Leveraging OpenID
To connect Vehicle to the Cloud

ALS 2017 Tokyo
Fulup Ar Foll Lead Architect
fulup@iot.bzh

Who Are We ?

Commits by Company in 2017

Company	Commits
IoT.bzh	1039
Linux Foundation	79
Konsulko	77
Individual	38
Mentor Graphics	36
TI	25
Advanced Telematics Systems	21
Xevo	20
AisinAW	7
ALPS	7
Mitsubishi Electric	7
Renesas	7

Company	Commits
Toyota	5
Fujitsu-Ten	4
Intel	4
Samsung	4
ADIT	3
Panasonic	3
Qt Company	3
Microchip	2
Trust Point Innovation	2
LG	1

1394 Total Commits
45 Committers
21 Companies

- 01 Jan 2017 – 26 May 2017
- Commits to master

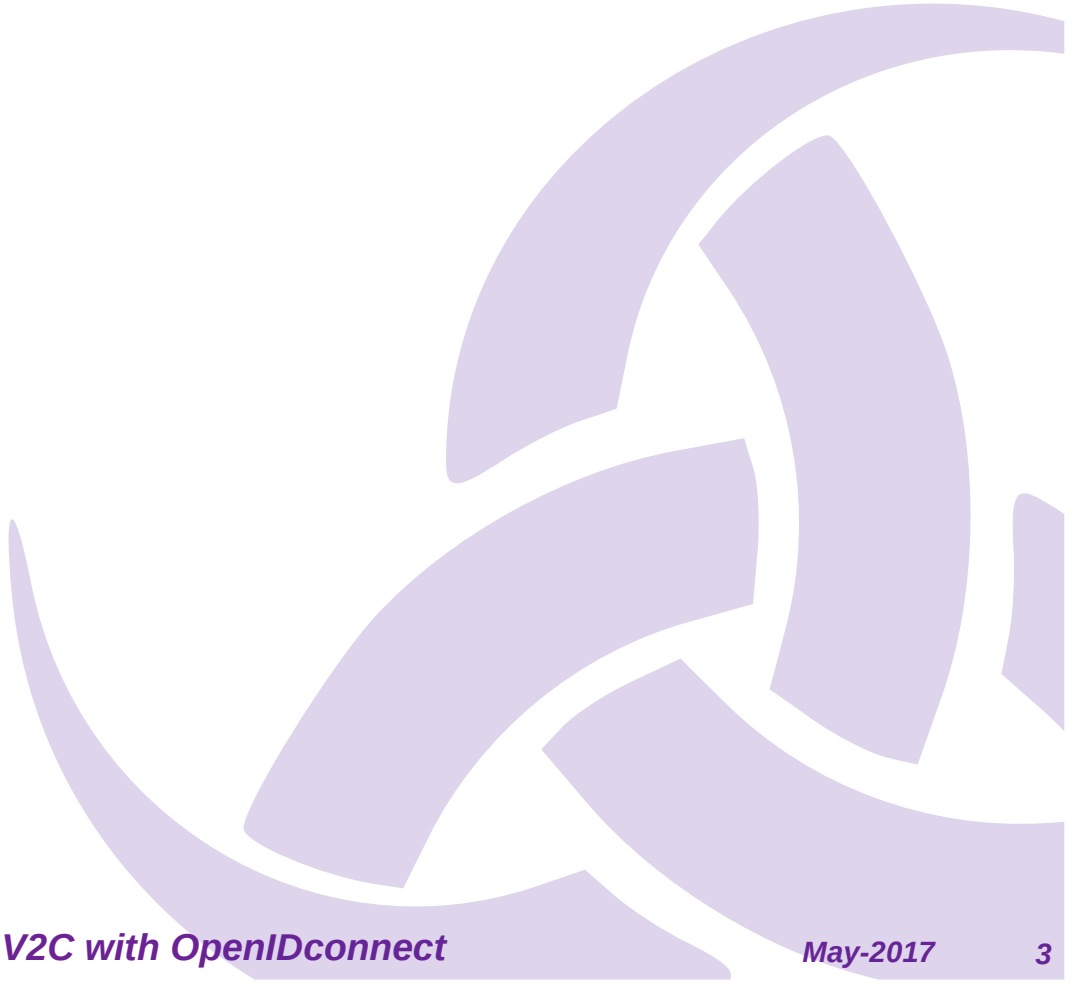
LINUX FOUNDATION

Slide 11

AUTOMOTIVE GRADE LINUX

V2C Multiple Requirements

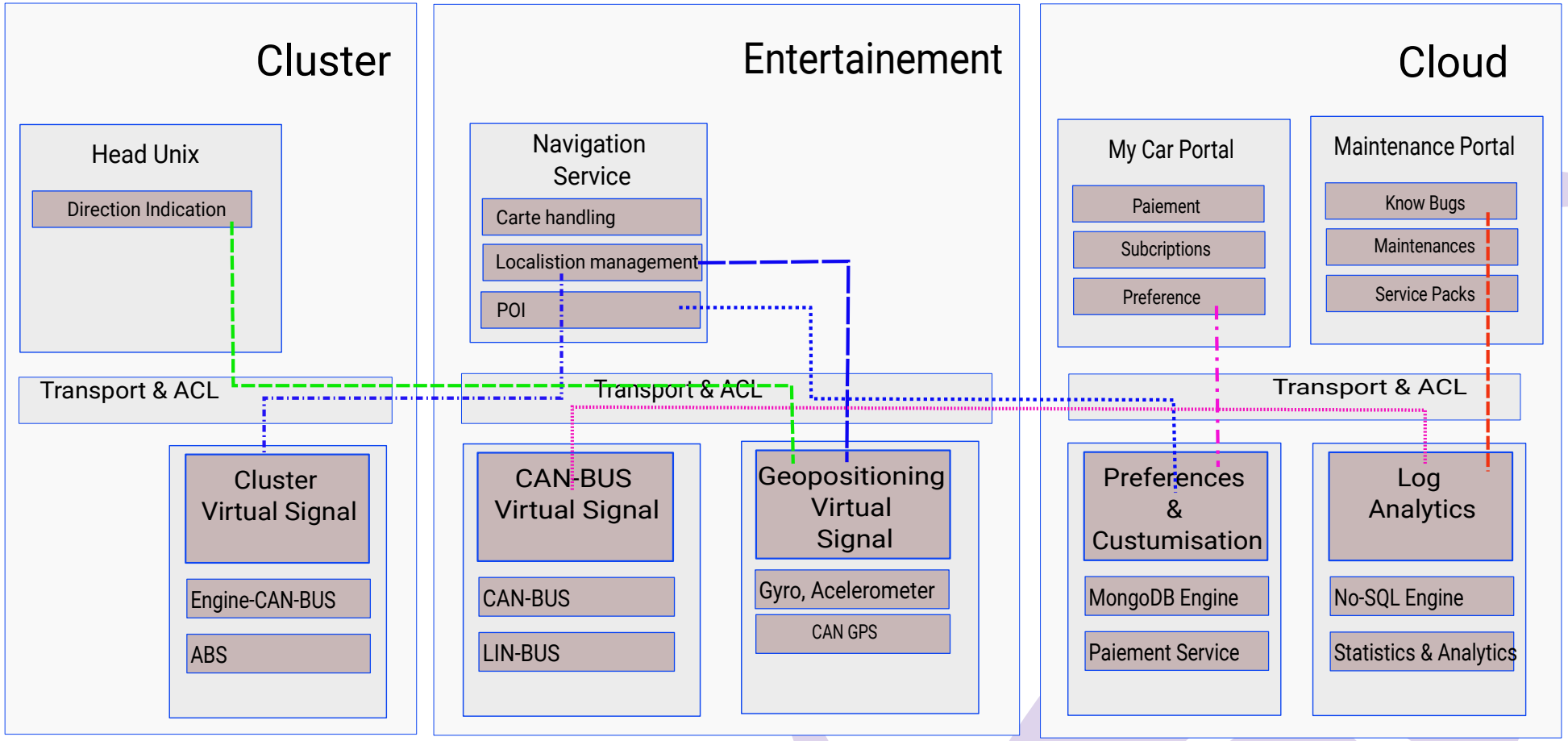
- Car to Cloud
  - Telematics
  - Car sharing, Fleet management
  - Profiling
  - Real time Update Traffic/Map
- Cloud to Car
  - User Preferences
  - SOTA, Streaming Music, Traffic
- Car to Infrastructure
  - Payment
  - Car to City
  - Car to Home



V2C MUST fix issues

- Potential open door for cyber-attack ?
- Who own and controls the data ? What's about user privacy ?
- How to provide the right user experience with on time to the market innovations ?
- How to open popular to non-automotive services (Spotify, Facebook, Paypal, …)
- How to keep the service running for 25 years?
- ...
- Last but not least, where to find skill developers ?

AGL Microservices Architecture



Multi ECU & Cloud Aware Architecture

AGL-DD API Description Model

schema-agl-api-v2.json | can-sginal-api-v2.json | can-sginal-api-v2.c

```c
static struct afb_auth auths[] = {
  { .type = afb_auth_Permission, .text = "urn:AGL:permission:low-can:partner:read" },
  { .type = afb_auth_Permission, .text = "urn:AGL:permission:low-can:partner:write" },
  { .type = afb_auth_And, .first = &auths[0], .next = &auths[1] }
};

static const struct afb_verb_v2 verbs_v2[] = {
    {.verb = "subscribe", .callback = f_subscribe, .auth = &auths[2], .session = AFB_SESSION_CHECK,    },
    {.verb = "unsubscribe", .callback = f_unsubscribe, .auth = &auths[2], .session = AFB_SESSION_CHECK,},
    {.verb = NULL }
};

/* the integer data used by binder for the verbosity of the binder */
int afbBindingV2verbosity;

/* the structure for describing the binder */
const struct afb_binding_v2 afbBindingV2 = {
    .api = "low-can", .specification = /* the JSON description */ .verbs = verbs,
    .init = NULL    , .start = start_low_can, .onevent = NULL,
};
```

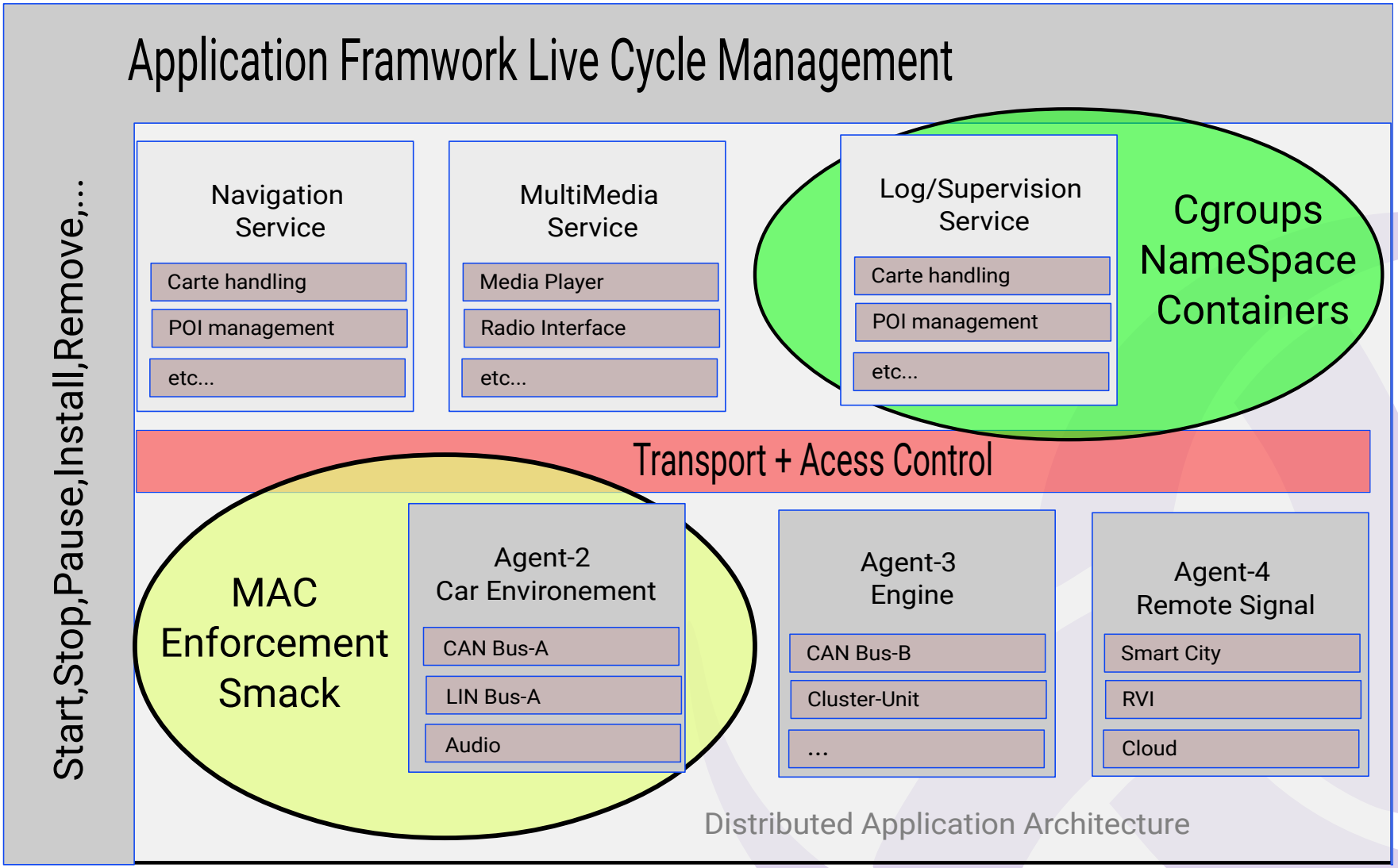
OpenAPI Binding Description

schema-agl-api-v2.json can-sginal-api-v2.json

```
1
2   {
3       "openapi": "3.0.0",
4       "$schema": "file:schema-agl-api-v2.json",
5       "info": {
6           "description": "Can Signal Low Level API", "title": "low-can", "version": "2.0"
7       },
8       "servers": [{
9               "url": "ws://{host}:{port}/api/low-can", "description": "The API server.",
10              "variables": { "host": { "default": "localhost" }, "port": {"default": "1234"}
11              },
12              "X-afb-events": [
13                  { "$ref": "#/components/schemas/afb-event" }
14              ]
15          }
16      ],
17      "components": {
18          "schemas": {
19              "afb-reply": {
20                  "properties": {
21                      "jtype": {
22                          "type": "string"
23                      },
24                      "request": {
25                          "$ref": "#/components/schemas/afb-request"
26                      },
27                      "response": {
28                          "type": "object"
29                      }
```

AGL-DD Security Model

Not ready yet for Cloud SaaS



Why OpenID Connect ?

- Inherit from SAML2 protocols models
  - Over 10 years of lesson learn on massive deployment
  - Support of privacy and data protection built in
- Simpler to deploy than SAML2
  - Low level based on REST, SSL, JSON
  - High Level based on oAuth2, JWT *(Json Web Token)*,JWS*(Json Web Signature)*
  - Toolkit available in multiple languages
  - Supported natively or flavoured by many internet providers (Facebook, Google, Paypal, …), but also by many governments
- Community
  - Active & well known
  - Open to custom profile
  - Ready to work with AGL

OpenID members

Sustaining Corporate Members

Google KDDI Microsoft

NRI The Office of the National Coordinator for Health Information Technology ORACLE

PayPal PingIdentity Symantec

Corporate Members

10Duke aplcomp Auth0 AYOY Coherent Cloud

Deutsche Telekom FORGEROCK gigya gluu GSMA

IDCIA intuit janrain loginradius mydex

nextiva okta onelogin Peercraft Ribose

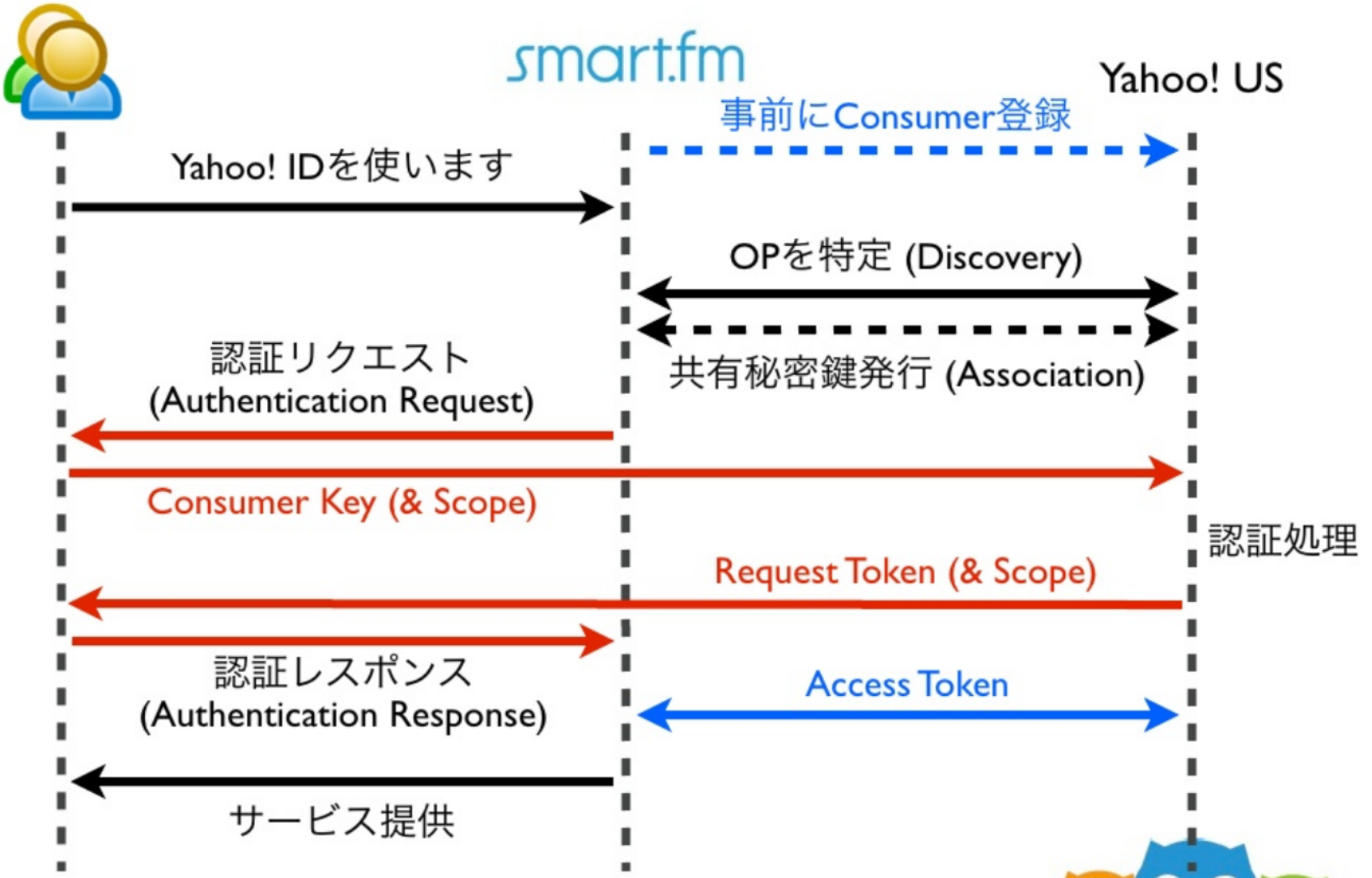
RSA salesforce.com SANDA technologies SECURE KEY SyncForce let the brand rule

TrustX viewds identity solutions vmware

Companies involve OpenId Development

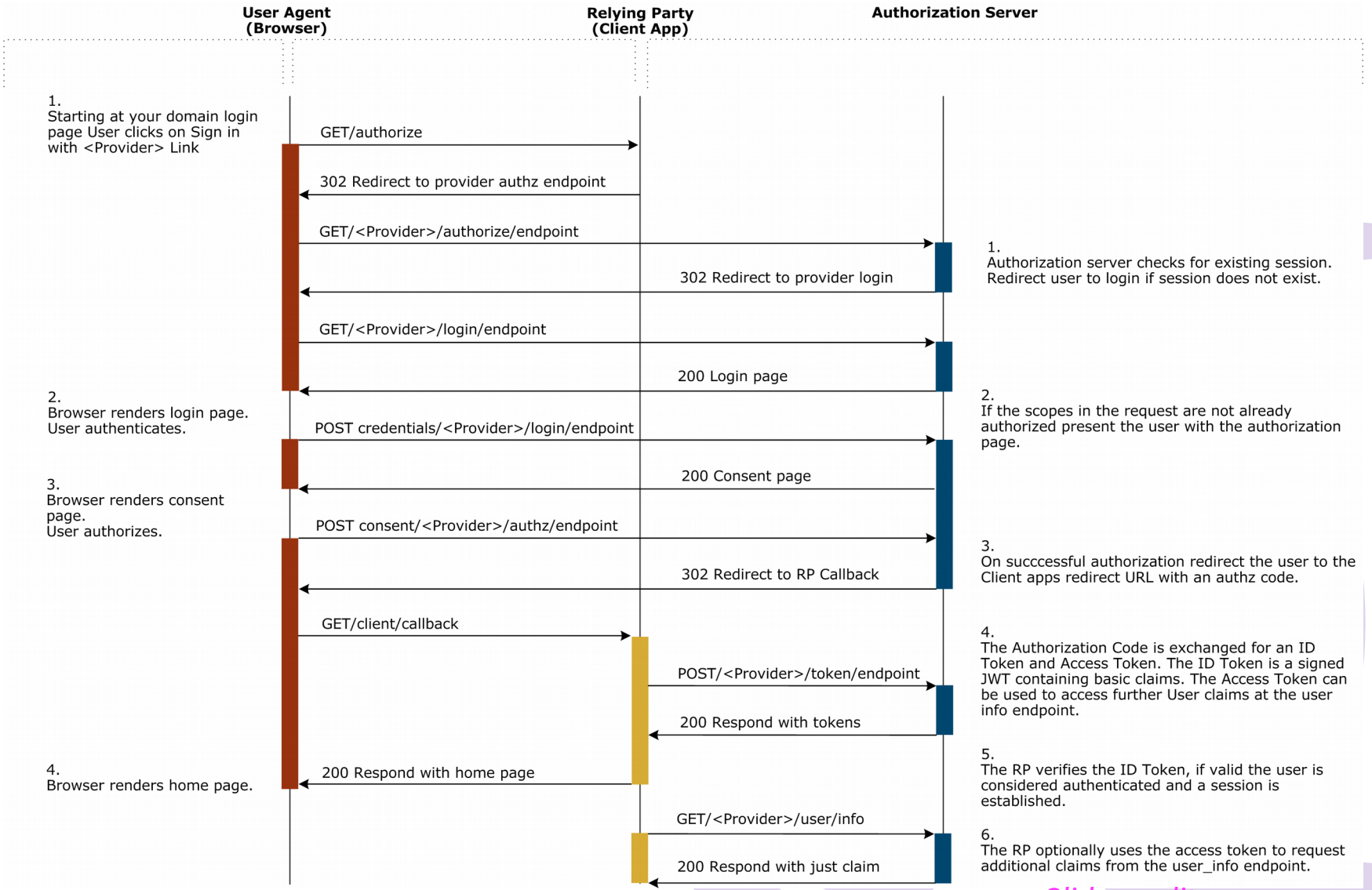
Contributors included a diverse international representation of industry, academia and independent technology leaders: AOL, Deutsche Telekom, Facebook, Google, Microsoft, Mitre Corporation, mixi, Nomura Research Institute, Orange, PayPal, Ping Identity, Salesforce, Yahoo! Japan, among other individuals and organizations.

OpenID Simple Flow



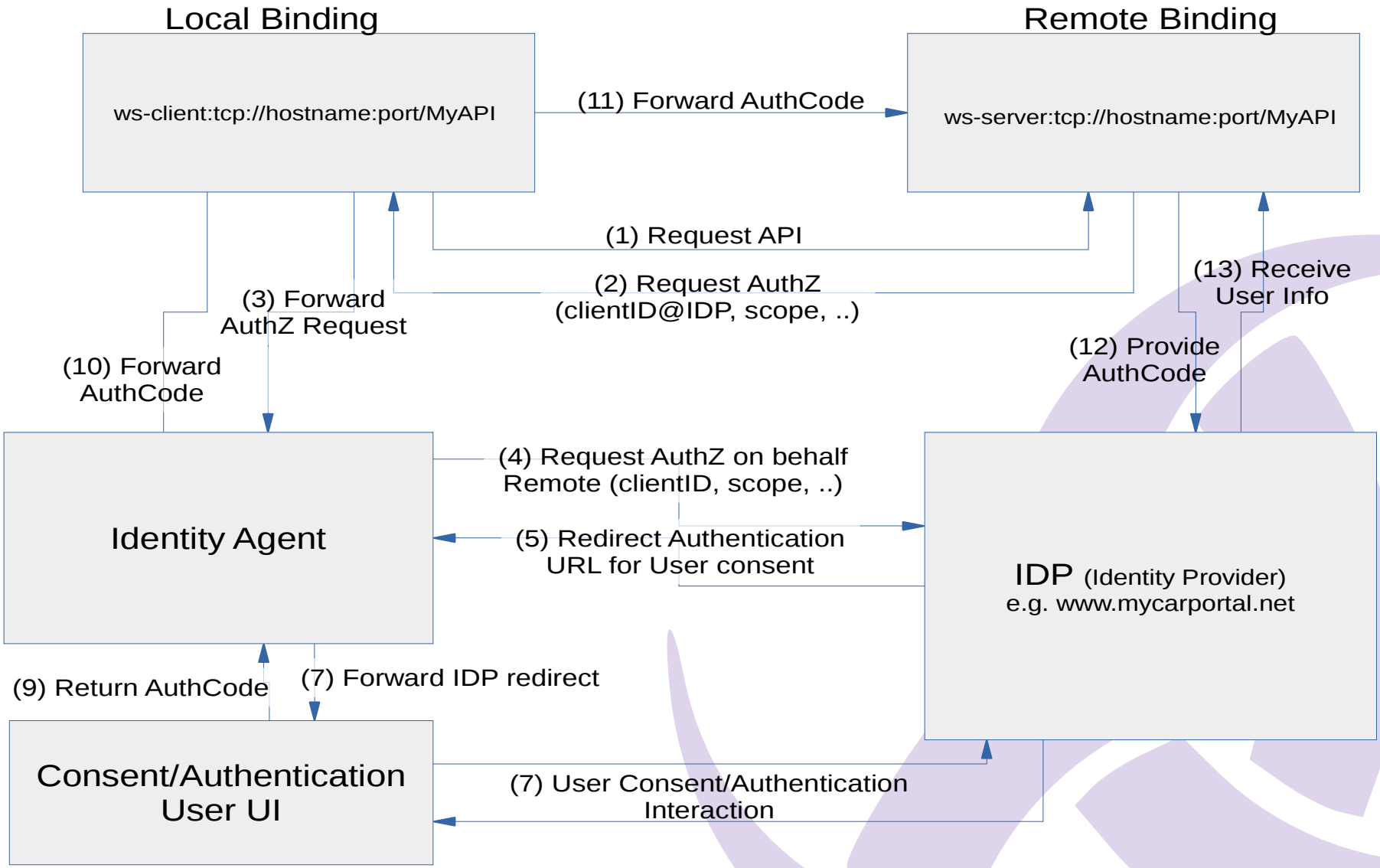
Slide Credit Nov Matake, OpenID Japan

OpenID Connect Detail Flow



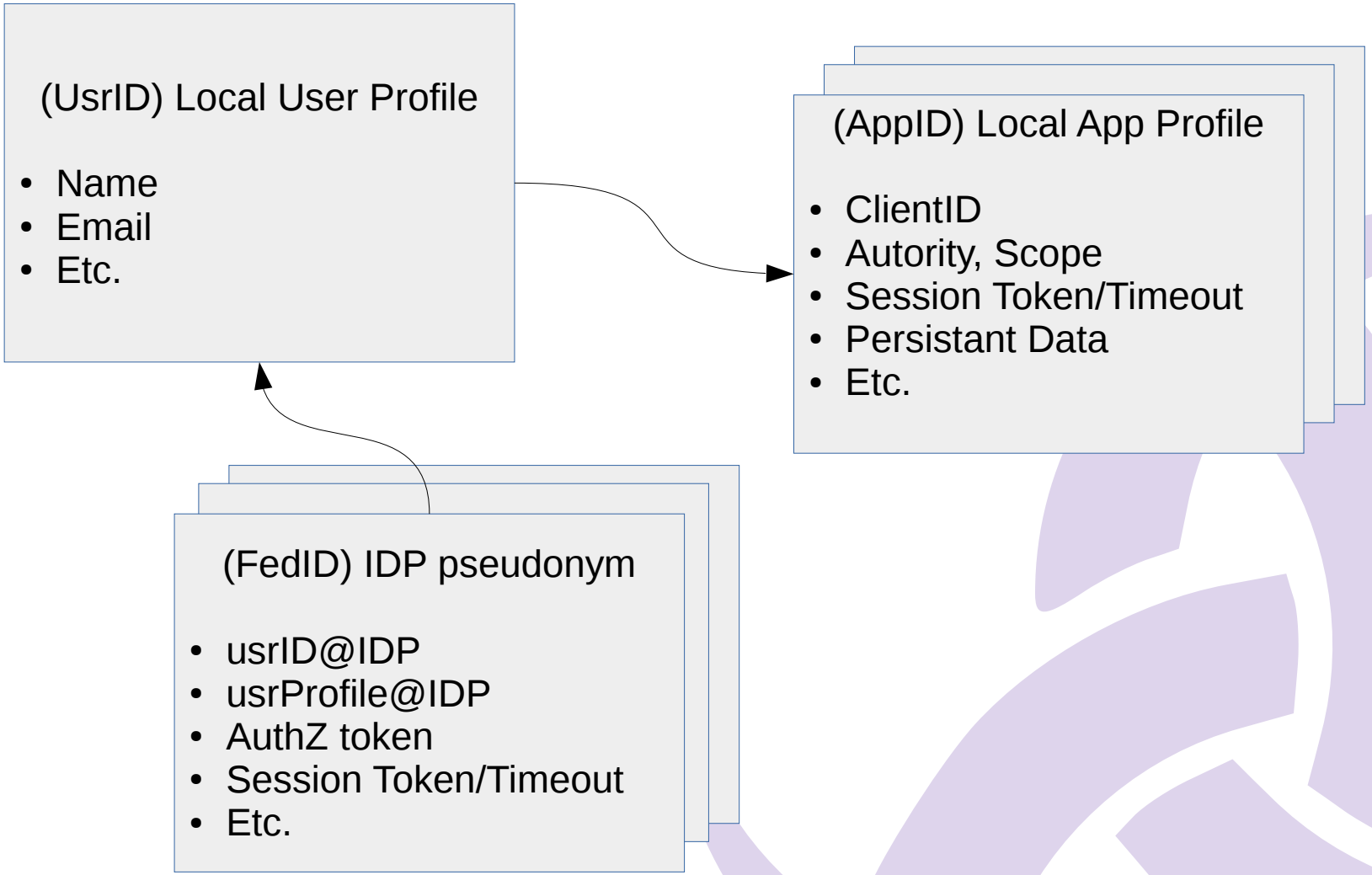
Slide credit axway.com

Global Architecture



Data Model

Identity Agent Data Structure



Work To Be Done

- AGL Binding Protocol Extension
  - Native integration of OpenID Connect
  - Support for use interaction (consent, authentication)
- Access Controls
  - LOA
  - Hook for roles/group
  - Link with existing privilege model
- Authentication
  - Webview for Authentication/Consent
  - Map authentication devices (NFC, FiDO)
  - Define API for custom API

Further Information

- Specifications: http://openid.net/connect
- Introduction http://openid.net/connect/faq

- Deep dive in protocols: *[Following videos are pretty technical, while they relates to one of pevious live project they may help to understand OpenID protocols. Please ignore 1st videos which are related to the installation of the project, last ones demonstrate protocols through a live debug session]*
    - French http://breizhme.net/fr/video-technique (2nd & 3rd videos)
    - English http://breizhme.net/en/ (last video)

Warning: When searching for information you should be aware that OpenID-connect has 100% different from OpenID-v1/v2.