

@Web Conference
6 Jan 2021

FAPI-SIG Community 10th Meeting

Table of Contents

Major Topics

Status Updates from 9th Meeting

FAPI-RW

FAPI-CIBA (poll mode)

Client Policy Official Support

Future Topics Recalled

Major Topics

Major Topics

- Project : FAPI-RW

Confirmed that keycloak 12 can pass both conformance test of FAPI-RW OP w/MTLS and w/Private Key on local environment.

- Project : FAPI-CIBA (poll mode)

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

CIBA Implementation Practical Guide was uploaded.

- Project : Client Policy Official Support

Subproject : External Interfaces

KEYCLOAK-16137 Client Policy : Support New Admin REST API

Updated by incorporating feedback comments on its review.

Status Updates from 9th Meeting

FAPI-RW

Remaining Issues Status

16 Dec 2020

4 Issues in total

1 Resolved

1 In Progress

2 Assigned

0 Not Assigned



6 Jan 2021

3 Resolved

+2

1 In Progress

+0

0 Assigned

-1

0 Not Assigned

+0

Remaining Issues Details

[Conformance Test]

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

Resolved

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

Resolved

[Conformance Test Environment]

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

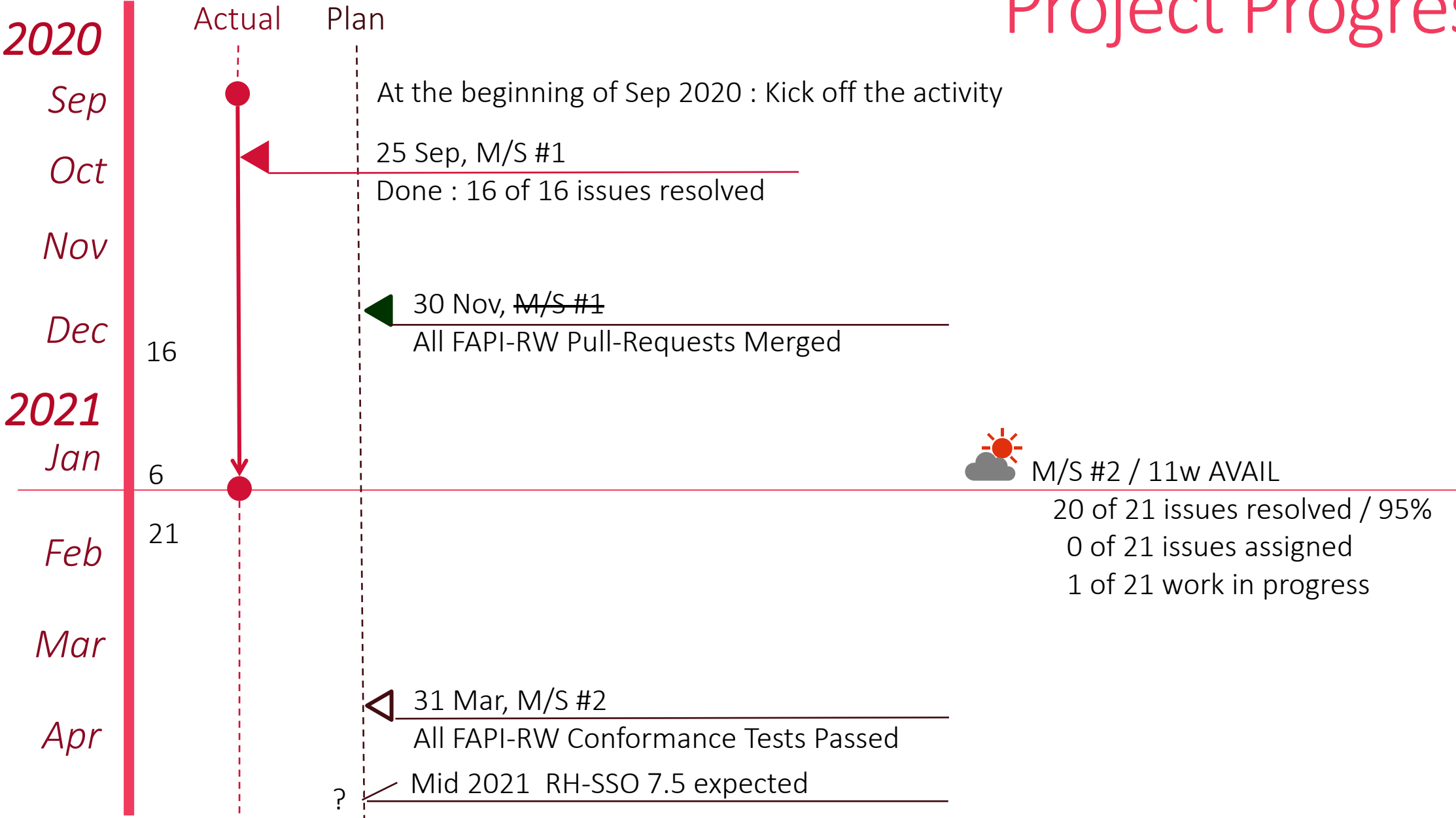
FAPI-RW conformance test run automation completed.

Integrating this automation onto keycloak codebase still remains open.

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

Resolved

Project Progress



Status Updates from 9th Meeting FAPI-CIBA (poll mode)

Remaining Issues Status

16 Dec 2020

13 Issues in total

8 Resolved [62%]

1 In Progress

4 Assigned

0 Not Assigned



6 Jan 2021

8 Resolved [62%] +0

2 In Progress +1

3 Assigned -1

0 Not Assigned +0

Remaining Issues Details 1/3

[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
In Review
- #57 support User Code
Resolved

Remaining Issues Details 2/3

[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

Resolved

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

Resolved

Remaining Issues Details 3/3

[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

Upstreaming CIBA Support

PR Sent



- 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

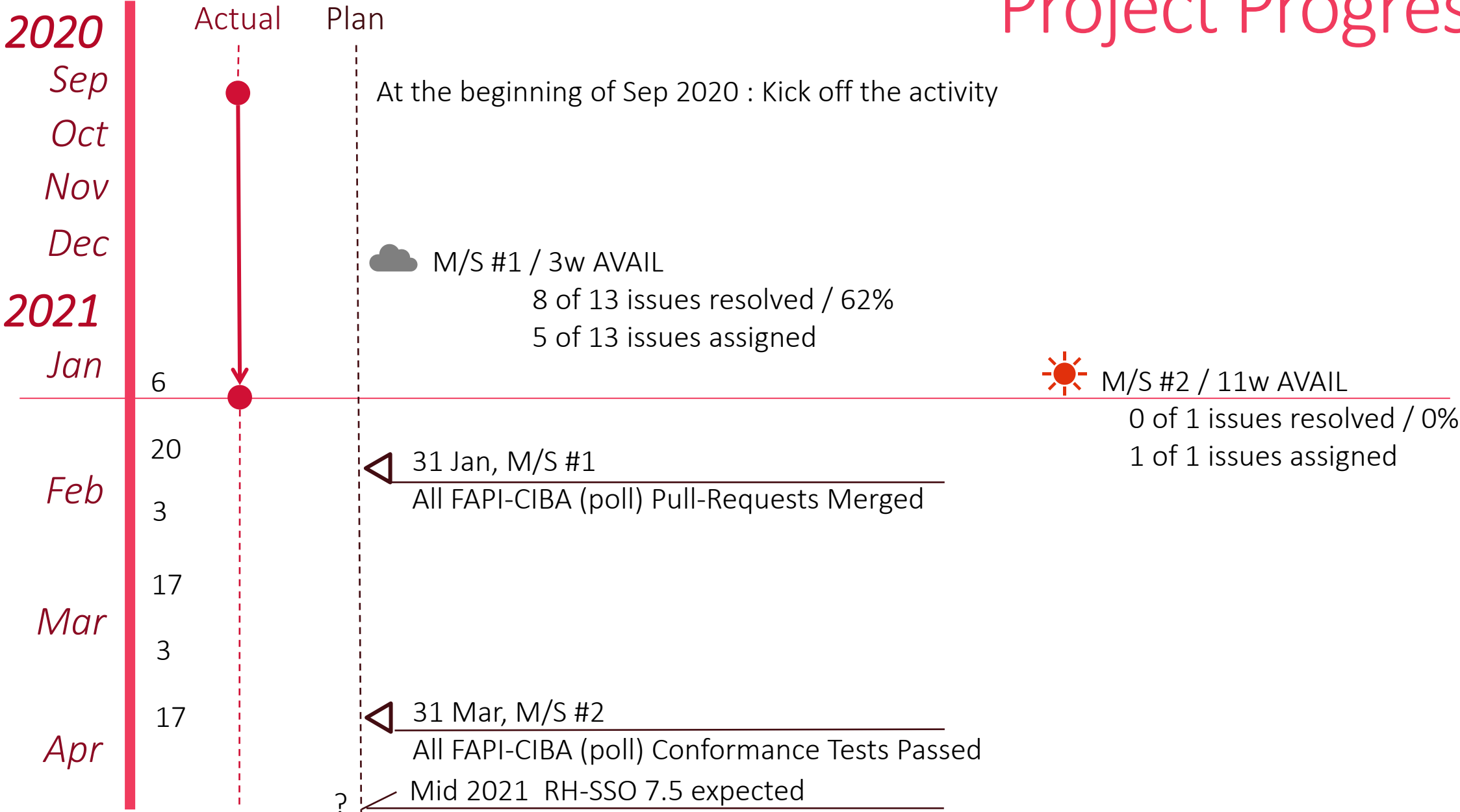
- [#53](#) encrypt/decrypt login_hint

...



PROPOSED DRAFT

Project Progress



Status Updates from 9th Meeting

Client Policy Official Support

Subprojects

[Mandatory]

Active

External Interfaces

Active

Client Policies for FAPI-RW

[Optional]

Pend

Built-in Default Client Policies

Active

Client Registration Policies Migration

Issues Status - External Interfaces

16 Dec 2020

6 Issues in total

0 Resolved [0%]

2 In Progress

1 Assigned

3 Not Assigned



6 Jan 2021

0 Resolved [0%] +0

2 In Progress +0

1 Assigned +0

3 Not Assigned +0

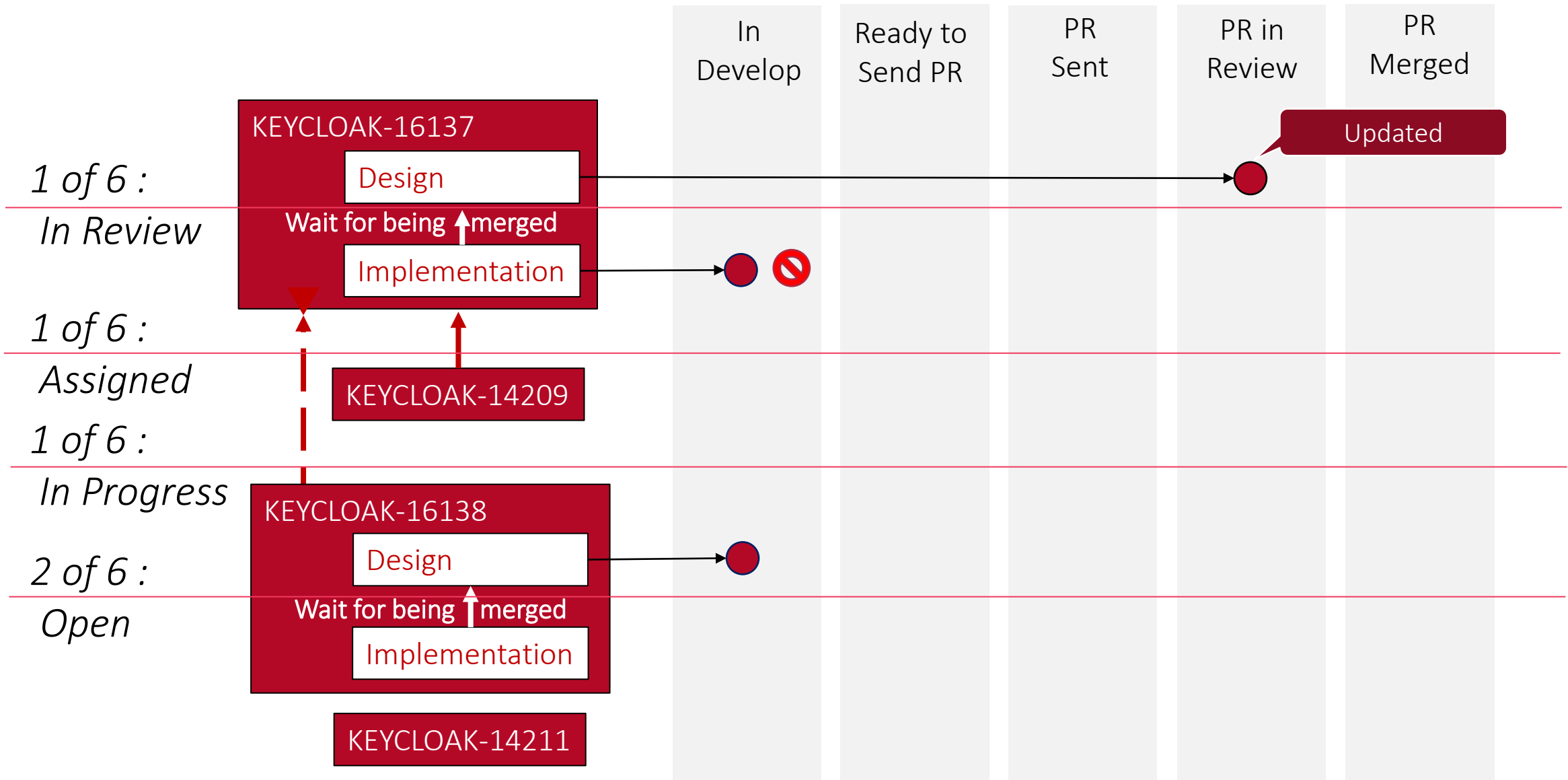
Subproject : External Interfaces

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

In Review Design

- Implementation
- KEYCLOAK-16138 Client Policy : Support New Admin Console UI
 - Design
 - Concept Design : <https://marvelapp.com/prototype/6e70eh2/screen/74918976>
 - Implementation
- 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

16 Dec 2020

17 Issues in total

15 Resolved [88%]

2 In Progress

0 Assigned

0 Not Assigned



2 Jan 2021

17 Issues in total

15 Resolved [88%] +0

2 In Progress +0

0 Assigned +0

0 Not Assigned +0

Subproject : Client Policies for FAPI-RW

- RESOLVED KEYCLOAK-14190 Client Policy - Condition : The way of creating/updating a client
- RESOLVED KEYCLOAK-14191 Client Policy - Condition : Author of a client - User Group
- RESOLVED KEYCLOAK-14192 Client Policy - Condition : Author of a client - User Role
- RESOLVED 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
- RESOLVED 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

PR Sent

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

RESOLVED

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

PR Sent

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

RESOLVED

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



Subproject : Client Policies for FAPI-RW



Issues Status - Subproject: Client Registration Policies Migration

16 Dec 2020

6 Jan 2021

3 Issues in total

0 Resolved [0%]



0 Resolved [0%] +0

2 In Progress

3 In Progress +3

0 Assigned

0 Assigned +0

1 Not Assigned

0 Not Assigned -1

Subproject : Client Registration Policies Migration

In Progress

KEYCLOAK-15533 Client Policy : Extends Policy Interface to Migrate Client Registration Policies

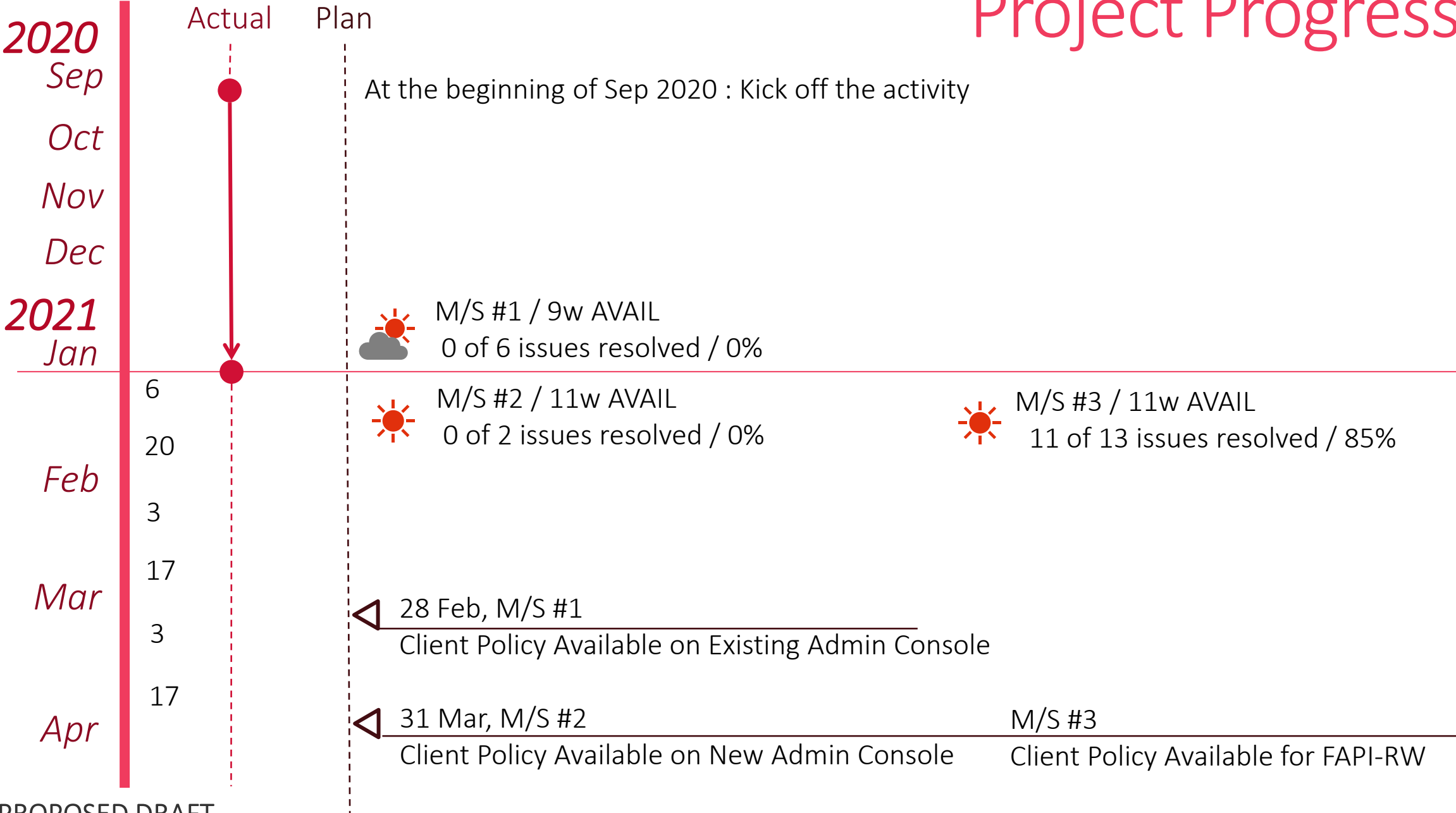
In Progress

KEYCLOAK-15534 Client Policy : Implement Existing Client Registration Policies as Client Policies

In Progress




KEYCLOAK-14210 Client Policy : Migrate Client Registration Policies to Client Policies

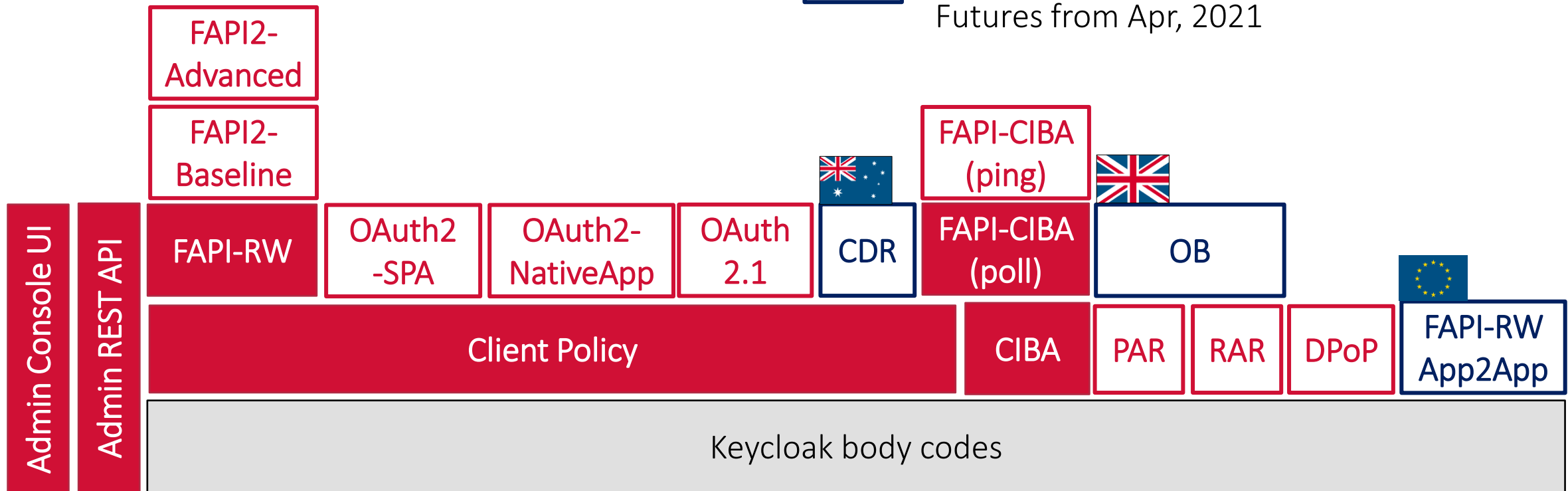
Project Progress



Future Topics Recalled

Security Profiles




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



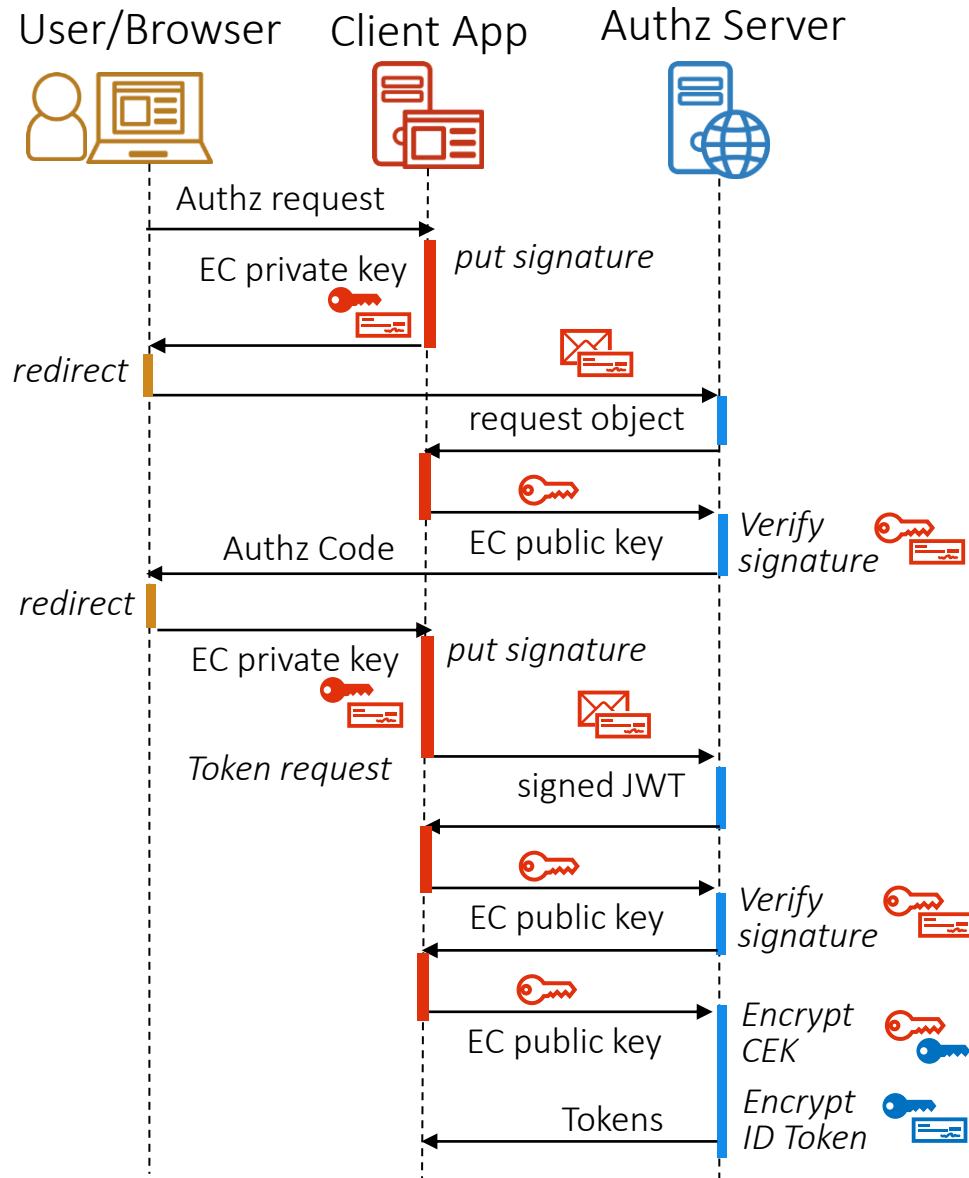
Security Profiles

- 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

- PSD2 
The Berlin Group NextGenPSD2
FAPI-RW App2App
- 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

OIDC Client's Public Key Management



PROPOSED DRAFT

[When client's public key is used]

- JWS Signature Verification
 - Message Authentication : Request Object
 - Client Authentication : JWT signed client authentication
- JWE CEK management (RSA1_5, RSA-OAEP)

[How to get client's EC public key]

- By Reference
 - Access URL specified by "jwks_uri" client metadata
- By Value
 - No way
- ➡
 - Dynamic Client Registration with "jwks" client metadata

[JIRA Ticket]

KEYCLOAK-10462 Improve support for setting keys for OIDC clients

END