@Web Conference

13 Oct 2021

FAPI-SIG Community 28th Meeting

Table of Contents

Major Topics

Discussion :

RAR & Dynamic Scopes

Working Items Status

PROPOSED DRAFT

Major Topics

Major Topics

● Open Banking Brasil FAPI 1.0 Security Profile draft version up (ID2 -> ID3).

- ID3 / published on 27 September 2021 :

  https://openbanking-brasil.github.io/specs-seguranca/open-banking-brasil-financial-api-1_ID3.html

- ID2 / published on 2 September 2021 :

  https://openbanking-brasil.github.io/specs-seguranca/open-banking-brasil-financial-api-1_ID2.html

- ID1 (keycloak 15 based on) / published on ??? :

  https://openbanking-brasil.github.io/specs-seguranca/open-banking-brasil-financial-api-1_ID1.html

  -> Not Found

Major Topics

● Changing the way of contribution's discussion

- Proposing features :

  google keycloak-dev ML to github keycloak repository's discussion

- Details of a proposal :

  github keycloak-community repository's PR (not changed)

- Low-level implementation discussions : keycloak-dev

  google keycloak-dev ML (not changed)

Major Topics

● Revised Client Policies

Its discussion has been moved from ML to github keycloak repository's discussion

https://github.com/keycloak/keycloak/discussions/8558

● Automated Conformance Test Run Environment has been updated.

• Conformance Suite : v4.1.21 to v4.1.29

• Keycloak : 15.0.1 to 15.0.2 (RH-SSO 7.5 based on)

• All FAPI 1.0 Advanced, FAPI-CIBA and OBB-FAPI 1.0 tests has been passed.

Discussion : RAR & Dynamic Scopes

Ongoing contributions with similar objectives

● Conveying a scope client expects to be authorized by a resource owner

- Dynamic : Need not to be registered in advance

- Rich : Can describe in detail a scope expected to be authorized by a resource owner

- Augment : Can be enriched by a resource owner

● Actual Implementation

- OAuth 2.0 Rich Authorization Requests (RAR) : by Internet Draft

  https://datatracker.ietf.org/doc/html/draft-ietf-oauth-rar

- Dynamic Scopes : by OBB-FAPI 1.0 ID2

  https://openbanking-brasil.github.io/specs-seguranca/open-banking-brasil-financial-api-1_ID2.html#section-7.1.2

- Parameterized Scopes : by FAPI 1.0 Lodging Intent
  https://bitbucket.org/openid/fapi/src/master/Financial_API_Lodging_Intent.md#markdown-header-631-parameterized-scope-values

- RAR : OAuth 2.0 Rich Authorization Requests

  - Contribution status : In progress as FAPI-SIG's activity

  - Details : github keycloak-community's PR

    https://github.com/keycloak/keycloak-community/pull/266

  - Implementation : prototype

    https://github.com/tnorimat/keycloak/pull/24

- Dynamic / Parameterized Scopes

  - Contribution status : In progress by some other contributor

  - Details : github keycloak discussion

    https://github.com/keycloak/keycloak/discussions/8532

PROPOSED DRAFT

Strategy in community

● RAR and Dynamic / Parameterized Scopes can be both treated.

  https://github.com/keycloak/keycloak/discussions/8486

● The following features need to be considered simultaneously.

- FAPI 2.0 Grant Management API

  current keycloak can only manage static scopes (registered in advance)

- Consent Screen Enhancement

  https://github.com/keycloak/keycloak/discussions/8495

  Enriching a scope by a resource owner

- Namespaced Roles

  https://github.com/keycloak/keycloak/discussions/8516

  Mapping a role to dynamic scopes

Working Items Status

Working Items

[Security Features]

<Common>

In Progress   OIDC Client's Public Key Management   Hitachi

     1st phase -> 2nd phase

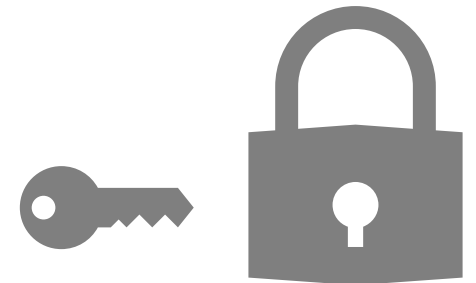In Progress   Client Policies Revised   Hitachi

[Security Features]

<SPA/Native App>

In Progress   OAuth 2.0 Demonstration of   Backbase
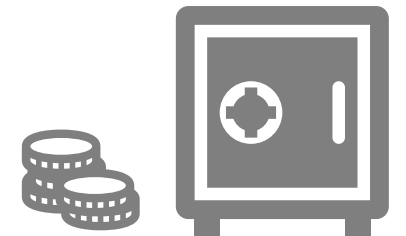
     Proof-of-Possession (DPoP)

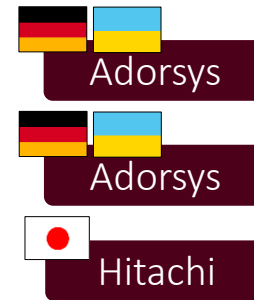[Security Features]

<High Level Security>

● FAPI 2.0 (baseline/advanced)

In Progress	Rich Authorization Request (RAR)	🇩🇪🇺🇦 Adorsys
In Progress	Grant Management API	🇩🇪🇺🇦 Adorsys
In Progress	Other requirements support	🇯🇵 Hitachi

[Market Specific Features]

<PSD2>

● Following eIDAS regulations

In Progress QWAC verification Adorsys
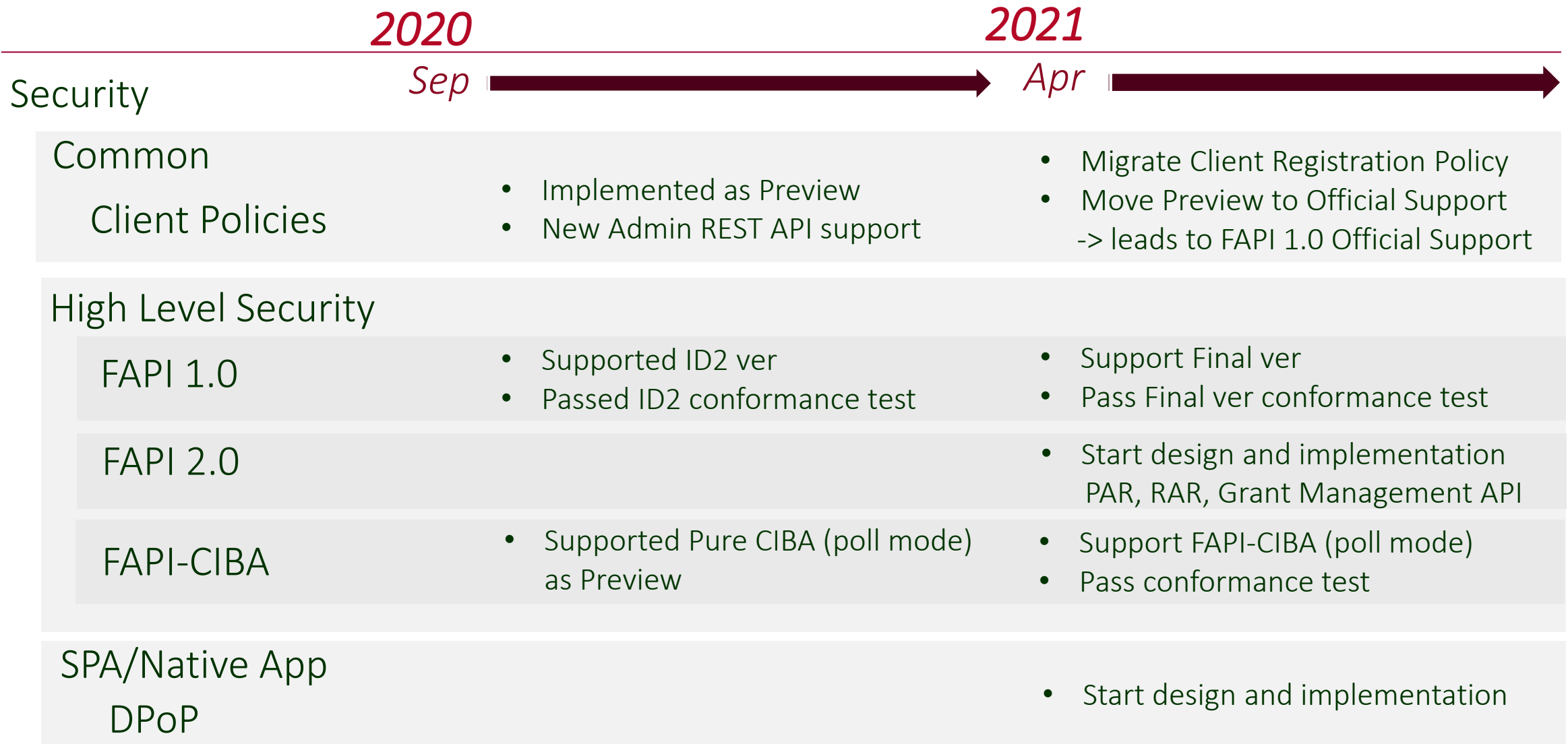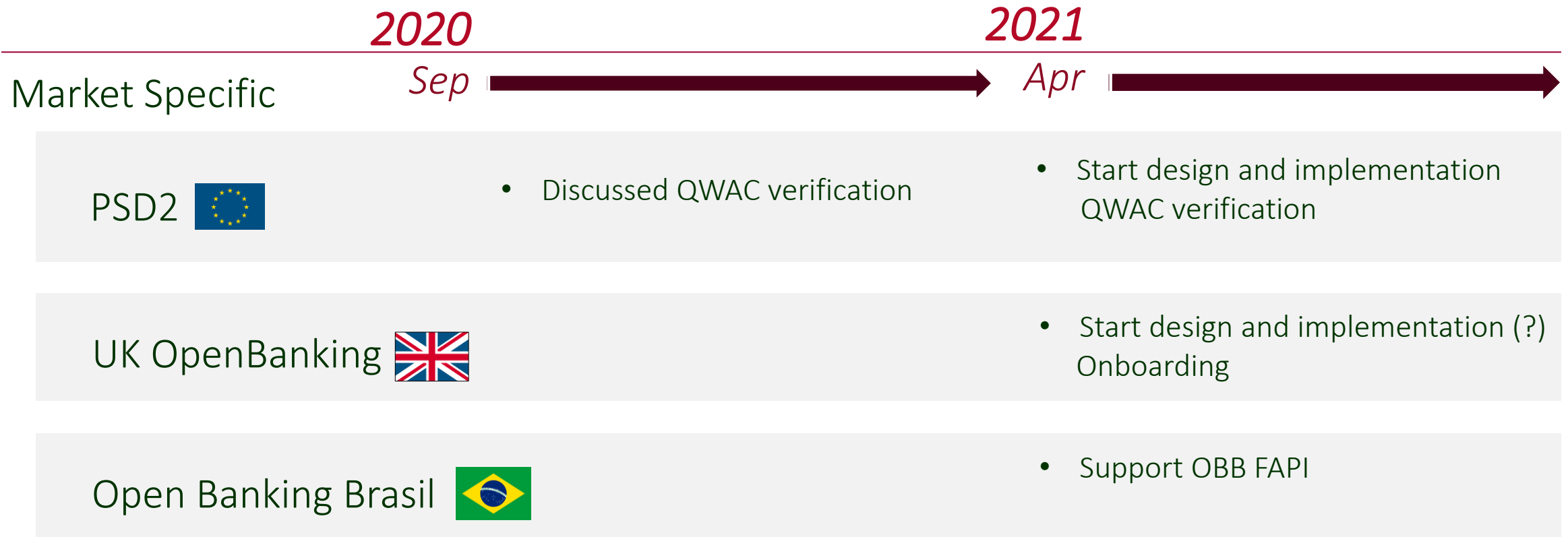
● Consent Management

<UK OpenBanking>

● Onboarding

• Software Statement Support

• Software Statement Assertion (SSA) Verification

Roadmap

Security

2020 — Sep ⟶ **2021** — Apr ⟶

Common

Client Policies
- Implemented as Preview
- New Admin REST API support
- Migrate Client Registration Policy
- Move Preview to Official Support
  -> leads to FAPI 1.0 Official Support

High Level Security

FAPI 1.0
- Supported ID2 ver
- Passed ID2 conformance test
- Support Final ver
- Pass Final ver conformance test

FAPI 2.0
- Start design and implementation
  PAR, RAR, Grant Management API

FAPI-CIBA
- Supported Pure CIBA (poll mode) as Preview
- Support FAPI-CIBA (poll mode)
- Pass conformance test

SPA/Native App

DPoP
- Start design and implementation

PROPOSED DRAFT

Roadmap

Market Specific

2020   **2021**

Sep   Apr

PSD2 🇪🇺

- Discussed QWAC verification
- Start design and implementation QWAC verification

UK OpenBanking 🇬🇧

- Start design and implementation (?) Onboarding

Open Banking Brasil 🇧🇷

- Support OBB FAPI

END