METEOR ON FHIR - USE CASE - OAUTH ACCESS

Identifier	Title	Priority Level	Status
meteor-on-fhir/002	OAuth Access	Argonaut - Sprint 2	Prototyped

Description / Intent

In this use case, Organization A offers a federated authentication mechanism that allows a Patient to authorize Organization B to query and access Patient’s health data from Organization A. The use case requires the Patient to sign in and authenticate their Organization A credentials while access Organization B’s website. After authenticating, Organization B will give Organization A an access token. This token can then be used to query for the Patient records, but no others.

For example, John Doe might access the Meteor on FHIR Interface Engine using the “Sign In With Withings” button, which will authorize Meteor on FHIR to access the Withing’s website, and query it for John’s blood pressure and weight measurements. Once authenticated, the access token remains in the Patient’s profile until it’s explicitly removed.

Primary Actor

Patient

Additional/Supporting Actors

Application – operated by Organization A, which requests and (on approval) accesses EHR data on the patient's behalf
Authorization server – operated by Organization A, and used to authenticate the clinician or patient and to authorize the application to access EHR data on behalf of the clinician or patient
Resource server – operated by Organization B, which hold and retrieve EHR data as authorized

Other Stakeholders

Organization A
Organization B
System Administrator

Endpoints

http://localhost:3200/metadata

http://localhost:3100/_oauth/OAuth2Server

http://localhost:3100/login

Preconditions

OAuth Client Access must be configured by a System Administrator. To continue the previous example, the System Administrator would need to register Meteor on FHIR as a Client Application on the Withings website.

Withings would then provide the System Administrator with a clientId and clientSecret, which are then used to configure Meteor on FHIR. The “Sign in With Withings” button then uses the clientId and clientSecret to provision John Doe with an access token.

Postconditions

The provider systems has recorded the access in the audit log.
The patient profile has an auth token.

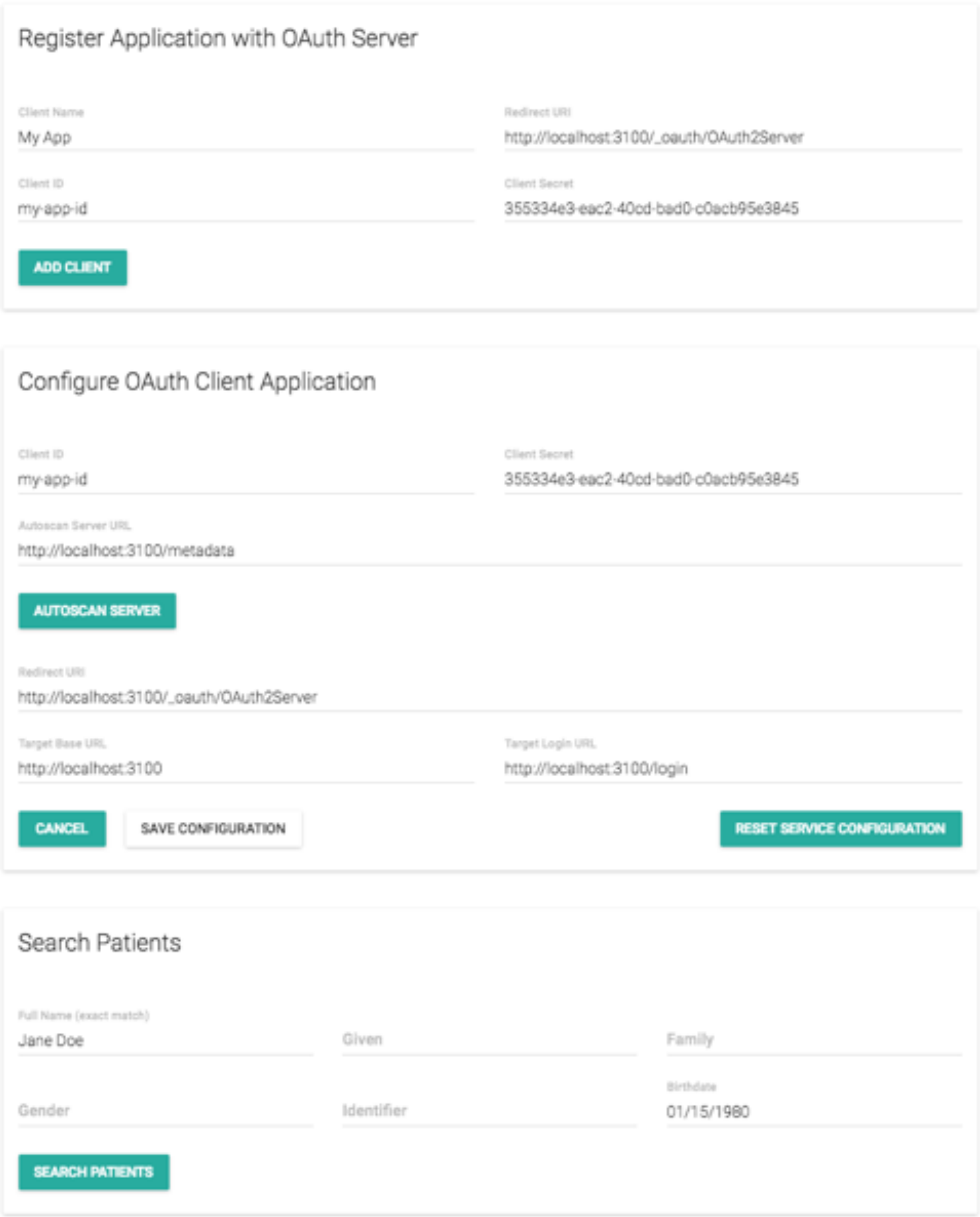
Basic Flow

1. Patient opens web browser and launches the application.
2. Patient selects “Sign in with” login button
3. Patient selects an application option that requires that data be retrieved from the patient’s EHR
4. Application requests access to the desired data.
5. Authorization server authenticates the application’s identity.
6. Authorization server authenticates the patient’s identity.
7. Authorization server authorizes the application to retrieve requested data within a limited timewindow
8. Application queries Resource Server for data elements
9. Resource Server returns the requested data elements, or indicates that the are unavailable.
10. Application works with the retrieved data as requested by the patient.
11. This use case ends when the patient logs out of the application.

References

http://argonautwiki.hl7.org/images/e/ec/Argonaut_UseCasesV1-1.pdf
https://fhirblog.com/2014/06/17/fhir-and-oauth2/

METEOR ON FHIR - USE CASE - OAUTH ACCESS - SCREENSHOTS



Register Application with OAuth Server

Client Name: My App

Redirect URI: http://localhost:3100/_oauth/OAuth2Server

Client ID: my-app-id

Client Secret: 355334e3-eac2-40cd-bad0-c0acb95e3845

Configure OAuth Client Application

Client ID: my-app-id

Client Secret: 355334e3-eac2-40cd-bad0-c0acb95e3845

Autoscan Server URL: http://localhost:3100/metadata

Redirect URI: http://localhost:3100/_oauth/OAuth2Server

Target Base URL: http://localhost:3100

Target Login URL: http://localhost:3100/login

Search Patients

Full Name (exact match): Jane Doe

Birthdate: 01/15/1980