User Login Manual

National Informatics Centre

4th Floor, Block III, Delhi IT Park, Shastri Park,
New Delhi – 110053
Telephone: 011 – 22180332
Website: www.nic.in

1 INTRODUCTION

This manual contains a step-by-step process of understanding how to login Parichay with different authentication methods. Once you understand all the authentication methods, you can select the best option to secure your Parichay account.
This manual is an extremely helpful document for the user logging for the first time.

2 HOW TO LOGIN PARICHAY

Step 1: Enter Parichay credentials (**Username and Password**). Username should be in the format of "userid@domainname" (Example: xxxxx@nic.in). Click **Next.**
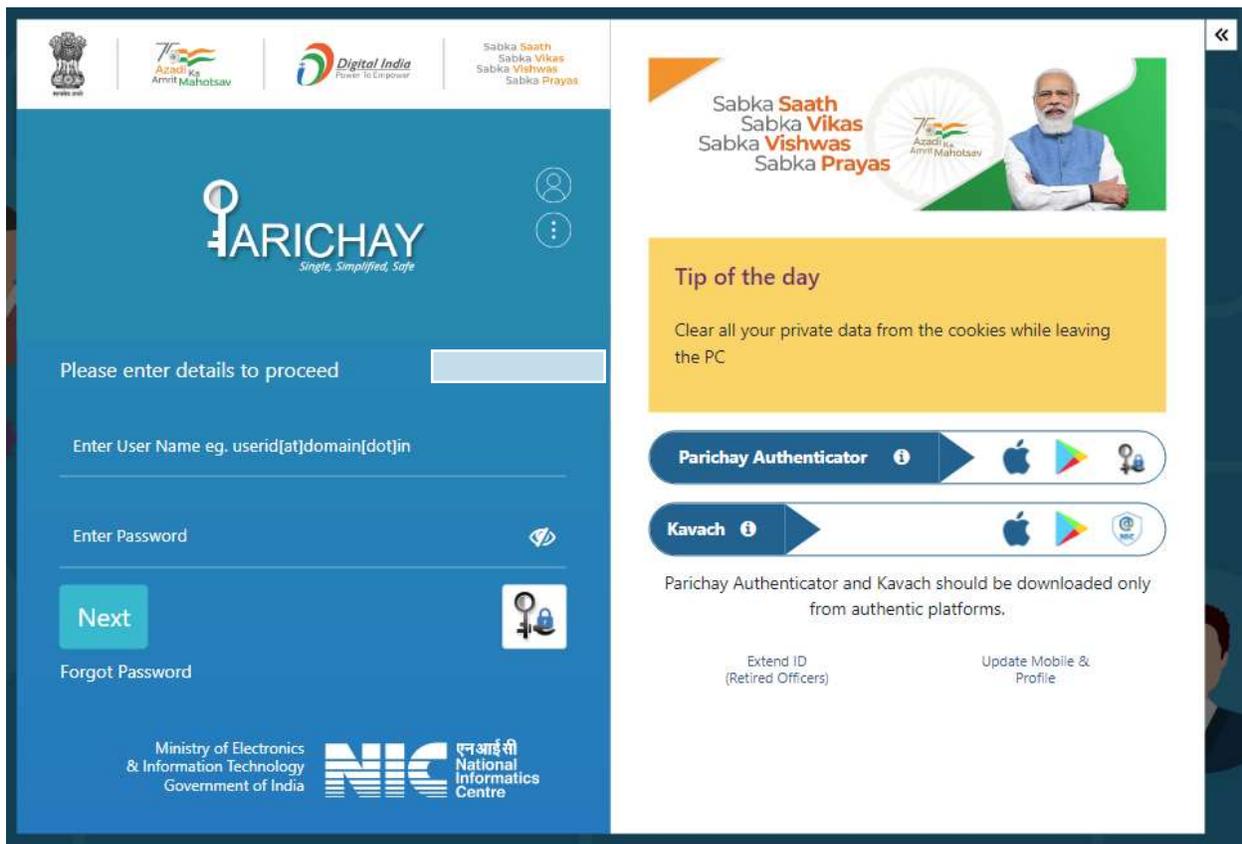
Fig. 1

**Please Note: After 3 unsuccessful username and password attempts, the user will be redirected to the login with Captcha page.

Click on the Menu button given over the login fields and then, choose "**Register Complaint**" to register any complaint or
"FAQ" to see the frequently asked questions.
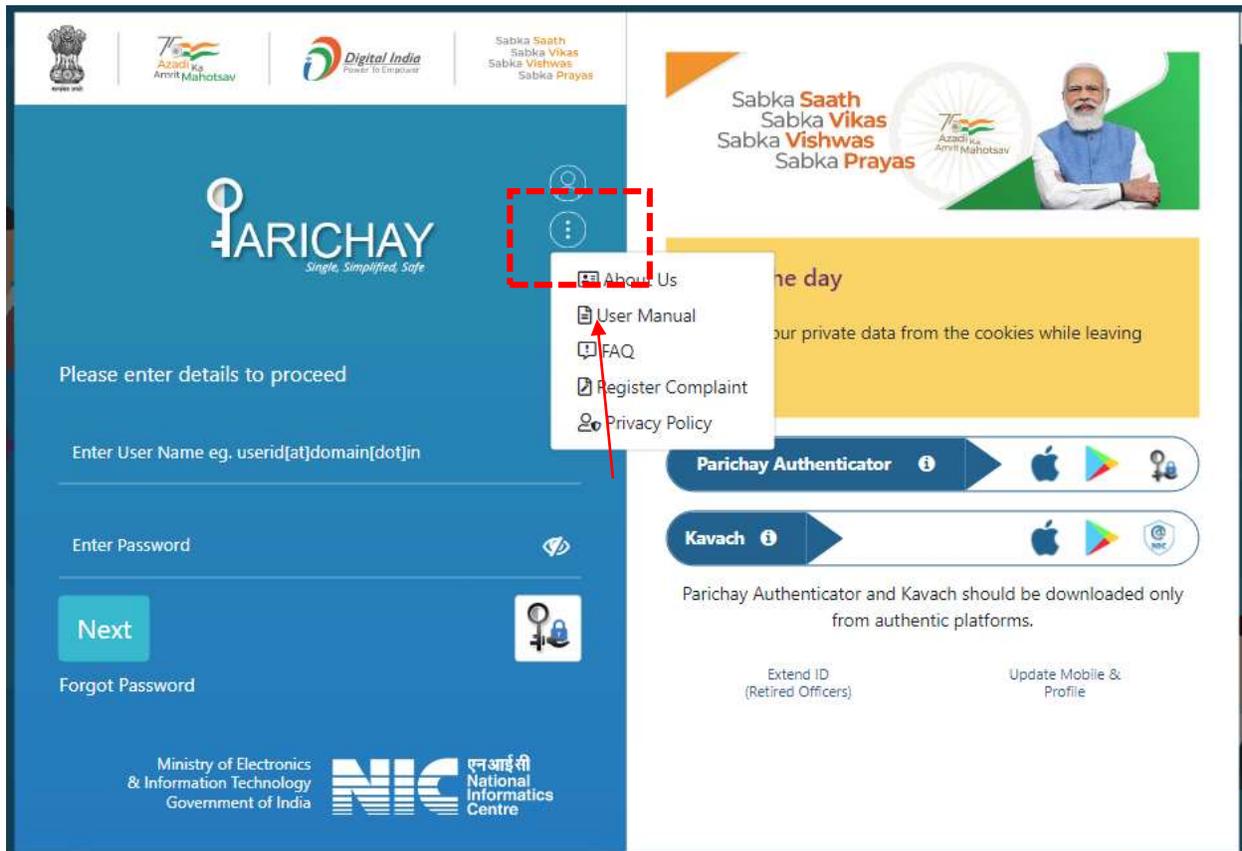
Fig. 2

Step 2: Now, the user will be prompted to the **Two-step Authentication page** when logged in from Non-remembered Device*. Select an authentication method and click **Next.**

Fig. 3

a) <u>OTP Authentication via Mobile</u>

Enter **6-digit OTP** received on the registered mobile no. and click **Next** to login.
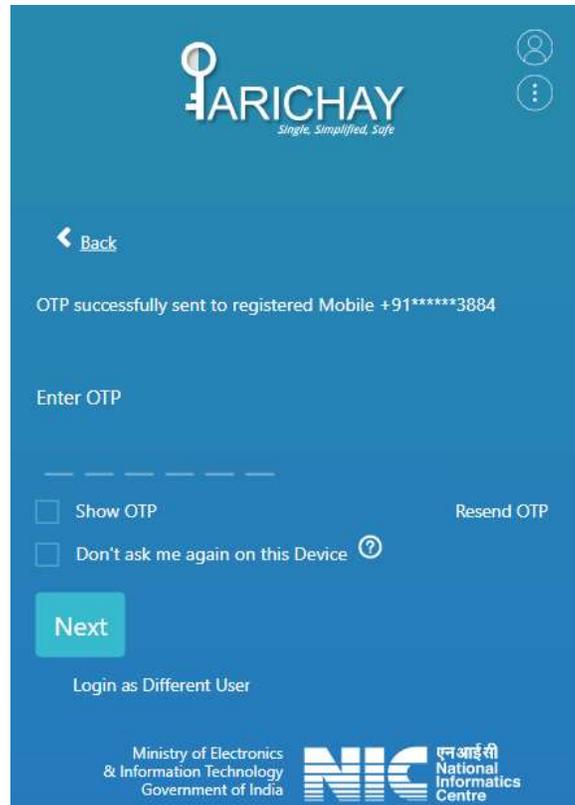
Fig. 4

**Please Note: *After 3 unsuccessful OTP attempts, the user will be redirected to the login page and resend OTP option will be disabled after 3 attempts.*

**Please Note: *After 3 unsuccessful token attempts, the user will be redirected to the login page.*

b) Tap Authentication
   Accept the tap notification received on the registered Parichay Authenticator device to log in.

Fig. 6

**Please Note: *To use TAP or TOKEN as an authentication method, download Parichay Authenticator App and enable Multi-factor authentication from your Parichay account.*

Go to Settings > Account Settings > Enable Multi-factor

c) Token Authentication

   Enter the **token** generated by Parichay Authenticator App and click **Next** to login.
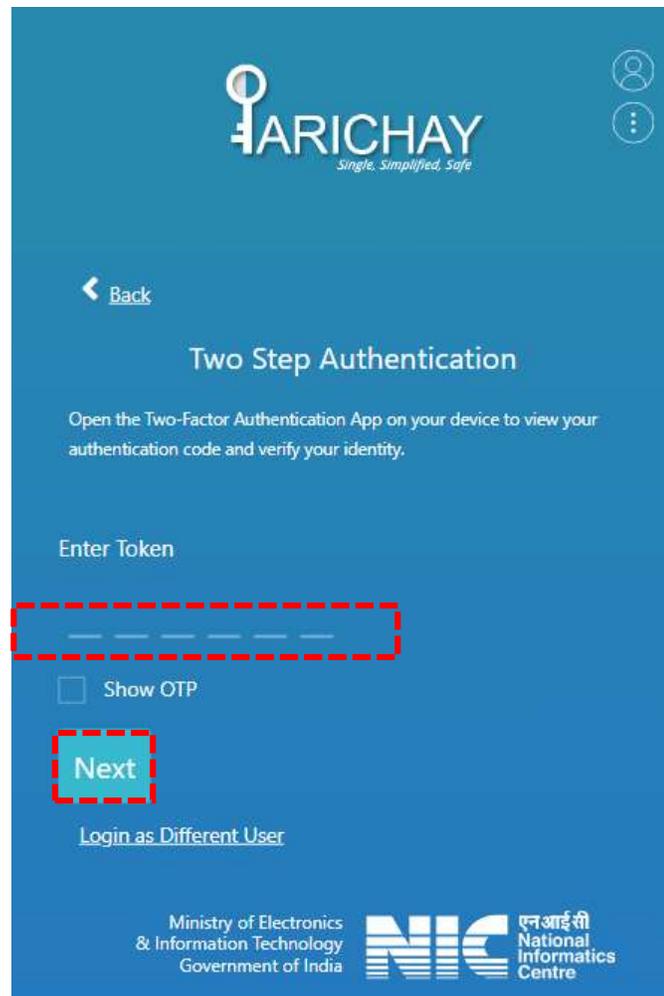
Fig. 7

The user can select '**Don't ask me again on this device**' checkbox to remember the device (identified by IP, Browser ID, and User-Agent) thus skipping the two-step authentication process when log in from the same device in future. However, if the service has enabled the force authentication, the user needs to authenticate irrespective of the remembered browser.

User may want to sign in with a different ID within the same browser. In this case, the user may click on **Login as Different Browser** to login with different account.

**Please Note: After 3 unsuccessful token attempts, the user will be redirected to the login page.

3 TIMEOUT

The session expiration time may vary from service to service. After the service timeout, the user will be redirected to the password page.
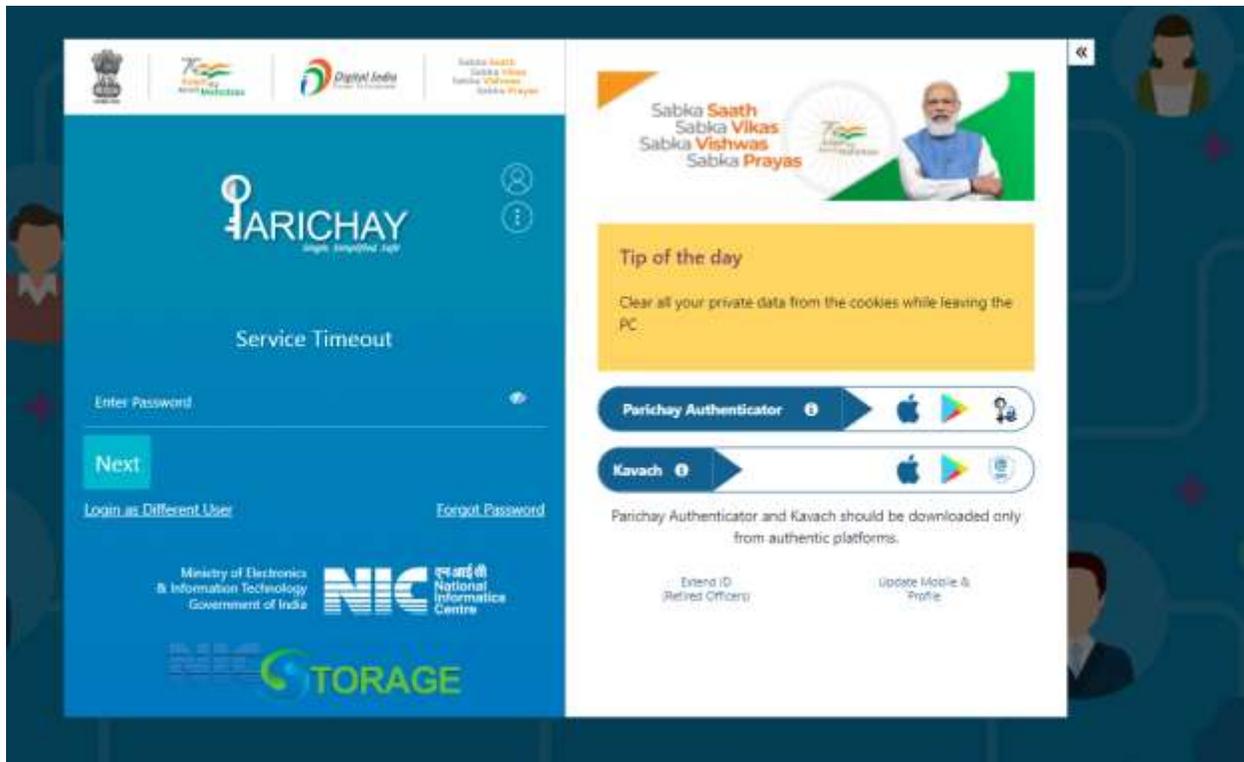
Fig. 8

Step 1: Enter Password again

Step 2: User will be prompted for the two-step authentication in case of forced authentication settings by the service.