सत्यमेव जयते

JanParichay Partners

User Manual

Submitted by

National Informatics Centre
4th Floor, Block III, Delhi IT Park, Shastri Park
New Delhi – 110053
Website: www.nic.in

JanParichay Partners

JanParichay-MeriPehchaan helps expanding the reach of application by providing seamless and secure user authentication and authorization service. Application Owners can become JanParichay Partners by performing a straightforward procedure.

Prerequisites:

- User must have JanParichay-MeriPehchaan account with linked email id (Refer to user manual -- for new account creation on JanParichay)
- Refer Annexure A to update email id in JanParichay account

Following are the steps to become a JanParichay Partner by integrating the application with JanParichay:

1. Sign UP Process

Step 1: Go to Jan Parichay Partner Portal using the URL: https://jppartners.meripehchaan.gov.in/

Step 2: Click on the "**Login**" button to proceed. (Refer fig. 1)

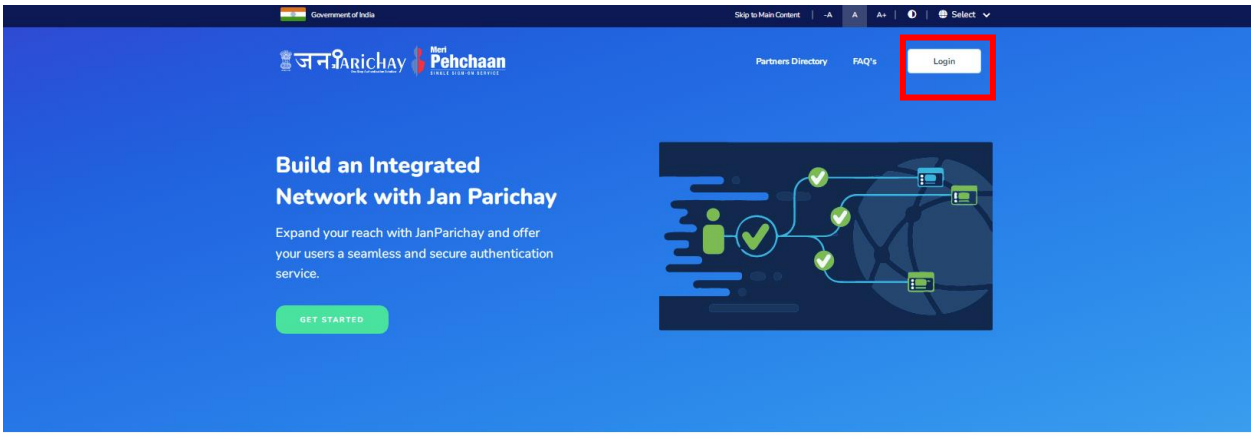


Fig 1

Step 3: Enter your login credentials, mark the check box to provide your consent, and click the "Sign In" button to proceed.

(Note: User must have logged in with JanParichay before signing up as an organization.)

Now, an organization Signup form will appear on your screen. (Refer fig 2)

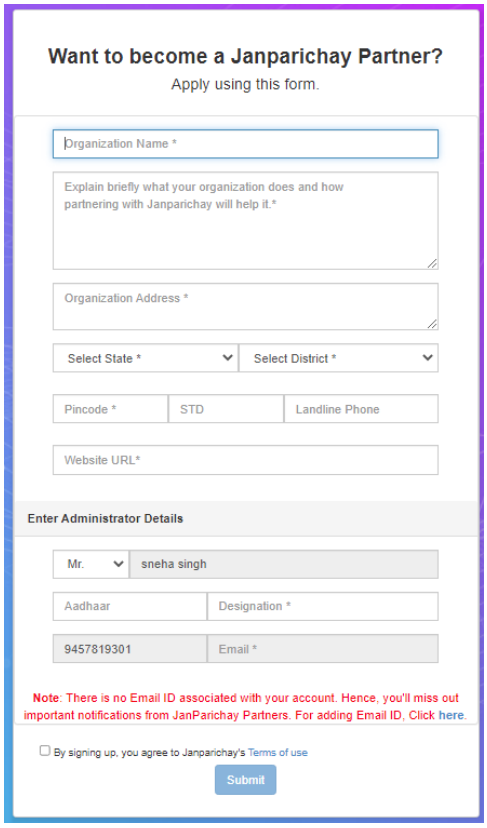


Fig. 2

Step 3: Fill the basic details related to your organization and its administrator.

(Note: If the link "There is no Email ID associated with your account. Hence, you'll miss out important notifications from JanParichay Partners. For adding Email ID, Click here." Then, use the steps as follows:

- Click on the "here" link to proceed. (Refer fig. 3)

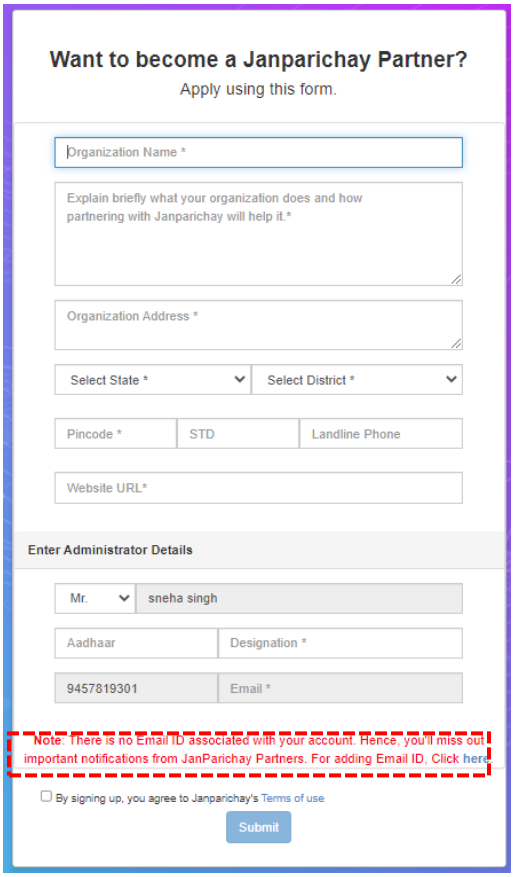


Fig. 3

- The link will redirect you to your JanParichay profile page.
- Now, follow the further steps provided in Annexure A.
  (A text “you have updated your profile details successfully” will appear on your screen.)
- Now, you have to relogin https://meripehchaan.gov.in and fill that signup form to proceed further.) (Refer fig. 4)

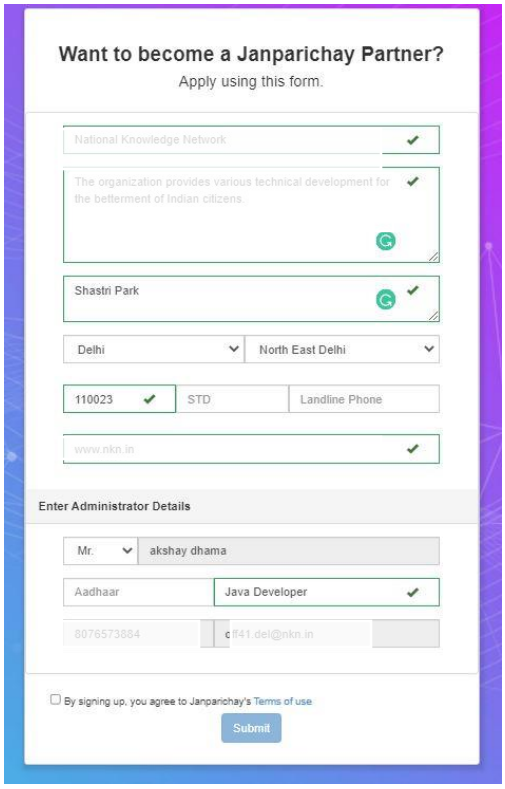


Fig. 4

Step 4: Click on the “terms of use” check box after reading JanParichay terms of use and then click on the submit button to proceed. (Refer fig. 5)

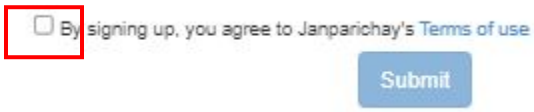


Fig. 5

(A pop-up text “Signup form submitted successfully” will appear on your screen.) (Refer fig. 6)

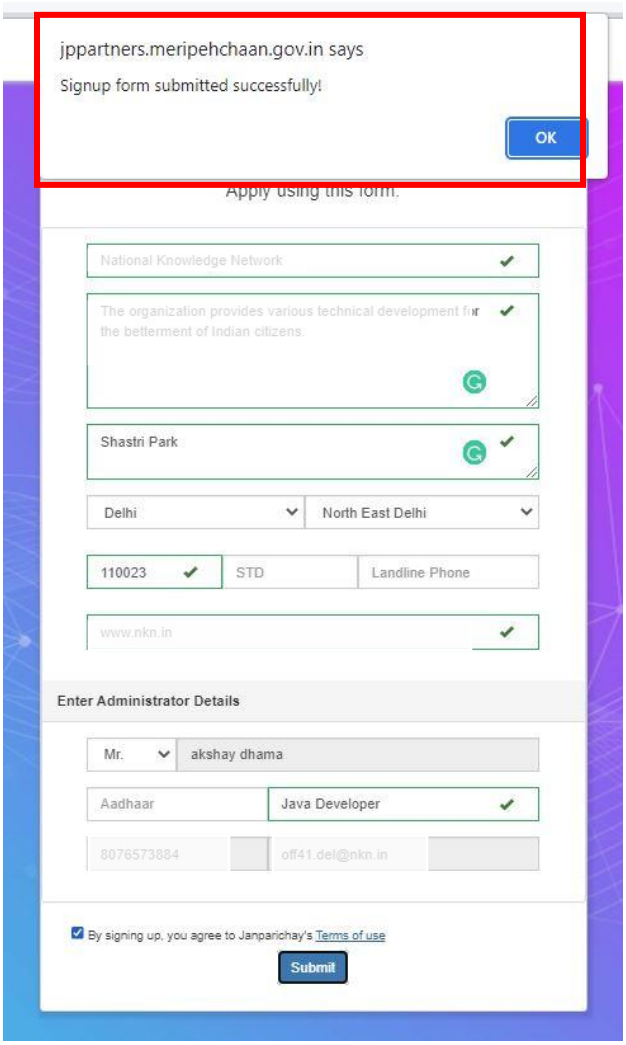


Fig. 6

Step 5: Tap on the “OK” button that will redirect you to a page showing text

“Hi Mr. YOUR NAME, Thank you for registering to become a JanParichay Partner. We have received your application and will contact you for more details. You will hear from us within the next 48 hours through a confirmation mail on your email address. After receiving that please login again to continue with the further processing of your application.”

Now wait until you receive the account activation confirmation on your email id. (Refer fig. 7)

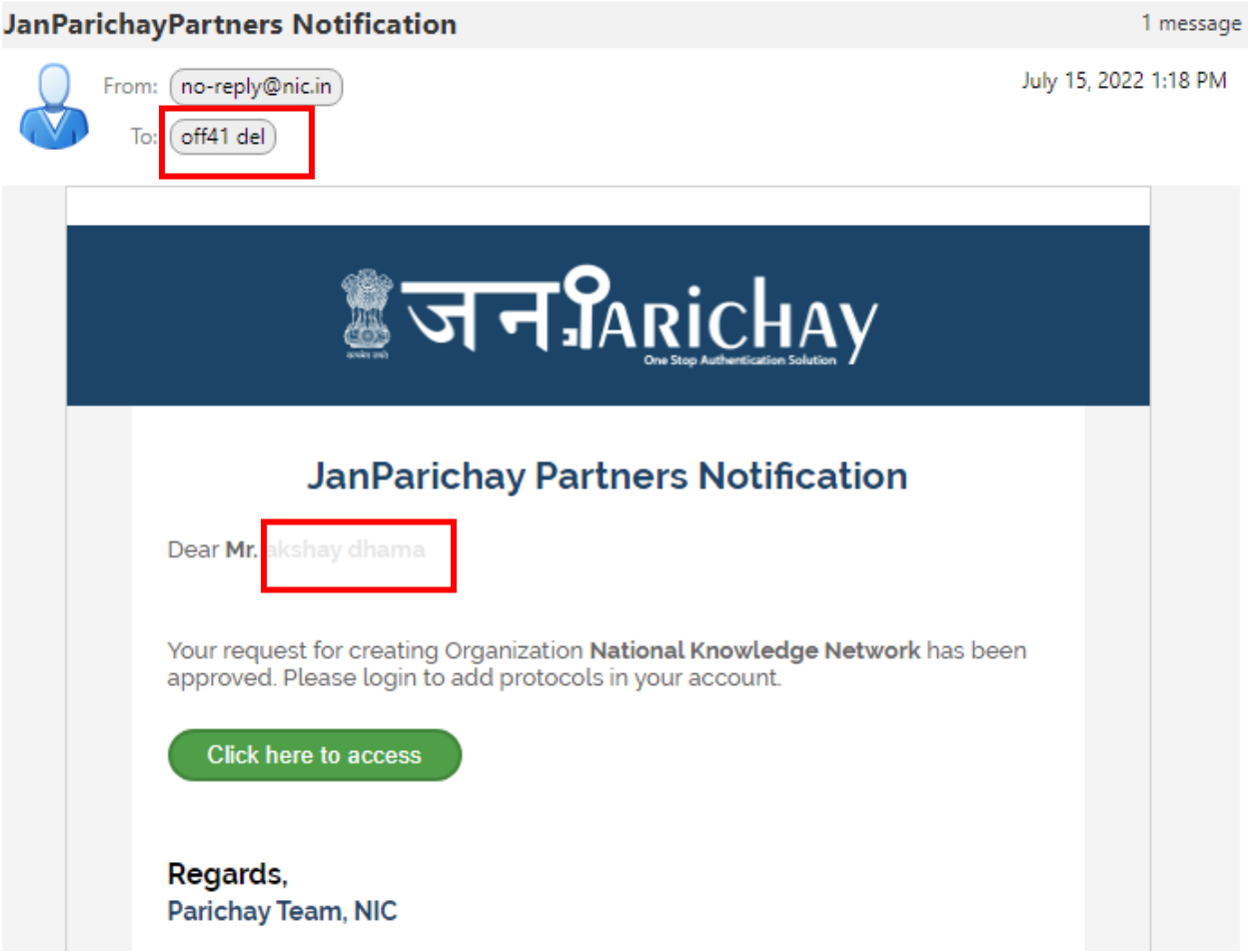


Fig. 7

After receiving the confirmation mail.

>>>>>>

2. Service Management

2.1 Service Registration for RestAPI

2.2 Service Registration for OAuth2

2.3 Service Registration for SAML2

Demo Flow for RestAPI

Step 1: Click on the “Registration” button available in the right-column menu. (Refer fig. 8)



Fig 8

Step 2: Choose any one of the three integration methods as per your requirements. (Refer fig. 9)

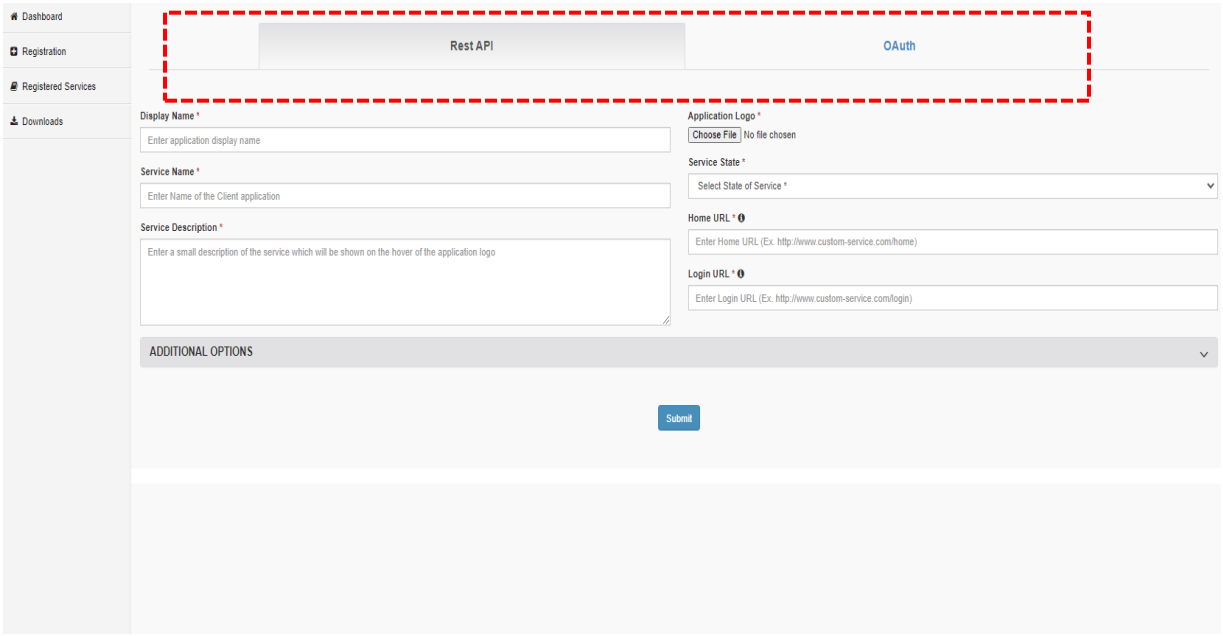


Fig 9

Step 3: Fill the required fields of registration form and if you want some advanced functionalities or changes then please choose from the **"additional"** fields. (Refer fig.10)

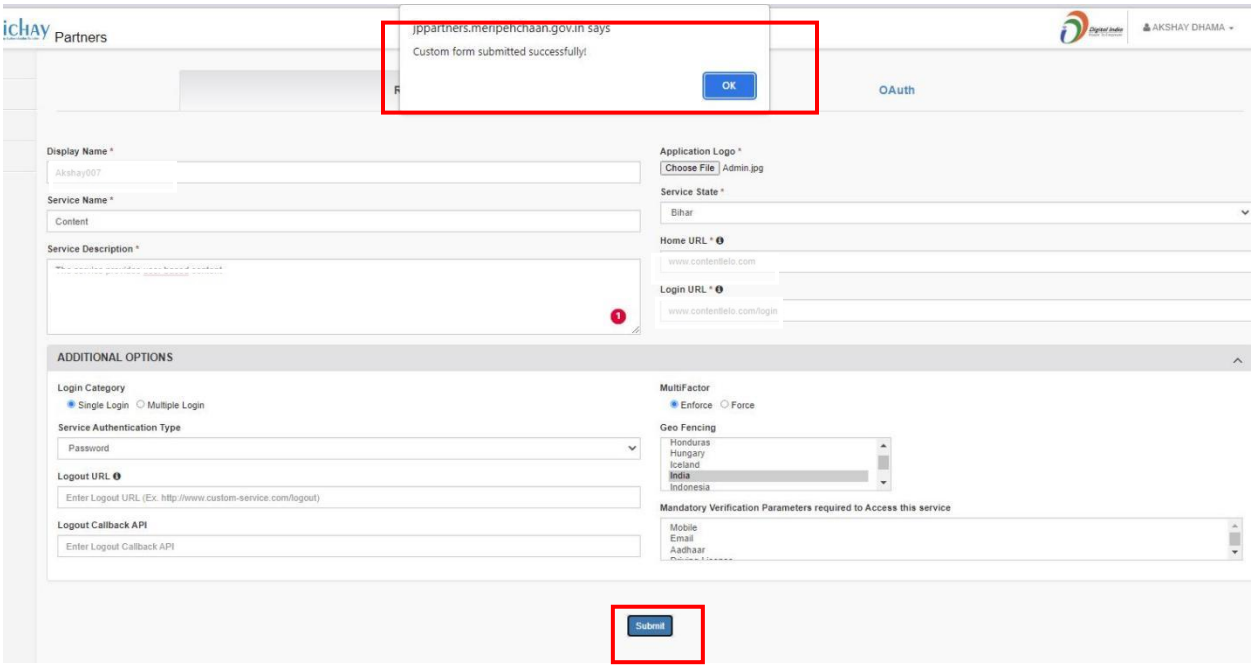


Fig 10

Step 4: Click on the “submit” button to proceed.

A pop-up text “custom form submitted successfully” will appear on your screen.

Note: Details required to be filled in the custom form may be different while you opt the SSO type. For example, the OAuth requires **Mobile Package details. (Refer Fig 11)**

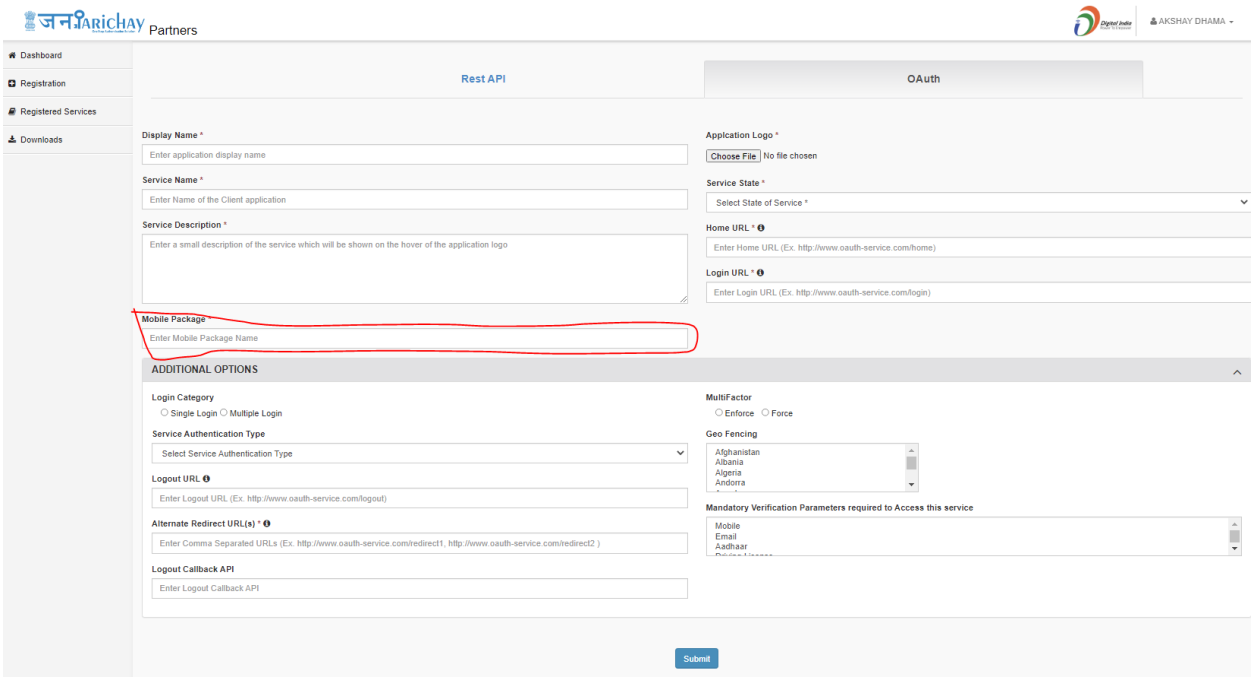


Fig 11

Registered Services

Step 1: Click on the “**Registered Services”** button. There, you can check the details related to your requests and application registered with JanParichay such as SSO Type, environment, configuration, etc. (Refer fig.12)



Fig 12

Step 2: For migrating the service content from Staging to Production, click on the button below "Environment tab" to provide your confirmation. Then, type COFIRM in the required field and click on "Confirm" to proceed. (Fig. 13)

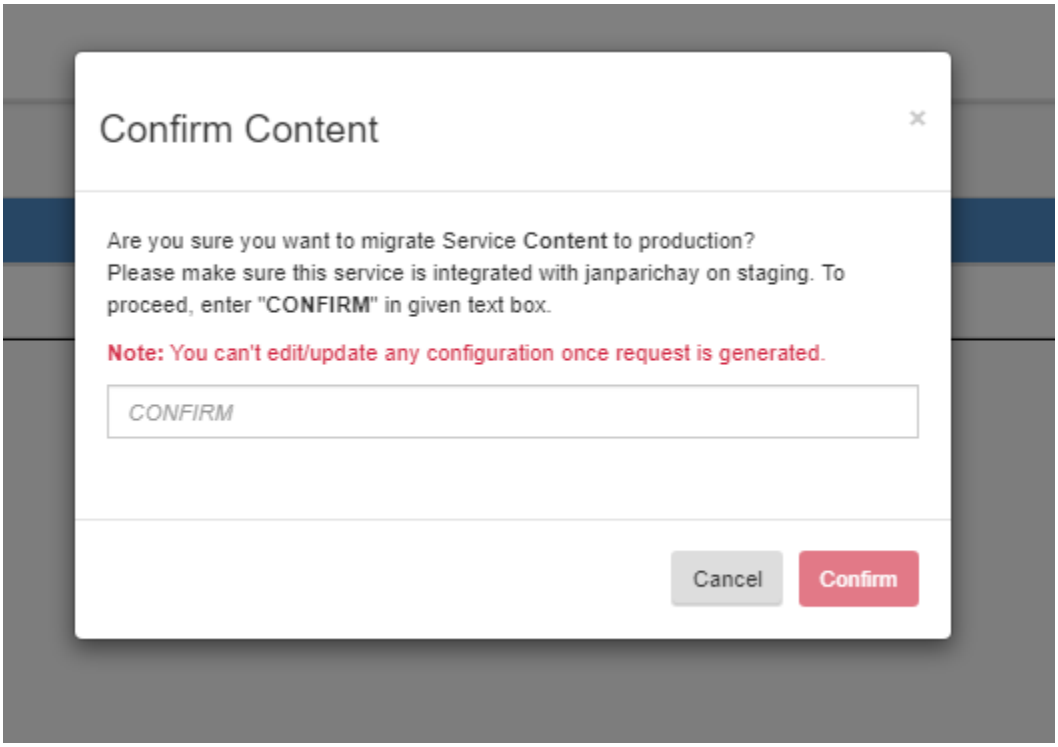
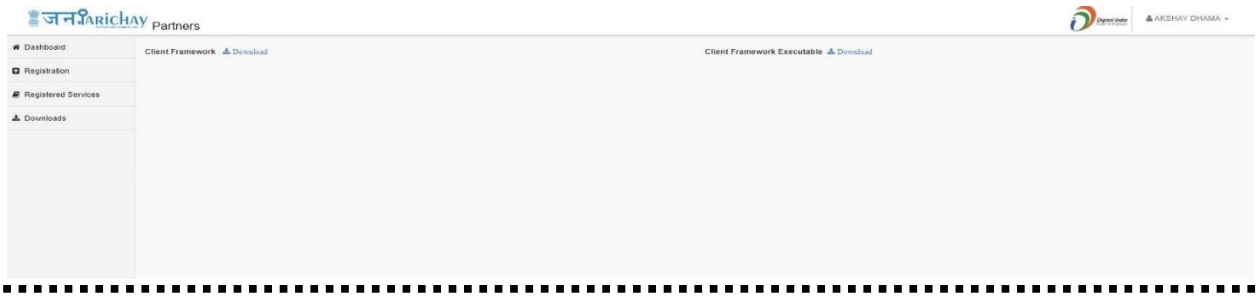


Fig 13

Downloads

Click on the "downloads" button to download the client framework or client framework executable files.



Annexure A

- Login to http://janaparichay.meripehchaan.gov.in
- Click on your name link provided on the top-right screen to choose the “Settings” option. (refer fig.1)

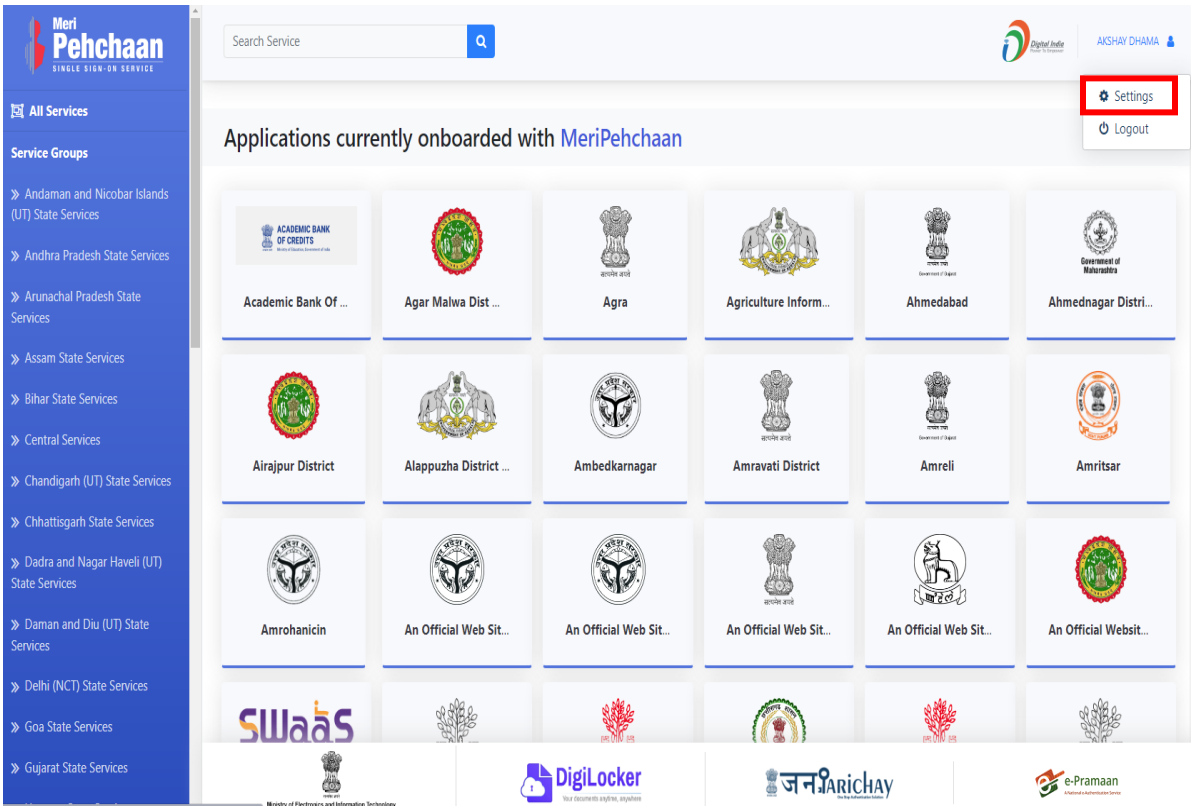


Fig. 1

- Now, click on the “Profile” option from menu.
- Click on the button in front of “Edit” option. (refer fig.2)

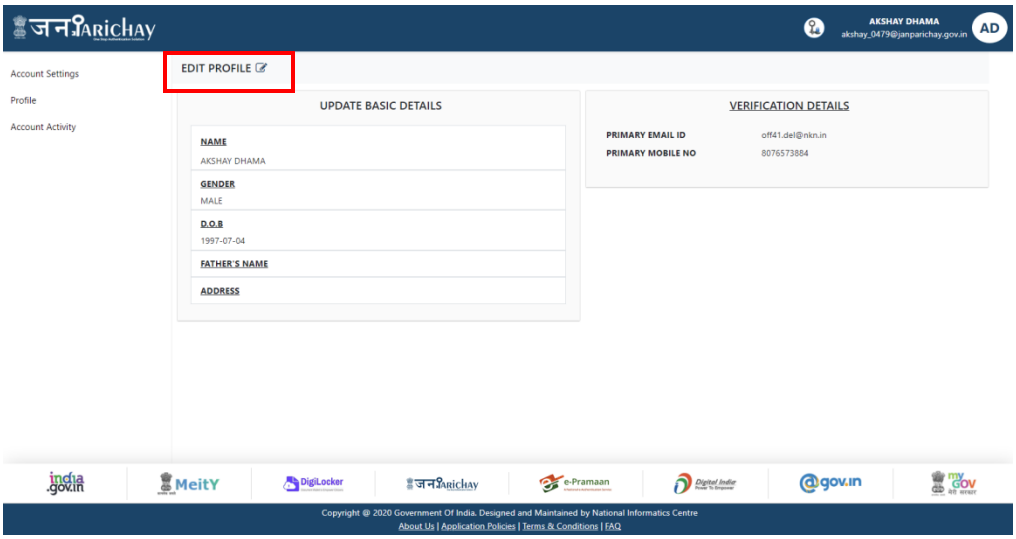


Fig. 2

(An otp verification pop-up will appear on your screen.)

- Now, click on the “send otp” button. (refer fig.3)

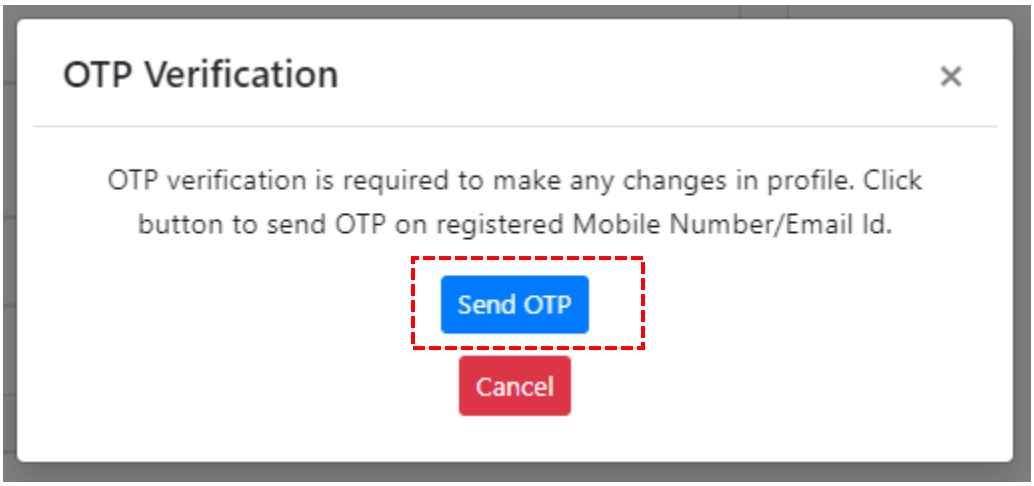


Fig. 3

- Enter the “OTP” you have received on your registered Mobile Number/Email Id. (refer fig.4)

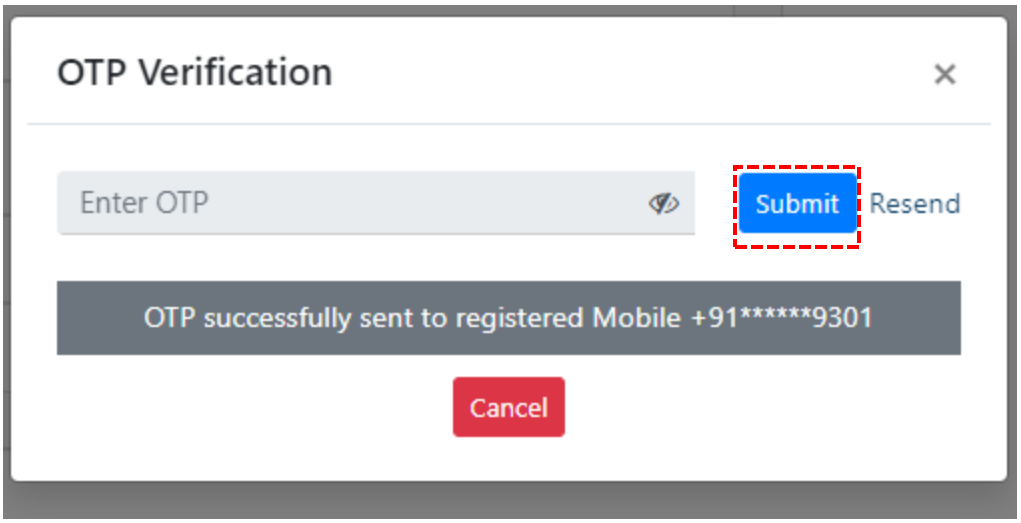


Fig. 4

- Now, choose the primary email id option from the drop-down menu. (refer fig.5)

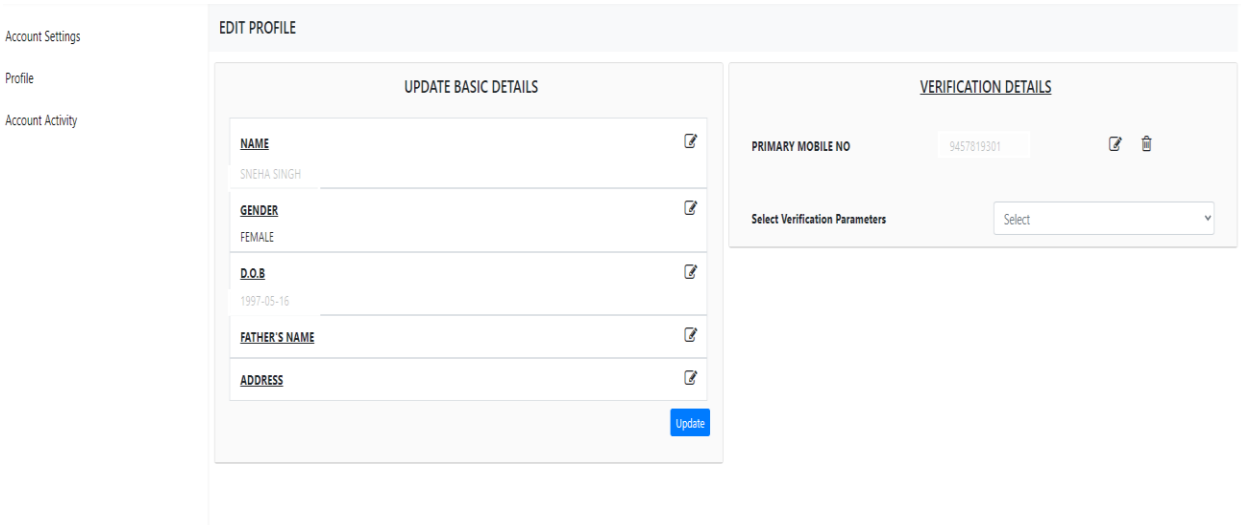


Fig. 5

- Then, enter your primary email ID you want to verify. (refer fig.6)

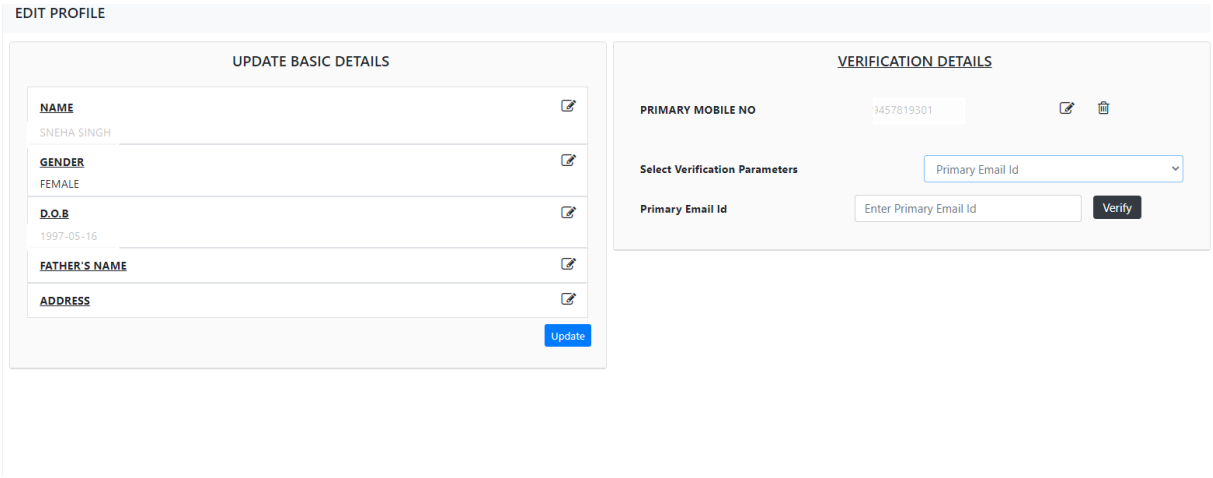


Fig. 6

(You will receive an OTP on that email you have entered.)

- Enter the OTP and click on the “Verify” button to complete the verification process.

(refer fig.7)

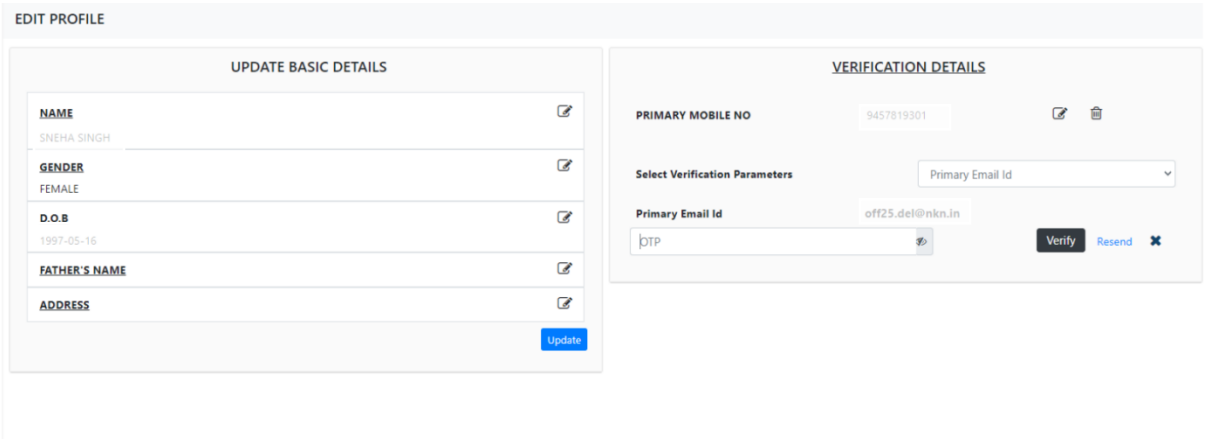


Fig. 7

(A text “you have updated your profile details successfully” will appear on your screen.)

Annexure B: JanParichay partners Service Integration Annexure

REST API	
Sr. No.	
1.	**Display Name** * *This name will be visible to the users on boarded
2.	**Service Name** * *Unique name to identify the service
3.	**Service Description** * *A brief introduction of the service to be integrated(At least 200 words)
4.	**Application Logo** * * Logo of the client service or the service group
5.	**Service State** * *Name of the State the service belongs
6.	**Home URL** * *Landing URL of the client application. User will be redirected back to this URL after successful authentication from Parichay
7.	**Login URL** * *Login page URL of the client service. User will be redirected to this URL in case of any error while accessing the service
8.	**Login Category** Single Login/Multiple Login *Single login services can be accessed only in Single browser at a time while multiple login services can be accessed in multiple browsers (e.g. Chrome and Mozilla) at a time
9.	**Logout URL** *A re-direct Logout URL of the client service
10.	**Logout Callback API** *An API required to inform the service that Logout event was triggered
11.	**Multi-Factor** Enforce /Force *Should all users enforced for Multi-factor authentication by client service or not.

	*Should all users forced for Multi-factor authentication by client service or not
12.	**Geo Fencing** Geofencing per user: Yes/No Geofencing per service: Yes/No * Should a service restricts access to a particular state or a country

OAUTH2

Sr. No.	
1.	**Display Name** * * This name will be visible to the users on boarded
2.	**Service Name** * * Unique name to identify the service
3.	**Service Description** * *A brief introduction of the service to be integrated(At least 200 words)
4.	**Mobile Package** * *The package name of the project (only valid for native apps)
5.	**Application Logo** * *Logo of the client service or the service group
6.	**Service State** * *Name of the State the service belongs
7.	**Home URL** * *Landing URL of the client application. User will be redirected back to this URL after successful authentication from Parichay
8.	**Login URL** * *Login page URL of the client service. User will be redirected to this URL in case of any error while accessing the service
9.	**Login Category** Single Login/Multiple Login

	*Single login services can be accessed only in Single browser at a time while multiple login services can be accessed in multiple browsers (e.g. Chrome and Mozilla) at a time
10.	**Logout URL** *A re-direct Logout URL of the client service
11.	**Logout Callback API** *An API required to inform the service that Logout event was triggered
12.	**Alternate Redirect URL(s)** *A service can choose the Alternate Dynamic URL(s) to redirect the users
13.	**Multi-Factor** Enforce /Force *Should all users enforced for Multi-factor authentication by client service or not. *Should all users forced for Multi-factor authentication by client service or not
14.	**Geo Fencing** Geofencing per user: Yes/No Geofencing per service: Yes/No * Should a service restricts access to a particular state or a country