MHDFC
(Move Health Data Forward Challenge)

Sharing API Designs and USE Case Scenarios as per HEART WG Specifications…..

by **SHAKTI SOLUTIONS**

Abstract

- Allows consumer to securely authorize the movement of their Health data to destinations they choose
- The destinations could be any other public and private health providers, EHRs , Payers and Govt. Agencies.
- Need to design API interface as per the standards and specifications set by HEART WG.
- Specifications are clearly defined in FHIR (Fast Healthcare Interoperability Resources) OAUTH 2.0 scopes, OAUTH 2.0 , Open Id Connect 1.0 (SSO) and UMA 1.0 (User Managed Access)

Move Health Data Forward Challenge - Application Architecture

Browser

Connect to Health Data Actions

Login with Credentials

EHR/Provider /Authorized 3rd party Web Server

HEART Client (OAUTH)

RESTful Web services

Database

Access/Request Grant

Access Token

Request / Register Endpoints URIs

Get Endpoints

Client Registration

Client Key Credentials

ONC's Centralized HEART Authentication Server (Identity Provider)

HEART Auth Services

HEART Endpoint Services

OAUTH DB + Audit Logger

Mobile Apps

Thin HEART (OAUTH) Client

MHDFC
MOVE HEALTH
DATA FORWARD
CHALLENGE

Technologies Recommended

- OAUTH Framework : Apache OLTU (OAuth Protocol Implementation)
- Back-end : Java, Spring, Hibernate, JMS, MongoDB / MySQL / Memcached / Redis , Tomcat/JBoss
- Front-end Demo : HTML5, AngularJS and CSS3

** API will be a wrapper (Decorator Pattern) on top of OLTU based on HEART WG Spec.

Scenario 1: (Web browser)

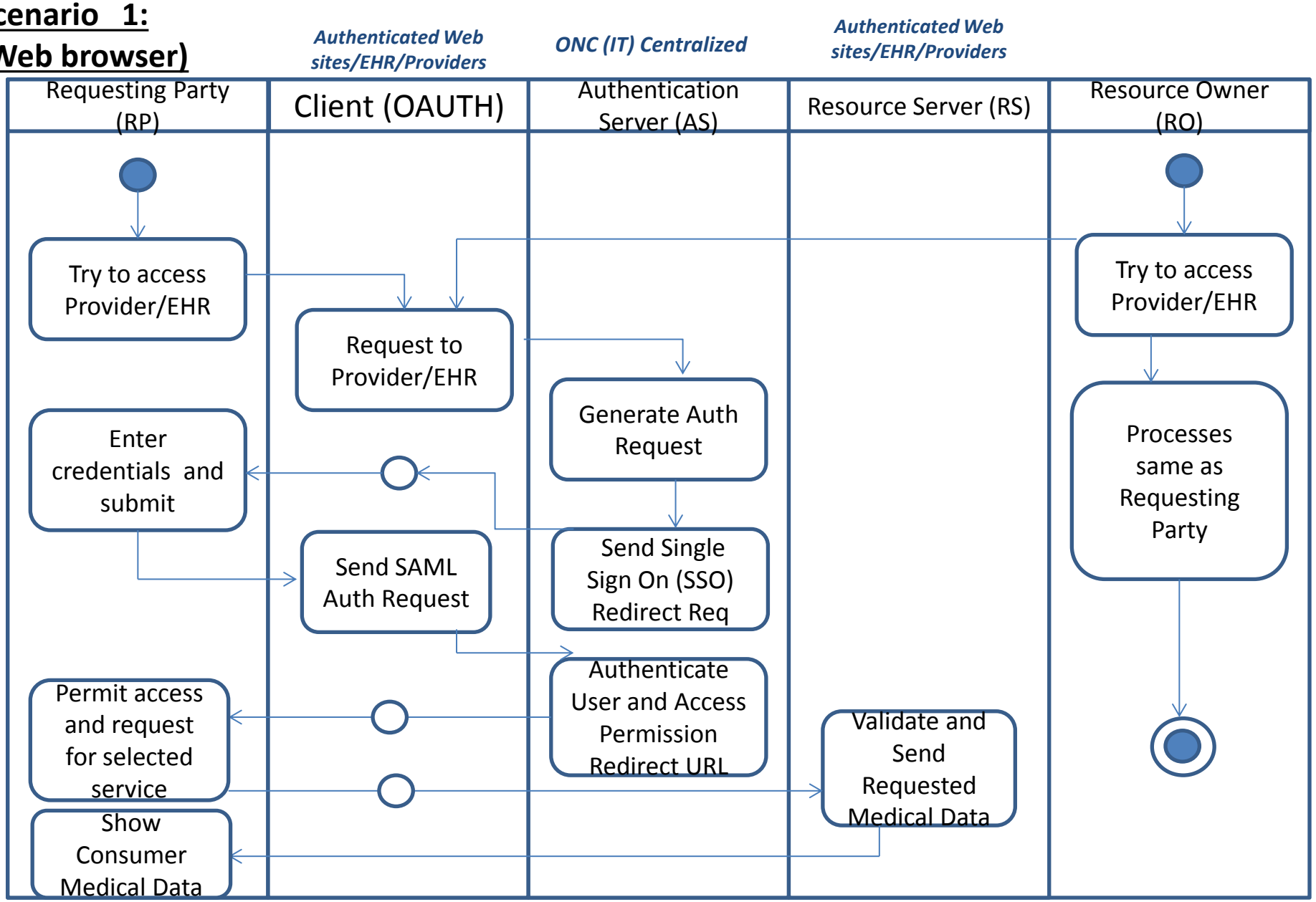
The users access their health records from relevant EHR System using the public authorized web sites.

Steps:

- The user opens website in browser and select relevant EHR vendor that keeps his/her health records. (Assuming that the site is registered with ONC Authentication server)
- Redirect to EHR vendor's authentication page and oblige to enter credentials of user.
- The vendor site asks the user to confirm /denial permission for accessing the user's health records through the public web site.
- if confirmed , The user is asked to select types of services provided from vendor's aspect for the registered website.
- Based on the health service selection, the relevant details will be fetched from EHR system and shown.

Activity Interaction diagram

Scenario 1: (Web browser)



Scenario 2: (Web browser)

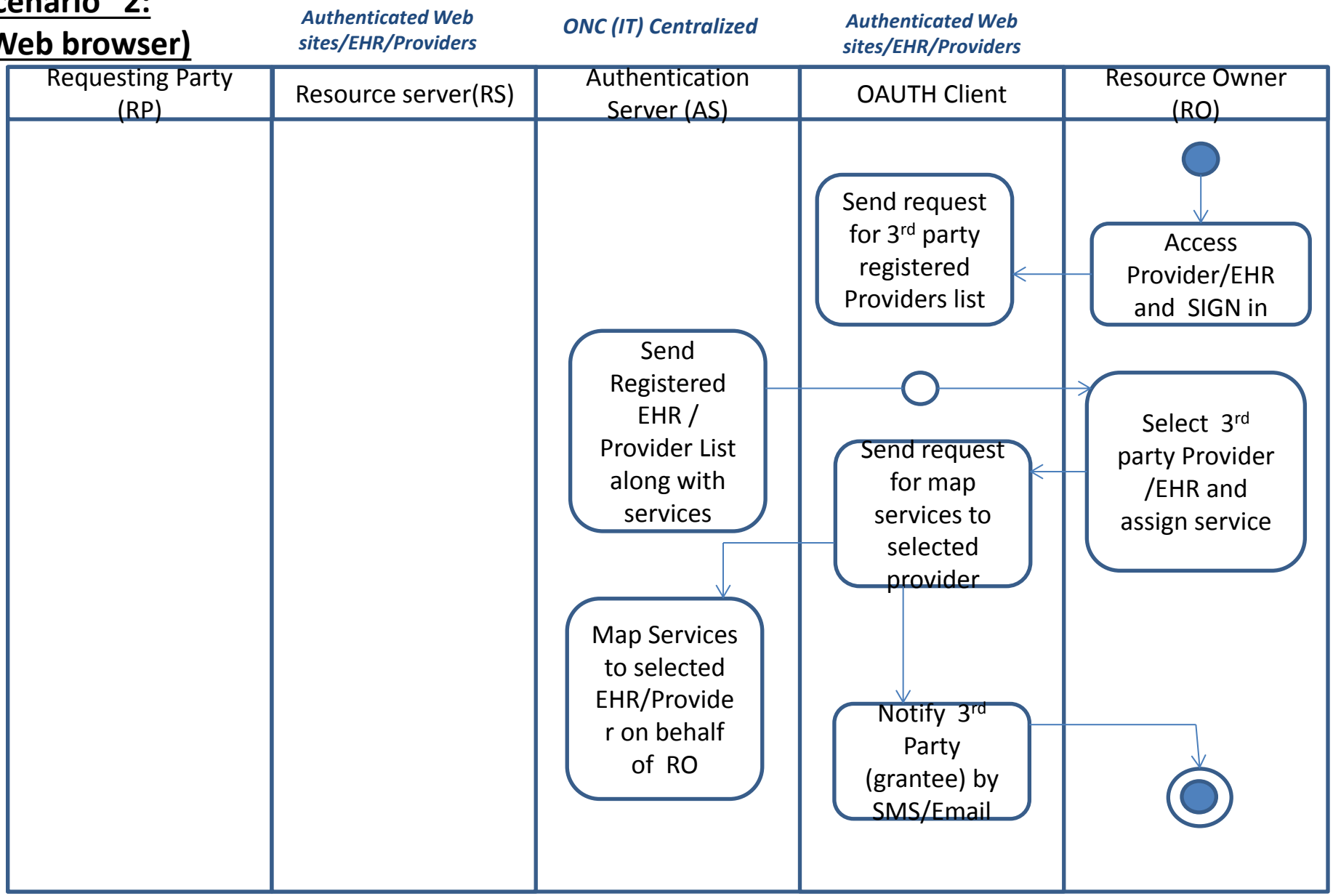
The users gives permission of access to another provider/EHR system to retrieve their health records from relevant Provider/EHR System.

Steps:

- The user opens the relevant provider/EHR website.
- The user will select the target provider/EHR (Assuming that provider is registered with ONC Authentication Server).
- The user will select multiple medical records from the list and assigned to selected target provider and confirm the data exchange.

Activity Interaction diagram

Scenario 2: (Web browser)



Scenario 3: (Web browser/Desktop Client)

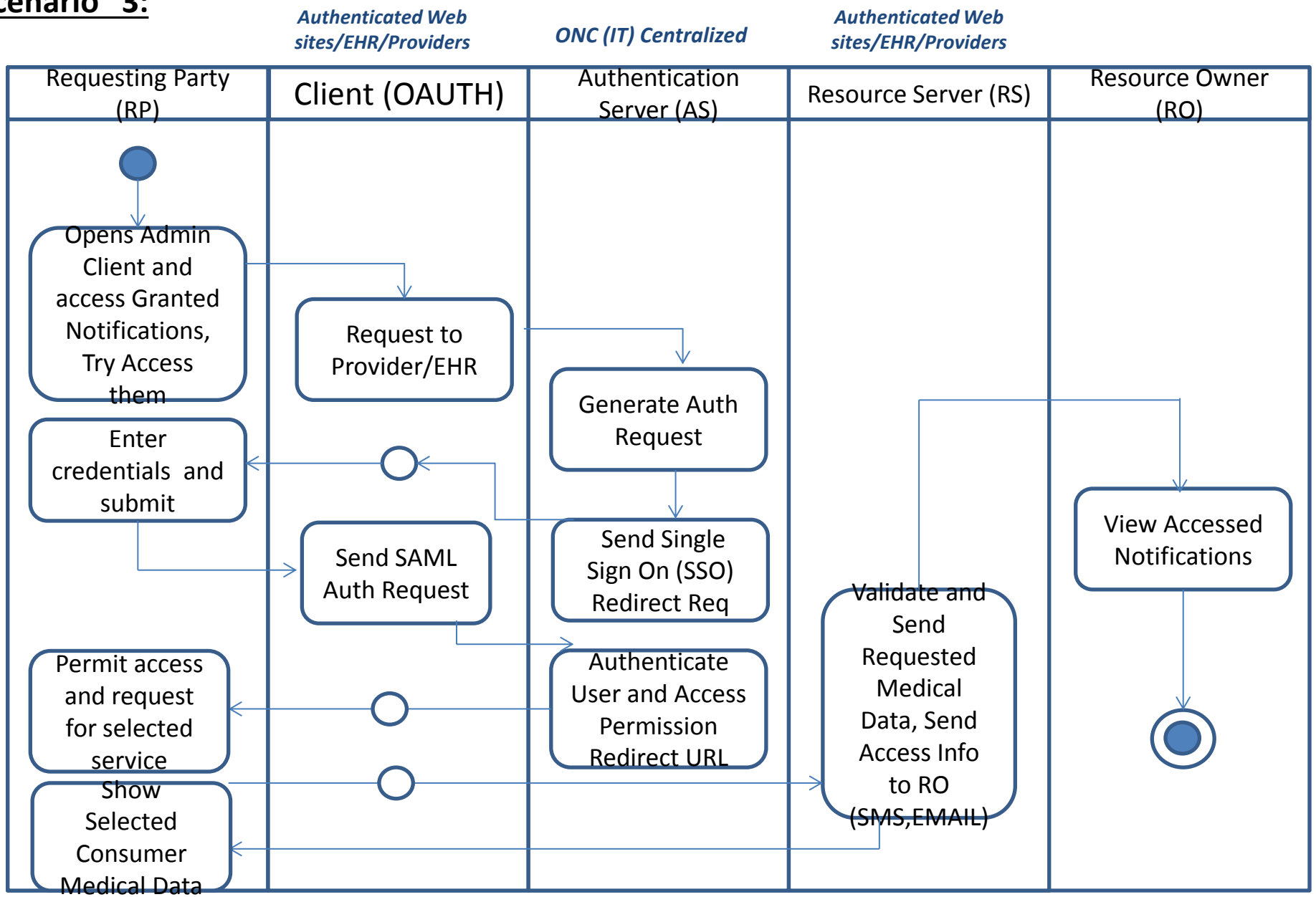
The provider/EHR which are given access permissions can retrieve medical records of patients of other provider/ EHR.

Steps:

- The provider/EHR opens admin web client application.
- In the dashboard message panel, the count of access grants of medical records will be shown, the admin has to select that which shows all permission access list and ask for confirming the access grant.
- On confirmation, the admin can able to access all relevant granted medical records and download into their systems.
- The concerned granters will be informed through SMS and Email of theirs.

Activity Interaction diagram

Scenario 3:



Scenario 4: (Mobile Client)

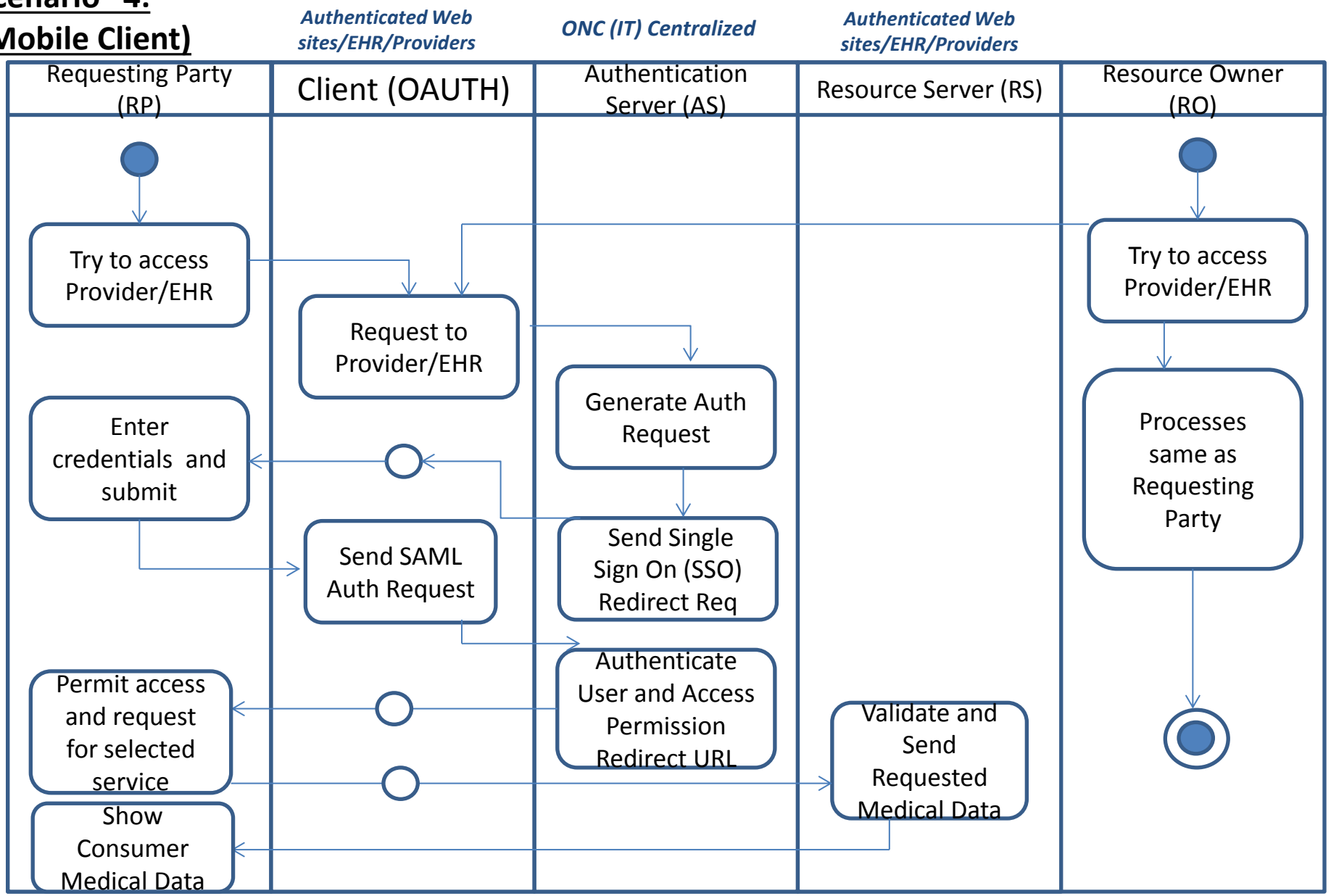
The users access their health records from relevant EHR System using Authorized Mobile application (Hybrid/Native) which integrates many EHR systems.

Steps:

- The user opens application and select relevant EHR vendor that keeps his/her health records. (Assuming that the site is registered with ONC Authentication Server)
- Redirect to EHR vendor's authentication page and oblige to enter credentials of user.
- The vendor site asks the user to confirm /denial permission for accessing the user's health records through the public web site.
- if confirmed , The user is asked to select types of services provided from vendor's aspect for the registered website.
- Based on the health service selection, the relevant details will be fetched from EHR system and shown.

Activity Interaction diagram

Scenario 4: (Mobile Client)



Scenario 5: (Mobile Client)

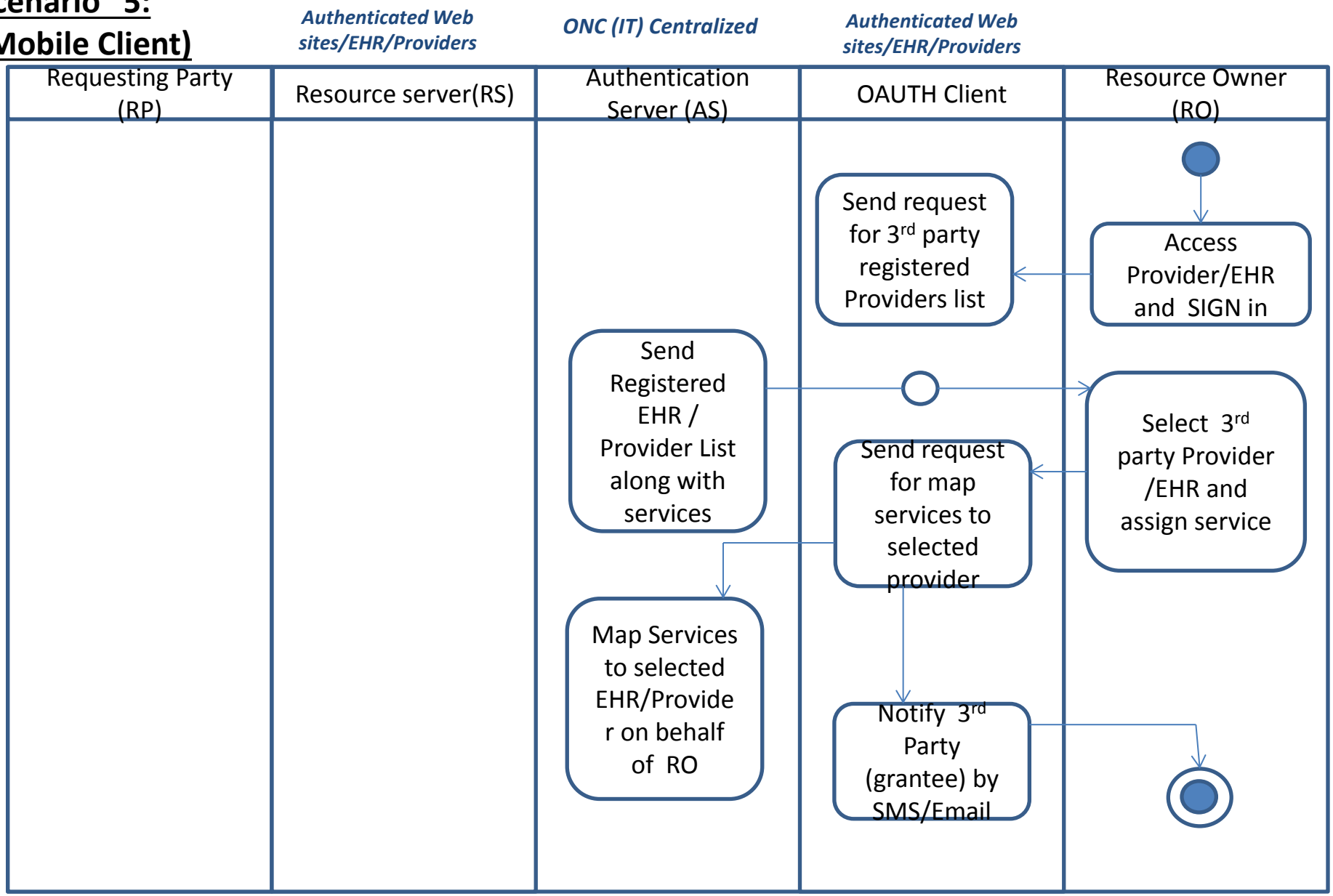
The users gives permission of access to another provider/EHR system to retrieve their health records from relevant Provider/EHR System using provider/EHR's authorized Mobile application (Hybrid/Native) which integrates many other Provider/EHR systems.

Steps:

- The user opens the relevant provider/EHR's Mobile application.
- The user will select the target provider/EHR from the registered providers list with ONC Authentication Server.
- The user will select multiple medical records from the list and assigned to selected target provider and confirm the data exchange.

Activity Interaction diagram

Scenario 5: (Mobile Client)



Scenario 6: (Web browser)

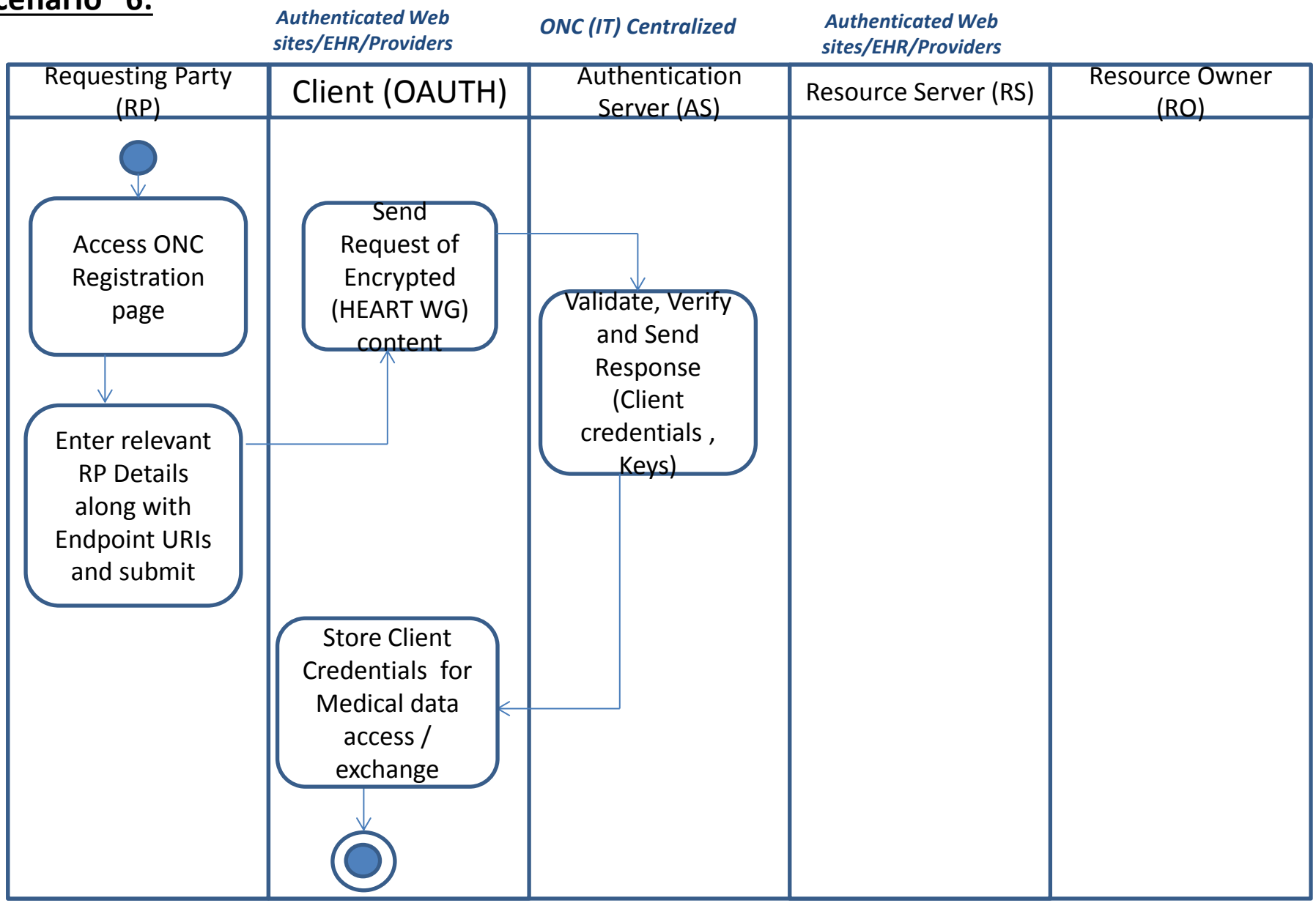
The provider/EHR system can register with ONC Authentication Server by providing registration details along with end point URIs for proper call backs. So that they can able to securely exchange/access the medical records of patients with consumer mediation.

Steps:

- The provider/EHR admin user opens the secured ONC's registration page.
- The admin user enters the relevant details along with Call back URIs and submits the page.
- The ONC authentication server validate the input details sends back some secured information such as client id, secret code, asymmetric keys (RSA private and public) which will be kept in the database as encrypted.
- The shared keys and codes will be used for every access/data exchange request made for target provider/EHR Systems through ONC Authentication server.

Activity Interaction diagram

Scenario 6:



Anticipated Benefits

For General Public/EHRs/ Private & Public Health Providers/Payers/Govt. Agencies

- Can access their health details recorded in different EHRs/Providers through authenticated public (Ex. Govt. Medicare) web sites.
- Can grant privilege to other users, EHRs, Health providers, Payers to have access of their Health data.
- The Providers or EHRs can transfer bulk of patients Medical records to other providers.
- Reduce time as the consumers don't have to wait for test results or medical data in transit.
- Reduce costs by avoiding the repetition of taking medical tests in transit.
- Notification to consumers in case of their delegates (grantee) access their Medical data.
- Patient vital medical conditions and status will be accessible across the country through the secured channel.
- Security prevail high level standards that put forth on top of open authentication services.
- Improve better health, better care , better value through quality improvement.
- Direct attention to new market opportunities.

MHDFC
MOVE HEALTH
DATA FORWARD
CHALLENGE

THANK YOU

Gapps/Murugan from
Shakti Solutions
PO Box 164330
Austin, TX 78716, USA
Tel. (512) 328-9880