FAPI-SIG Community 11th Meeting

@Web Conference

20 Jan 2021

PROPOSED DRAFT

Table of Contents

Major Topics

Status Updates from 10th Meeting

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

Future Topic Proposal

PROPOSED DRAFT

Major Topics

Major Topics

- Project : FAPI-RW

  OpenID Foundation will fix the final version of FAPI 1.0

  (FAPI-RO -> FAPI 1.0 Baseline, FAPI-RW -> FAPI 1.0 Advanced).

  Need to follow this final version of FAPI 1.0.

- Project : Client Policy Official Support

  Subproject : Client Policies for FAPI-RW

  All PRs needed to support FAPI-RW by using only Client Policy have been merged.

- Project : Client Policy Official Support

  Subproject : External Interfaces

  KEYCLOAK-16137 Client Policy : Support New Admin REST API

  Its design document has been approved and merged.

Status Updates from 10th Meeting FAPI-RW

PROPOSED DRAFT

Remaining Issues Status

6 Jan 2021		20 Jan 2021	
4 Issues in total			
3 Resolved	→	3 Resolved	+0
1 In Progress		1 In Progress	+0
0 Assigned		0 Assigned	+0
0 Not Assigned		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

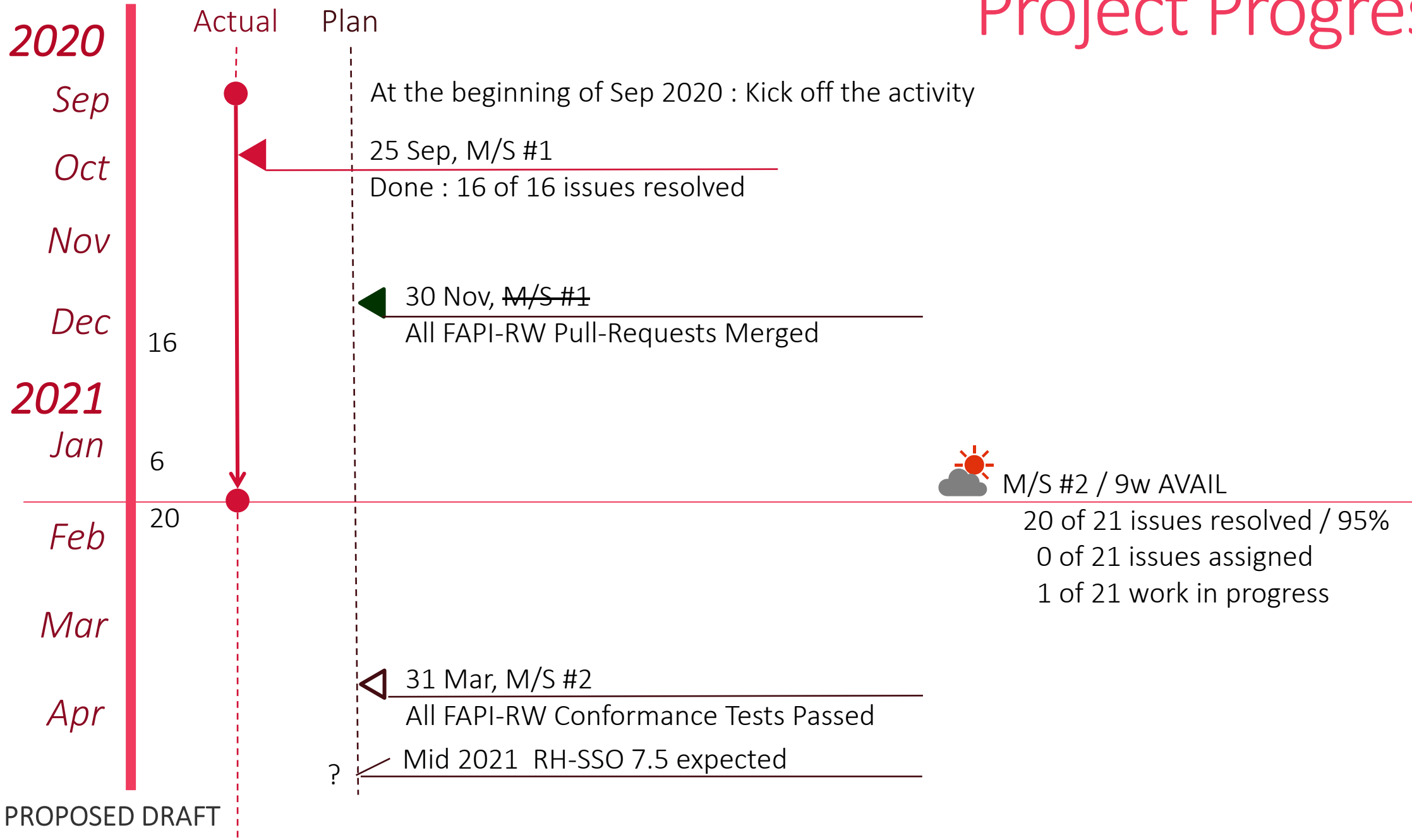
  FAPI-RW conformance test run automation completed.

  Integrating this automation onto keycloak codebase remains open.

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

  Resolved

Project Progress



Last Stretch - Following Final version of FAPI 1.0

[Motivation]

The current keycloak (12.0.1) 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]

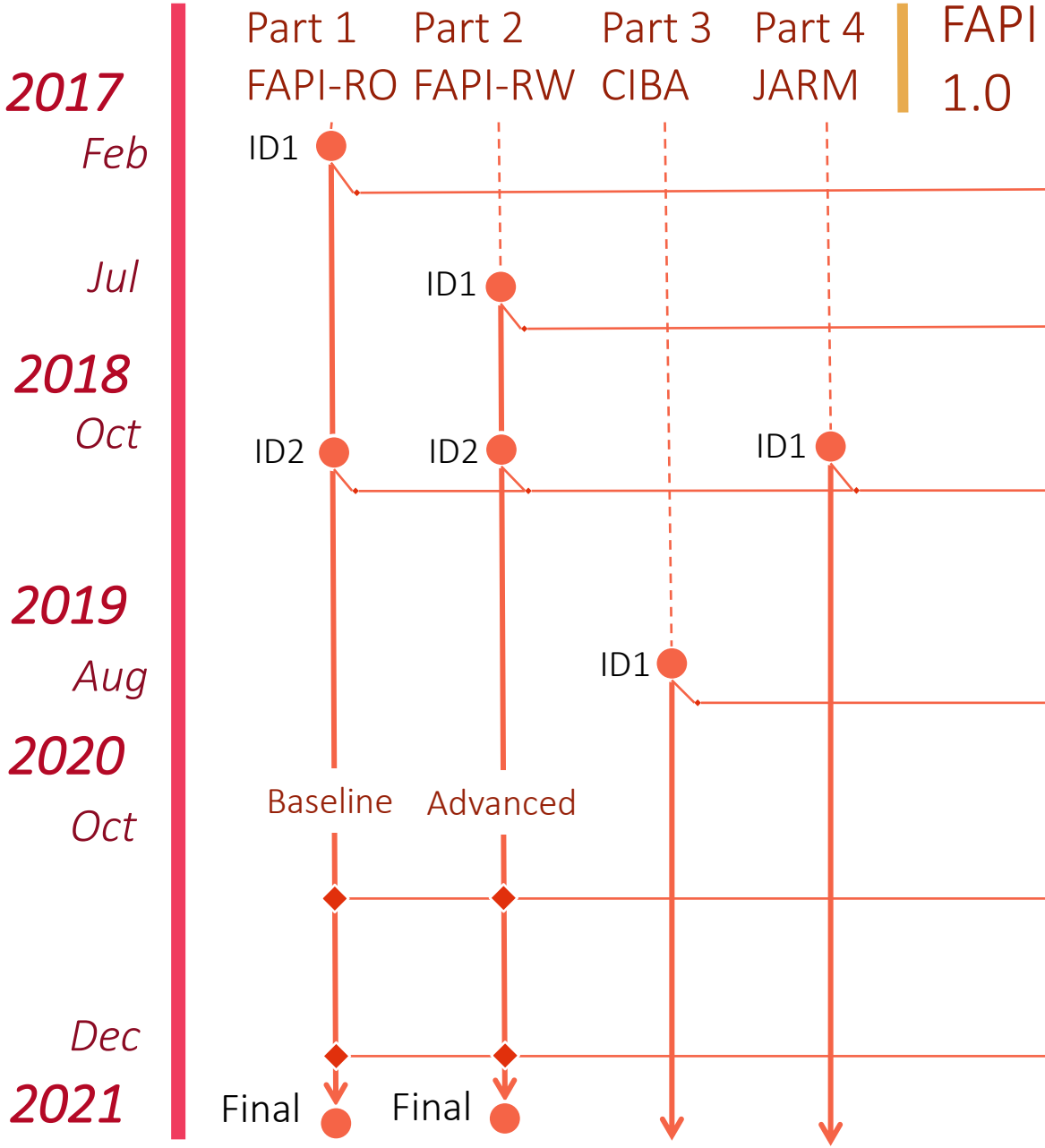
We need to do the following works :

- 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.

FAPI Milestone



19 Feb 2017 : FAPI Part 1 Implementer's Draft Approved[*1]

*1 : https://openid.net/2017/02/19/fapi-part-1-implementers-draft-approved/
http://openid.net/specs/openid-financial-api-part-1-ID1.html

24 Jul 2017 : FAPI Part 2 Implementer's Draft Approved[*2]

*2 : https://openid.net/2017/07/24/fapi-part-2-implementers-draft-approved/
http://openid.net/specs/openid-financial-api-part-2-ID1.html

24 Oct 2018 : Implementer's Drafts of Three FAPI Specifications Approved [*3]

*3 : https://openid.net/2018/10/24/implementers-drafts-of-three-fapi-specifications-approved/
http://openid.net/specs/openid-financial-api-part-1-ID2.html
http://openid.net/specs/openid-financial-api-part-2-ID2.html
http://openid.net/specs/openid-financial-api-jarm-ID1.html

23 Aug 2019 : Implementer's Draft of FAPI Client Initiated Backchannel Authentication (CIBA) Profile Approved [*4]

*4 : https://openid.net/2019/08/23/implementers-draft-of-fapi-client-initiated-backchannel-authentication-ciba-profile-approved/
https://openid.net/specs/openid-financial-api-ciba-ID1.html

29 Oct 2020 - 28 Dec 2020 : Public Review Period for Proposed Final FAPI 1.0 Part 1 and Part 2 Specifications[*5]

*5 : https://openid.net/2020/10/29/public-review-period-for-proposed-final-fapi-1-0-part-1-and-part-2-specifications/

29 Dec 2020 - 5 Jan 2021 : Vote for Proposed Final FAPI 1.0 Part 1 and Part 2 Specifications[*6]

*6 : https://openid.net/2020/11/30/notice-of-vote-for-proposed-final-fapi-1-0-part-1-and-part-2-specifications/

Status Updates from 10th Meeting FAPI-CIBA (poll mode)

Remaining Issues Status

6 Jan 2021		20 Jan 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

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) overriden 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

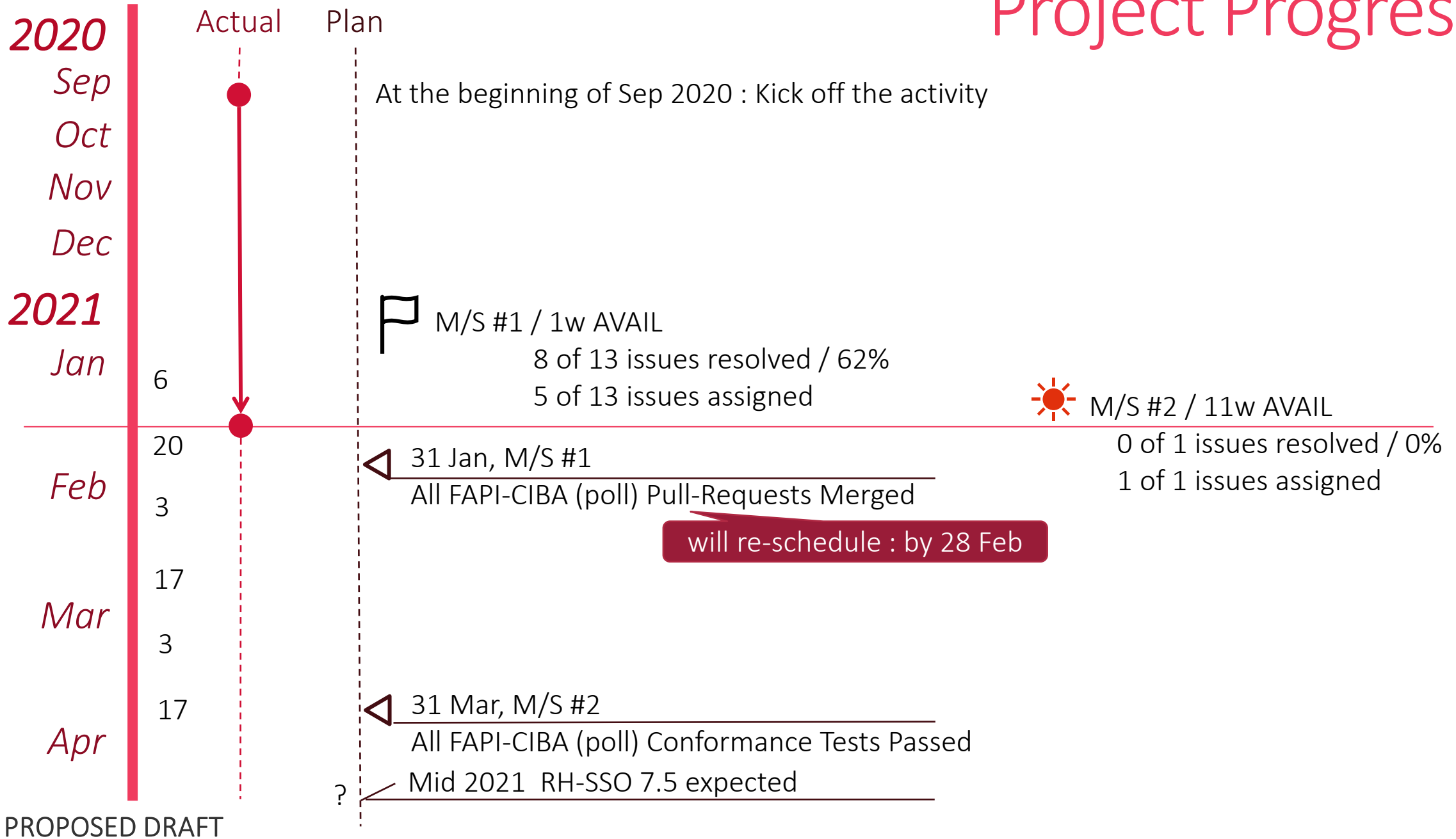
- FAPI-CIBA
  - #55 support id_token_hint

- FAPI-CIBA
  - #54 support login_hint_token

- FAPI-CIBA
  - #53 encrypt/decrypt login_hint

• • •

Project Progress



Status Updates from 10th 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

6 Jan 2021		20 Jan 2021	
6 Issues in total			
0 Resolved [0%]	→	1 Resolved [17%]	+1
2 In Progress		1 In Progress	-1
1 Assigned		1 Assigned	+0
3 Not Assigned		3 Not Assigned	+0

Issue status in detail : External Interfaces

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

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

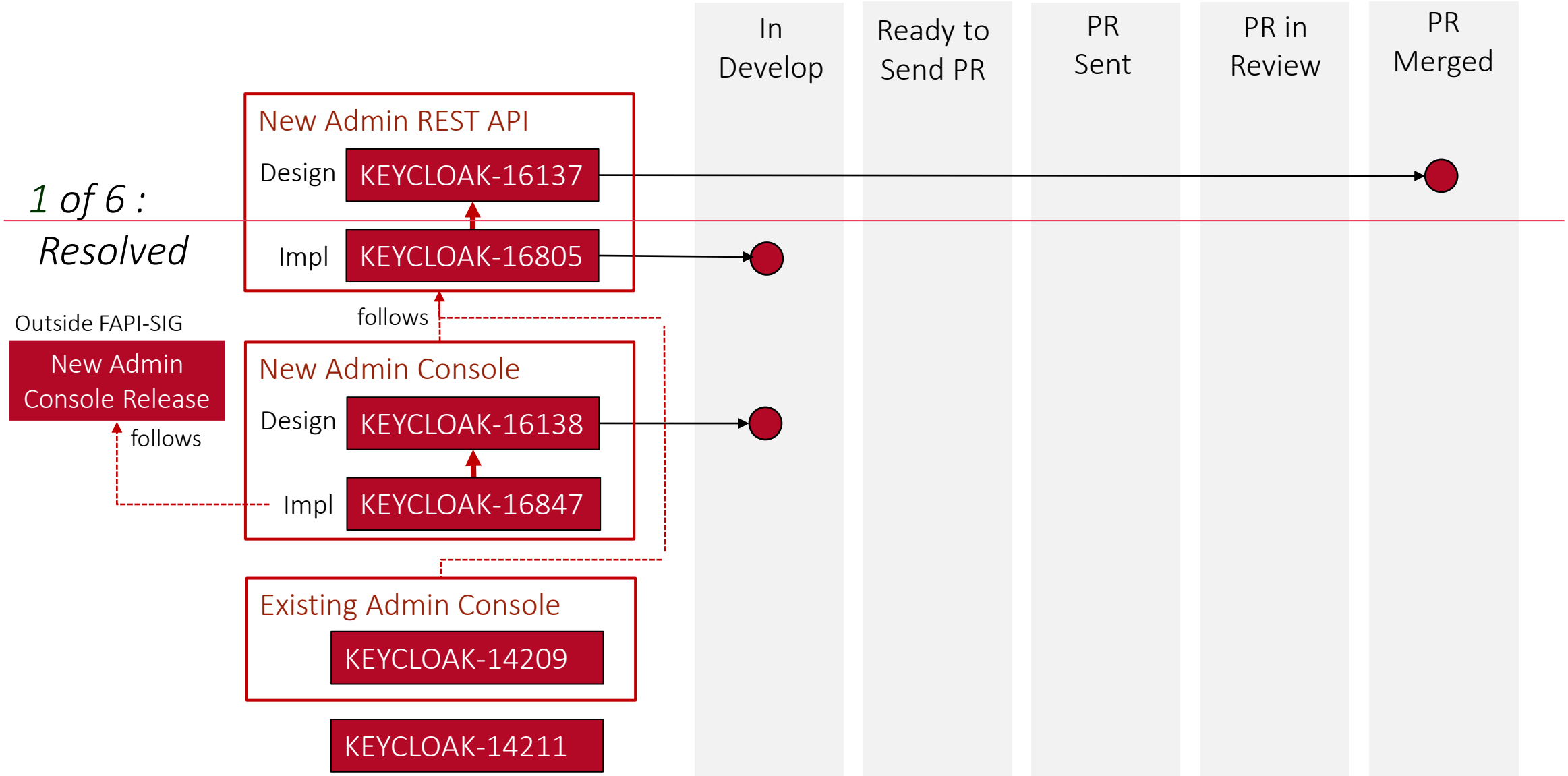
In Progress KEYCLOAK-16138 Client Policy : Support New Admin Console UI (Design)

- Concept Design by RH UXD team : https://marvelapp.com/prototype/6e70eh2/screen/74918976
- KEYCLOAK-16847 Client Policy : Support New Admin Console UI (Implementation)
- KEYCLOAK-14209 Client Policy : UI on Admin Console
- KEYCLOAK-14211 Client Policy : Remove Client Policy related individual settings on Admin Console

[Potential Blocking Factor]

- New Admin Console Release (not yet released)

Issue status in detail : External Interfaces



Issues Status - Client Policies for FAPI-RW

6 Jan 2021

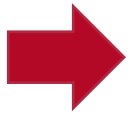
17 Issues in total

15 Resolved [88%]

2 In Progress

0 Assigned

0 Not Assigned



20 Jan 2021

17 Issues in total Completed

17 Resolved [100%] +2

2 In Progress -2

0 Assigned +0

0 Not Assigned +0

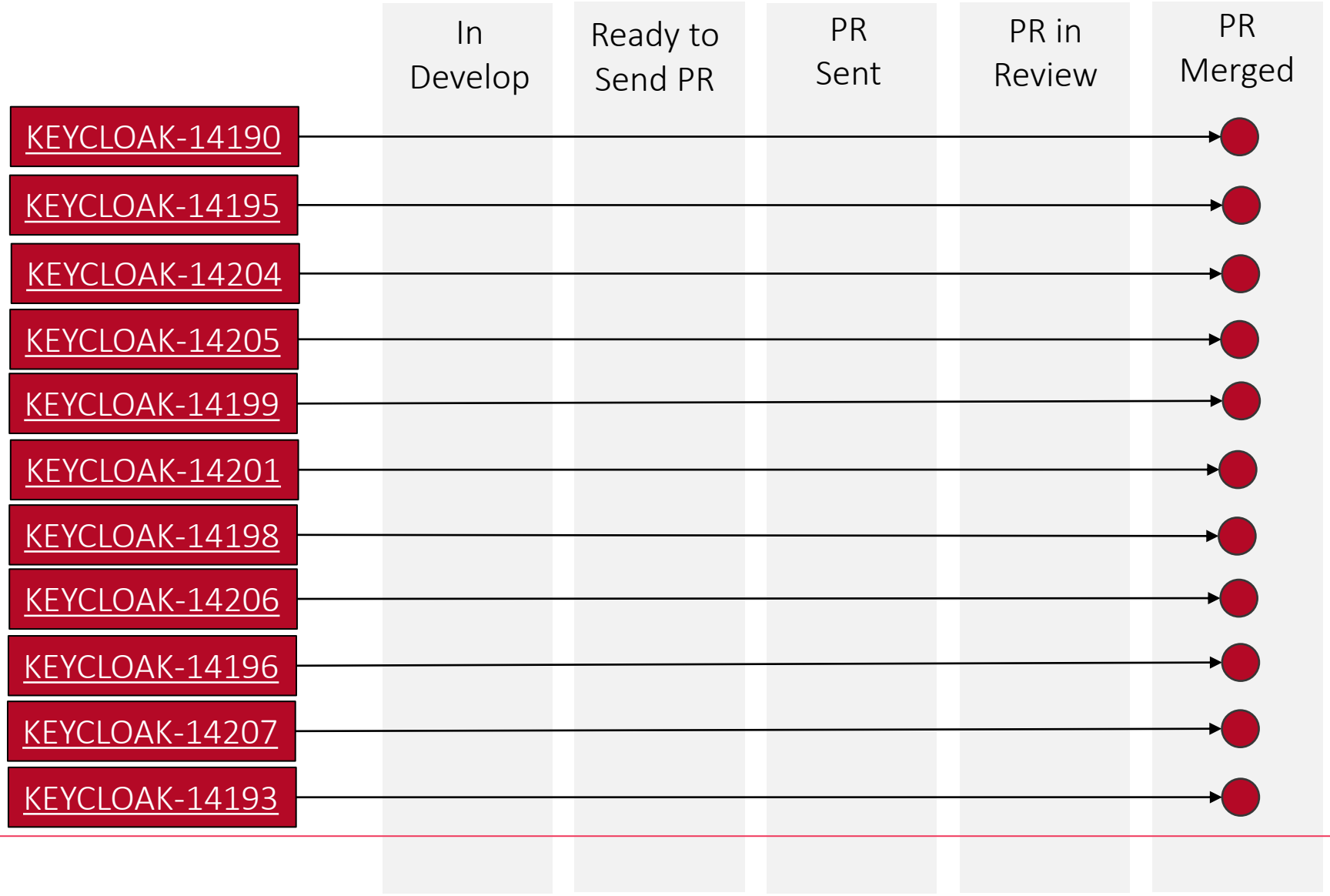
Issue status in detail : Client Policies for FAPI-RW

- 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

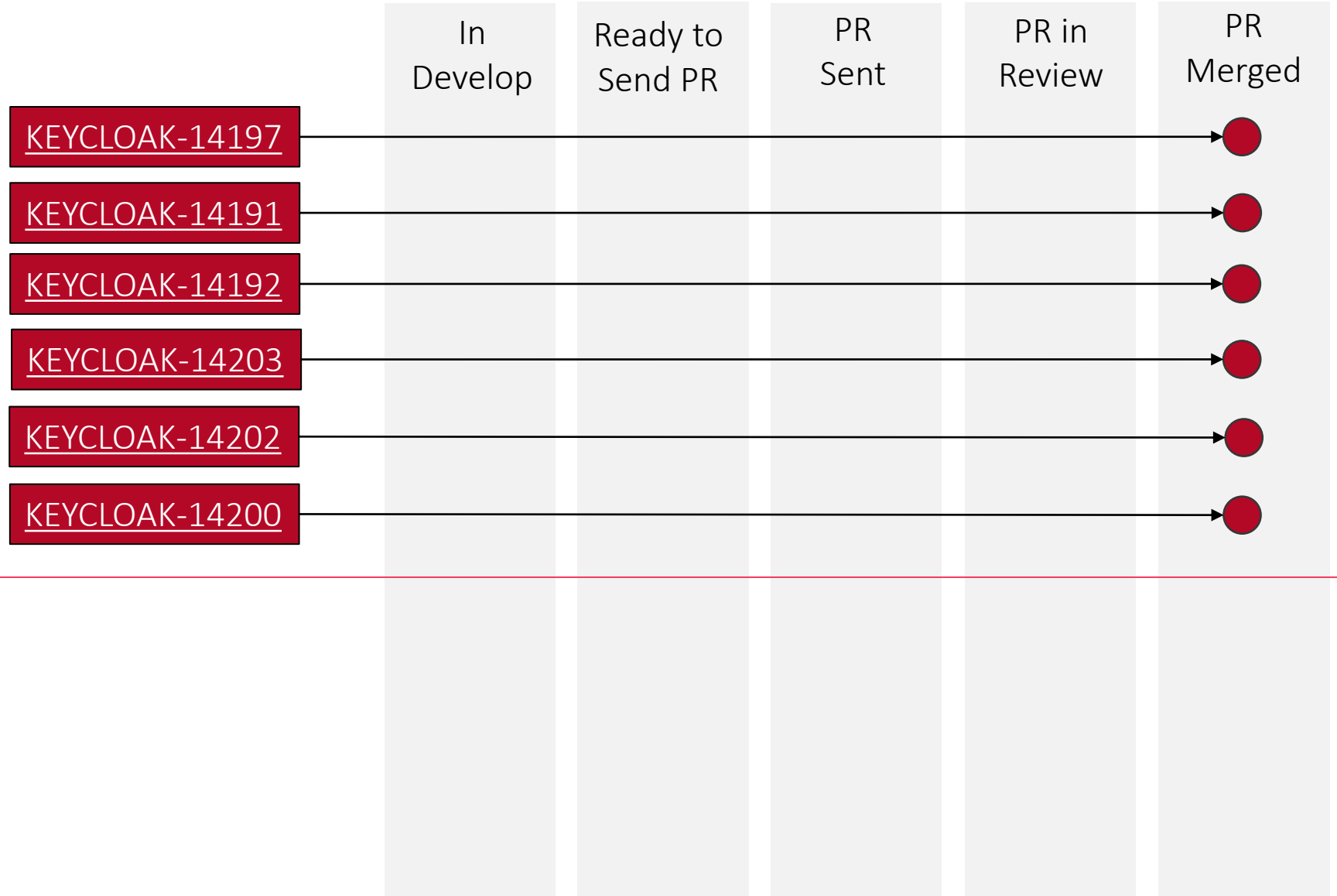
Issue status in detail : Client Policies for FAPI-RW

- Resolved — KEYCLOAK-14199 Client Policy - Executor : Enforce more secure client authentication method when client registration
- Resolved — KEYCLOAK-14200 Client Policy - Executor : Enforce Holder-of-Key Token
- Resolved — KEYCLOAK-14201 Client Policy - Executor : Enforce Proof Key for Code Exchange (PKCE)
- Resolved — 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

Issue status in detail : Client Policies for FAPI-RW



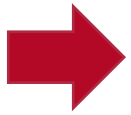
Issue status in detail : Client Policies for FAPI-RW



17 of 17 :

Resolved

Issues Status - Client Registration Policies Migration

6 Jan 2021		20 Jan 2021	
3 Issues in total			
0 Resolved [0%]		0 Resolved [0%]	+0
3 In Progress		9 In Progress	+6
0 Assigned		0 Assigned	+0
0 Not Assigned		1 Not Assigned	+1

Issue status in detail : Client Registration Policies Migration

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

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

PR Ready KEYCLOAK-16806 Client Policy : Implement existing "ClientDisabledClientRegistrationPolicy" as Client Policies' executor

PR Ready KEYCLOAK-16807 Client Policy : Implement existing "ClientScopesClientRegistrationPolicy" as Client Policies' executor

PR Ready KEYCLOAK-16808 Client Policy : Implement existing "ConsentRequiredClientRegistrationPolicy" as Client Policies' executor

PR Ready KEYCLOAK-16809 Client Policy : Implement existing "MaxClientsClientRegistrationPolicy" as Client Policies' executor

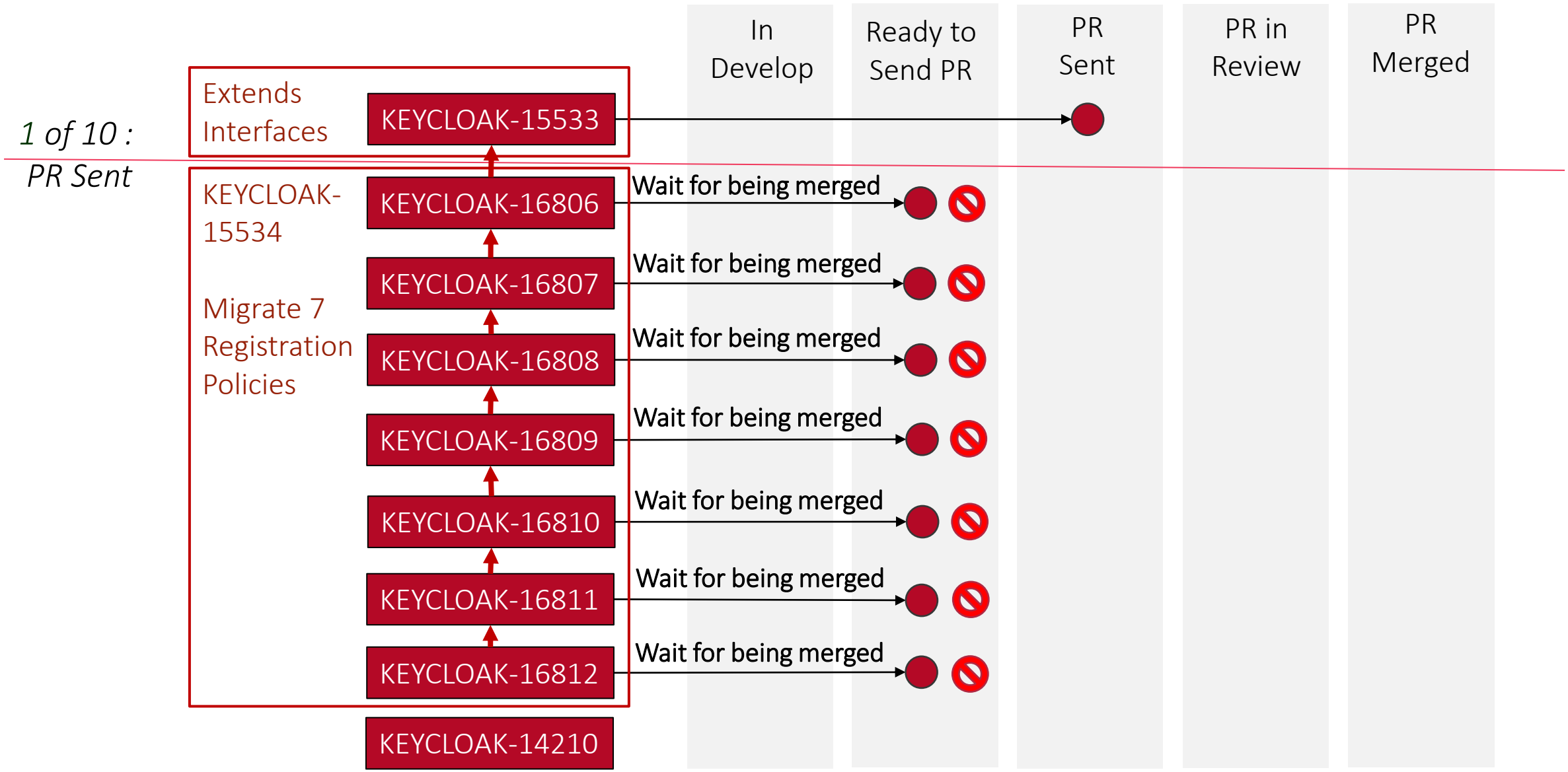
PR Ready KEYCLOAK-16810 Client Policy : Implement existing "ProtocolMappersClientRegistrationPolicy" as Client Policies' executor

PR Ready KEYCLOAK-16811 Client Policy : Implement existing "ScopeClientRegistrationPolicy" as Client Policies' executor

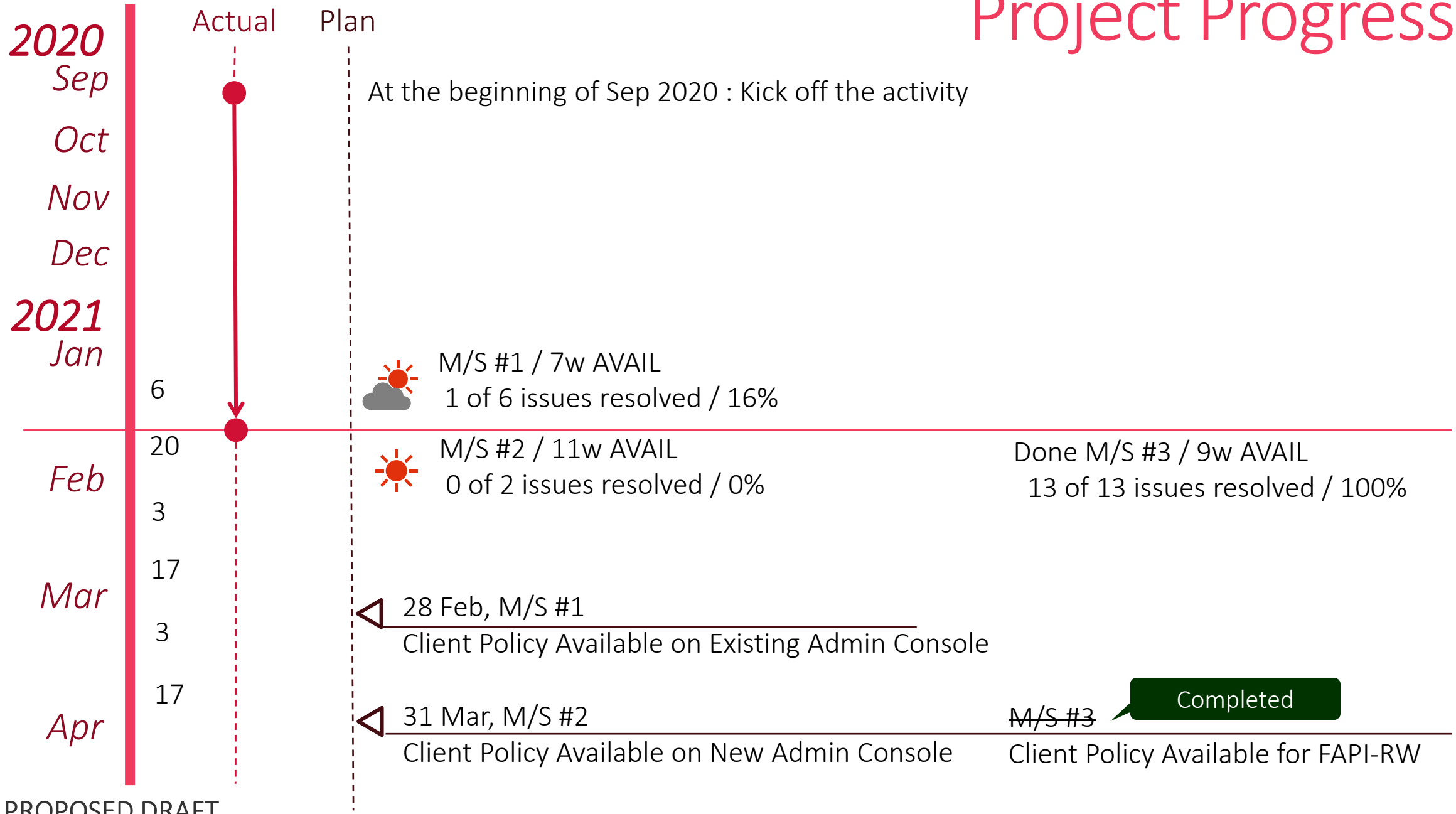
PR Ready KEYCLOAK-16812 Client Policy : Implement existing "TrustedHostClientRegistrationPolicy" as Client Policies' executor

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

Issue status in detail : Client Registration Policies Migration



Project Progress



PROPOSED DRAFT

Future Topic Proposal

Keycloak PSD2 support

- PSD2 
  - Support requirements from eIDAS

    TPP’s QWAC verification of Client Authentication on TLS layer

    1. Confirm that TPP’s certificate is QWAC that was issued from QTSP.
    2. Confirm that TPP’s certificate as QWAC does not expire and was not revoked.
    3. Confirm that TPP’s certificate follows QWAC profile.
    4. Confirm that what TPP’s certificate as QWAC states is true (roles, PSP ID).

Keycloak PSD2 support - Current Status

- PSD2 
  - Support requirements from eIDAS

    TPP's QWAC verification of Client Authentication on TLS layer

    1. Confirm that TPP's certificate is QWAC that was issued from QTSP.

       -> It can realize it by using only QTSP's certificates as keycloak's trust anchors and manage them.

    2. Confirm that TPP's certificate as QWAC does not expire and was not revoked.

       -> The end user authentication by X.509 has already supported revocation check by CRL/OCSP while the client authentication by X.509 not.

    3. Confirm that TPP's certificate follows QWAC profile.

    4. Confirm that what TPP's certificate as QWAC states is true (roles, PSP ID).

END