FAPI-SIG Community 18th Meeting

@Web Conference

12 May 2021

PROPOSED DRAFT

Table of Contents

Major Topics

Status Updates from 17th Meeting

   Common Security Features

   Client Policies

   FAPI 1.0

   FAPI 2.0

   FAPI-CIBA

   SPA/Native App

   Market Specific Features - PSD2

Help Wanted

Working Items Status

PROPOSED DRAFT

Major Topics

Major Topics

- **FAPI 1.0**

  The FAPI specification's version gap has been found.
  KC13 : FAPI 1.0 Advanced Final vs Conformance Test : FAPI RW ID2
  Try to make KC14 support both Final and ID2.

- **FAPI 2.0**

  Review of PR for PAR design document is still in progress.
  Review of PR for RAR design document is still in progress.
  Review of PR for Grant Management API design document is still in progress.

- **FAPI-CIBA**

  KC13 has supported OIDC CIBA.

  Try to add FAPI-CIBA feature onto keycloak to pass FAPI-CIBA conformance tests and get its certificate.

  Wait for review : FAPI-CIBA Signed Authentication Request support

Major Topics

- Common Security Features

  Wait for review : PR for OIDC Client's Public Key Management 1st phase

- Client Policies

  Refining client policies for KC14 is in progress by RH KC dev team.

- SPA/Native App

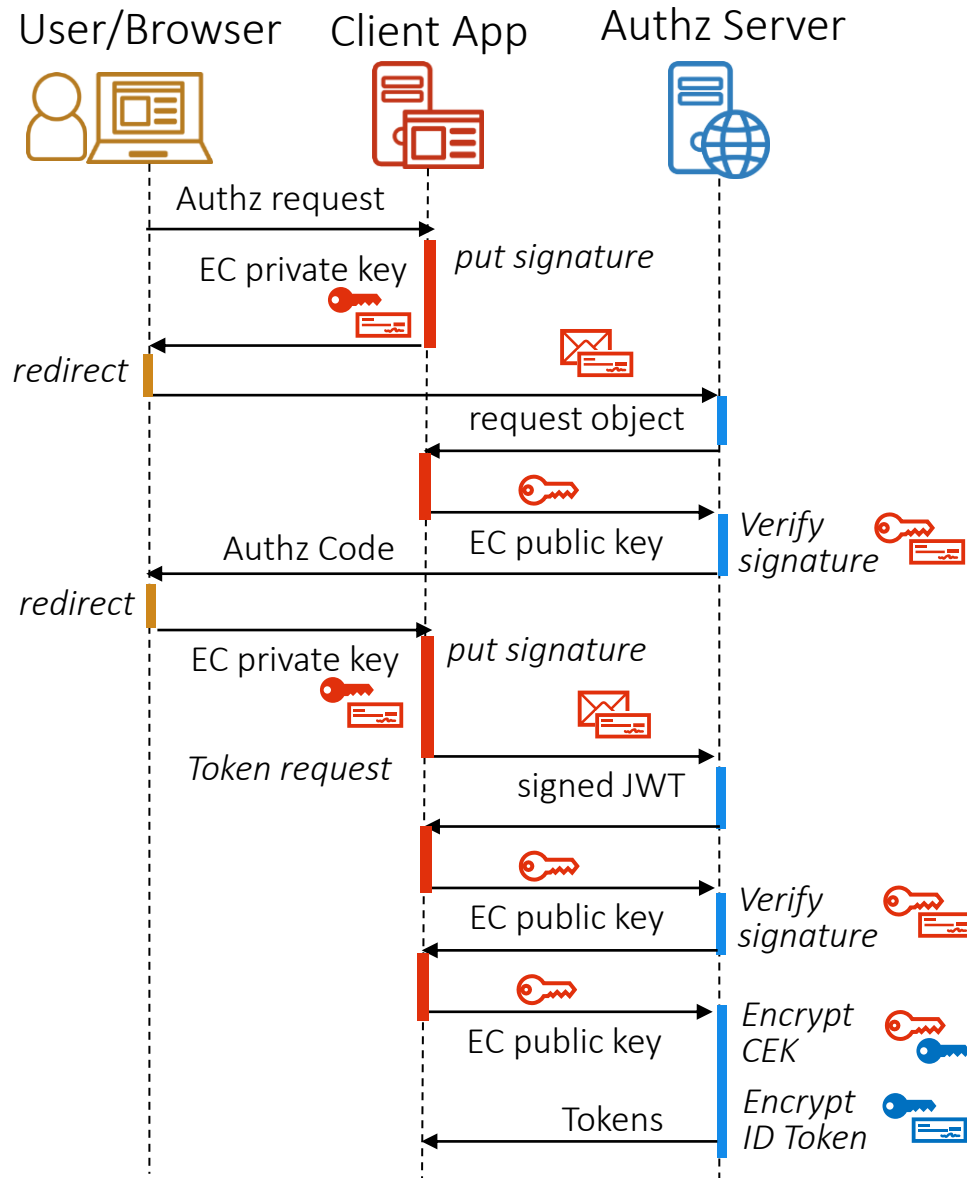 Review of PR for DPoP design document is still in progress.

- PSD2

  Review of PR for MTLS validation extension design document is still in progress.

Status Updates from 17th Meeting Common Security Features

OIDC Client's Public Key Management

Make it ease to manage and use client's public keys of ECDSA and RSASSA-PSS.

[JIRA Ticket]

KEYCLOAK-10462 Improve support for setting keys for OIDC clients

[Specification]

https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/OIDC-Client-Keys/FAPI-SIG-Annex_OIDC_Client_Keys.pdf

[Implementation]

PR sent as 1st step :

KEYCLOAK-17491 Move the key settings to the new Keys tab

https://github.com/keycloak/keycloak/pull/7874

https://github.com/keycloak/keycloak-documentation/pull/1143

PROPOSED DRAFT

Status Updates from 17th Meeting Client Policies

PROPOSED DRAFT

Client Policies Refinement toward KC14

In Progress Support existing Admin UI + revise JSON representation

🔥 KEYCLOAK-14209 Client Policy : UI on old Admin Console

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-14209

GH PR: https://github.com/keycloak/keycloak/pull/7969

dev-ml: https://groups.google.com/g/keycloak-dev/c/iMu1oz6yFdM

In Progress Preset profiles for FAPI

🔥 KEYCLOAK-14208 Client Policy : Pre-set Policies (including FAPI preset policies)

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-14208

GH PR: N/A

dev-ml: https://groups.google.com/g/keycloak-dev/c/Hyzib1Tm3zY

PROPOSED DRAFT

Client Policies Refinement

🚫 Support new Admin UI `Not available new admin console UI`

- KEYCLOAK-16138 Client Policy : Support New Admin Console UI (Design)

- KEYCLOAK-16847 Client Policy : Support New Admin Console UI (Implementation)

⚫ Complete Client Registration Policies Migration

- KEYCLOAK-16806 to 16812 Implement existing client registration policies as client policies

- KEYCLOAK-15534 Client Policy : Implement Existing Client Registration Policies as Client Policies

  - KEYCLOAK-16806 to 16812

Status Updates from 17th Meeting
FAPI 1.0

Version Gap : KC vs Conformance Test

Test/KC		FAPI Spec Version	
		FAPI-RW ID2	FAPI 1.0 Advanced Final
FAPI Conformance Suite	release-v4.1.10	X	-
	release-v4.1.11	X	X?
Keycloak	KC12	X	-
	KC13	-	X
	KC14	X?	X?

Not sure when release-v4.1.11 is released and whether release-v4.1.11 support FAPI 1.0 Advanced Final or not.

KC14 tries to support both FAPI-RW ID2 and FAPI 1.0 Advanced Final

Status Updates from 17th Meeting
FAPI 2.0

PROPOSED DRAFT

Components of FAPI 2.0 Advanced

In Progress   OAuth 2.0 Pushed Authorization Requests (PAR)

🔥 Design Document : https://github.com/keycloak/keycloak-community/pull/255

🔥 Implementation : (WIP) https://github.com/tnorimat/keycloak/pull/20

In Progress OAuth 2.0 Rich Authorization Requests (RAR)

🔥 Design Document : https://github.com/keycloak/keycloak-community/pull/266

- Implementation

In Progress Grant Management for OAuth 2.0

🔥 Design Document : https://github.com/keycloak/keycloak-community/pull/265

- Implementation

Status Updates from 17th Meeting
FAPI-CIBA

Upstreaming CIBA Support

Completed   Support OIDC CIBA

✔   KEYCLOAK-12137 OpenID Connect Client Initiated Backchannel Authentication (CIBA)

   JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-12137

   GH PR: https://github.com/keycloak/keycloak/pull/7679

In Progress   Support signed authentication request

   KEYCLOAK-17936 FAPI-CIBA : support Signed Authentication Request

   JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-17936

   GH PR: https://github.com/keycloak/keycloak/pull/8006

                  . . .

Status Updates from 17th Meeting
SPA/Native App

PROPOSED DRAFT

Holder-of-Key Bound Token in SPA/Native App

In Progress   OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)

🔥 Design Document : https://github.com/keycloak/keycloak-community/pull/254

- Implementation

Status Updates from 17$^\text{th}$ Meeting Market Specific Features – PSD2

PROPOSED DRAFT

QWACS Verification et al.

In Progress MTLS Validation Extension (MTLS_Ext)

🔥 Design Document : https://github.com/keycloak/keycloak-community/pull/267

- Implementation

Help Wanted

Help Wanted

#1. OIDC Client's Public Key Management

KEYCLOAK-17491 Move the key settings to the new Keys tab

To : KC Dev Member   FAPI-SIG Member

What : Review   Merge   Review

https://github.com/keycloak/keycloak/pull/7874

https://github.com/keycloak/keycloak-documentation/pull/1143

#2. Support existing Admin UI

KEYCLOAK-14209 Client Policy : UI on old Admin Console

To : FAPI-SIG Member

What : Review

https://github.com/keycloak/keycloak/pull/7969

PROPOSED DRAFT

#3. OAuth 2.0 Pushed Authorization Requests (PAR)

To :   `KC Dev Member`   `FAPI-SIG Member`

What :   `Review`   `Merge`   `Review`

Design Document : https://github.com/keycloak/keycloak-community/pull/255

#4. OAuth 2.0 Rich Authorization Requests (RAR)

To :   `KC Dev Member`   `FAPI-SIG Member`

What :   `Review`   `Review`

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

#5. Grant Management for OAuth 2.0

To :   `KC Dev Member`   `FAPI-SIG Member`

What :   `Review`   `Review`

Design Document : https://github.com/keycloak/keycloak-community/pull/265

PROPOSED DRAFT

Help Wanted

#6 OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)

To :   `KC Dev Member`   `FAPI-SIG Member`

What : `Review`   `Review`

Design Document : https://github.com/keycloak/keycloak-community/pull/254

#7 MTLS Validation Extension (MTLS_Ext)

To :   `KC Dev Member`   `FAPI-SIG Member`

What : `Review` `Merge` `Review`

Design Document : https://github.com/keycloak/keycloak-community/pull/267

Working Items Status

[Security Features]

<Common>

`In Progress` OIDC Client's Public Key Management

🇯🇵 Hitachi

● Client Policies

`Completed` New Admin REST API in JSON Representation

🇯🇵 Hitachi

`In Progress` Admin Console UI + Refine JSON Representation

🇨🇿 Red Hat

- Completing Client Registration Policies Migration

<High Level Security>

● FAPI 1.0 (baseline/advanced)

`Completed` Final version support

🇯🇵 Hitachi

`In Progress` Passing conformance tests for final version

🇯🇵 Hitachi
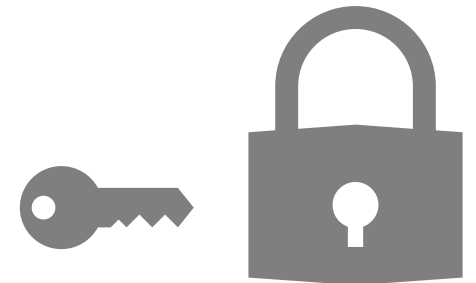
[Security Features]

<High Level Security>

● FAPI 2.0 (baseline/advanced)

| In Progress | Pushed Authorization Request (PAR) | Adorsys |

| In Progress | Rich Authorization Request (RAR) | Adorsys |

| In Progress | Grant Management API | Adorsys |

● FAPI-CIBA

NEW | Completed | OIDC CIBA | Hitachi |

NEW | In Progress | FAPI-CIBA : Signed Authentication |

<SPA/Native App>

| In Progress | OAuth 2.0 Demonstration of Proof-of-Possession (DPoP) | Backbase |
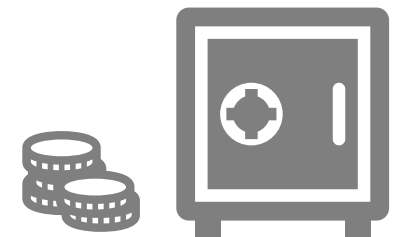
[Market Specific Features]

<PSD2> 🇪🇺

● Following eIDAS regulations

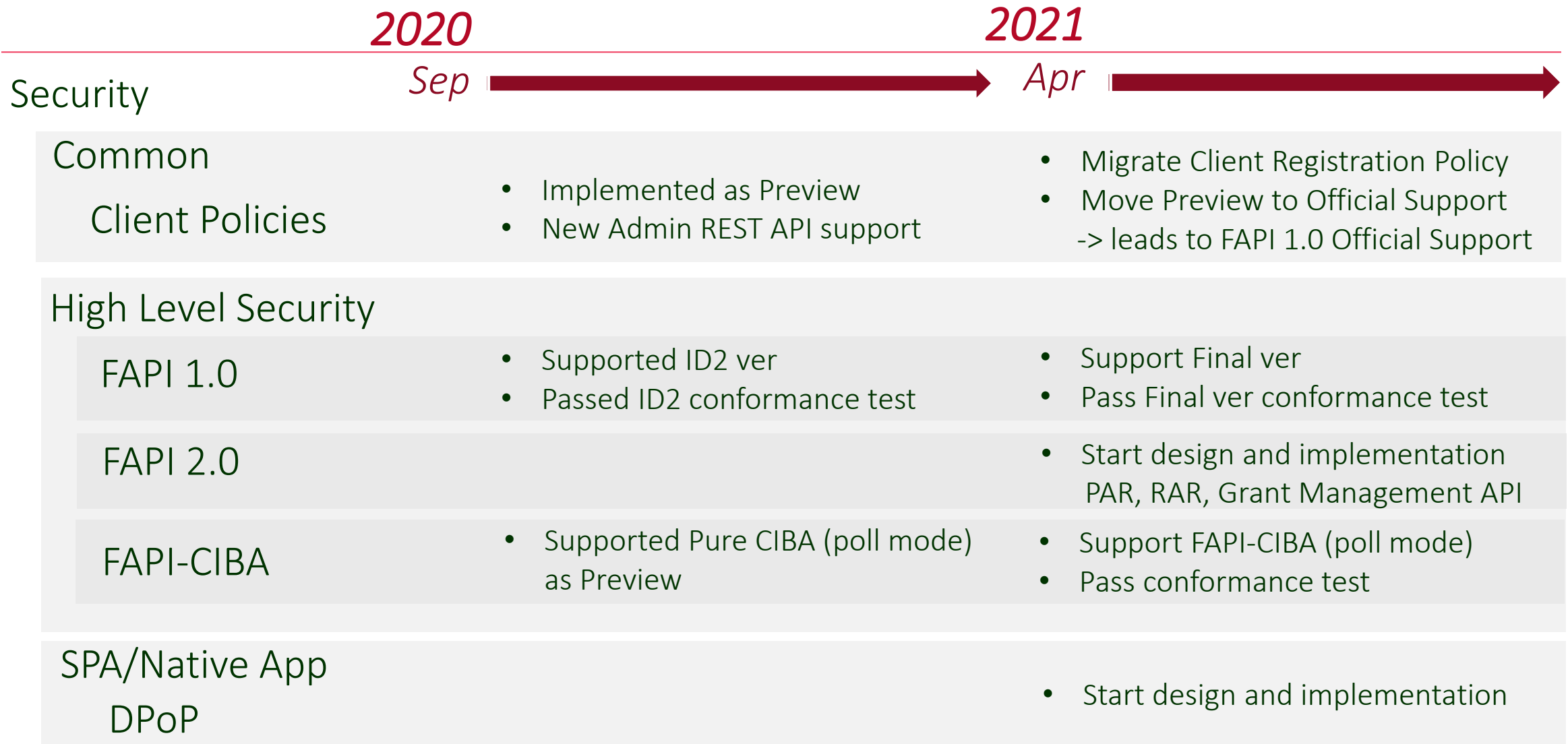In Progress QWAC verification 🇩🇪🇺🇦 Adorsys
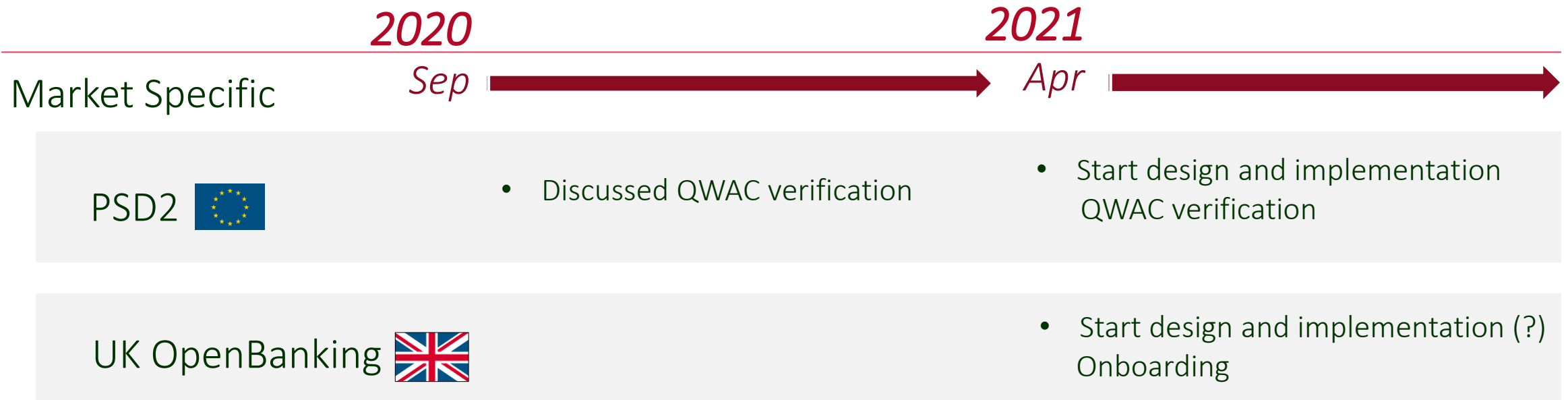
● Consent Management

<UK OpenBanking> 🇬🇧

● Onboarding

- Software Statement Support

- Software Statement Assertion (SSA) Verification

Roadmap

	2020	2021
Security	Sep →	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

2020   **2021**

Sep ➤   *Apr* ➤

Market Specific

PSD2 🇪🇺

- Discussed QWAC verification
- Start design and implementation QWAC verification

UK OpenBanking 🇬🇧

- Start design and implementation (?) Onboarding

END