

@Web Conference
28 Apr 2021

FAPI-SIG Community 17th Meeting

Table of Contents

Major Topics

Status Updates from 16th 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

Major Topics

Major Topics

- FAPI 1.0

PRs supporting additional security features for FAPI 1.0 final have been merged.
Confirmed keycloak passed conformance tests for FAPI 1.0 final.

- FAPI 2.0

Review of PR for PAR design document is in progress.

Review of PR for RAR design document is in progress.

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

- FAPI-CIBA

Review of PR supporting OIDC CIBA is still in progress.

Major Topics

- Common Security Features

PR for OIDC Client's Public Key Management 1st phase has been submitted.

- Client Policies

PRs revising existing client policies for JSON representation have been merged.

- SPA/Native App

Review of PR for DPoP design document is in progress.

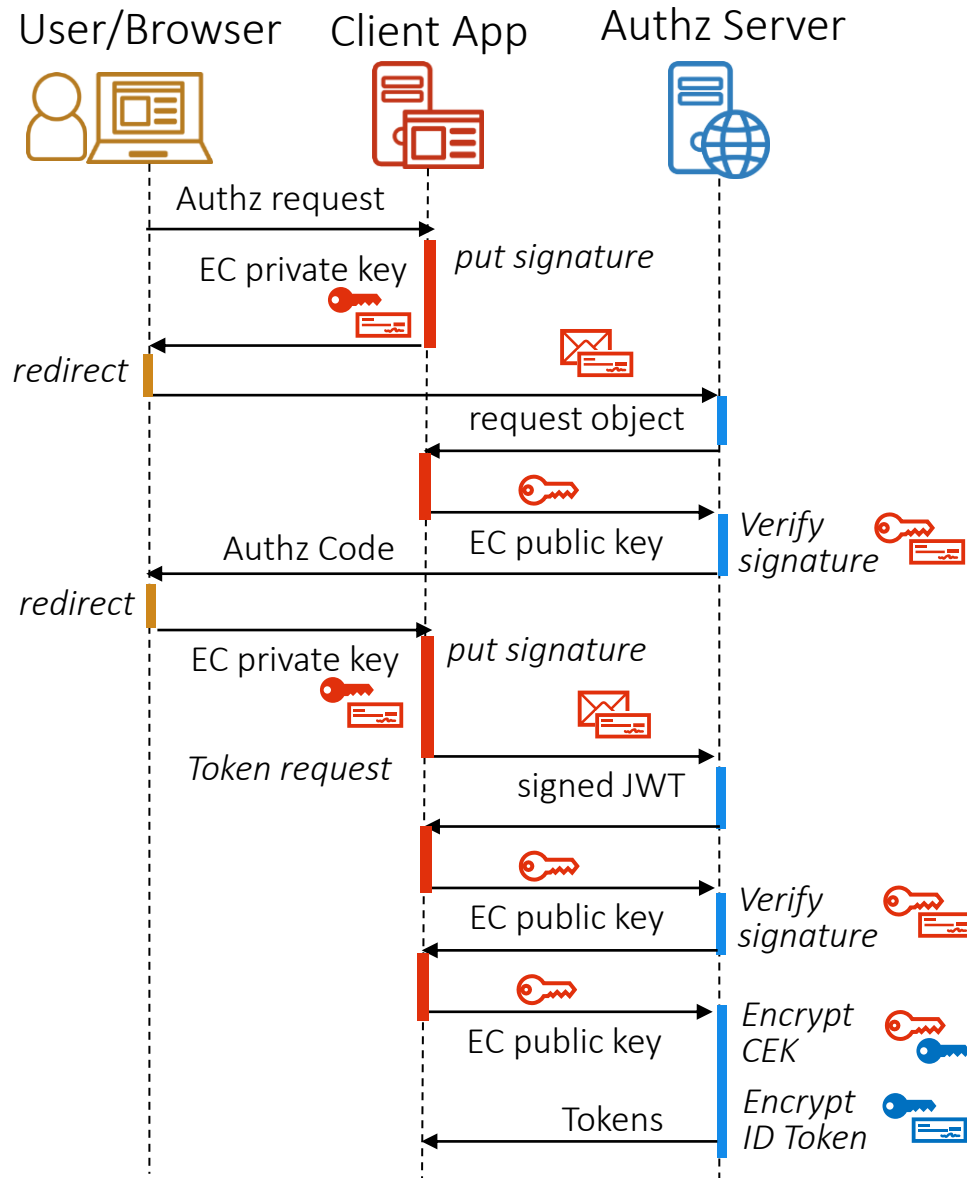
- PSD2

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

Status Updates from 16th Meeting

Common Security Features

OIDC Client's Public Key Management



PROPOSED DRAFT

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>

Status Updates from 16th Meeting

Client Policies

Client Policies Refinement

Completed

Support new Admin REST API in JSON Representation

- ✓ KEYCLOAK-16137 Client Policy : Support New Admin REST API (Design)
- ✓ KEYCLOAK-16805 Client Policy : Support New Admin REST API (Implementation)

In Progress

Support existing Admin UI

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

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

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 16th Meeting

FAPI 1.0

Following Final version of FAPI 1.0

Completed

Support additional security features for FAPI 1.0 final

- ✓ KEYCLOAK-17666 Client Policy - Executor : Limiting available period of Request Object
- ✓ KEYCLOAK-17667 Client Policy - Executor : Only Accept Confidential Client

In Progress

Confirm keycloak passed conformance tests for FAPI 1.0 final

- ✓ Run and pass conformance tests for final against keycloak on local environment
 - Conformance test version : release-v4.1.10
 - Test Plan : FAPI-RW-ID2 (and OpenBankingUK / CDR): Authorization server test (latest version)
 - Result : Passed both FAPI-RW OP w/Private Key and w/MTLS on each PS256 and ES256
- ⊘ Run and pass conformance tests for final against released keycloak (v13)

Not available KC13

Status Updates from 16th Meeting

FAPI 2.0

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 16th Meeting

FAPI-CIBA

Upstreaming CIBA Support

In Review



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

<https://github.com/keycloak/keycloak/pull/7679>

- CIBA Implementation based on its prototype (tnorimat/ciba-prototype)
- [#59](#) Use Only Auth Result Cache by Infinispan For CIBA Flow Session Binding
- [#60](#) Use Only Auth Result Cache on Communication with Decoupled Auth Server
- [#61](#) Token Request Throttling Information Not Cluster-wide Sync

● FAPI-CIBA

- [#57](#) support User Code

● FAPI-CIBA

- [#55](#) support id_token_hint

● FAPI-CIBA

- [#54](#) support login_hint_token

● FAPI-CIBA

- [#53](#) encrypt/decrypt login_hint

...



PROPOSED DRAFT

Status Updates from 16th 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 16th 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

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>

Help Wanted

#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>

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

Working Items

[Security Features]

<Common>

In Progress OIDC Client's Public Key Management



● Client Policies

Completed New Admin REST API in JSON Representation



In Progress Admin Console UI



- Completing Client Registration Policies Migration

<High Level Security>

● FAPI 1.0 (baseline/advanced)

Completed Final version support



In Progress Passing conformance tests for final version



Working Items

[Security Features]

<High Level Security>

- FAPI 2.0 (baseline/advanced)

In Progress Pushed Authorization Request (PAR)

In Progress Rich Authorization Request (RAR)

In Progress Grant Management API

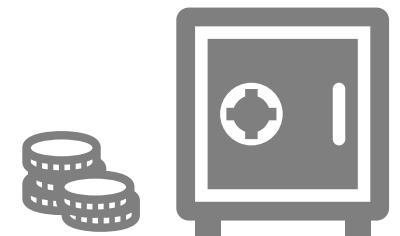
- FAPI-CIBA

In Progress OIDC Client Initiated Backchannel

Authentication Flow


<SPA/Native App>

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



Working Items

[Market Specific Features]

<PSD2> 

- Following eIDAS regulations

 QWAC verification



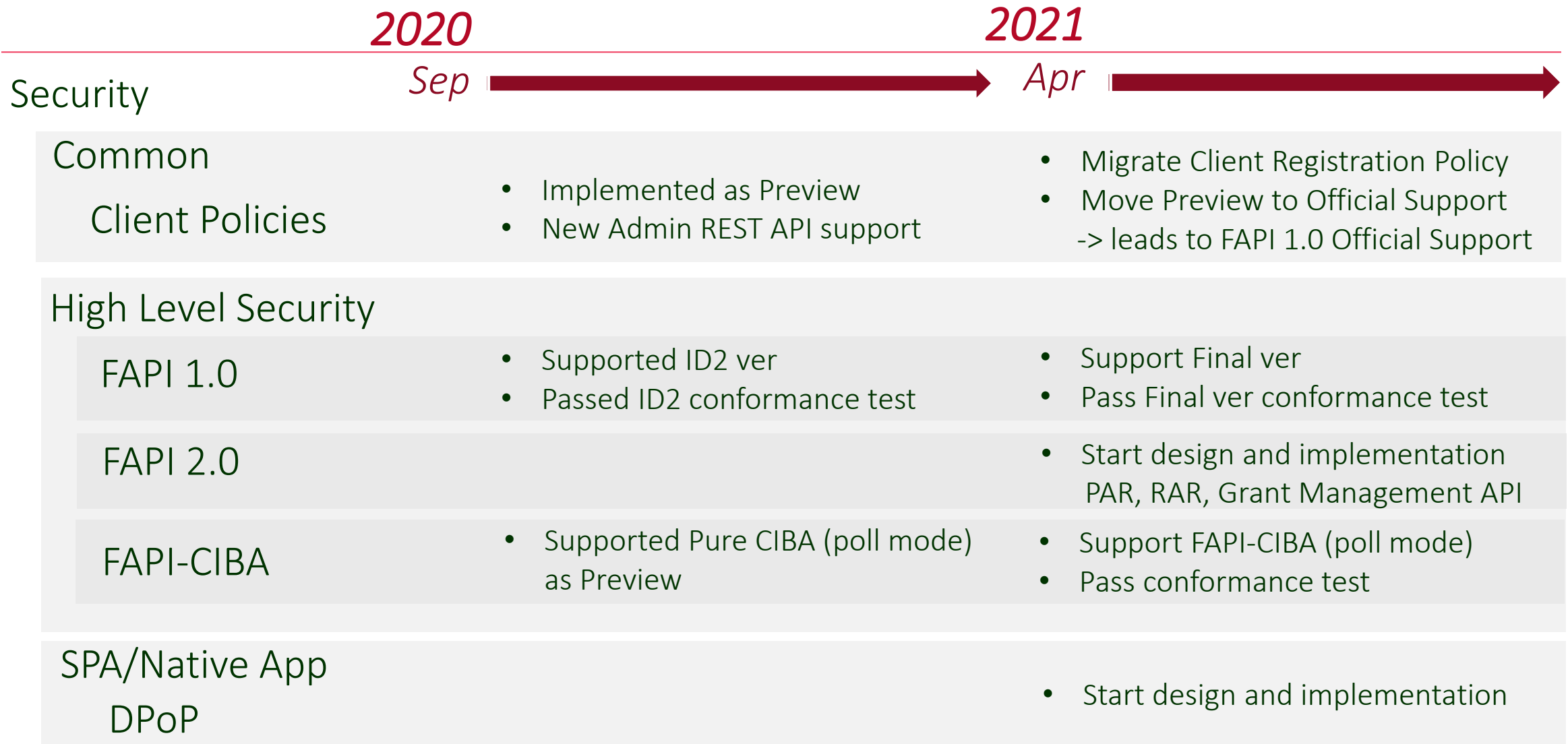
- Consent Management

<UK OpenBanking> 

- Onboarding

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

Roadmap



Roadmap

