

@Web Conference  
17 Mar 2021

# FAPI-SIG Community 15<sup>th</sup> Meeting

# Table of Contents

Major Topics

Follow-up of FAPI-RW

Status Updates from 14<sup>th</sup> Meeting

FAPI-CIBA (poll mode)

Client Policy Official Support

Proposing Working Items in FY 2021

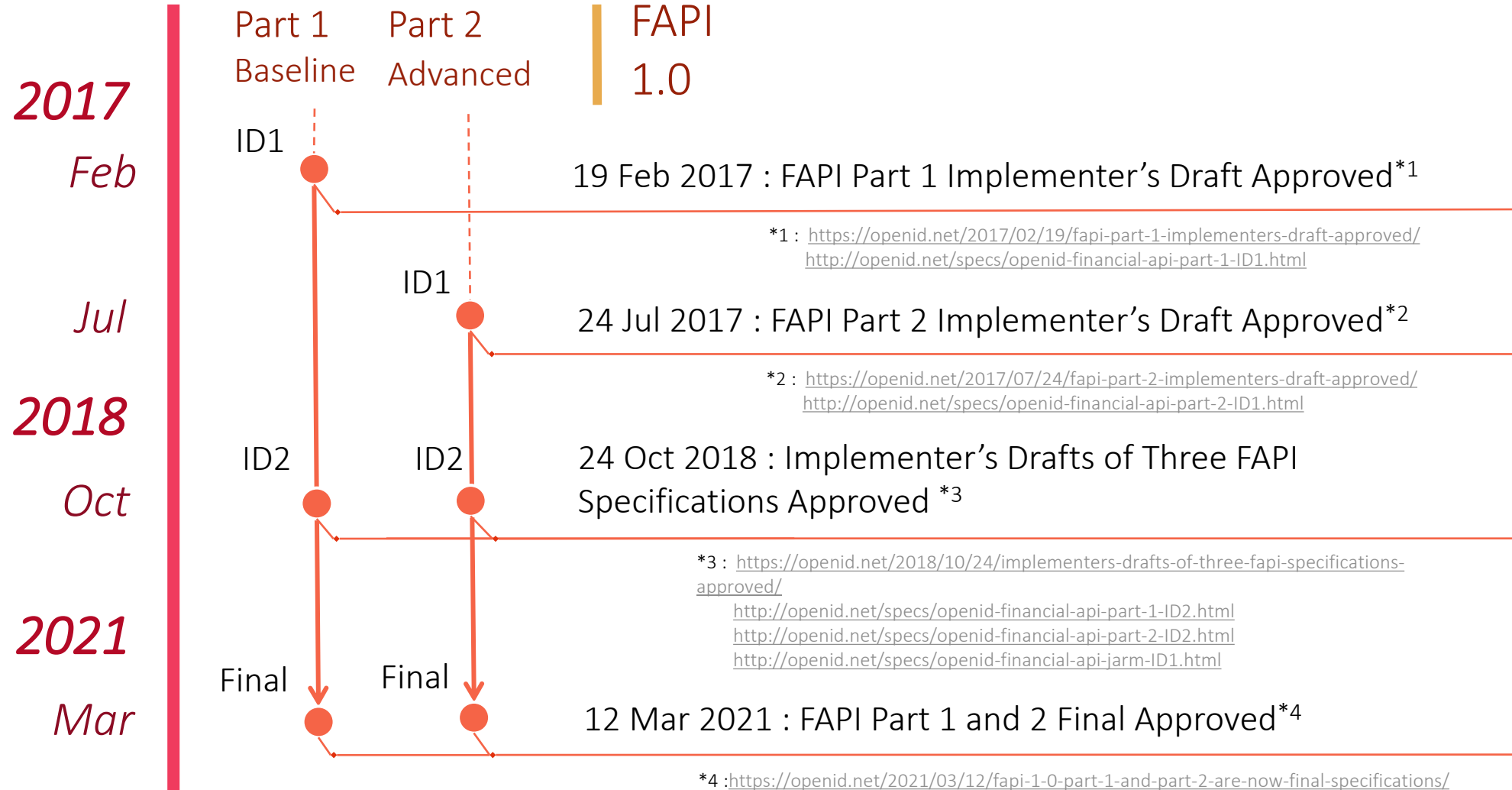
# Major Topics

# 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



# 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

Send PR

Modify existing Executor of Client Policies

- Only supporting Confidential Client

Send 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 14<sup>th</sup> Meeting FAPI-CIBA (poll mode)

# Remaining Issues Status

3 Mar 2021

13 Issues in total

8 Resolved [62%]

2 In Progress

3 Assigned

0 Not Assigned



17 Mar 2021

8 Resolved [62%] +0

2 In Progress +0

3 Assigned +0

0 Not Assigned +0

# Remaining Issues Details

- #56 support Signed Authentication Request  
In Review
- #58 Realm Settings (CIBA Policy) overridden by Client Settings  
In Review
- #63 Confirm CIBA Implementation Works Well in Clustering Environment  
Assigned
- #64 Confirm CIBA Implementation Works Well in Cross-DC Environment  
Assigned
- #65 Establish the way of running FAPI-CIBA OP poll w/ MTLS and w/ Private Key against CIBA Implementation  
Assigned

# 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

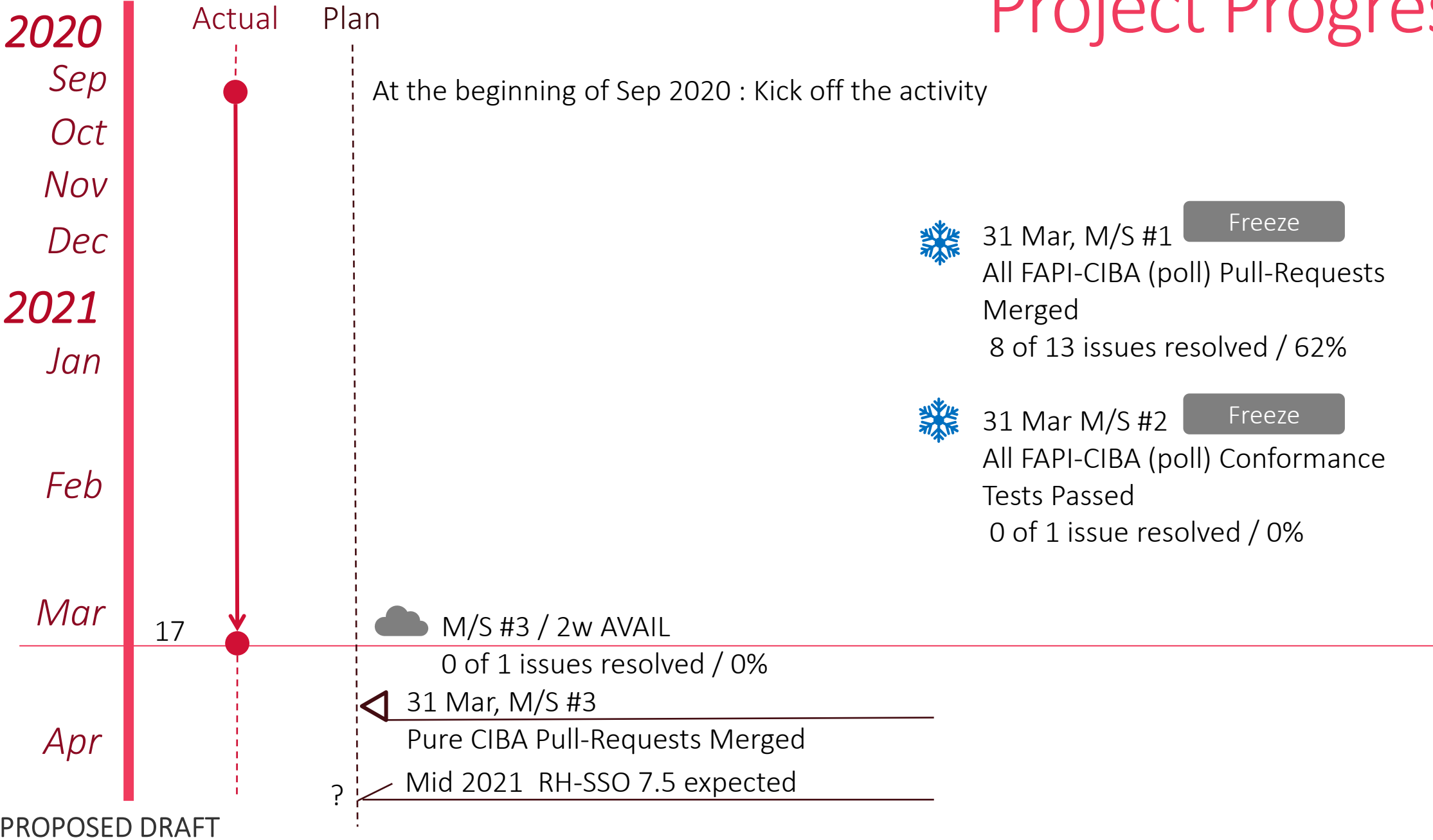
- [#53](#) encrypt/decrypt login\_hint

...



PROPOSED DRAFT

# Project Progress



# Status Updates from 14<sup>th</sup> 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

3 Issues in total

1 Resolved [33%]

1 In Progress

1 Assigned

0 Not Assigned



17 Mar 2021

3 Issues in total

1 Resolved [33%] +0

1 In Progress +0

1 Assigned +0

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

[New Admin Console]

Deferred

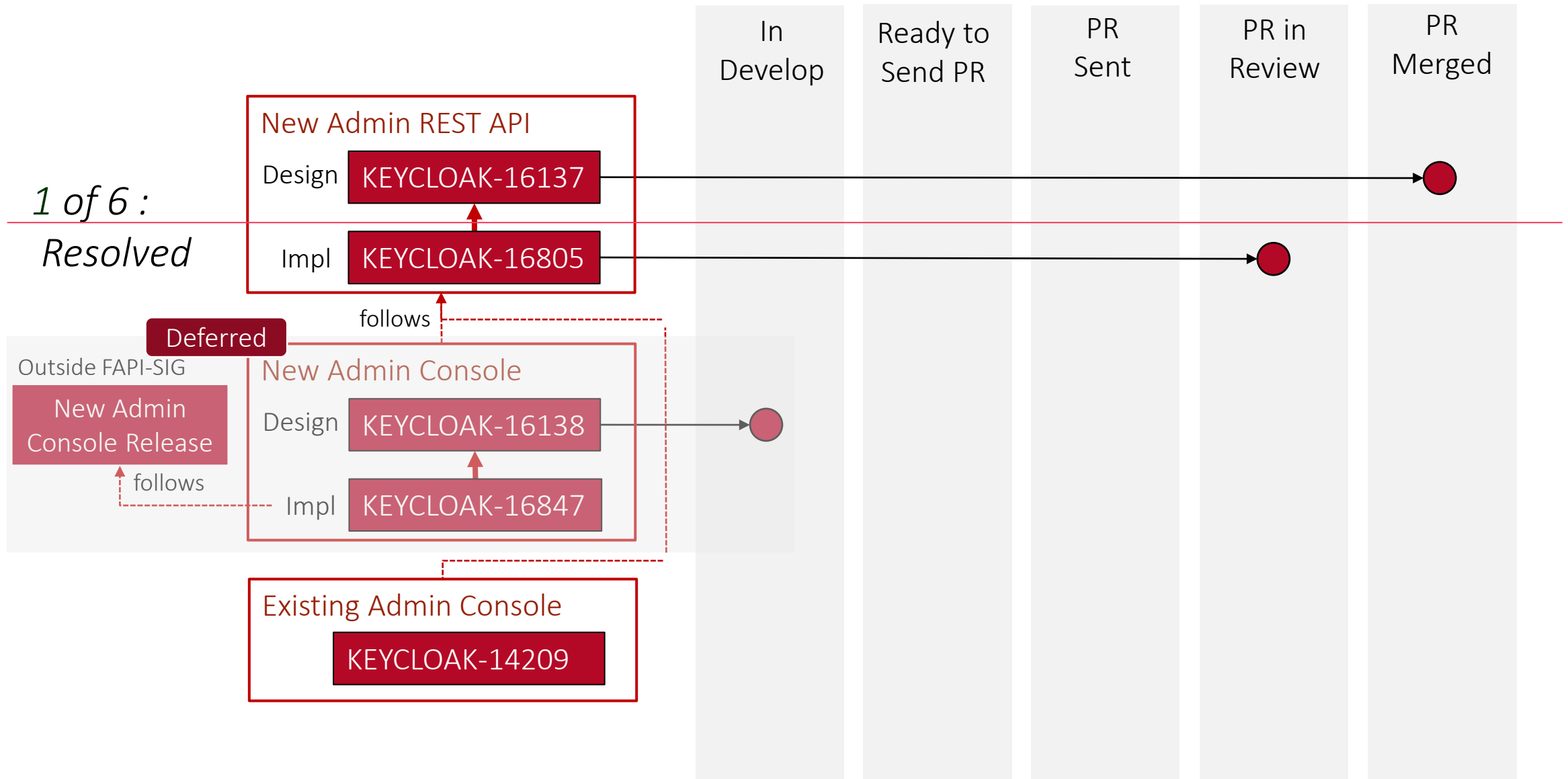
- KEYCLOAK-16138 Client Policy : Support New Admin Console UI (Design)

- Concept Design by RH UXD team :

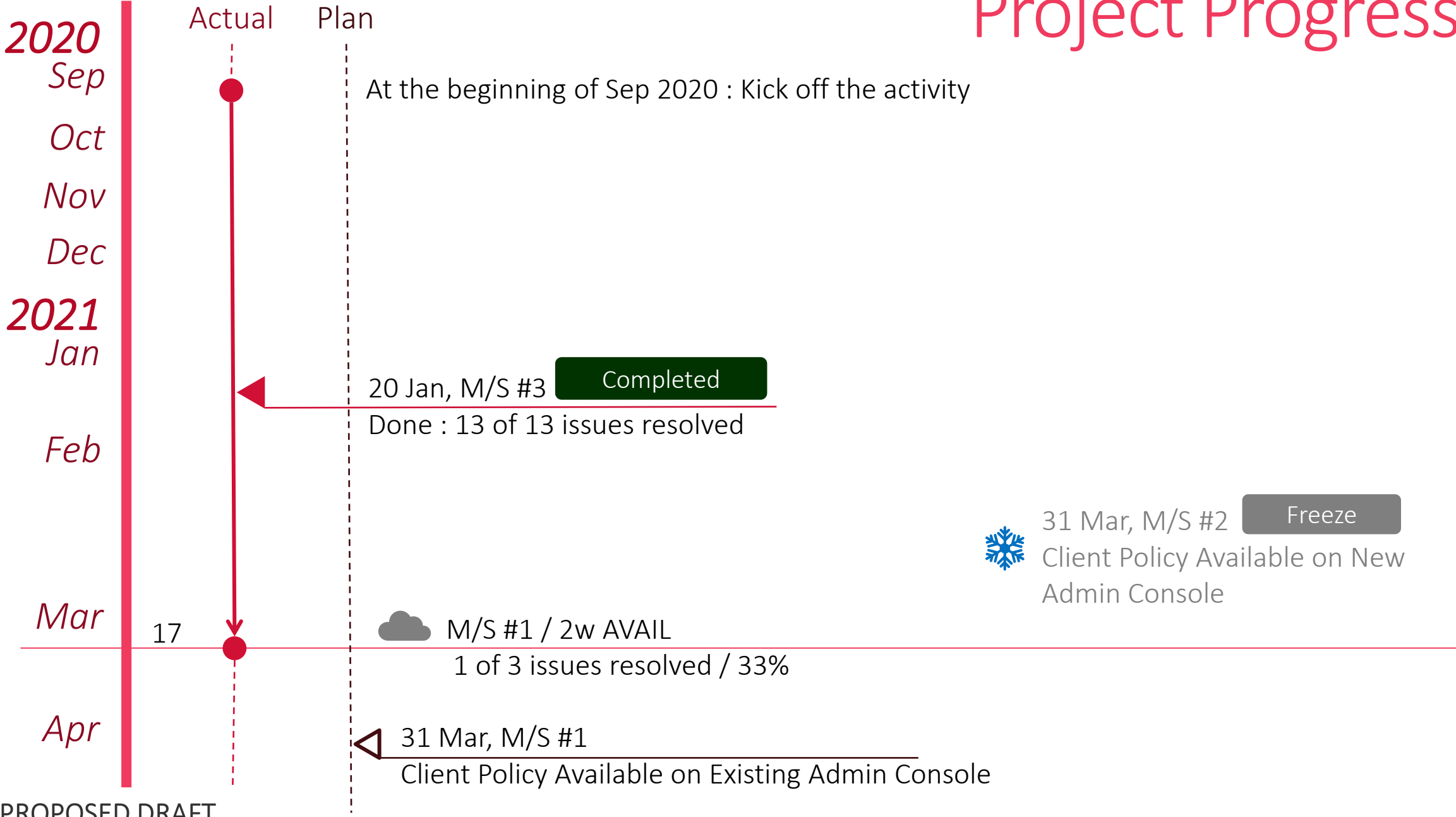
<https://marvelapp.com/prototype/6e70eh2/screen/74918976>

- KEYCLOAK-16847 Client Policy : Support New Admin Console UI (Implementation)
- KEYCLOAK-14211 Client Policy : Remove Client Policy related individual settings on Admin Console

# Issue status in detail : External Interfaces



# Project Progress

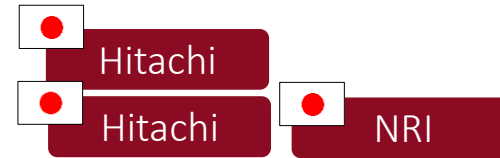


# Proposing Working Items in FY 2021

# 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



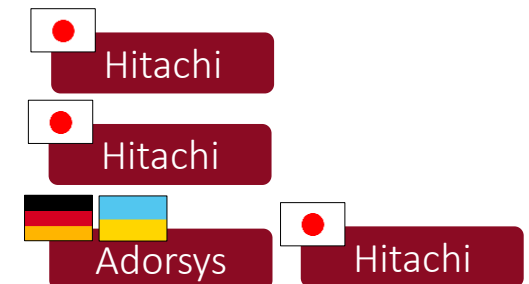
## ● Project : FAPI-CIBA (poll mode)

- 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]

- OAuth 2.0 Demonstration of Proof-of-Possession (DPoP)
- OIDC Client's Public Key Management
- FAPI 2.0 (baseline/advanced)
  - Pushed Authorization Request (PAR)
  - Rich Authorization Request (RAR)
  - Grant Management API



Backbase



Hitachi

## [Market Specific Features]

- PSD2/UK OpenBanking market related features
  - Following eIDAS regulations
    - QWAC verification
  - Consent Management



Adorsys



END