FAPI-SIG Community 15th Meeting

@Web Conference

17 Mar 2021

PROPOSED DRAFT

Table of Contents

Major Topics

Follow-up of FAPI-RW

Status Updates from 14th Meeting

- FAPI-CIBA (poll mode)
- Client Policy Official Support

Proposing Working Items in FY 2021

PROPOSED DRAFT

Major Topics

Major Topics

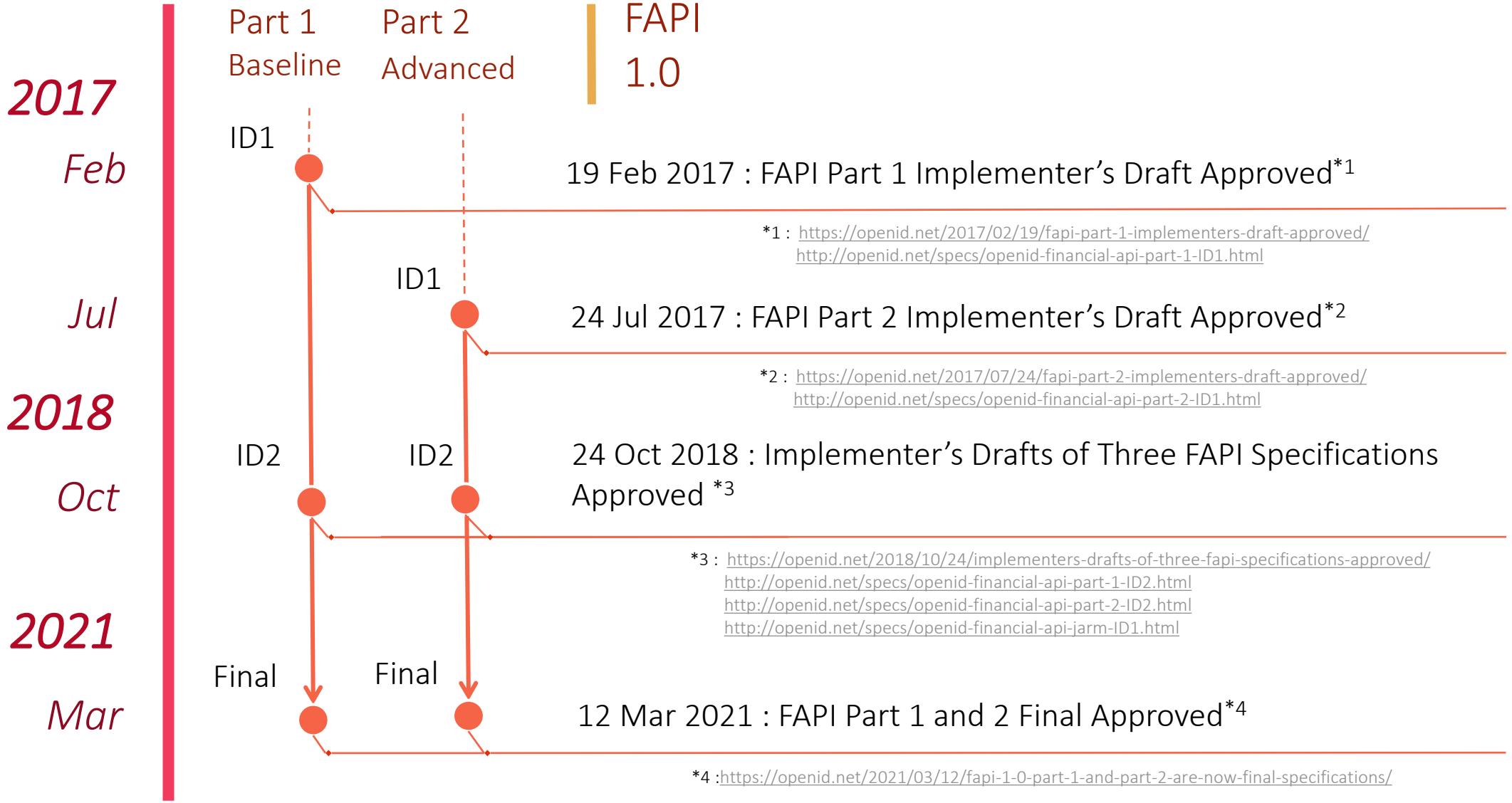
- Project : Follow-up of FAPI-RW
  The final version of FAPI 1.0 has been released by OID-F.
  Start working on following this final version.
- Project : FAPI-CIBA (poll mode)
  PR review/revise code in progress

  KEYCLOAK-12137 OpenID Connect Client Initiated Backchannel Authentication (CIBA)
- Project : Client Policies Official Support
  PR review/revise code in progress

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

Follow-up of FAPI-RW

FAPI Milestone



PROPOSED DRAFT

Following Final version of FAPI 1.0

[Motivation]

The current keycloak (12.0.4) has supported FAPI-RW security profile which version is Implementer's Draft ver 2(ID2). It also has passed all corresponding conformance tests on local environment.

On Jan, OID-F will fix the final version of FAPI 1.0 which have some changes compared with ID2.

IMO, we must support the **final** version of FAPI 1.0.

[Additional works needed]

We need to do the following works :

- Clarify the difference between the final version and ID2
- Clarify whether additional implementation is needed
- If needed, implement features needed to support the final version of FAPI 1.0
- Confirm whether the keycloak incorporating these features can pass all conformance tests for the final version of FAPI 1.0.
- After PRs for such the implementation are merged and the new version of keycloak is released, confirm whether this version of keycloak can pass all conformance tests for the final version of FAPI 1.0.

[Milestone]

The works above need to be done by the end of Mar to meet the release of RH-SSO 7.5.

Additional Works Needed

- Clarify the difference between the final version and ID2
- Clarify whether additional implementation is needed
- If needed, implement features needed to support the final version of FAPI 1.0

- Part 1. Baseline

  Nothing
- Part 2. Advanced
  - Limiting available period of Request Object

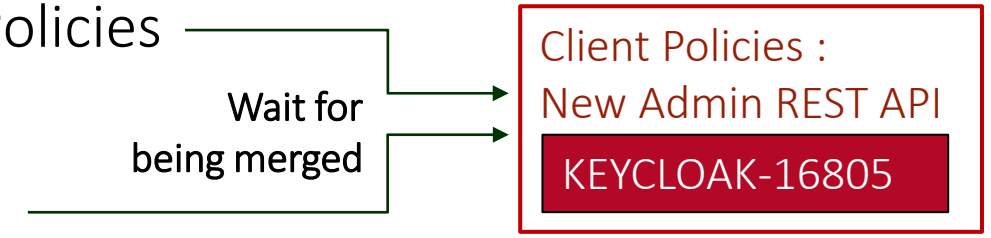
Need PR Modify existing Executor of Client Policies

  - Only supporting Confidential Client

Need PR Add new Executor of Client Policies

  - Excluding PKCE enforcement

  Nothing



Additional Works Needed

- Confirm whether the keycloak incorporating these features can pass all conformance tests for the final version of FAPI 1.0.

  The conformance test has not yet released the test plan for the final version.

  The below shown are the latest conformance test run status.

- The latest tagged version of the conformance test

release-v4.1.6

- The latest version of keycloak

12.0.4

- 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 as Client's signature algorithm.

Status Updates from 14th Meeting FAPI-CIBA (poll mode)

Remaining Issues Status

3 Mar 2021		17 Mar 2021	
13 Issues in total			
8 Resolved [62%]	→	8 Resolved [62%]	+0
2 In Progress		2 In Progress	+0
3 Assigned		3 Assigned	+0
0 Not Assigned		0 Not Assigned	+0

Upstreaming CIBA Support

In Review

- Pure CIBA

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

- 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

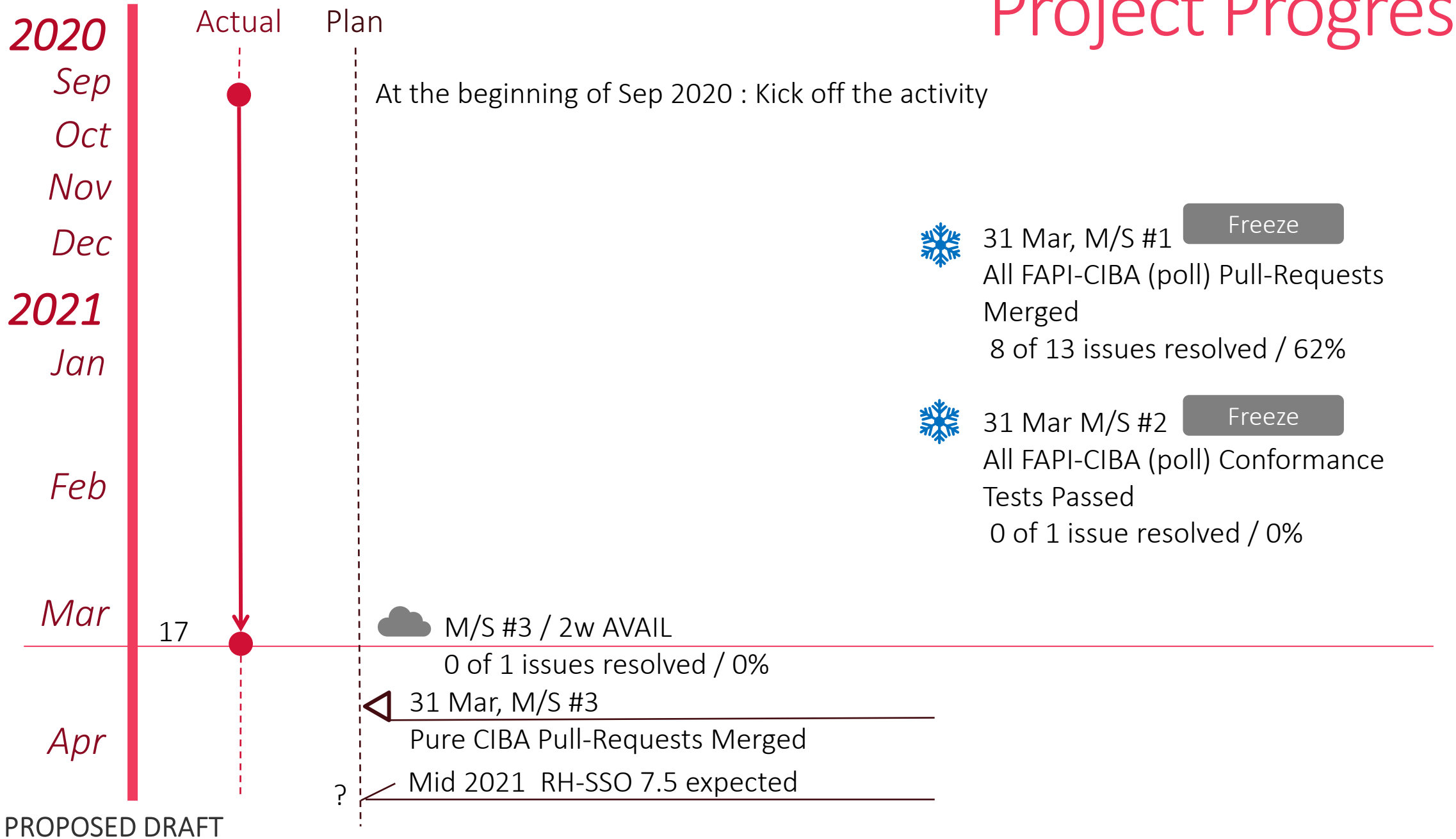
- FAPI-CIBA
  - #55 support id_token_hint

- FAPI-CIBA
  - #54 support login_hint_token

- FAPI-CIBA
  - #53 encrypt/decrypt login_hint

• • •

Project Progress



Status Updates from 14th Meeting Client Policy Official Support

Subprojects

[Mandatory]

Active External Interfaces

Completed Client Policies for FAPI-RW

[Optional]

Pend Built-in Default Client Policies

Active Client Registration Policies Migration

Issues Status - External Interfaces

3 Mar 2021		17 Mar 2021	
3 Issues in total		3 Issues in total	
1 Resolved [33%]	→	1 Resolved [33%]	+0
1 In Progress		1 In Progress	+0
1 Assigned		1 Assigned	+0
0 Not Assigned		0 Not Assigned	+0

Issue status in detail : External Interfaces

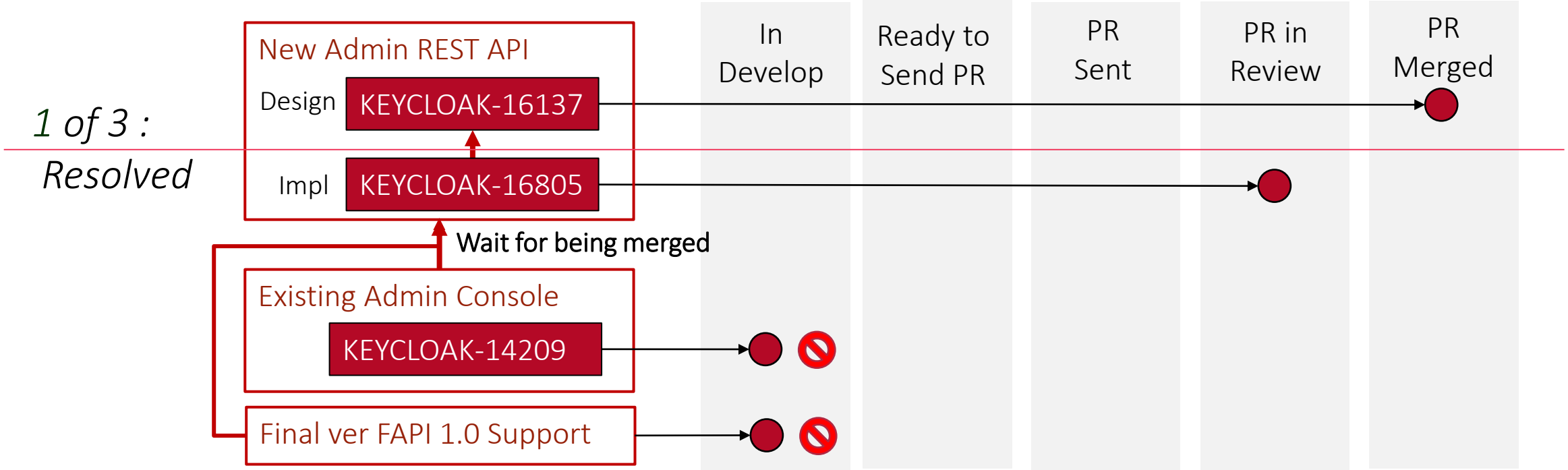
[New Admin REST API]

Resolved KEYCLOAK-16137 Client Policy : Support New Admin REST API (Design)

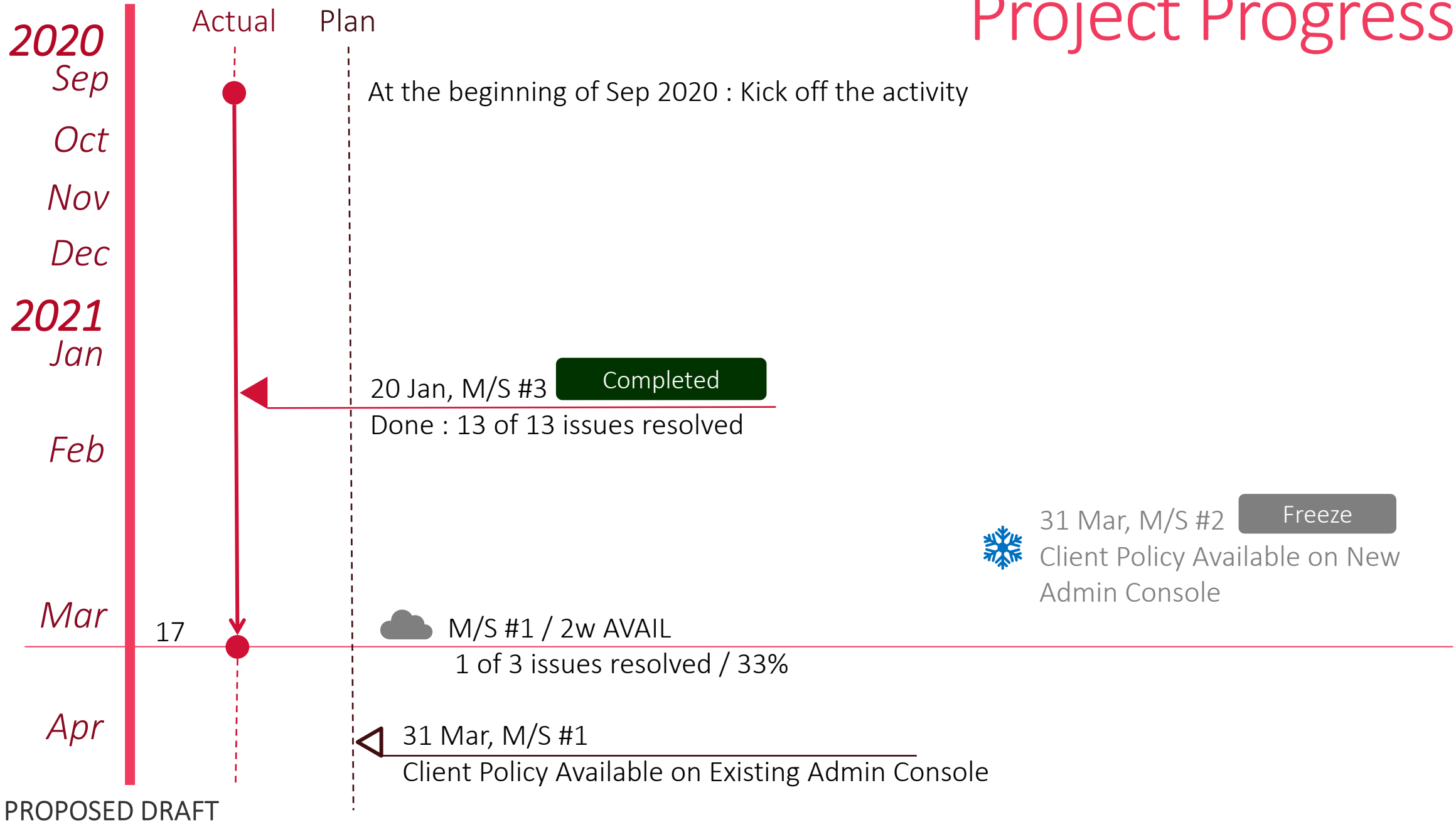
PR in Review KEYCLOAK-16805 Client Policy : Support New Admin REST API (Implementation)

[Existing Admin Console]

- KEYCLOAK-14209 Client Policy : UI on Admin Console



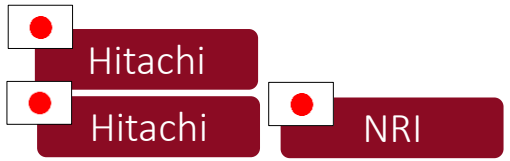
Project Progress



Proposing Working Items in FY 2021

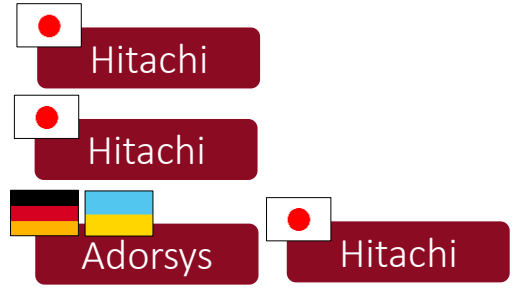
Result (Sep 2020 – Mar 2021)

- Project : FAPI-RW
  - Supporting FAPI-RW Implementer's Draft 2 (ID2)
  - Passing all conformance tests for ID2
    - FAPI-RW OP w/MTLS
    - FAPI-RW OP w/Private Key
  - Automating conformance tests run



- Project : FAPI-CIBA (poll mode)
  - Supporting CIBA (expected by the end of Mar)

- Project : Client Policies Official Support
  - Initial support
  - Refinement for New Admin REST API in JSON Representation
  - Initial extension for Client Registration Policy migration



Proposal : Take-Over Items (Apr 2021 -)

- Project : FAPI-RW
  - Supporting final version of FAPI 1.0 (baseline/advanced)
  - Passing all conformance tests for its final version
    - FAPI-RW OP w/MTLS
    - FAPI-RW OP w/Private Key
  - Contributing automating conformance tests run to keycloak's code base
- Project : FAPI-CIBA (poll mode)
  - Supporting FAPI-CIBA (poll mode)
  - Passing all conformance tests
    - FAPI-CIBA OP poll w/MTLS
    - FAPI-CIBA OP poll w/Private Key
- Project : Client Policies Official Support
  - Supporting for New Admin Console UI
  - Completing Client Registration Policy migration

Proposal : New Items (Apr 2021 -)

[Security Features]

<Common>

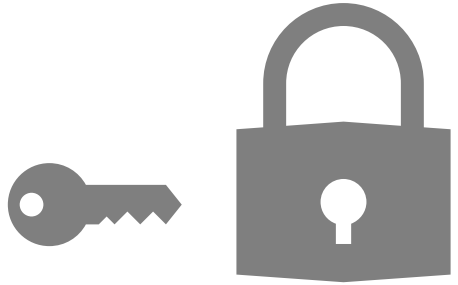
- OIDC Client's Public Key Management — Hitachi

<SPA/Native App>

- OAuth 2.0 Demonstration of Proof-of-Possession (DPoP) — Backbase

<High Level Security>

- FAPI 2.0 (baseline/advanced)
  - Pushed Authorization Request (PAR)
  - Rich Authorization Request (RAR)
  - Grant Management API



Proposal : New Items (Apr 2021 -)

[Market Specific Features]

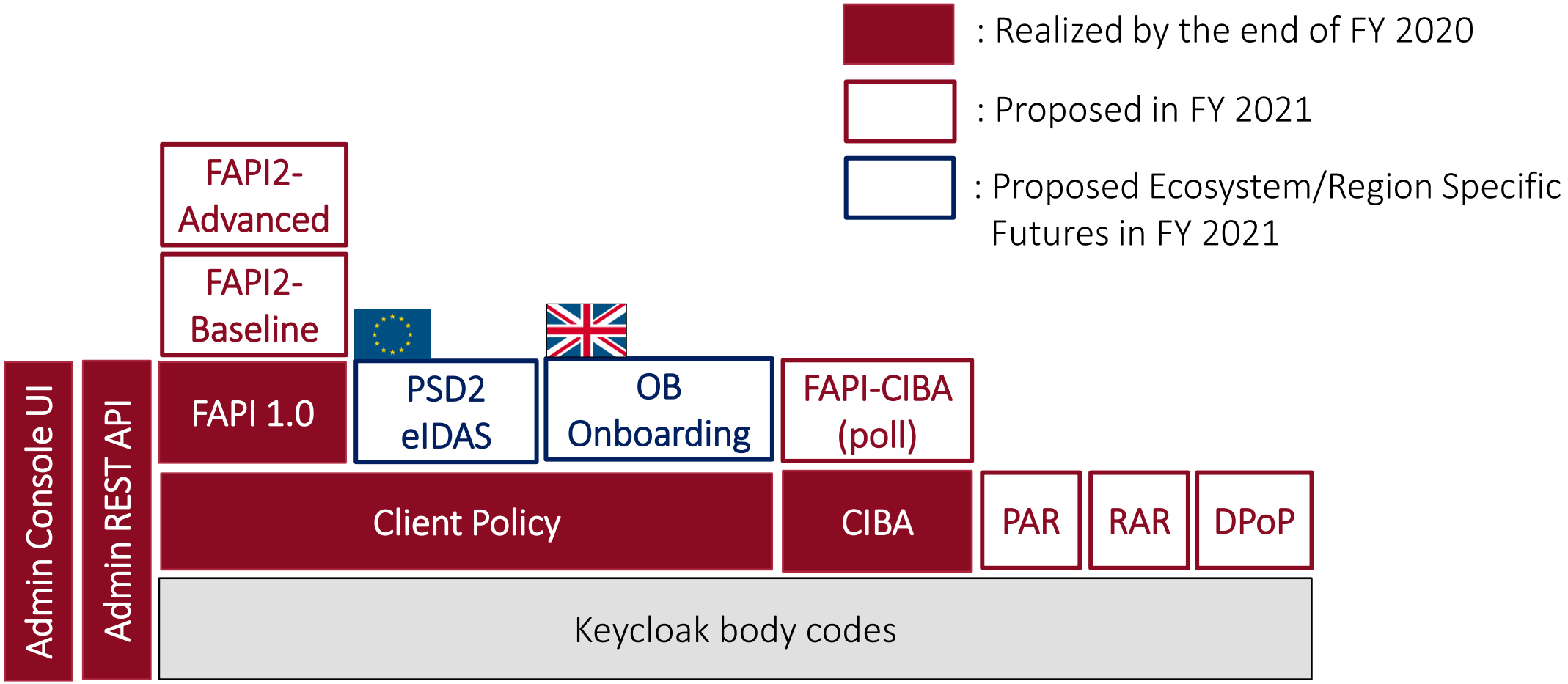
<PSD2>

- Following eIDAS regulations
  - QWAC verification
- Consent Management

<UK OpenBanking>

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

Proposal : Security Profiles Layout



Proposal : Load Map

	2020 Sep	2021 Apr
Security		
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

Proposal : Load Map

Market Specific		
PSD2	• Discussed QWAC verification	• Start design and implementation QWAC verification
UK OpenBanking		• Start design and implementation (?) Onboarding

END