  "username": "administrator",
  "clientId": "ad-hrms"
}
```

   b. Backend gets the access token and logs the user in.

Result: User accesses HRMS seamlessly without re-entering credentials.

7 SSO Integration Onboarding Guide

To onboard new applications under the AnnaDarpan SSO umbrella, follow these steps:

i. Register Application in Anna Darpan’s Keycloak – Define client ID, redirect URIs, and assign necessary roles.

ii. Ensure LDAP Connectivity – All user credentials must be in the central LDAP.

iii. Configure Application to Use OIDC Authorization Code Flow – Redirect to Anna Darpan for login, handle callback, exchange code for tokens.

iv. Token Validation & Session Handling – Application must validate tokens with Keycloak before granting access.

v. Testing & Go-Live – Verify login from Anna Darpan dashboard as well as direct access.

8 Open Questions

Not Applicable.