

@Web Conference  
9 Jun 2021

# FAPI-SIG Community 20<sup>th</sup> Meeting

# Table of Contents

Major Topics

Status Updates from 19<sup>th</sup> Meeting

Common Security Features

Client Policies

FAPI 1.0

FAPI 2.0

FAPI-CIBA

SPA/Native App

Market Specific Features - PSD2

Working Items Status

# Major Topics

# Major Topics

- FAPI 1.0
  - FAPI 1.0 Baseline/Advanced support are available as default client profile.
- FAPI 2.0
  - [PAR]
    - Ready for sending PR to keycloak upstream.
  - [RAR]
    - Review of PR for design document is still in progress.
    - Review of PR for prototype codes is still in progress.
  - [Grant Management]
    - Review of PR for design document is still in progress.
    - Review of PR for prototype codes is still in progress.
- FAPI-CIBA
  - Wait for review : FAPI-CIBA Signed Authentication Request support

# Major Topics

- Common Security Features

PR for OIDC Client's Public Key Management 1<sup>st</sup> phase has been merged.

PR for OIDC Client's Public Key Management 2<sup>nd</sup> phase is waiting for its review.

- Client Policies

Changed from preview feature to default feature.

- 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.

Review of PR for MTLS validation extension prototype codes is still in progress.

# Status Updates from 19<sup>th</sup> Meeting

## Common Security Features

# OIDC Client's Public Key Management

Completed

Phase-1/4 Add key setting UI

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

Wait for Review

Phase-2/4 Allow to register client public key for ECDSA/RSASSA-PSS



KEYCLOAK-18341 Support JWKS OAuth2 Client Metadata in the "by value" key loading method

JIRA Ticket: <https://issues.redhat.com/browse/KEYCLOAK-18341>

GH PR: <https://github.com/keycloak/keycloak/pull/7874>

GH PR: <https://github.com/keycloak/keycloak-documentation/pull/1195>

Spec: [https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/OIDC-Client-Keys/FAPI-SIG-Annex\\_OIDC\\_Client\\_Keys.pdf](https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/OIDC-Client-Keys/FAPI-SIG-Annex_OIDC_Client_Keys.pdf)

# Status Updates from 19<sup>th</sup> Meeting

## Client Policies



# Client Policies Refinement toward KC14

Completed Preview to Default feature

✓ KEYCLOAK-17939 Enable Client policies feature by default

JIRA Ticket: <https://issues.redhat.com/browse/KEYCLOAK-17939>

GH PR: <https://github.com/keycloak/keycloak/pull/8093>

◆ Client Policies Practical Guide has been updated.

<https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/ClientPolicies/ClientPoliciesPracticalGuide.pdf>

# Status Updates from 19<sup>th</sup> Meeting

## FAPI 1.0

# FAPI as default client profile

Completed

Provide FAPI profile as default

✓ KEYCLOAK-14208 Default client profiles for FAPI

GH PR: <https://github.com/keycloak/keycloak/pull/8093>

providing default profiles for both FAPI 1.0 Basic and Advanced Final

-> keycloak's admin need not create these FAPI profiles by themselves.

# Status Updates from 19<sup>th</sup> Meeting

## FAPI 2.0

# Components of FAPI 2.0 Advanced

In Progress

OAuth 2.0 Pushed Authorization Requests (PAR)

🔥 KEYCLOAK-18353 Implement Pushed Authorization Request inside the Keycloak

JIRA Ticket: <https://issues.redhat.com/browse/KEYCLOAK-18353>

GH PR: TBD

# Components of FAPI 2.0 Advanced

## In Progress OAuth 2.0 Rich Authorization Requests (RAR)

- 🔥 Design Document : <https://github.com/keycloak/keycloak-community/pull/266>
- 🔥 Implementation : (WIP) <https://github.com/tnorimat/keycloak/pull/24>

## In Progress Grant Management for OAuth 2.0

- 🔥 Design Document : <https://github.com/keycloak/keycloak-community/pull/265>
- 🔥 Implementation : (WIP) <https://github.com/tnorimat/keycloak/pull/23>

# Status Updates from 19<sup>th</sup> Meeting

## FAPI-CIBA

# Upstreaming CIBA Support

## [Features]

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>

etc ...

## [Conformance tests]

In Progress

Pass conformance test for ID1



#65 FAPI-CIBA Conformance Test : Establish the way of running FAPI-CIBA OP poll w/ MTLS and w/ Private Key against CIBA Implementation

GH Issue: <https://github.com/keycloak/kc-sig-fapi/issues/65>



# Upstreaming CIBA Support

◆ CIBA Implementation Practical Guide has been updated.

[https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/FAPI-CIBA/CIBA\\_ImplPracticalGuide.pdf](https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/FAPI-CIBA/CIBA_ImplPracticalGuide.pdf)

# Status Updates from 19<sup>th</sup> Meeting

## SPA/Native App

# 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 19<sup>th</sup> Meeting

## Market Specific Features – PSD2

# QWACS Verification et al.

In Progress

MTLS Validation Extension (MTLS\_Ext)

- 🔥 Design Document : <https://github.com/keycloak/keycloak-community/pull/267>
- 🔥 Implementation : (WIP) <https://github.com/tnorimat/keycloak/pull/21>

# Working Items Status

# Working Items

## [Security Features]

### <Common>

**In Progress** OIDC Client's Public Key Management



Hitachi

NEW 1<sup>st</sup> phase -> 2<sup>nd</sup> phase

### ● Client Policies

NEW **Completed** Changed from preview feature to default



Red Hat

### <High Level Security>

### ● FAPI 1.0 (baseline/advanced)

**In Progress** Passing conformance tests for final version



Hitachi

NEW **Completed** Default client profiles for FAPI



Red Hat



## [Security Features]

### <High Level Security>

#### ● FAPI 2.0 (baseline/advanced)

**In Progress** Pushed Authorization Request (PAR)

NEW

- Ready for upstreaming PR

**In Progress** Rich Authorization Request (RAR)

**In Progress** Grant Management API

#### ● FAPI-CIBA

**In Progress** FAPI-CIBA : Signed Authentication

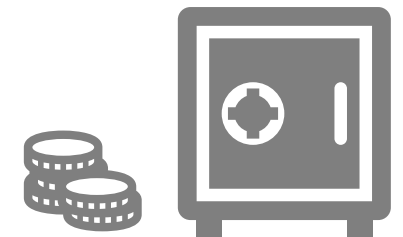
**In Progress** Passing conformance tests for ID1

### <SPA/Native App>

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

PROPOSED DRAFT


# Working Items





# Working Items

## [Market Specific Features]

<PSD2> 

- Following eIDAS regulations

 QWAC verification

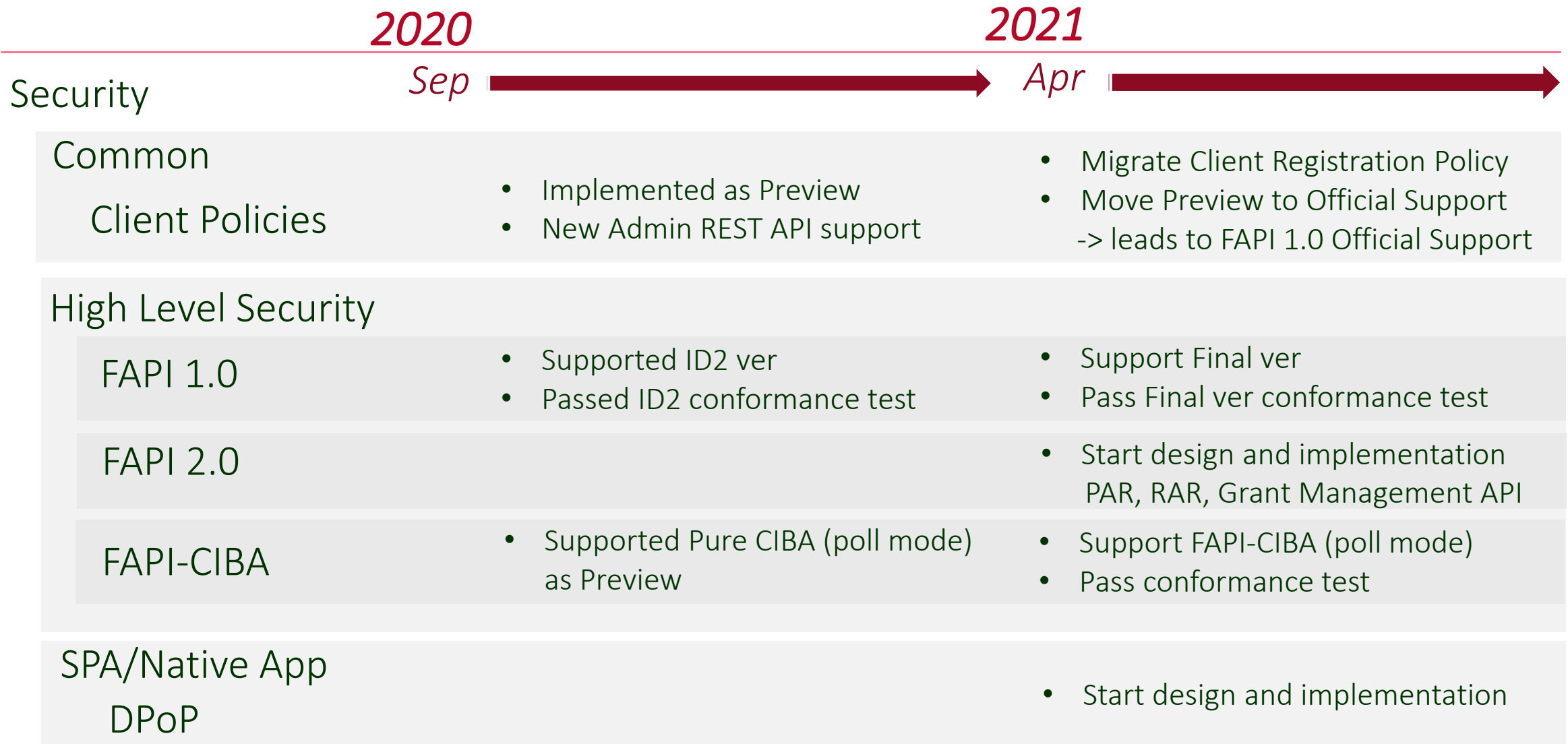


- Consent Management

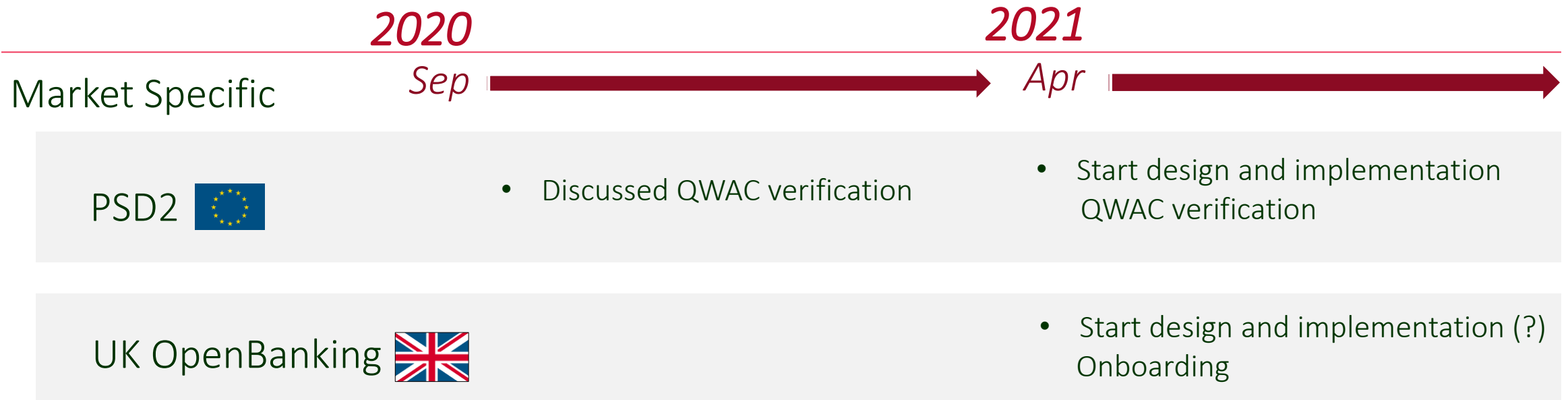
<UK OpenBanking> 

- Onboarding
  - Software Statement Support
  - Software Statement Assertion (SSA) Verification

# Roadmap



# Roadmap



END