

@Web Conference
18 Nov 2020

FAPI-SIG Community 7th Meeting

Table of Contents

Status Updates from 6th Meeting

FAPI-RW

FAPI-CIBA (poll mode)

Client Policy Official Support

Project Progress

Project in the Future

Status Updates from 6th Meeting

FAPI-RW

Remaining Issues Status

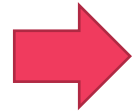
4 Nov 2020

4 Issues in total

1 Resolved

2 Assigned

1 Not Assigned
(but in progress)



17 Nov 2020

1 Resolved

+0

2 Assigned

+0

1 Not Assigned

+0

(but in progress)

Remaining Issues for FAPI-RW project

[Conformance Test]

- #39 Confirm all FAPI R/W OP w/ MTLS conformance tests are passed by the released keycloak

Assigned

- #40 Confirm all FAPI R/W OP w/ Private key conformance tests are passed by the released keycloak

Assigned

Both waiting for the next version release.

[Conformance Test Environment]

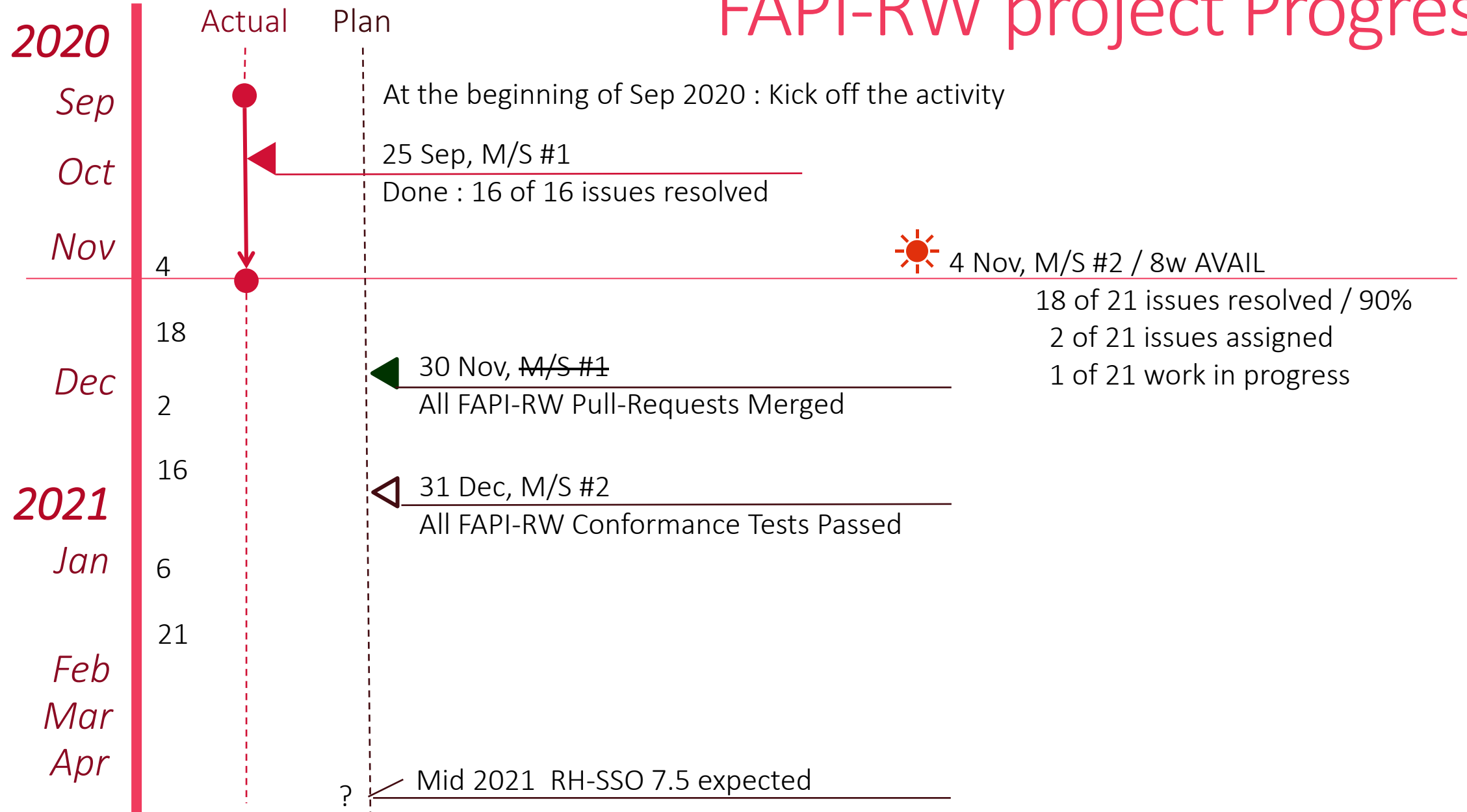
- #45 Integrating FAPI-RW conformance tests run into keycloak's CI/CD pipeline

✓ Automation of FAPI Conformance Tests has been completed.

- #46 Consider alternative for keycloak-gatekeeper used in FAPI-RW conformance test run environment

Resolved

FAPI-RW project Progress



Status Updates from 6th Meeting FAPI-CIBA (poll mode)

Subtasks Status

4 Nov 2020

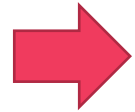
13 Subtasks in total

6 Resolved [46%]

0 PR sent, in review

7 Assigned

0 Not Assigned



17 Nov 2020

6 Resolved [46%] +0

3 PR sent, in review +3

4 Assigned -3

0 Not Assigned +0

Remaining Issues for FAPI-CIBA project

[Backchannel Authentication Request]

- #53 encrypt/decrypt login_hint
Resolved
- #54 support login_hint_token
Resolved
- #55 support id_token_hint
Resolved
- #56 support Signed Authentication Request
Assigned
- #57 support User Code
Resolved

Remaining Issues for FAPI-CIBA project

[Settings]

- #58 Realm Settings (CIBA Policy) overridden by Client Settings

✓ In Review

[Internals]

- #59 Use Only Auth Result Cache by Infinispan For CIBA Flow Session Binding

Resolved

- #60 Use Only Auth Result Cache on Communication with Decoupled Auth Server

Resolved

- #61 Token Request Throttling Information Not Cluster-wide Sync

✓ In Review

- #62 Use Security Event Token (SET) as message format between keycloak and Decoupled Auth Server

✓ In Review

Remaining Issues for FAPI-CIBA project

[Arquillian Integration Test]

- #63 Confirm CIBA Implementation Works Well in Clustering Environment

Assigned

- #64 Confirm CIBA Implementation Works Well in Cross-DC Environment

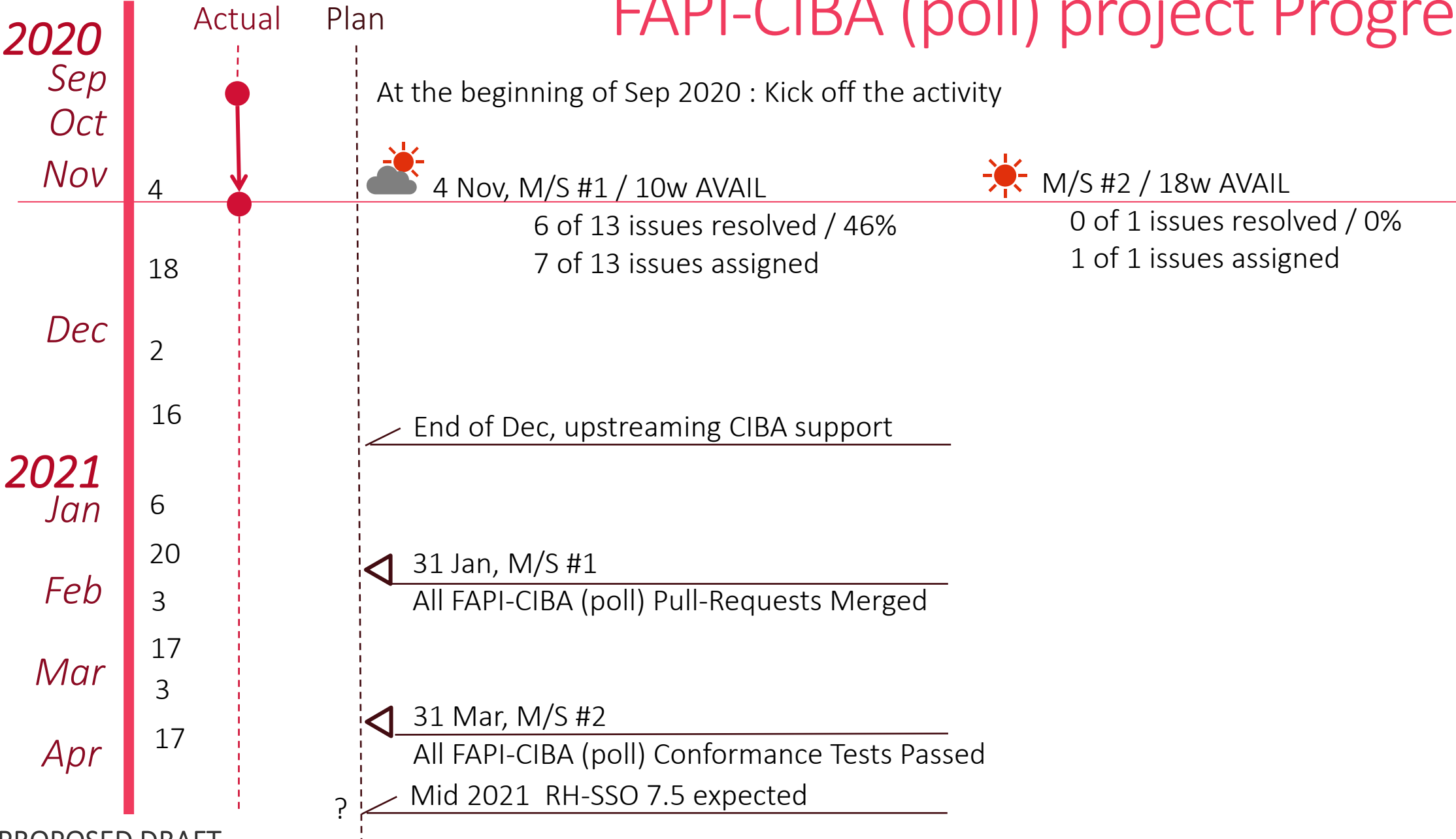
Assigned

[Conformance Test]

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

Assigned

FAPI-CIBA (poll) project Progress



Status Updates from 6th Meeting

Client Policy Official Support

Subprojects

[Mandatory]

Active

External Interfaces

Active

Client Policies for FAPI-RW

[Optional]

Pend

Built-in Default Client Policies

Pend

Client Registration Policies Migration

Issues Status - Subproject: External Interfaces

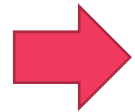
4 Nov 2020

5 Issues in total

0 Resolved [0%]

0 Assigned

5 Not Assigned



17 Nov 2020

0 Resolved [0%] +0

2 Assigned +2

3 Not Assigned -2

Subproject : External Interfaces

- KEYCLOAK-16137 Client Policy : Support New Admin REST API (Clear JSON Representation)

PR Sent
Wait Review

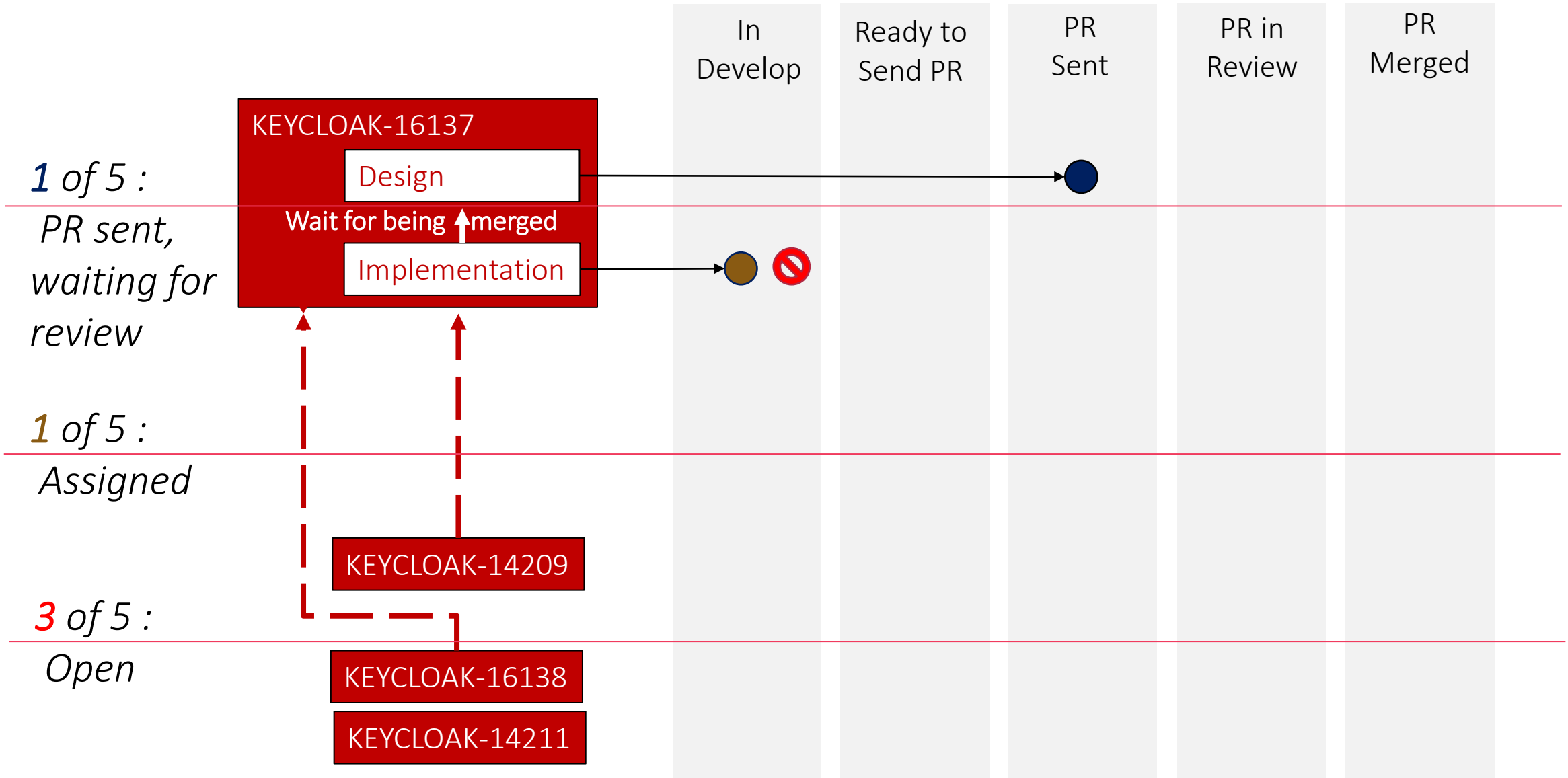
Design

Assigned

Implementation

- KEYCLOAK-16138 Client Policy : Support New Admin Console UI
- KEYCLOAK-14209 Client Policy : UI on Admin Console
- KEYCLOAK-14211 Client Policy : Remove Client Policy related individual settings on Admin Console

Subproject : External Interfaces



Issues Status - Subproject: Client Policies for FAPI-RW

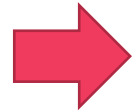
4 Nov 2020

18 Issues in total

4 Resolved [22%]

11 Assigned

3 Not Assigned



17 Nov 2020

7 Resolved [39%] +3

10 Assigned -5

1 Not Assigned +2

Subproject : Client Policies for FAPI-RW

RESOLVED

KEYCLOAK-14190 Client Policy - Condition : The way of creating/updating a client

Ready to
Send PR

KEYCLOAK-14191 Client Policy - Condition : Author of a client - User Group

Ready to
Send PR

KEYCLOAK-14192 Client Policy - Condition : Author of a client - User Role

PR Sent
Wait Review

KEYCLOAK-14193 Client Policy - Condition : Client - Client Access Type

- KEYCLOAK-14194 Client Policy - Condition : Client - Client Domain Name

RESOLVED

KEYCLOAK-14195 Client Policy - Condition : Client - Client Role

RESOLVED

KEYCLOAK-14196 Client Policy - Condition : Client - Client Scope

Ready to
Send PR

KEYCLOAK-14197 Client Policy - Condition : Client - Client Host

RESOLVED

KEYCLOAK-14198 Client Policy - Condition : Client - Client IP

Subproject : Client Policies for FAPI-RW

RESOLVED

KEYCLOAK-14199 Client Policy - Executor : Enforce more secure client authentication method when client registration

Assigned

KEYCLOAK-14200 Client Policy - Executor : Enforce Holder-of-Key Token

RESOLVED

KEYCLOAK-14201 Client Policy - Executor : Enforce Proof Key for Code Exchange (PKCE)

Assigned

KEYCLOAK-14202 Client Policy - Executor : Enforce secure signature algorithm for Signed JWT client authentication

Ready to
Send PR

KEYCLOAK-14203 Client Policy - Executor : Enforce HTTPS URIs

RESOLVED

KEYCLOAK-14204 Client Policy - Executor : Enforce Request Object satisfying high security level

RESOLVED

KEYCLOAK-14205 Client Policy - Executor : Enforce Response Type of OIDC Hybrid Flow

RESOLVED

KEYCLOAK-14206 Client Policy - Executor : Enforce more secure state and nonce treatment for preventing CSRF

RESOLVED

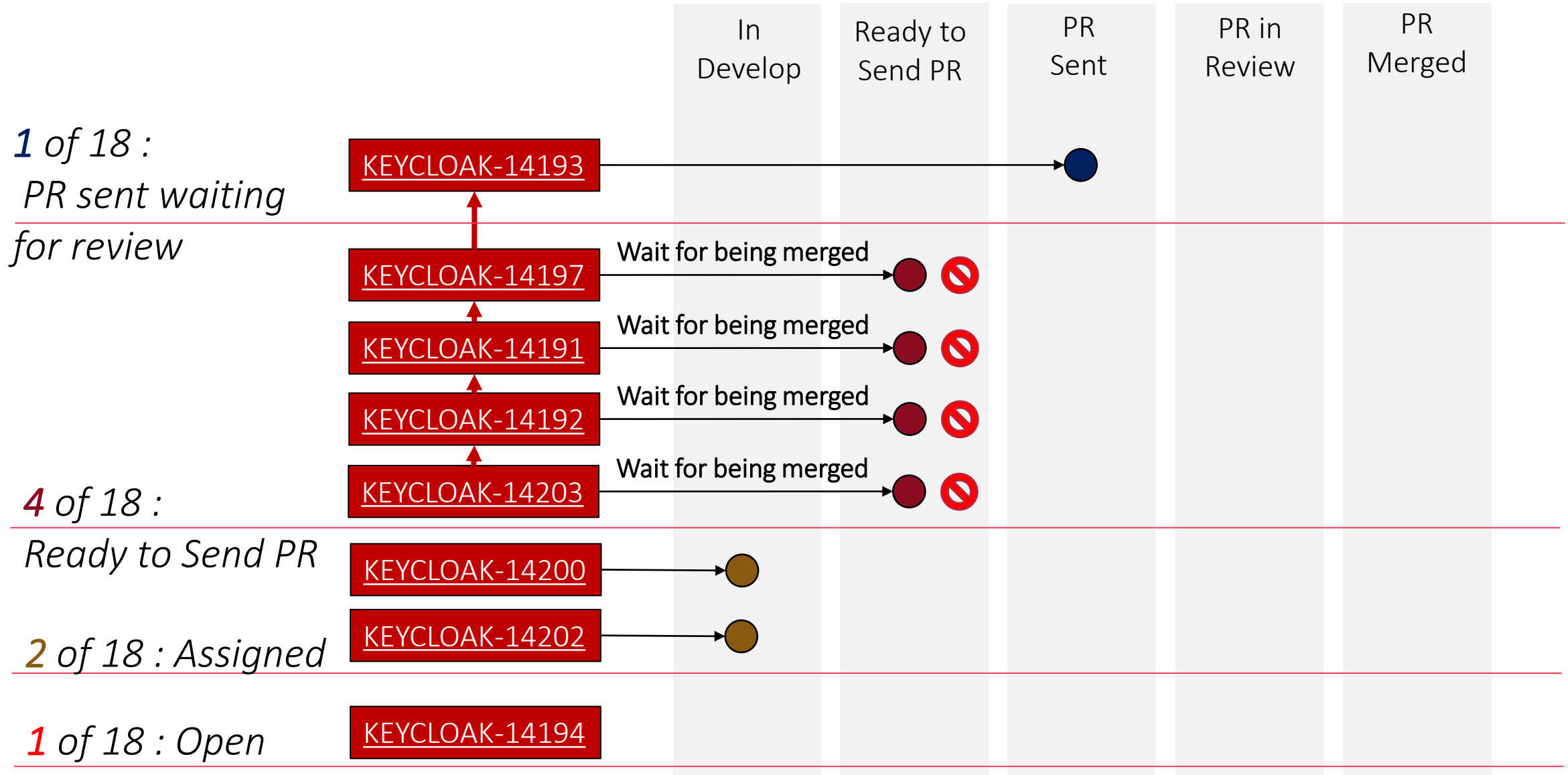
KEYCLOAK-14207 Client Policy - Executor : Enforce more secure client signature algorithm when client registration

Subproject : Client Policies for FAPI-RW

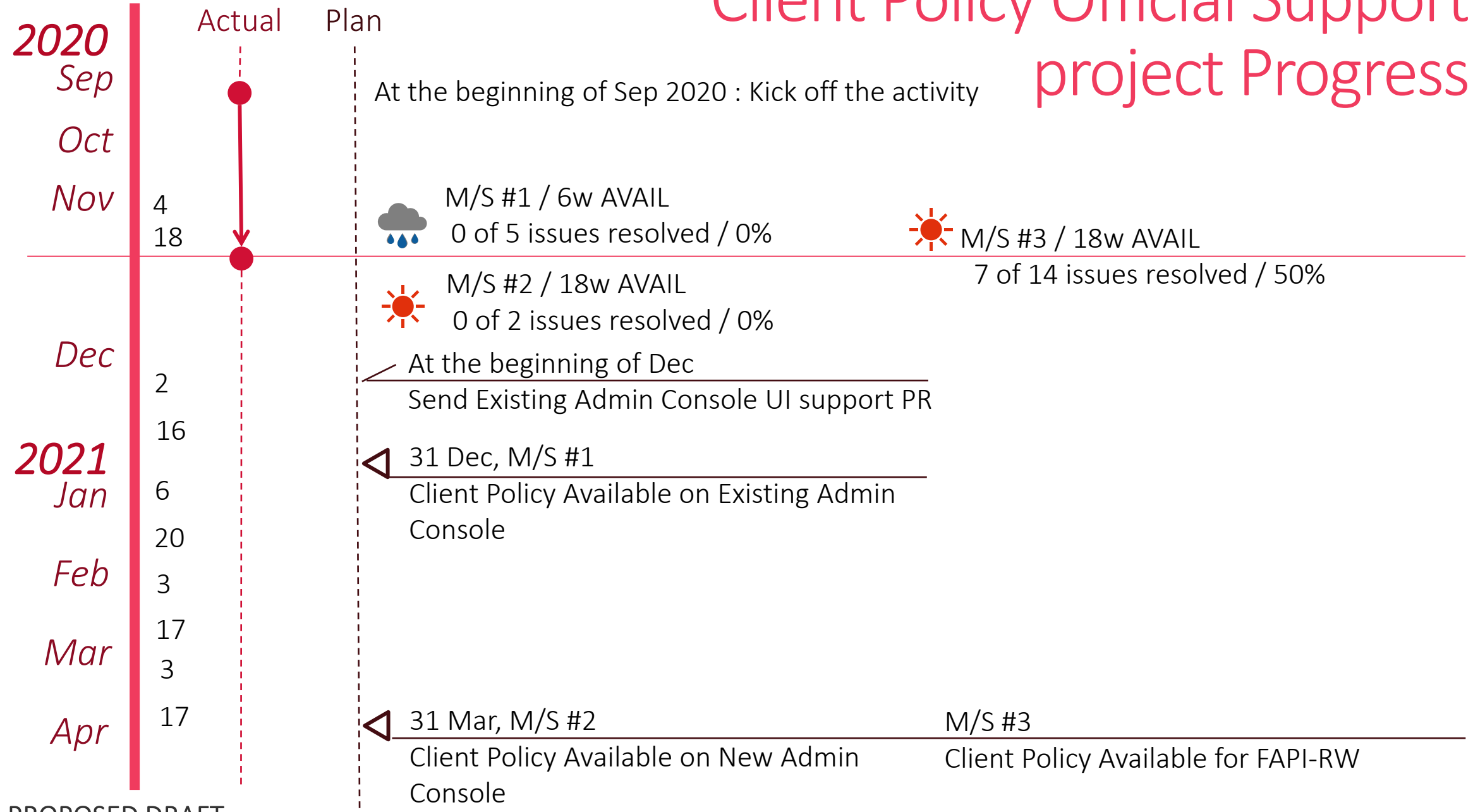


*10 of 18 :
Resolved*

Subproject : Client Policies for FAPI-RW

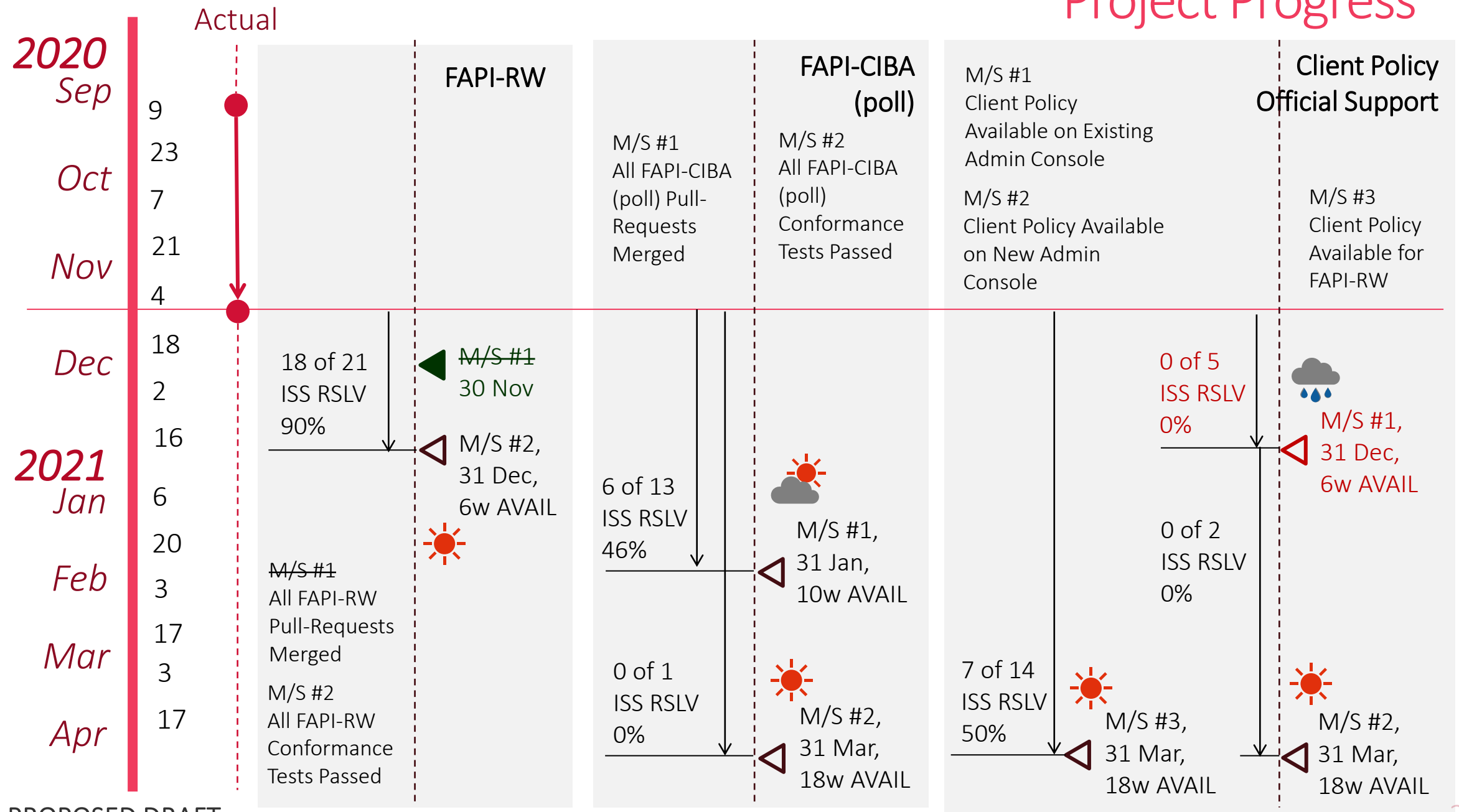


Client Policy Official Support project Progress






Project Progress

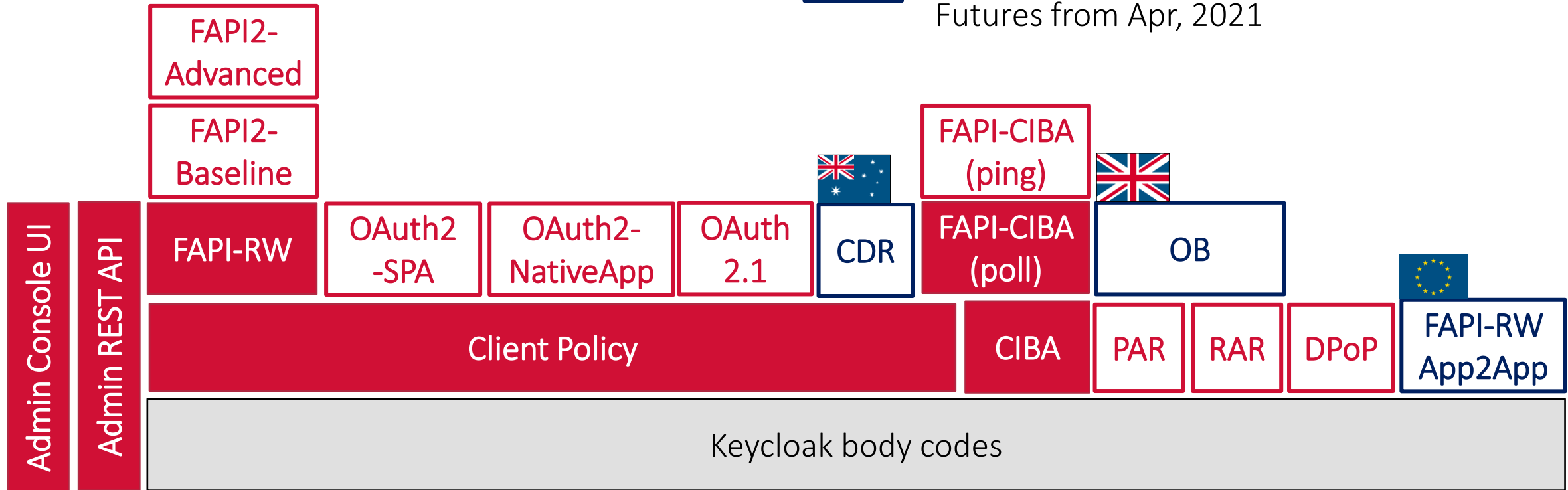
Project Progress



Project in the Future

Proposal for Projects in the Future

-  : Realized Futures by the end of Mar, 2021
-  : Proposed Futures from Apr, 2021
-  : Proposed Ecosystem/Region Specific Futures from Apr, 2021



Security Profiles

- Financial-grade API (FAPI)
 - FAPI 2.0 Baseline
 - FAPI 2.0 Advanced (no working draft)
 - Pushed Authorization Requests (PAR)
 - Rich Authorization Request (RAR)
- Client Initiated Backchannel Authentication (CIBA)
 - FAPI-CIBA (ping mode)
- OAuth 2.0 for Native Apps
- OAuth 2.0 for Browser-Based Apps
 - Demonstration of Proof-of-Possession at the Application Layer (DPoP)
- OAuth 2.1

Ecosystem/Region Specific Features

- UK Open Banking (In service) 

Its security profile is on FAPI 1.0

- Australia Consumer Data Right (launched on July 2020) 

Its security profile is based on FAPI 1.0

- FAPI-RW App2App 

END