National Knowledge Network (NKN)
National NOC, New Delhi

PARICHAY
Client Service Integration

DOCUMENT CONTROL

DOCUMENT NAME: Client Service Integration for Parichay Application.

DOCUMENT ID REFERENCE:

AUTHORIZATION:

Prepared By	Reviewed By	Reviewed By	Authorized By
Name: Kratika Chauhan	Name:	Name:	Name:
Designation: Content Writer	Designation:	Designation:	Designation:

SECURITY CLASSIFICATION: Restricted

VERSION HISTORY:

Issue Date	Effective Date	Description

DISTRIBUTION LIST:

The following persons hold the copies of the documents; all amendments and updates to the document must be distributed to the distribution list.

S.No.	Name	Location	Document type
1		NKN, New Delhi	Soft copy, Hardcopy
2		NKN, New Delhi	Soft copy, Hardcopy

CONFIDENTIAL:

This document contains restricted information pertaining to the National Knowledge Network. The access level for the document is specified above. The addressee should honor this access right by preventing intentional or accidental access outside the access scope.

DISCLAIMER:

This document is solely for the information of National Knowledge Network and should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

Table of Contents

Introduction

- Accounts application provides a CDSSO (Cross-Domain Single Sign-On) framework for various services. It offers a single portal for all the services with a single URL and therefore the user needs to remember only one password to access multiple services.
- Being a service holder, the clients must have ample knowledge to maintain and handle the service integrated with the Accounts.

Purpose

The sole purpose of this document is to offer a framework for the clients to understand the functioning and working of the service with respect to the Accounts application. In case of minor issues, clients can resolve the issue by going through this document.

How to Connect with Parichay

- Open CMD in window system.
- Ping parichay.staging.nic.in
  - Start response [10.122.34.136]
- Telnet Parichay.staging.nic.in 8080
  - Connect with port
- Ping 10.122.34.117
  - Start response [10.122.34.136]
- Telnet 10.122.34.177 8081
  - Connect with port

NOTE: In case, IP or Port doesn't response, ask Network or Firewall team to check respectively.

Highlights

1. As soon as the user hit the service URL, the client service checks for local application Session validation by looking at the session cookie for the service domain. In this case, the service does not find the required Session cookies or the Session cookies found are already invalidated previously by the server, the client service web server redirects the user to the Parichay application.

   API: https://parichay.staging.nic.in:8080/Accounts/Services?service=ServiceName

   HTTP Method: GET

   Where Service Name is the client service name such as "vpn"

   Response: Re-direct to Parichay login page with the service.

2. On Parichay application, the user enters the credentials and after successful authentication, it redirects the user to the OTP/Token/FIDO page (if applied). Then, Parichay sends an encrypted string to the client service.

3. After receiving the encrypted string, client service performs handshaking with the Parichay and Parichay respond to the client service with the same string.

   API:https://parichay.staging.nic.in:8080/Accounts/openam/login/validateClientToken/string/clientService

   HTTP Method: GET

4. If the string before and after handshaking matches, the client service starts the session. Service decrypts the string with Application key and saves parameters in the session.
   If the strings don't match or application gets any other response such as null or false, the client service displays an error message.

5. Every time the user performs any functionality, the service will call the same Rest Service.

   API:
   https://10.122.34.117:8081/Accounts/openam/login/isTokenValid?localTokenId=LocalTokenId&userName=user_name&service=ServiceName&browserId=BrowserId
   HTTP Method: GET

Where localTokenId = Client Token respective to each client
userName = User processed the request
service = Client Service Name
browserId = Unique key to identify the browser

Response: true/false

- **If true, json format {"status":"success", "tokenValid", "true"}**
  Execute the performed action
- **If false, json format {"status":"failure", "tokenValid", "false"}**
  Client local session invalidates forcefully and re-direct to the Parichay login page
  (https://parichay.staging.nic.in:8080/Accounts/Services?service=ServiceName)

6. If the session timeout (client service), the client service re-direct the user to the Parichay password page.

API:https://parichay.staging.nic.in:8080/Accounts/ClientManagement?sessionTimeOut=true& service=clientService

HTTP Method: GET

Response: Forward URL on Password Page

OR

API:https://10.122.34.117:8080/Accounts/openam/login/clientSessionTimeout?userName=userName&sessionId=sessionId&service=serviceName&browserId=browserId&localTokenId=clientLocalTokenId

HTTP Method: POST

Where localTokenId = Client Token respective to each client
userName = User processed the request
service = Client Service Name
browserId = Unique key to identify the browser
sessionId = Unique key to identify the sessionId

Response: True or False

If True, Redirect to password page (https://parichay.staging.nic.in:8080/Accounts/NIC/PasswordPage.html?service=ServiceName)

If False, stay on the same page

7. If a single application logout from Parichay, then all the applications get auto-logout.

Process (In detail)

Login Process

1. As soon as the user hit the service URL, the service checks for local application Session validation by looking at the session cookie for the service domain.

2. In this case, the service does not find the required Session cookies or the Session cookies found are already invalidated previously by the server, the service web server redirects the user to the Parichay application.

API: https://parichay.staging.nic.in:8080/Accounts/Services?service=ServiceName

HTTP Method: GET

Where Service Name is the client service name such as "VPN"

Response: Re-direct to Parichay login page with the service.

NOTE: For adding a new parameter in above API, append that parameter at the end of the above API. Like as below API.

API:https://parichay.staging.nic.in:8080/Accounts/Services?service=ServiceName&subservice=SubServiceName

HTTP Method: GET

Where Service Name is the client service name such as "vpn"

3. The browser checks for the Parichay cookie "tokenId" in the request and if the Parichay find the "tokenId" cookie, it will redirect on the following API

API:http://10.122.34.117:8081/Accounts/openam/login/isTokenValid?localTokenId=LocalTokenId&userName=user_name&service=ServiceName&browserId=BrowserId&sessionId=SessionId

HTTP Method: GET

Where localTokenId = Client Token respective to each client
userName = User processed the request
service = Client Service Name
browserId = Unique key to identify the browser
sessionId = Unique key to identify the session

Response: true/false

- **If true, json format {"status":"success", "tokenValid", "true"}**
  Execute the performed action
- **If false, json format {"status":"failure", "tokenValid", "false"}**
  Client local session invalidates forcefully and re-direct to the Parichay login page
  (https://parichay.staging.nic.in:8080/Accounts/Services?service=ServiceName)

4. If Parichay does not find the "tokenId" cookie or the "tokenId" presented has been previously invalidated and so a login page with Username and Password fields would be presented to the user.

5. While submitting, Parichay validates credentials from the LDAP and after successful authentication; it creates a string including user attributes, tokenId (UUID) with its expiry time and encrypts the string with the service API-key.

6. Then it redirects the user back to the registered home URL of the service and set the encrypted string as URL parameter of the service. Additionally, an Parichay cookie named "tokenId" is created with domain accounts.nic.in.

7. The user's browser saves the "tokenId" cookie and access the registered service home URL taking the encrypted string. The service takes out the encrypted string and validates from the Accounts. In reply, the Parichay response with “string/false/null”, depending upon the status of the token present in the encrypted string. This step is Handshaking and it must be accomplished within 10 sec or else the response will be null/false.

NOTE: Instead of forwarding the encrypted string as a URL parameter to the Parichay, client service must send the encrypted string as an API response in the backend.

NOTE: Token validation is one of the mandatory API of the Parichay (SSO) application as it handles the user session throughout the Parichay (SSO) dependent applications. This will handle the logout done by user from applications other than client Application.

API:https://parichay.staging.nic.in:8080/Accounts/openam/login/validateClientToken/string/clientService

HTTP Method: GET

Where Service Name is the client service name such as "vpn"

Response: string/false/null

If string value is equivalent to the response string

- **Decrypt the string with service API key**
- **Start client application session**
- **Set parameters in the session**

If response is false,

It implies that Parichay has invalidated the response string because the time frame was more than 10 seconds.

If response is null,

It implies that there may be some technical issues in the backend

8. If the response is "string", the service does a session start and saves the user details as session attributes and sends back a cookie with a session identifier to the user's browser along with the application home page.

9. Every time the user performs any functionality, the service will call the same Rest Service.

API:https://10.122.34.117:8081/Accounts/openam/login/isTokenValid?localTokenId=LocalTokenId&userName=user_name&service=ServiceName&browserId=BrowserId

HTTP Method: GET

Where localTokenId = Client Token respective to each client

userName = User processed the request
service = Client Service Name
browserId = Unique key to identify the browser

Response: true/false

- **If true, json format {"status":"success", "tokenValid", "true"}**
  Execute the performed action
- **If false, json format {"status":"failure", "tokenValid", "false"}**
  Client local session invalidates forcefully and re-direct to the Parichay login page
  (https://parichay.staging.nic.in:8080/Accounts/Services?service=ServiceName)

Logout Process

10. On clicking the Logout button on service, the service first checks its own session. If the session does not exist or session timeout then, there is a Timeout process.

API:https://parichay.staging.nic.in:8080/Accounts/ClientManagement?sessionTimeOut=true& service=clientService

HTTP Method: GET

Response: Forward URL on Password Page.

OR

API:https://10.122.34.117:8081/Accounts/openam/login/clientSessionTimeout?userName=userName&sessionId=sessionId&service=serviceName&browserId=browserId&localTokenId=clientLocalTokenId

HTTP Method: POST

Where localTokenId = Client Token respective to each client
userName = User processed the request
service = Client Service Name
browserId = Unique key to identify the browser
sessionId = Unique key to identify the sessionId

Response: True or False

If True, Redirect to password page (https://parichay.staging.nic.in:8080/Accounts/NIC/PasswordPage.html?service=ServiceName)

If False, stay on the same page

NOTE: The session timeout for Parichay is 12 hours, which can be extended to 24 hrs by selecting 'stay signed in' checkbox while login. However, each service also has its own local session timeout

11. If a session exists, it redirects to Parichay with the parent 'TokenId' and the respective service.

API:http://10.122.34.117:8081/Accounts/openam/login/logoutAll?userName=userName&service=serviceName&sessionId=sessionId&browserId=browserId

HTTP Method: POST

Where userName = User processed the request
service = Client Service Name
sessionId = Unique key acts as a reference to Accounts' session
browserId = Unique key to identify the browser

Response: Json Format:- {"status":"success","reason":"Successfully Logged out","url":"https://parichay.staging.nic.in:8080/Accounts/Services?service=serviceName"}

12. After redirecting to Parichay, the service will clear the local cookies.

NOTE: clientService is the name of the Service