SSO (Single-Sign-On) in JISF (Part - 2)

Identity Provider / Identity Server:

An identity provider (abbreviated as IDP) is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying on software systems within a distributed network.

Identity providers offer user authentication as a service. Relying party software systems outsource the user authentication step to a trusted Identity Provider.

In generic terms, an Identity Provider is a trusted provider that lets users use single sign-on (SSO) to access other software systems.

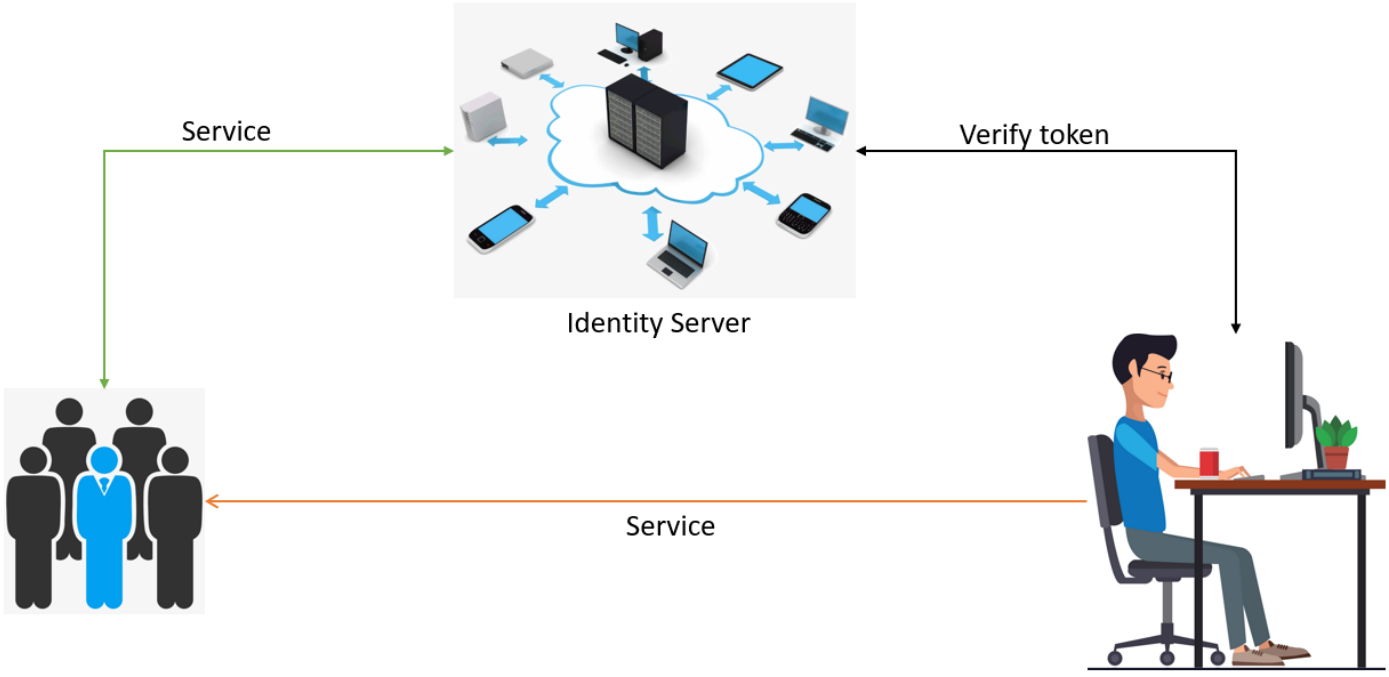

Figure : JISF Service widget in SSO

Use Cases --> 1

1. User will put http://jisf.gov.bd on browser, it will redirect to Identity Provider (the central

authentication system of users).
2. User will put username and
3. After successful authentication, the user will be redirected to the landing page of JISF
4. Here user will see a configurable dashboard with all permitted software
5. By clicking on the software systems icon, the user will be able to go landing page of the corresponding software

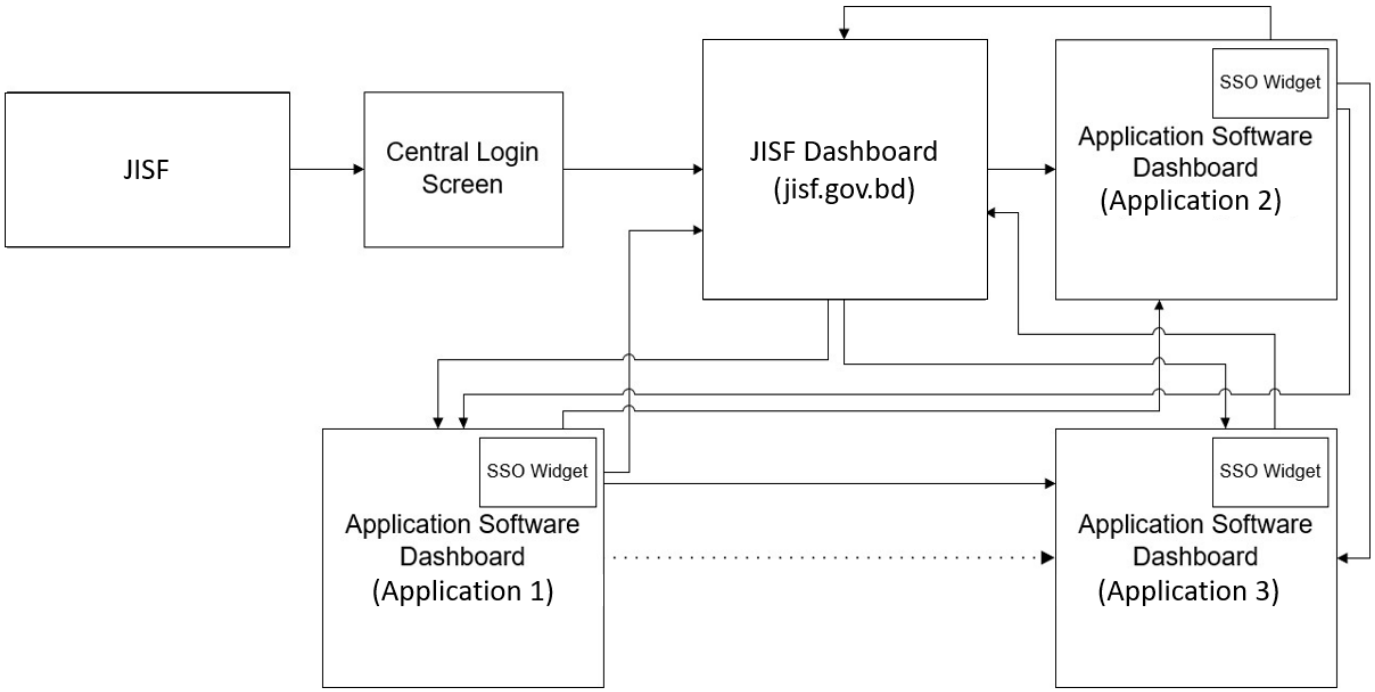

Figure: Use case 1

Use Cases --> 2

1. User will put URL of application software (as an example, http://App1.gov.bd) in the browser, it will redirect to Identity Provider (central authentication system of users).
2. The user will put a username and password.
3. After successfully authentication, the user will redirect to the landing page of the corresponding software (as an example, Dashboard of App1).
4. Here user will see Widget (an independent web element with a set of features) with all permitted software By clicking on the software systems icon in Widget, the user will be able to go landing/dashboard page of the corresponding software system.

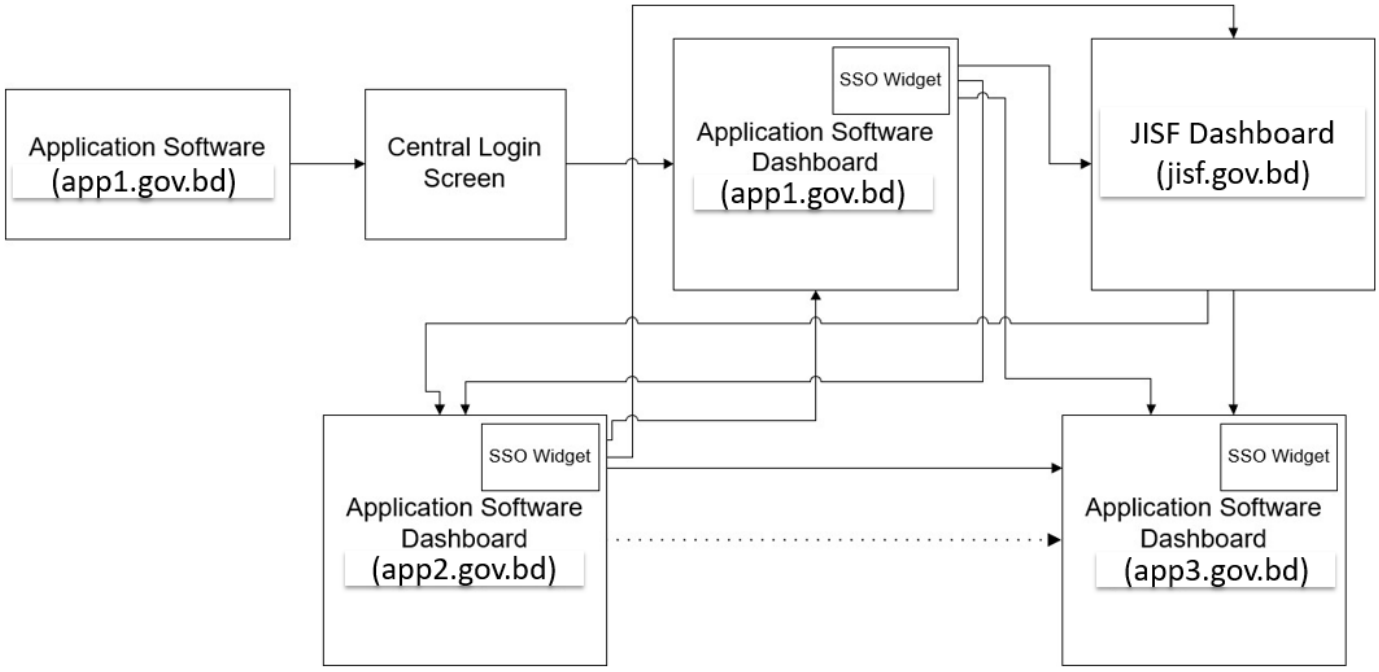

Figure: User case 2

Use Cases --> 3

1. User will put the URL of software (as an example, http://app1.gov.bd) in the browser which is the landing page of the software (here, the landing page of Application1 is http://app1.gov.bd).
2. After clicking on the login link, it will redirect to Identity Provider (central authentication system of users).
3. User will put username and password
4. After successfully authentication, the user will redirect to the landing page of the corresponding software (as an example, Dashboard of app1).
5. Here users will see Widget with all permitted software systems. By clicking on the software systems icon in Widget, the user will be able to go landing/dashboard page of the corresponding software.

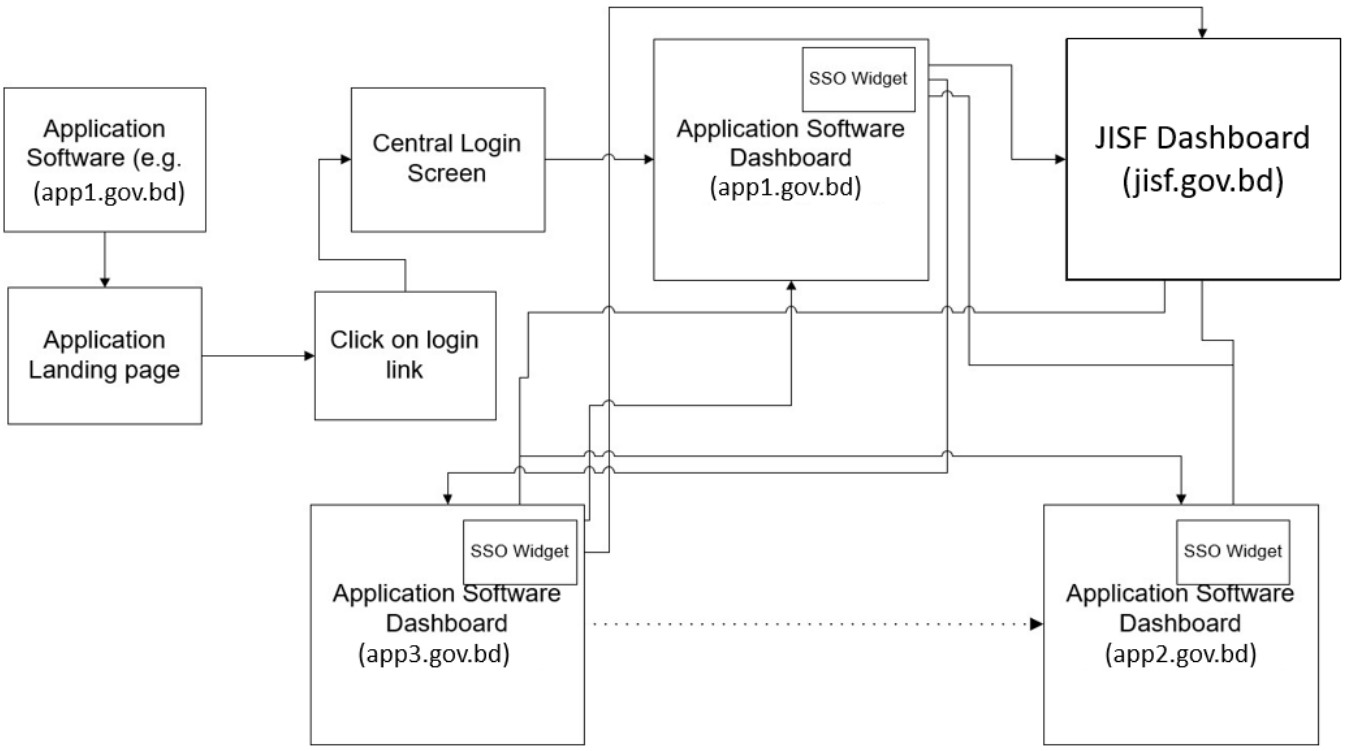

Figure : Use case 3

Steps of Single-Sign-On

The steps of SSO are explained as follows:

1. User needs to browse the URL of any software As an example for app1 e-Service: http://app1.gov.bd
2. The system will redirect the user to the Identity Provider Server (therefore, Identity Server): http://idp.jisf.gov.bd
3. The user will provide a username and password (therefore credentials).
4. Identity Server will authenticate the
5. Identity Server will send Token (JSON Web Token) to the software system with authentication
6. The software system will redirect the user to the landing page (therefore, Dashboard) after the authentication process is

The sequential flow of SSO is as follows:

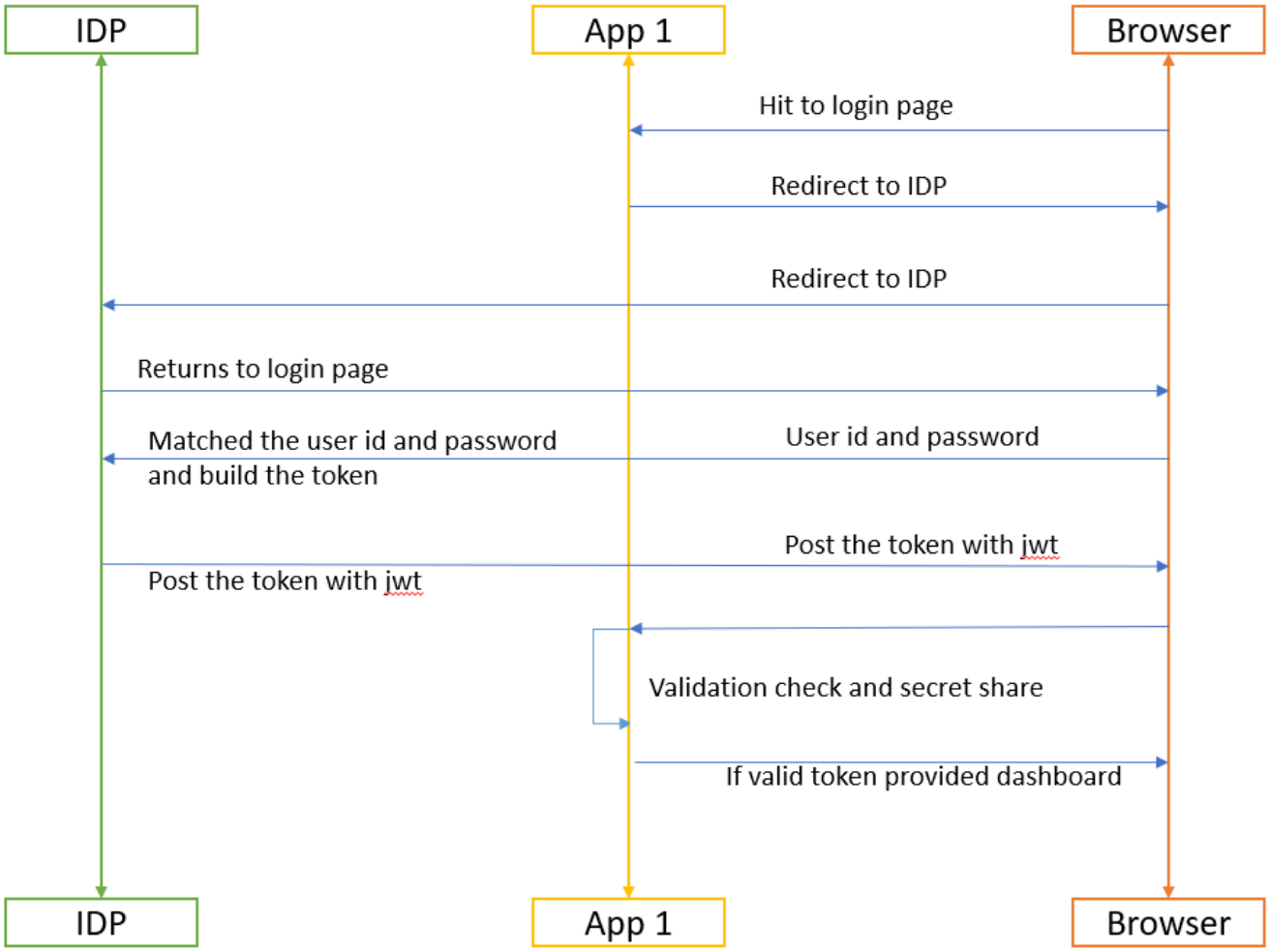

Figure : SSO Sequence Diagram

The Applicaiton to applicaiton login sequencetial flow of SSO is as follow:

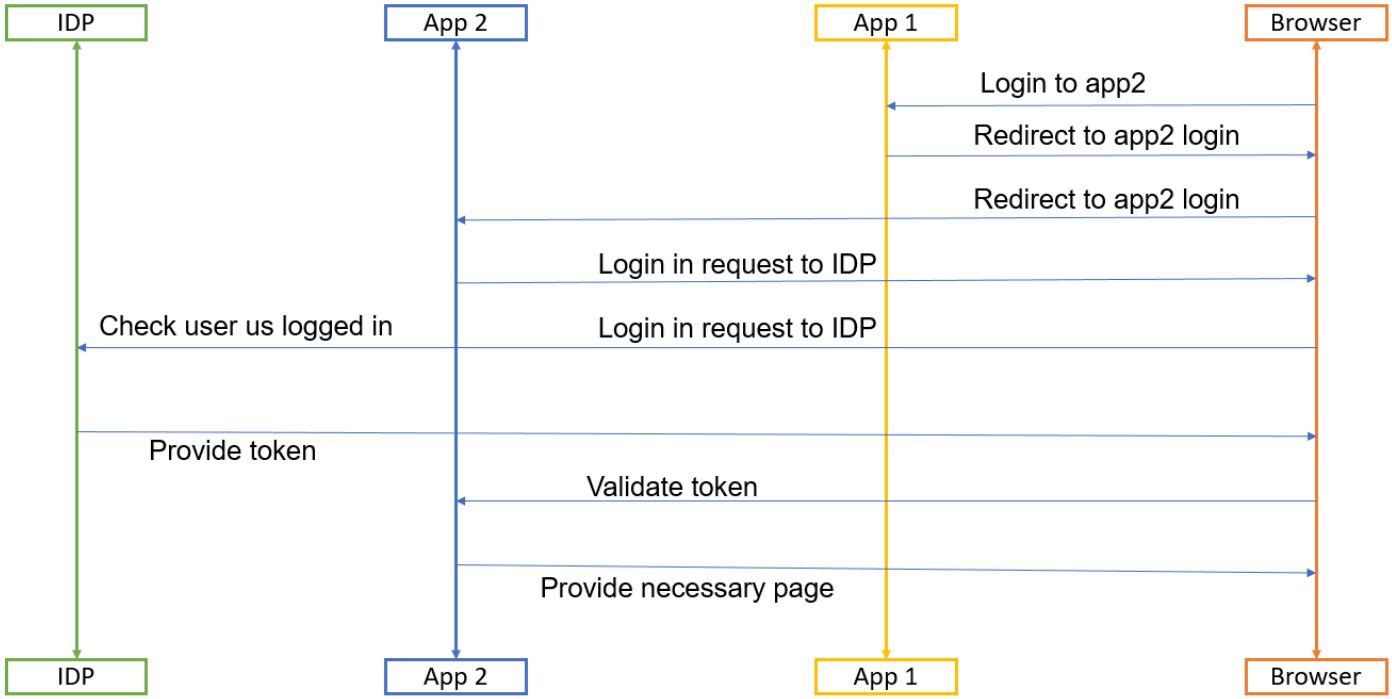

Figure: App to App login sequence

How to get Onboarded to avail the SSO Service of JISF

Any organization that is intending to get connected to the JISF ecosystem are required to follow the steps below:

FIgure: SSO flow

Revision #6
Created 28 September 2021 21:13:14 by Niton
Updated 5 October 2021 17:14:16 by Niton