Chapter 5 - SSO (Single-Sign-On) service

- SSO (Single-Sign-On) in JISF (Part - 1)
- SSO (Single-Sign-On) in JISF (Part - 2)

SSO (Single-Sign-On) in JISF (Part - 1)

What is Single-Sign-On (SSO)?

Single-Sign-On (SSO) is a mechanism to control access of users to a system, where a user logs in with a single username and password to gain access to a digital system(s). The major benefit of this mechanism is, the user does not need to remember or use multiple usernames and passwords.

When multiple digital services contain similar or correlated features, there comes a requirement of a Single-Sign-On facility, because otherwise for accessing each service there would require different usernames and passwords (therefore, credentials) which will become unmanageable. Moreover, accessing one service after another to do a task will become much troublesome. To solve this problem, Single-Sign-On is a wonderful mechanism.

In this mechanism of Single-Sign-On, there remains an Identity Provider which contains a lookup facility that provides a mapping between network resources (in our case, different digital services), and this Identity Provider facilitates the same credential, and same access token to enter multiple services.

If even different digital services are of different types of authentication and login processes, the Single-Sign-On mechanism makes it very simple by facilitating a single-way login mechanism.

FIgure : SSO Integraiton

Why SSO is used in JISF?

JISF is such a platform with which all government judiciary digital services (known as, e-Judiciary) will be connected. As one governmente-Judiciary will have relation to another e-Judiciary, therefore a common access mechanism should be there while a Judge or Court Stuff accesses an e-Judiciary to facilitate citizen.

As an example scenario, if a Court staff wants to process a pending case file to any citizen, he will require to access the e-service service portal for the Court office. Here, to verify a case file withthe applicant's NID the Court staff may require to access the e-service portal of ElectionCommission as well. In such a situation, if the staff of Court would get two different accesscredentials for wor e-service portals and if the officer would require to access them separately,then his task would become complex and time lengthy, For this reason, the JISF SSO Mechanismhas made the life of Court staff easy by making a single login credentials and single authenticationmechanism.

Benefits of using Single-Sign-On (SSO)?

There are so many benefits of SSO. The major benefits of SSO are:

- As SSO takes the responsibility of user authentication centrally, the services (that are going to use SSO) doesn’t require to think about implementing authentication
- The authentication and login management becomes centralized
- The user doesn’t require to remember multiple usernames and passwords for multiple services.
- The time to do activities on multiple services gets reduced as access to the services become so quicker using the same
- IT support expense reduces as calls regarding password change and recovery
- As it facilitates one URL, one Profile, one ID, one Password, therefore it removes the redundancy for the

For enterprise ecosystems where multiple digital services are centralized, and users of the ecosystem need to access each digital service quickly with a single credential, then SSO has no alternative.

How does SSO work?

There are different protocols (standard and of transmission) of Single-Sign-On. Among these, for JISF, the OpenID Connect (OIDC) is used on the top of OAuth2.0 Authorization Framework.

OpenID Connect (OIDC) is an authentication protocol that uses JSON Web Token (JWT), a type of token to validate and approve a login attempt.

And, **OAuth 2.0 Authorization Framework** uses this OIDC protocol and facilitates both authentication and authorization facility.

Here, **Authentication** is the process of verifying the identity of a user by obtaining some sort of credentials for example his username-password combination and using those credentials to verify the user’s identity.

While **Authorization** is the process of allowing an authenticated user to access his resources by checking whether the user has access rights to the system. You can control access rights by granting or denying specific permissions to an authenticated user. So, if the authentication was successful, the authorization process starts. The authentication process always proceeds to the

Authorization process.

When a user is authenticated using SSO to access any specific digital service, the “Identity Provider” of SSO issues an Access Token therefore an “Identity” to that the digital service can approve the user to access it.

Therefore, an **Identity Provider** offers user authentication as a service. An identity provider is a trusted provider that lets users use Single-Sign-On (SSO) to access software systems.

While implementing the SSO mechanism, Solution Architects use a type of Widget which helps users to switch among software systems that are connected with the SSO.

Widget, in general terms, is an independent web element that can be placed commonly on the user interface of any website or software to facilitate a set of features.

All the above-explained elements are part of the deployment of the SSO mechanism using OAuth

2.0. OAuth is not only a simple way to publish and interact with protected resource data, but it is also a safer and more secure way for people to give you access to their resource data. Organizations that have started to use OpenID Connect with OAuth 2.0 includes Amazon, Google, Facebook, IBM, Microsoft, Salesforce, VMWare etc.

Elements of SSO in JISF

OAuth 2.0 with OpenID Connect :-

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service. It works by delegating user authentication to the service that hosts the user account and authorizing third-party applications to access the user account. OAuth 2 provides authorization flows for web and desktop applications, and mobile devices.

Roles of OAuth: OAuth defines four **roles**:

- Resource Owner
- Client
- Resource Server
- Authorization Server

We will detail each role in the following subsections.

Resource Owner: *User*

The resource owner is the *user* who authorizes an *application* to access their account. The application's access to the user's account is limited to the "scope" of the authorization granted (as an example, read or write access).

Resource / Authorization Server: *API*

The resource server hosts the protected user accounts, and the authorization server verifies the identity of the *user* then issues access tokens to the *application*.

From an application developer's point of view, a service's API fulfills both the resource and authorization server roles. We will refer to both of these roles combined, as

the *Service* or *API* role.

Client: Application

The client is the *application* that wants to access the *user*'s account. Before it may do so, it must be authorized by the user, and the authorization must be validated by the API.

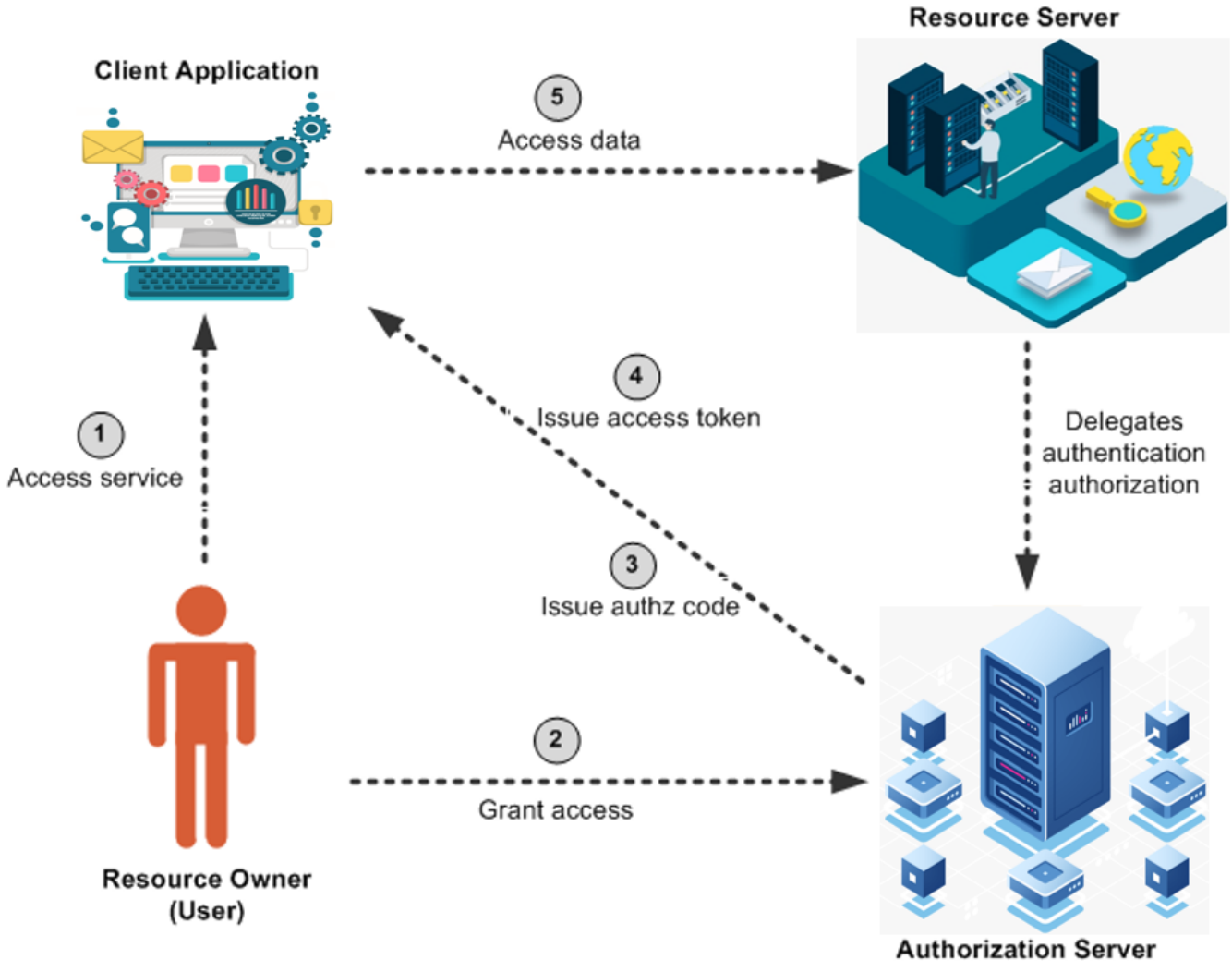

FIgure: Client Applicaiton

Single-Sign-On Widget

In general terms, a Widget is an independent web element that can be placed commonly on the

user interface of any website or software to facilitate a set of features

SSO Widget is placed in the header of all e-Services (Government Digital Services) that are connected to the JISF SSO. Using this widget users will be able to switch from one application to another. For example, users will be able to switch from Application 1 to Application 2 using this widget.

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.

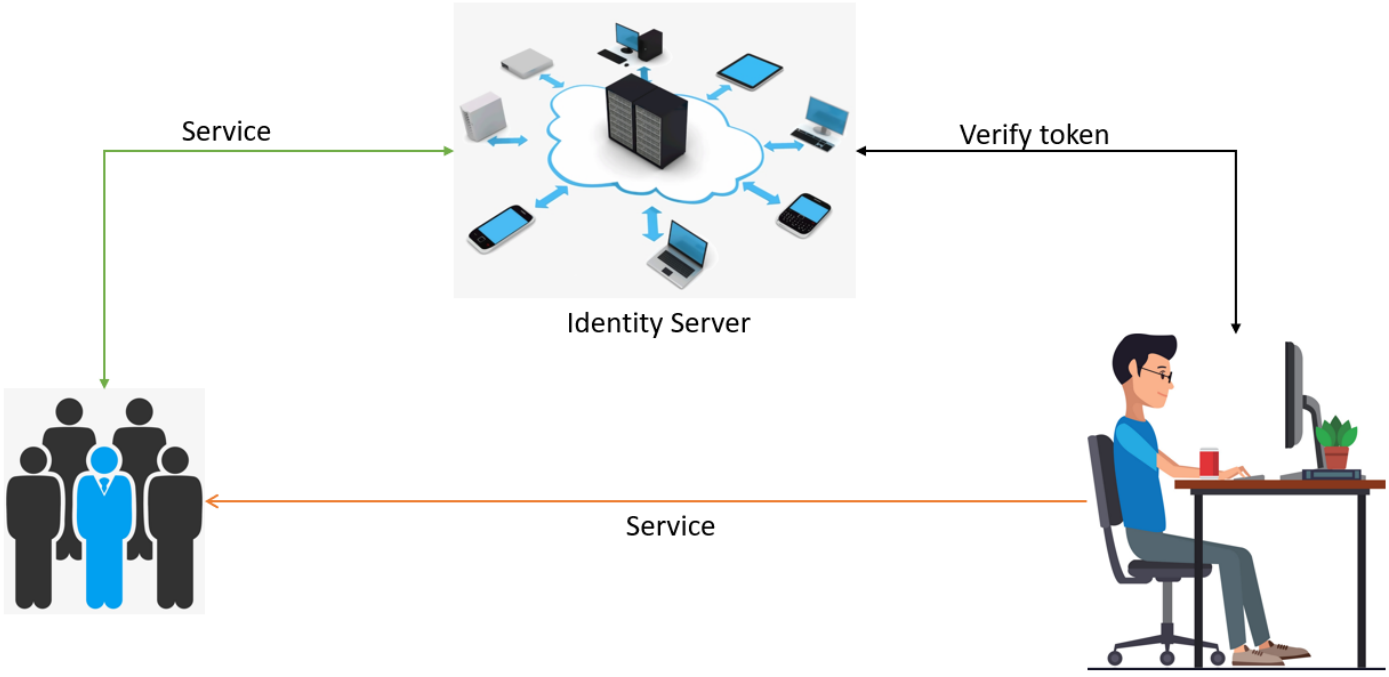

Figure : JISF Service widget in SSO

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

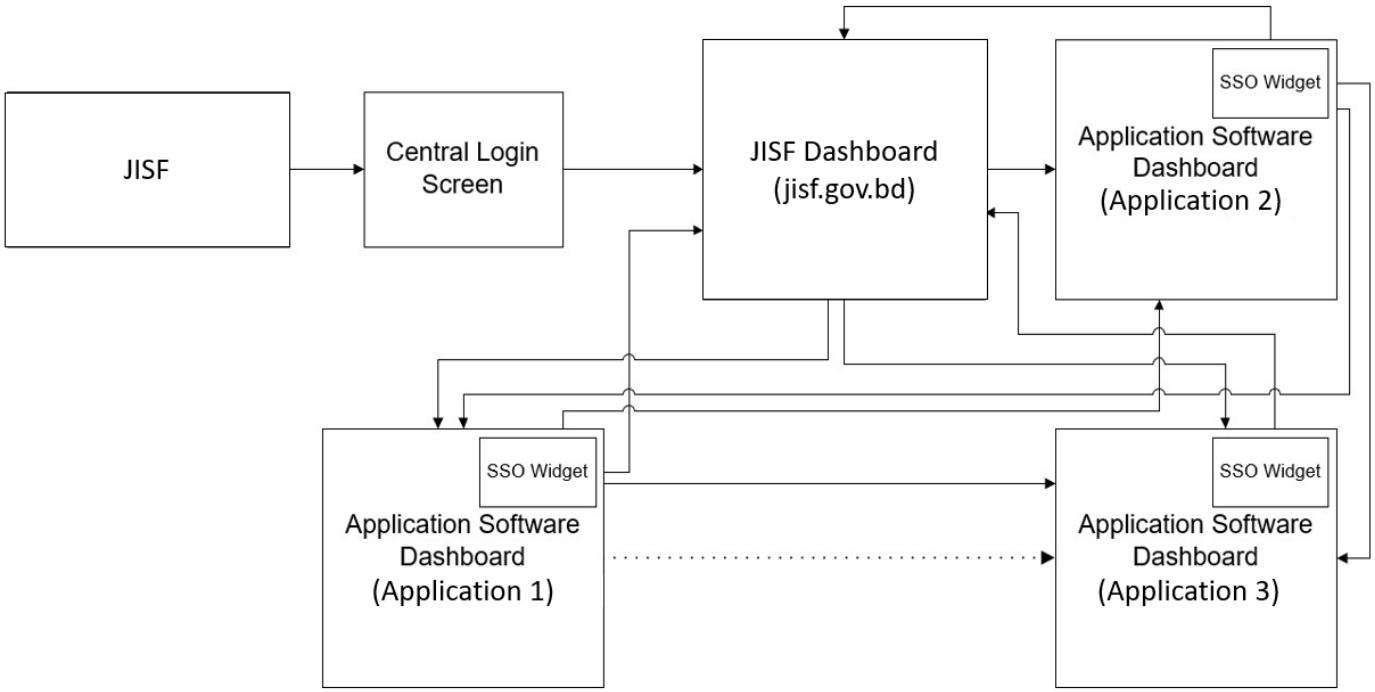

Figure: Use case 1

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.

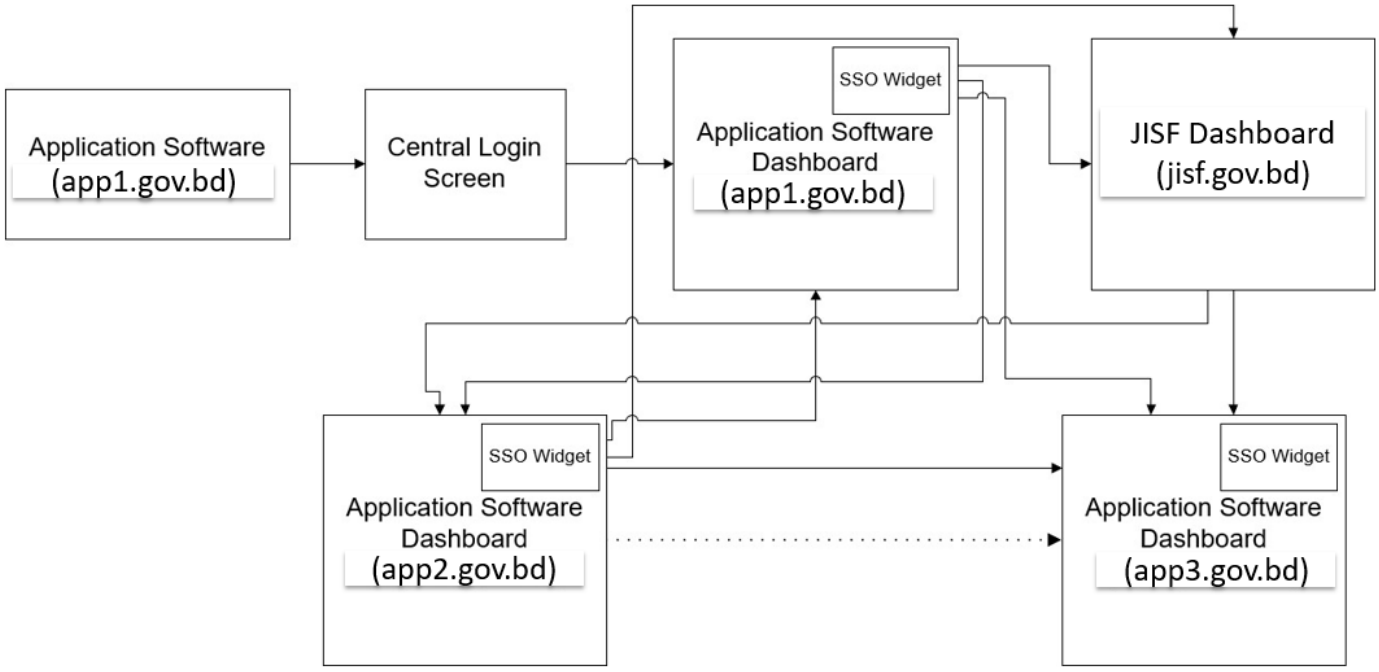

Figure: User case 2

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.

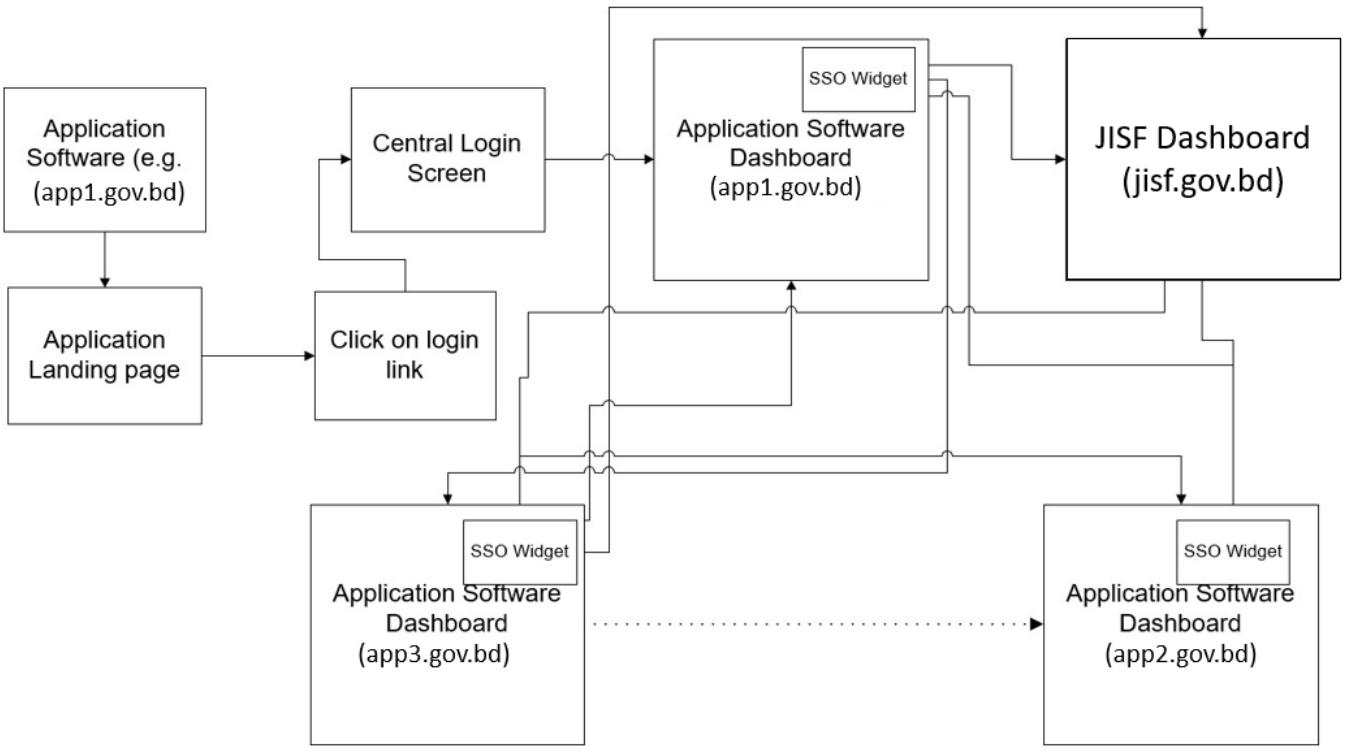

Figure : Use case 3

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:

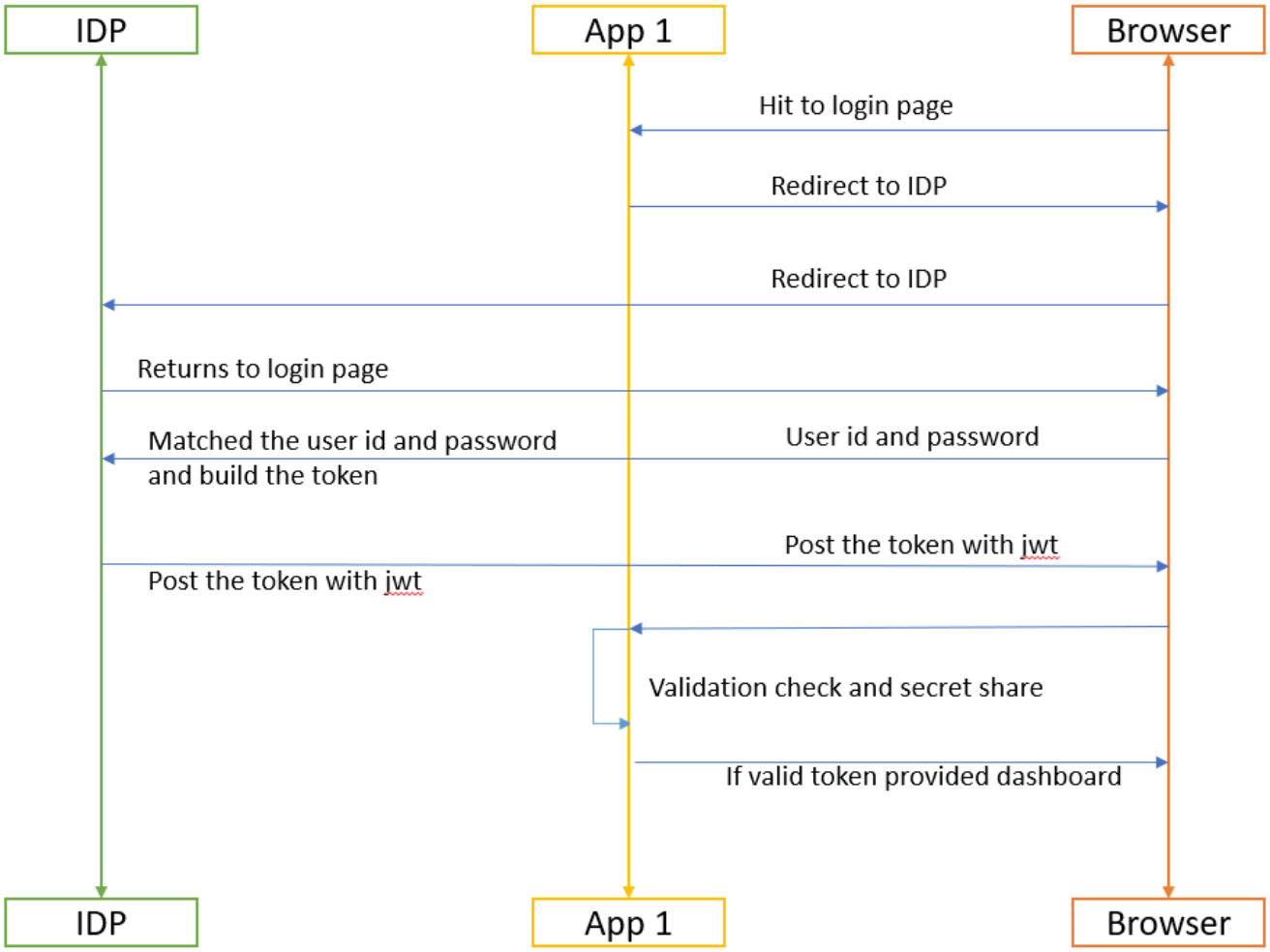

Figure : SSO Sequence Diagram

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

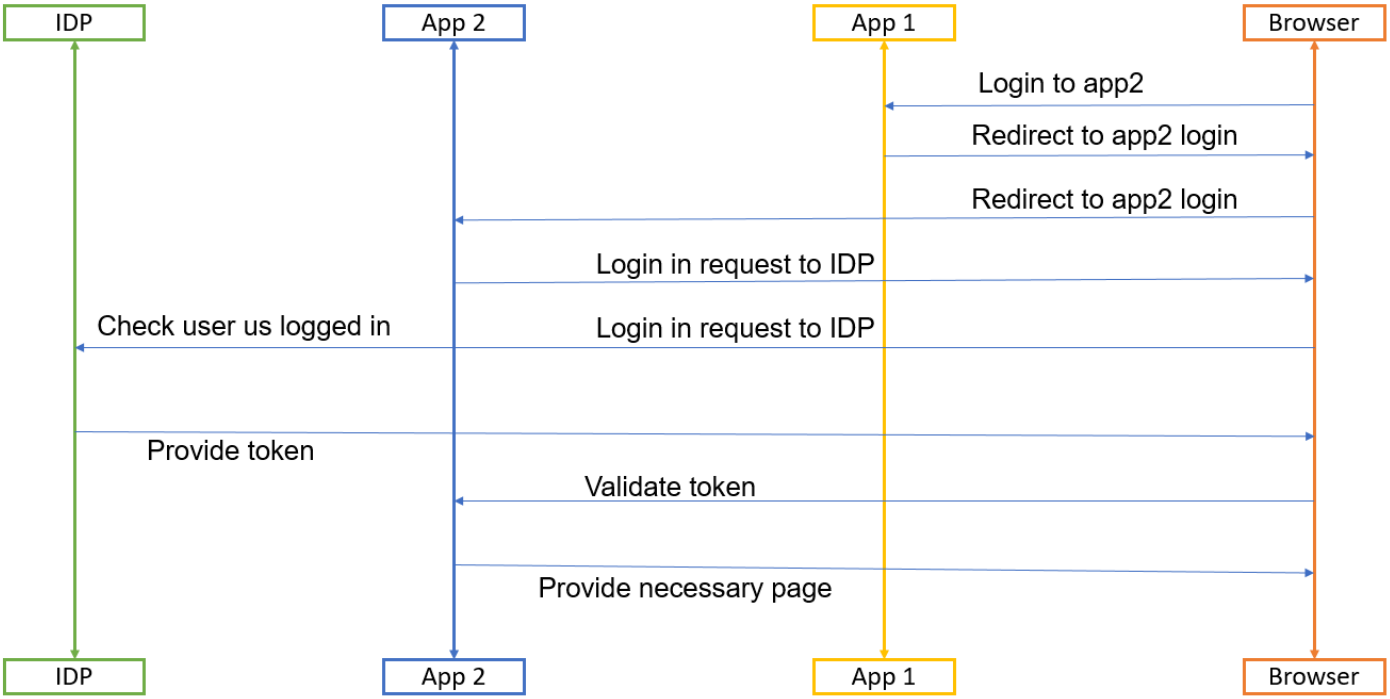

Figure: App to App login sequence

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