Building apps against Swedish healthcare API's

Christian Hilmersson, Hans Thunberg | callistaenterprise.se | 2013-01-16

CALLISTA
Enterprise

Agenda

- Welcome
- Practical info
- Introduction to SDK by VINNOVA
- HTTP overview
  - Lab on public data API's
- API's containing patient related data
  - OAuth 2.0, intro and lab
- Building the App
  - Need for an app backend
  - Lab, build the app backend
  - Front-end development for mobile apps, differences ?
  - Lab, Integrating with the backend API

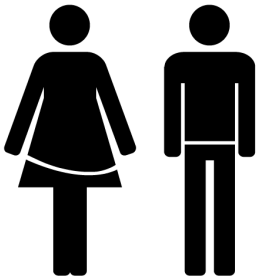
CALLISTA Enterprise

Welcome

- Hans Thunberg
- Christian Hilmersson

CALLISTA
Enterprise

Practical info



Introduction to SDK by VINNOVA

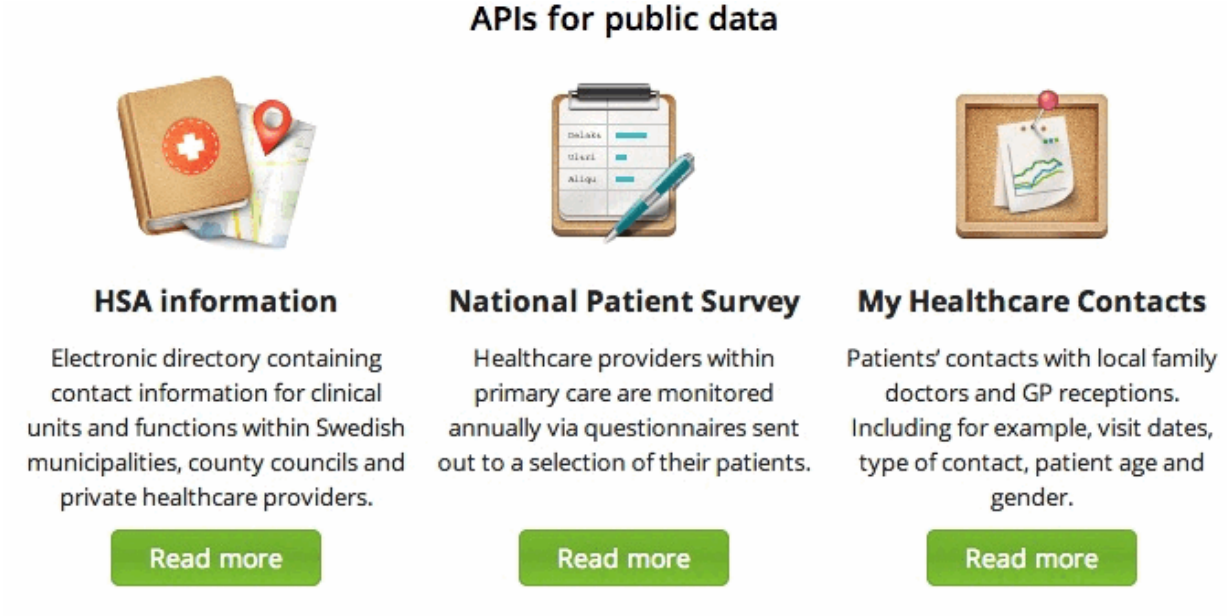
SDK by VINNOVA

- SDK by VINNOVA
- Background
  - SLL and Vinnova
  - Part of Mina Vårdflöden

CALLISTA
Enterprise

Introduction to SDK by VINNOVA

API's

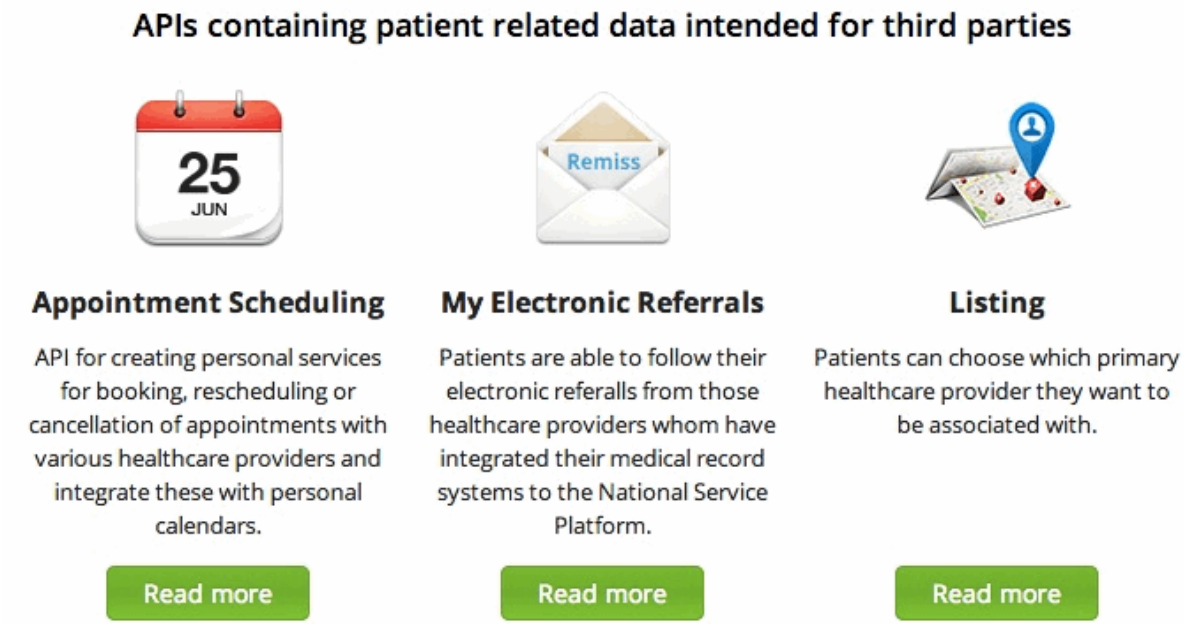


sdk by Vinnova

CALLISTA Enterprise

Introduction to SDK by VINNOVA

API's



sdk by Vinnova

CALLISTA Enterprise

HTTP overview

HTTP-request

- URL
  - Uniform Resource Locator is used to uniquely identify a resource over the web
  - Address + parameters
  - http://server.se/api/healthcarefacilities/123/bookings/1
- POST, GET, PUT, DELETE
  - CRUD mappings based on best practices within REST community.
- HTTP headers
  - Accept
  - Authorization
  - Content-Type
- Payload/Content

CALLISTA Enterprise

HTTP overview

HTTP-response

- Status codes
  - 2xx, 3xx, 4xx, 5xx
  - 418 I'm a teapot (RFC2324)
    - » Hyper Text Coffee Pot Control Protocol
- HTTP Headers
  - Location
  - Content-Type
- Example: Redirect, how does it work?

CALLISTA Enterprise

HTTP overview

Example: Redirect, how does it work?

Issue request from browser
http://host.com/path

```
> GET /path HTTP/1.1
> User-Agent: Mozilla/5.0
> Host: host.com
➢ .......

< HTTP/1.1 302 Found
< Date: Wed, 01 Jan 2013 20:11:48 GMT
< Server: Apache/2.2.23
< Location: http://anotherhost.com/path
< ......
```

host.com

```
> GET /path HTTP/1.1
> User-Agent: Mozilla/5.0
> Host: anotherhost.com
➢ .......

< HTTP/1.1 200 OK
< Date: Wed, 01 Jan 2013 20:11:49 GMT
< Server: Apache/2.2.23
< Content-Type: application/
json;charset=UTF-8
< ......
```

anotherhost.com

CALLISTA
Enterprise

HTTP overview

Exercise 1

Use Curl to make http requests against public data API

✓ Open lab/lab1/README and follow the instructions

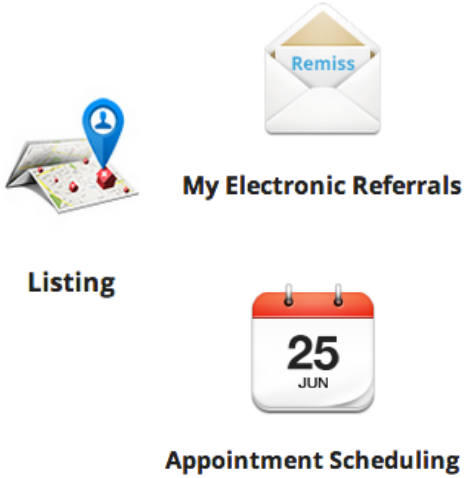
CALLISTA Enterprise

API's containing patient related data

Introduction

Requirements on Patient related data API's

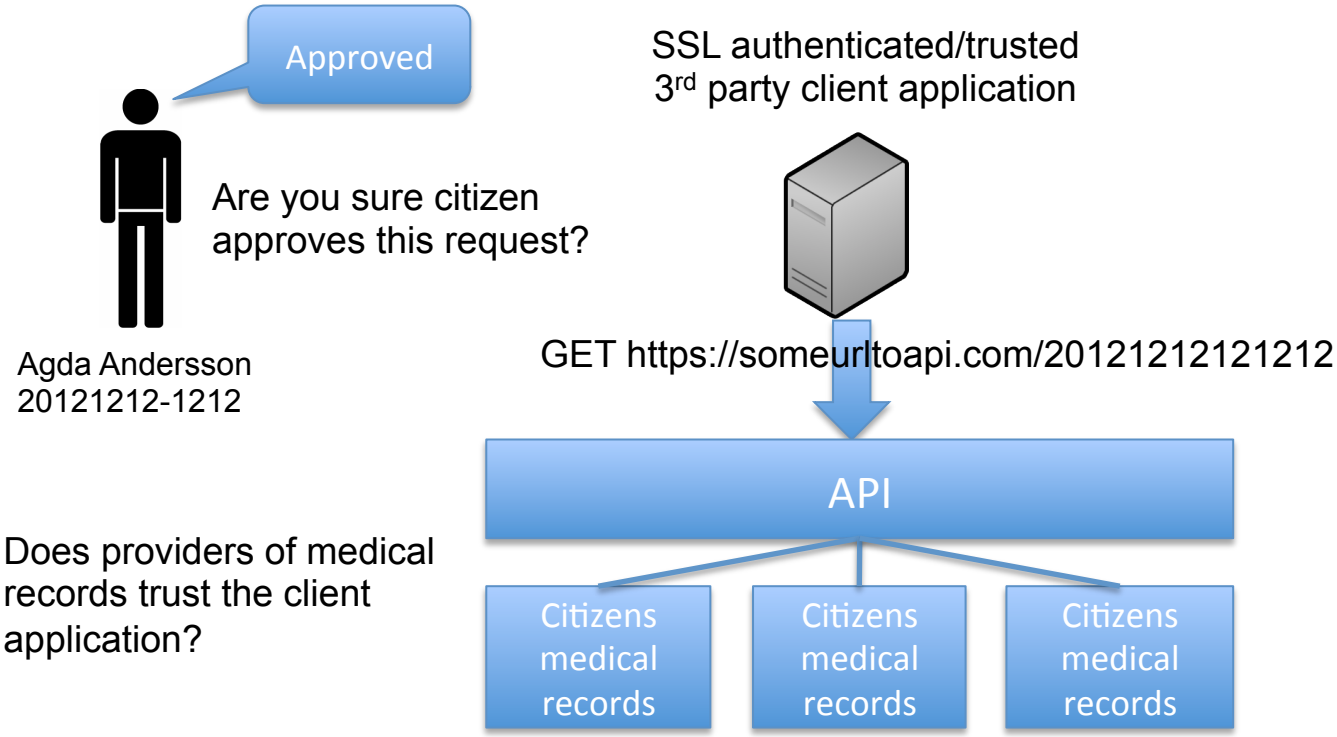
- Strong authentication of citizens
  - Demand from Datainspektionen
  - 2-factor
- Strong authentication of API clients
  - SSL/TLS certificate issued by trusted CA
  - Mutual authenticaton
- Strict authorization control
  - Citizen approved



CALLISTA Enterprise

API's containing patient related data

Introduction



API's containing patient related data

OAuth 2.0

- OAuth 2.0 addresses these kinds of issues
- From oauth.net

An **open protocol** to allow **secure authorization** in a **simple** and **standard** method from web, mobile and desktop applications.

Read the OAuth 2 specification »

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service.

CALLISTA Enterprise

API's containing patient related data

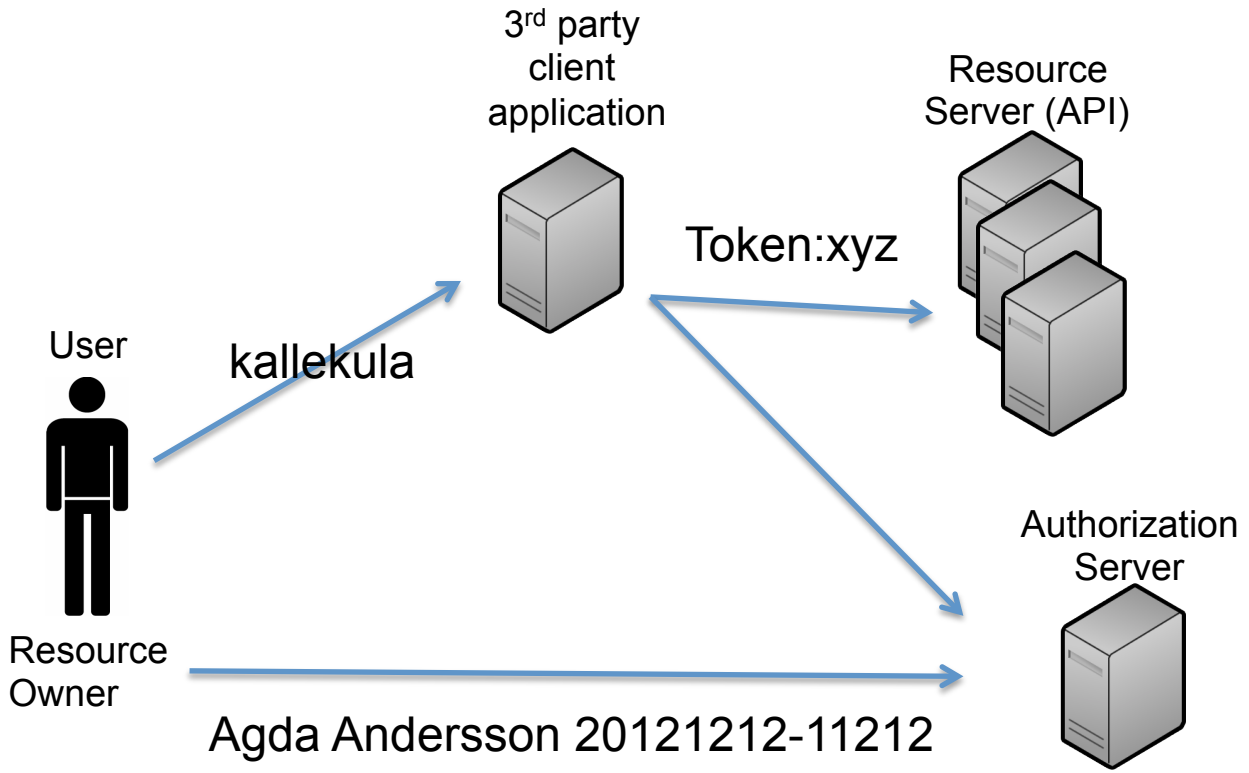
OAuth 2.0

- Possible to delegate authorization using tokens
  - I.e. without giving out the password
  - Twitter, Facebook, Google etc
- Possible for the citizen to be anonymous in the app
  - E.g. username kallekula
  - But still authenticated as Agda Andersson against MVK while authorizing the client
  - Generates a non-identifiable token representing the citizen authorization

CALLISTA Enterprise

API's containing patient related data

OAuth 2.0 Roles



API's containing patient related data

Exercise 2

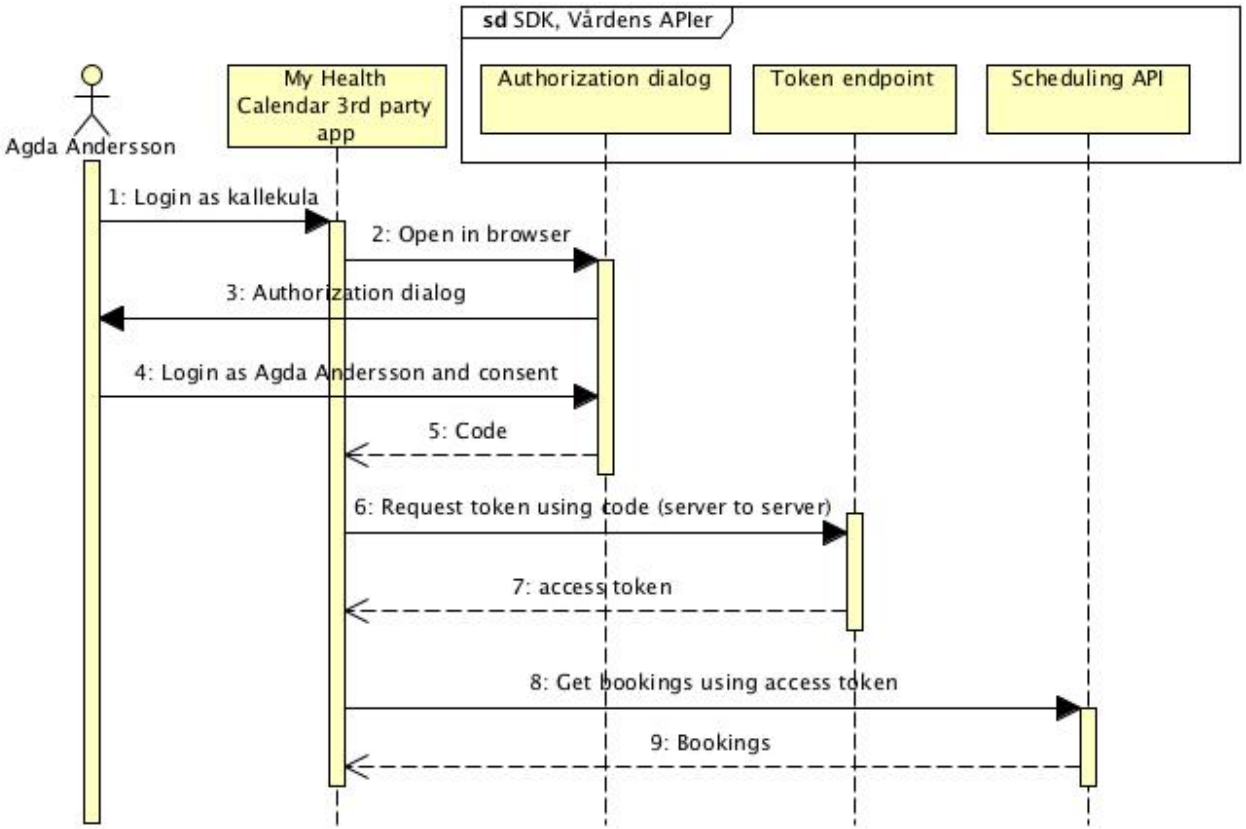
Use Curl to make http requests using pre-generated access tokens against API´s containing patient related data.

- ✓ Open lab/lab2/README and follow the instructions

CALLISTA Enterprise

API's containing patient related data

OAuth 2.0 Authorization code flow



CALLISTA Enterprise

API's containing patient related data

OAuth 2.0 Request authorization

Request authorization dialog, parameters:

- Response type
- Client ID
- Scope
- State
- Redirect URI

Request token using authorization code

- Token endpoint

CALLISTA Enterprise

API's containing patient related data

Demo

Demo of the OAuth dance

API's containing patient related data

Exercise 3, Simple OAuth 2.0 API Client

Get familiar with OAuth 2.0 and SDK by using a simple client letting the user authorize access.

- ✓ Open lab/lab3/README and follow the instructions

CALLISTA Enterprise

Kaffe

Building the App

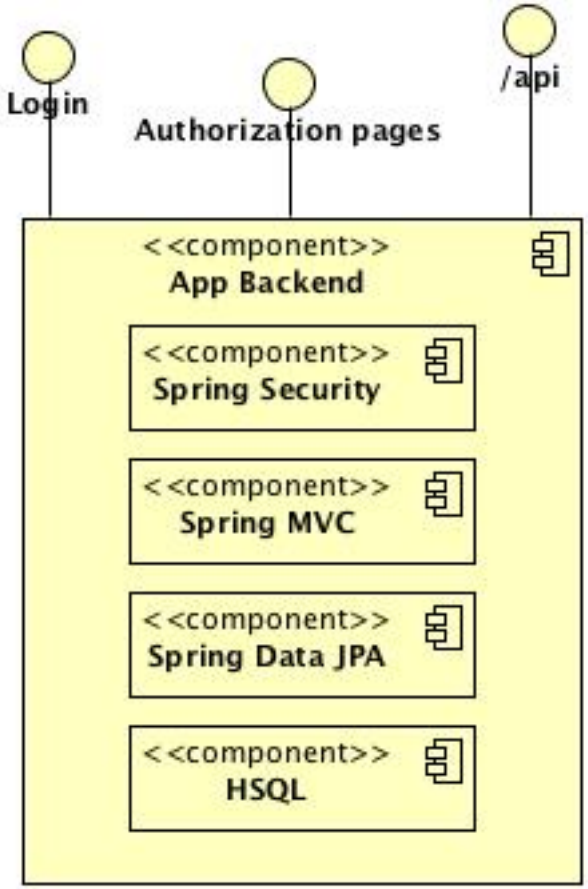
Backend, intro

Simple App backend uses:

- Spring MVC framework
- Spring Security to Secure API's
- Spring Data JPA for repository handling
- HSQL as persistence for user tokens

Simple App backend exposes:

- Login page
- OAuth authorization pages
- API´s for an app



Building the App

Exercise 4, backend

Complete the Simple App backend to provide a secure API for the frontend.

- Add JSON API
- Call SDK to fetch data
- Add security

✓ Open lab/lab4/README and follow the instructions

CALLISTA Enterprise

Building the App

Frontend

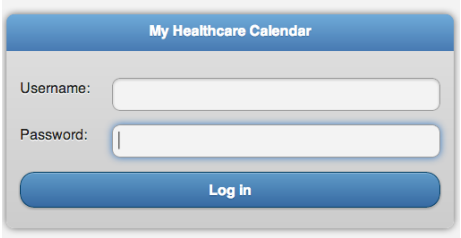
Frontend technologies

- What's happening on the frontend?
- Apps as independent HTML/JS solutions
  - Same origin policy
  - Cross Origin Resource Sharing
- My Healthcare Calendar
  - (Almost) Finished HTML/JS App built with backbone.js and jQuery mobile
  - How do we connect the app to our API?

CALLISTA Enterprise

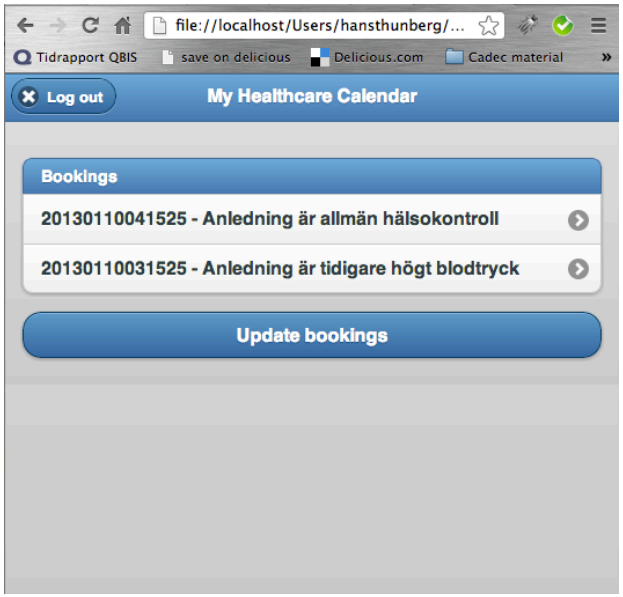
Building the App

Exercise 5, frontend



Complete a simple client that use the API provided by the backend.

- Alter JavaScript to login and to fetch bookings from our API



- Since we will use the backend we created in lab 4
  - Run mvn jetty:run from lab4/solution/simple-app-backend
  - Login user at http://localhost:8080
  - Authorize access for simple client

✓ Open lab/lab5/README and follow the instructions

CALLISTA Enterprise

Summary

- Introduction to SDK by VINNOVA
- HTTP overview
- OAuth 2.0
- Simple application

Questions?

CALLISTA Enterprise

Links

http://www.vinnova.se/

http://sdk.minavardkontakter.se/

http://oauth.net/2/

http://tools.ietf.org/html/draft-ietf-oauth-v2-31

https://developers.google.com/accounts/docs/OAuth2

https://developers.facebook.com/docs/reference/dialogs/oauth/

CALLISTA Enterprise