SSO Platform - Complete Flow Diagram & Presentation

*Single Sign-On Implementation with Keycloak*

# Table of Contents

1. 1. System Architecture Overview
2. 2. Authentication Flow Diagram
3. 3. SSO Token Generation Process
4. 4. Application Integration
5. 5. User Session Management
6. 6. Role-Based Access Control
7. 7. Security Implementation
8. 8. Configuration Details
9. 9. Error Handling & Troubleshooting
10. 10. Production Deployment Guide

# 1. System Architecture Overview

The SSO Platform consists of four main components:

|  |  |  |
| --- | --- | --- |
| Component | Port | Purpose |
| Keycloak Server | 8080 | Identity Provider & Authentication Server |
| CommonLogin Portal | 5000 | SSO Gateway & User Dashboard |
| Application 1 | 5101 | Business Application with SSO Integration |
| Application 2 | 5102 | Business Application with SSO Integration |

# 2. Complete Authentication Flow

## Phase 1: Initial Login Process

1. 1. User navigates to CommonLogin Portal (http://localhost:5000)
2. 2. User enters email: sandeepkumar1464@gmail.com
3. 3. CommonLogin redirects to Keycloak authorization endpoint
4. 4. Keycloak displays login form
5. 5. User enters password: Admin\_123
6. 6. Keycloak validates credentials and generates authorization code
7. 7. Keycloak redirects back to CommonLogin with authorization code
8. 8. CommonLogin exchanges code for access tokens
9. 9. CommonLogin displays user dashboard with session information

## Phase 2: SSO Token Generation

1. 1. User clicks "Launch App" from CommonLogin dashboard
2. 2. CommonLogin validates user roles against application requirements
3. 3. CommonLogin generates secure SSO token with user information
4. 4. CommonLogin redirects user to target application with SSO token
5. 5. Application validates SSO token and creates local session
6. 6. User gains automatic access without re-authentication

# 3. User Session Information Display

The CommonLogin dashboard displays comprehensive user session information:

|  |  |
| --- | --- |
| User ID | Keycloak subject identifier (sub claim) |
| Username | preferred\_username from Keycloak |
| Email | User email address |
| First Name | given\_name claim |
| Last Name | family\_name claim |
| Roles | Assigned roles from Keycloak |
| Session Started | Current timestamp |
| SSO Status | Active across all applications |

# 4. Role-Based Access Control Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| User Role | CommonLogin | App1 | App2 | Description |
| admin | ✓ | ✓ | ✓ | Full access to all applications |
| app1-user | ✓ | ✓ | ✗ | Access to App1 only |
| app2-user | ✓ | ✗ | ✓ | Access to App2 only |
| multi-user | ✓ | ✓ | ✓ | Access to App1 and App2 |

# 5. Security Implementation

## Token Security

* Token Expiry: 5-minute lifetime for SSO tokens
* Timestamp Validation: Prevents replay attacks
* Role Verification: Each application validates user roles
* Secure Transport: HTTPS in production environment

## Session Management

* HttpOnly Cookies: Prevent XSS attacks
* SameSite Policy: CSRF protection
* Secure Flag: HTTPS-only cookies in production
* Session Timeout: 8-hour sliding expiration

# 6. System Configuration

## Keycloak Configuration

Realm: sso-realm

Clients:

* common-login (http://localhost:5000)
* app1-client (http://localhost:5101)
* app2-client (http://localhost:5102)

## Test User Configuration

Primary User: sandeepkumar1464@gmail.com

Password: Admin\_123

Roles: admin, app1-user, app2-user

# 7. Logout Process Flow

1. 1. User clicks "Logout" button in CommonLogin dashboard
2. 2. CommonLogin clears all local session cookies
3. 3. CommonLogin initiates Keycloak logout with id\_token\_hint
4. 4. Keycloak terminates global SSO session
5. 5. All application sessions become invalid
6. 6. User redirected to login page
7. 7. Re-authentication required for next access

# 8. Error Handling & Troubleshooting

## Common Issues and Solutions

|  |  |
| --- | --- |
| Error | Solution |
| Client Not Found | Verify client exists in Keycloak sso-realm |
| Invalid Client Secret | Update appsettings.json with correct secret |
| Access Denied | Check user role assignments in Keycloak |
| Correlation Failed | Clear browser cookies and restart session |
| Port Binding Error | Use different ports or kill existing processes |

# 9. Production Deployment Considerations

## Security Enhancements

* Enable HTTPS for all communications
* Use strong client secrets (32+ characters)
* Implement proper JWT signing with RSA keys
* Add rate limiting and DDoS protection
* Enable comprehensive audit logging

## Performance Optimizations

* Use Redis for distributed session storage
* Implement connection pooling
* Enable token caching
* Configure load balancing
* Set up CDN for static assets

*SSO Platform Documentation  
Generated for AMAZONQ Project  
© 2025*

# 10. Login Credentials & Authentication Methods

The SSO Platform supports multiple authentication methods for different use cases:

## SSO Portal (CommonLogin) Credentials

Primary authentication method for accessing all applications via Single Sign-On:

|  |  |
| --- | --- |
| URL | http://localhost:5000 |
| Username | sandeepkumar1464@gmail.com |
| Password | Admin\_123 |

## Application 1 Direct Login

Direct authentication to App1 without SSO (fallback method):

|  |  |
| --- | --- |
| URL | http://localhost:5101/Home/AuthenticateApp1 |
| Username | app1user |
| Password | App1Pass123 |

## Application 2 Direct Login

Direct authentication to App2 without SSO (fallback method):

|  |  |
| --- | --- |
| URL | http://localhost:5102/Home/AuthenticateApp2 |
| Username | app2user |
| Password | App2Pass123 |

## Keycloak Admin Console

Administrative access to Keycloak server:

|  |  |
| --- | --- |
| URL | http://localhost:8080 |
| Username | admin |
| Password | Admin\_123 |

## Keycloak Client Secrets

Client secrets for application authentication with Keycloak:

|  |  |  |
| --- | --- | --- |
| Application | Client ID | Client Secret |
| CommonLogin | common-login | b4tvl5GQRT9oiVOSpWnFf2uQHK07jJhF |
| Application 1 | app1-client | 7xsGjfrgp4FjkKV0JcewMgECEKSXYft4 |
| Application 2 | app2-client | J5nyrCgOZQjqcWRSHIrlLDEHVXxZ3wSU |

## Authentication Flow Options

* SSO Flow: Login via CommonLogin → Automatic access to App1 and App2
* Direct App1: Login directly to App1 using app1user credentials
* Direct App2: Login directly to App2 using app2user credentials
* Mixed Flow: Use SSO for some apps, direct login for others

## Security Notes

* SSO credentials provide access to all authorized applications
* Direct login credentials are application-specific
* Client secrets should be kept secure in production
* All passwords should be changed in production environment
* Enable HTTPS for all communications in production