FAPI-SIG Community 8th Meeting

@Web Conference

2 Dec 2020

PROPOSED DRAFT

Table of Contents

Status Updates from 7th Meeting

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

Project Progress

Follow-up Tasks

Meeting Schedule Proposal

Status Updates from 7th Meeting FAPI-RW

Remaining Issues Status

17 Nov 2020

4 Issues in total

- 1 Resolved
- 1 In Progress
- 2 Assigned
- 0 Not Assigned

1 Dec 2020

1 Resolved	+0
1 In Progress	+0
2 Assigned	+0
0 Not Assigned	+0

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]

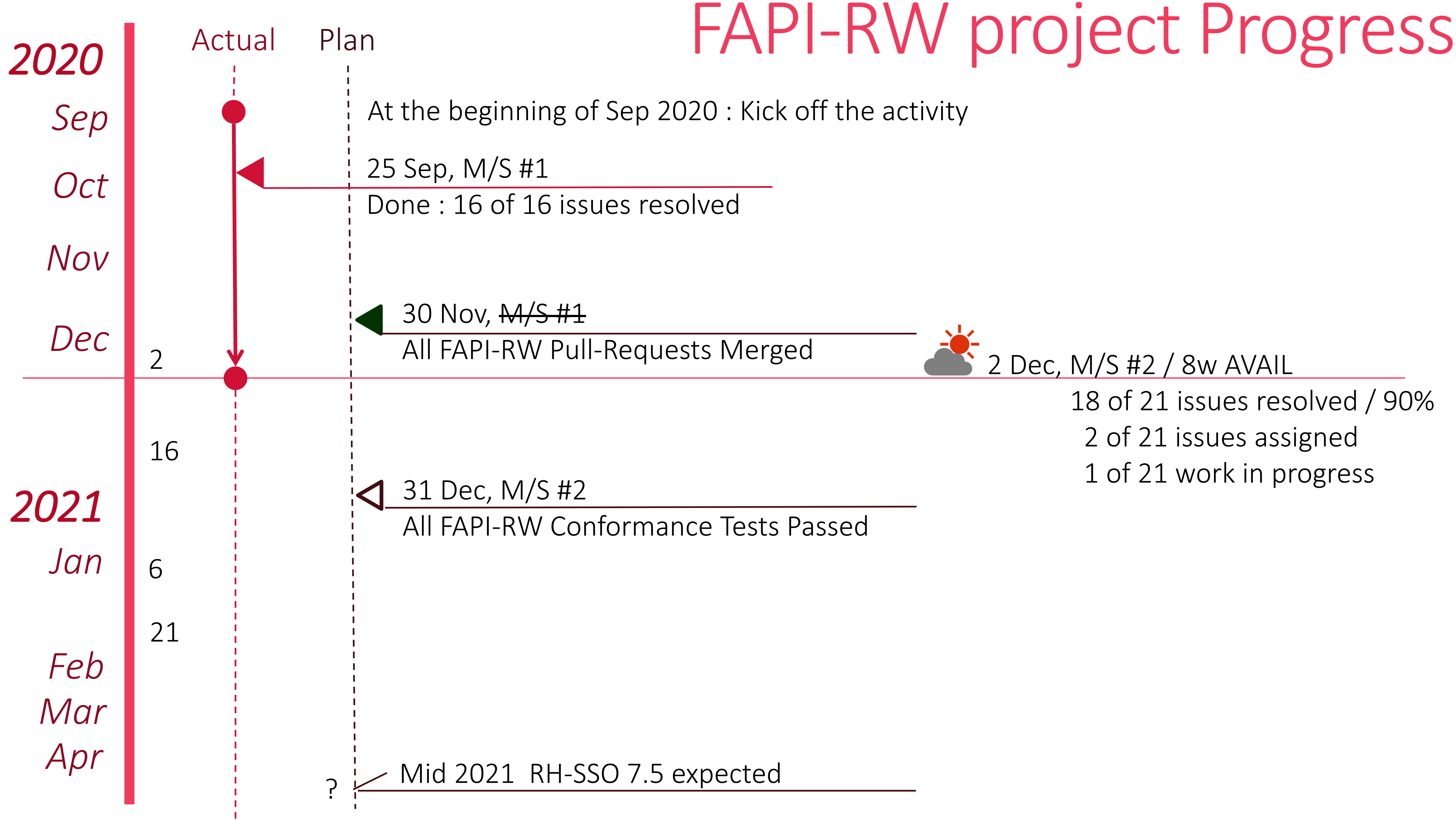
- #45 Integrating FAPI-RW conformance tests run into keycloak's CI/CD pipeline

  FAPI-RW conformance test run automation completed.

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

  Resolved

FAPI-RW project Progress



Actual Plan

2020

Sep At the beginning of Sep 2020 : Kick off the activity

25 Sep, M/S #1
Done : 16 of 16 issues resolved

Oct

Nov

30 Nov, ~~M/S #1~~
All FAPI-RW Pull-Requests Merged

Dec

2

⛅ 2 Dec, M/S #2 / 8w AVAIL
18 of 21 issues resolved / 90%
2 of 21 issues assigned
1 of 21 work in progress

16

31 Dec, M/S #2
All FAPI-RW Conformance Tests Passed

2021

Jan

6

21

Feb

Mar

Apr

? Mid 2021 RH-SSO 7.5 expected

PROPOSED DRAFT

Status Updates from 7th Meeting
FAPI-CIBA (poll mode)

Subtasks Status

17 Nov 2020	1 Dec 2020	
13 Subtasks in total		
7 Resolved [54%]	8 Resolved [62%]	+1
1 In Progress	1 In Progress	+0
5 Assigned	4 Assigned	-1
0 Not Assigned	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) 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

PROPOSED DRAFT

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

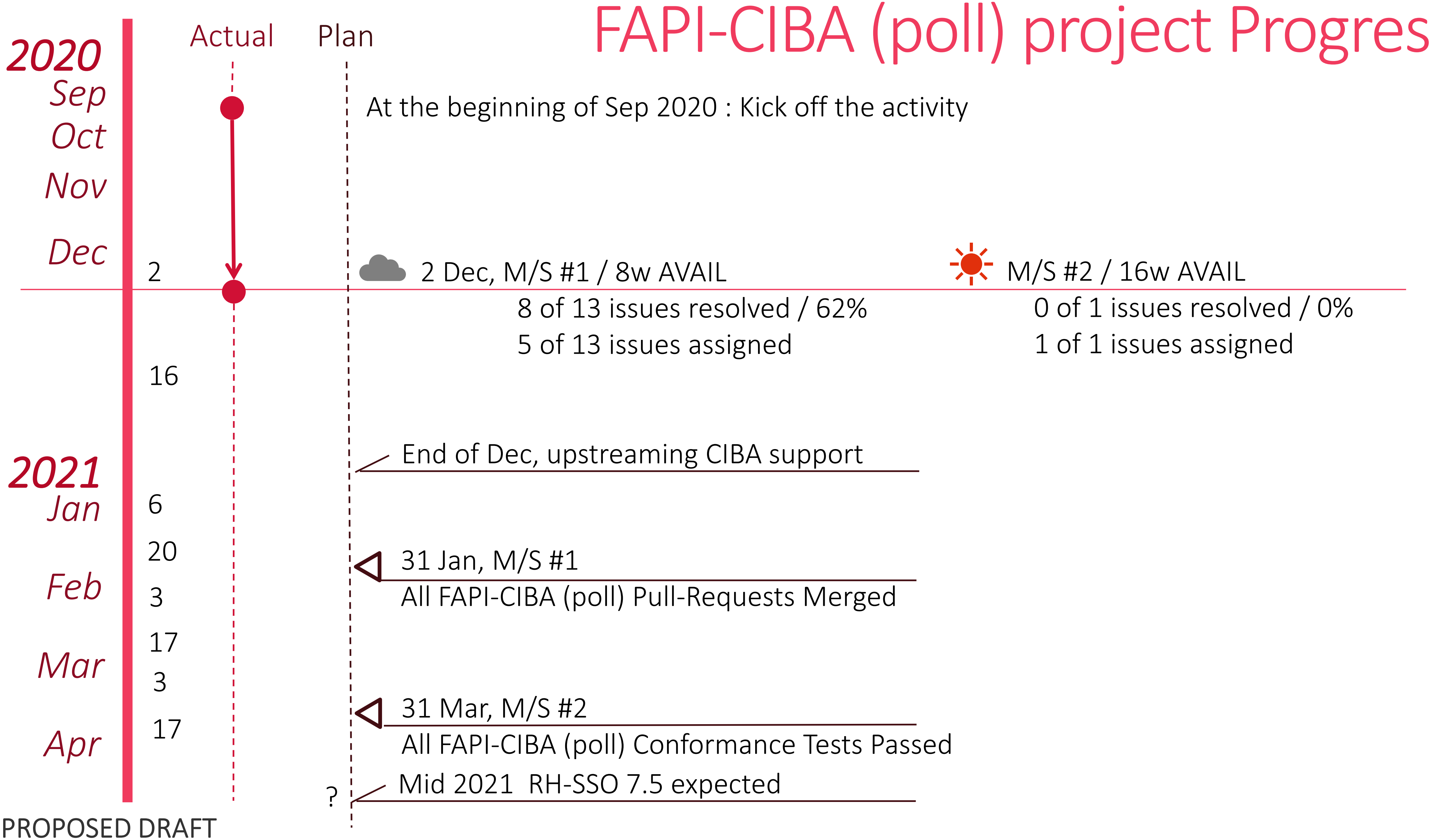
  Assigned

[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



Actual

Plan

2020 Sep

Oct

Nov

Dec

2

16

2021 Jan

6

20

Feb

3

17

Mar

3

17

Apr

At the beginning of Sep 2020 : Kick off the activity

☁ 2 Dec, M/S #1 / 8w AVAIL

8 of 13 issues resolved / 62%

5 of 13 issues assigned

☀ M/S #2 / 16w AVAIL

0 of 1 issues resolved / 0%

1 of 1 issues assigned

End of Dec, upstreaming CIBA support

◁ 31 Jan, M/S #1

All FAPI-CIBA (poll) Pull-Requests Merged

◁ 31 Mar, M/S #2

All FAPI-CIBA (poll) Conformance Tests Passed

? Mid 2021 RH-SSO 7.5 expected

PROPOSED DRAFT

Status Updates from 7th 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

17 Nov 2020

5 Issues in total

- 0 Resolved [0%]
- 0 In Progress
- 2 Assigned
- 3 Not Assigned

1 Dec 2020

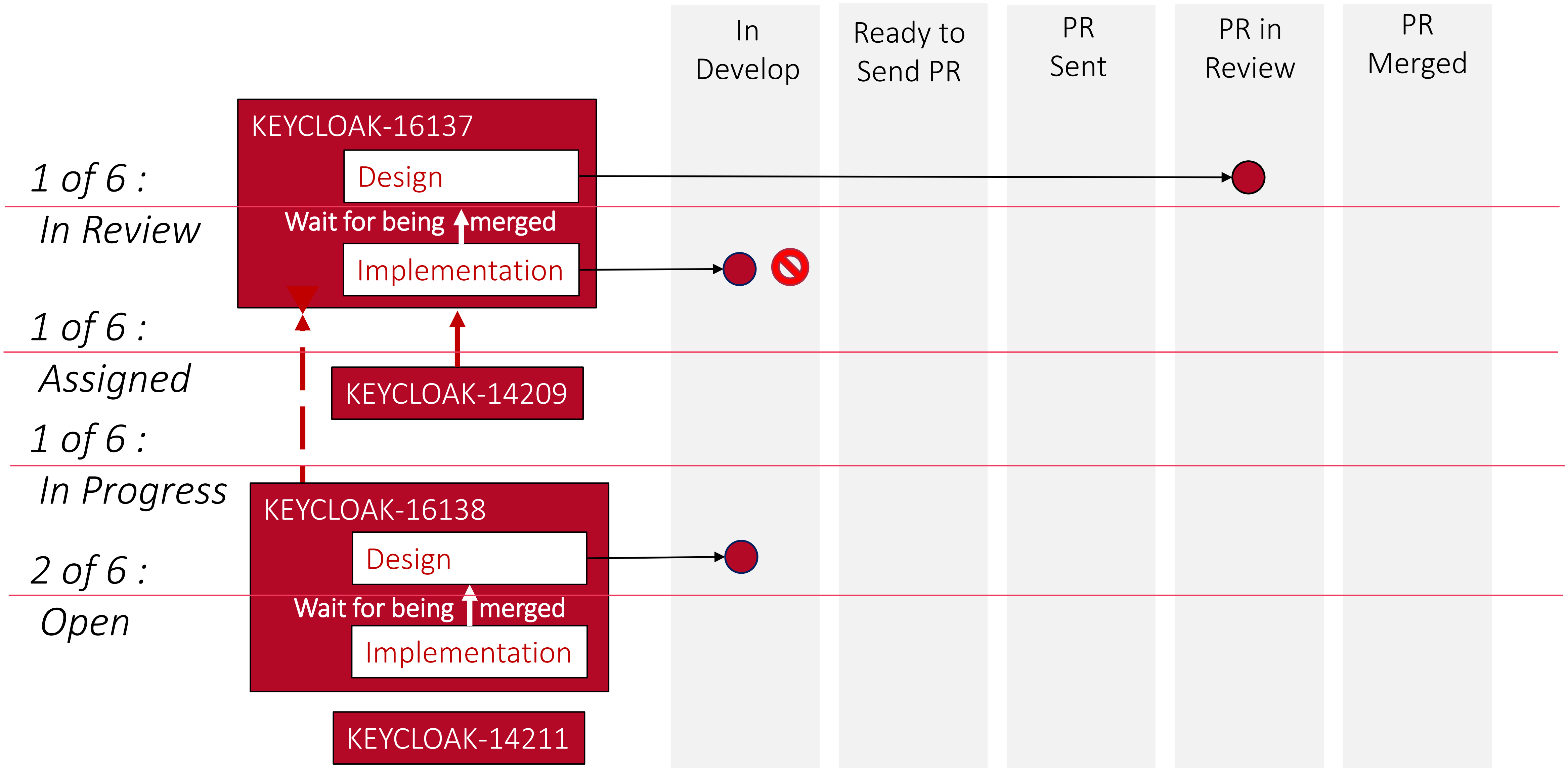
6 Issues in total

0 Resolved [0%]	+0
2 In Progress	+2
1 Assigned	-1
3 Not Assigned	-0

Subproject : External Interfaces

- KEYCLOAK-16137 Client Policy : Support New Admin REST API (Clear JSON Representation)
  - ✓ In Review Design
  - Assigned Implementation
- KEYCLOAK-16138 Client Policy : Support New Admin Console UI
  - ✓ In Progress 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



In Develop

Ready to Send PR

PR Sent

PR in Review

PR Merged

1 of 6 :

In Review

KEYCLOAK-16137

Design

Wait for being merged

Implementation

1 of 6 :

Assigned

KEYCLOAK-14209

1 of 6 :

In Progress

KEYCLOAK-16138

Design

Wait for being merged

Implementation

2 of 6 :

Open

KEYCLOAK-14211

Issues Status - Subproject: Client Policies for FAPI-RW

17 Nov 2020		1 Dec 2020	
18 Issues in total		17 Issues in total	
10 Resolved [56%]	→	11 Resolved [65%]	+1
2 In Progress		2 In Progress	+0
4 Assigned		4 Assigned	+0
1 Not Assigned		0 Not Assigned	-1

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
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
In Review	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
InProgress	KEYCLOAK-14200 Client Policy - Executor : Enforce Holder-of-Key Token
RESOLVED	KEYCLOAK-14201 Client Policy - Executor : Enforce Proof Key for Code Exchange (PKCE)
Ready to Send PR	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

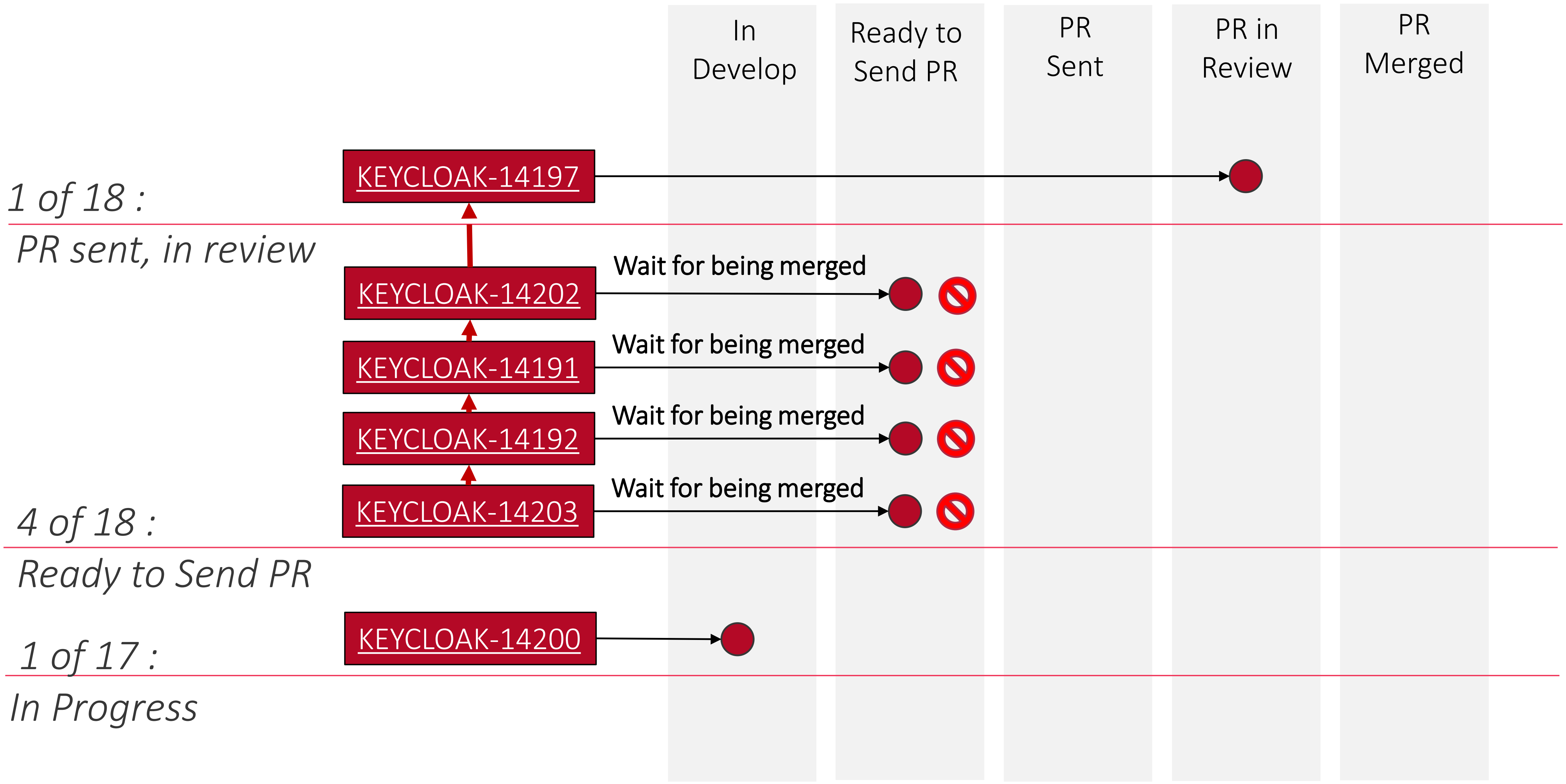
	In Develop	Ready to Send PR	PR Sent	PR in Review	PR Merged
KEYCLOAK-14190					●
KEYCLOAK-14195					●
KEYCLOAK-14204					●
KEYCLOAK-14205					●
KEYCLOAK-14199					●
KEYCLOAK-14201					●
KEYCLOAK-14198					●
KEYCLOAK-14206					●
KEYCLOAK-14196					●
KEYCLOAK-14207					●
KEYCLOAK-14193					●

11 of 17 :

Resolved

PROPOSED DRAFT

Subproject : Client Policies for FAPI-RW



In Develop

Ready to Send PR

PR Sent

PR in Review

PR Merged

1 of 18 :
PR sent, in review

KEYCLOAK-14197

KEYCLOAK-14202 — Wait for being merged

KEYCLOAK-14191 — Wait for being merged

KEYCLOAK-14192 — Wait for being merged

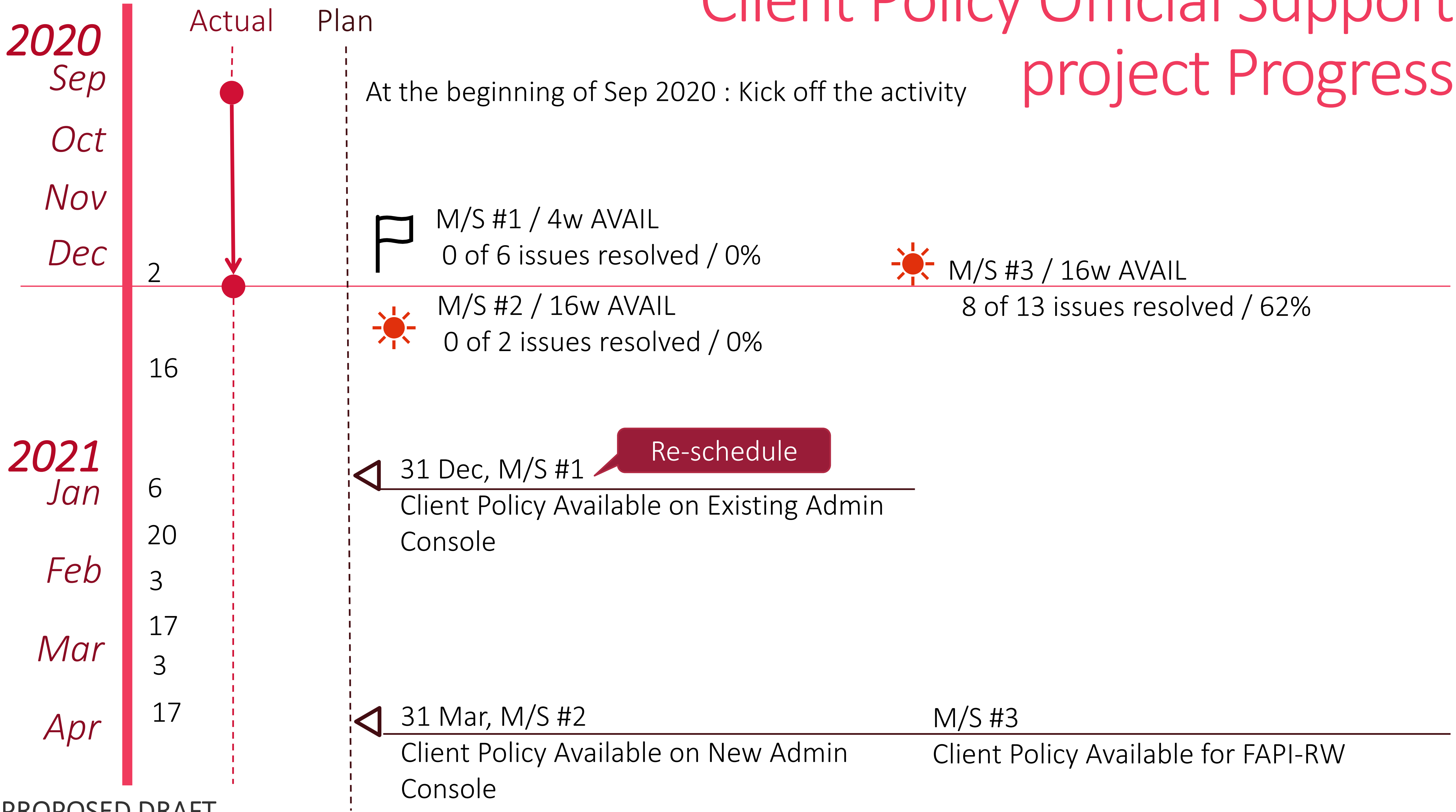
KEYCLOAK-14203 — Wait for being merged

4 of 18 :
Ready to Send PR

KEYCLOAK-14200

1 of 17 :
In Progress

Client Policy Official Support project Progress



Actual

Plan

2020
Sep
Oct
Nov
Dec

2021
Jan
Feb
Mar
Apr

2
16
6
20
3
17
3
17

At the beginning of Sep 2020 : Kick off the activity

⚑ M/S #1 / 4w AVAIL
0 of 6 issues resolved / 0%

☀ M/S #2 / 16w AVAIL
0 of 2 issues resolved / 0%

☀ M/S #3 / 16w AVAIL
8 of 13 issues resolved / 62%

◁ 31 Dec, M/S #1
Client Policy Available on Existing Admin Console

Re-schedule

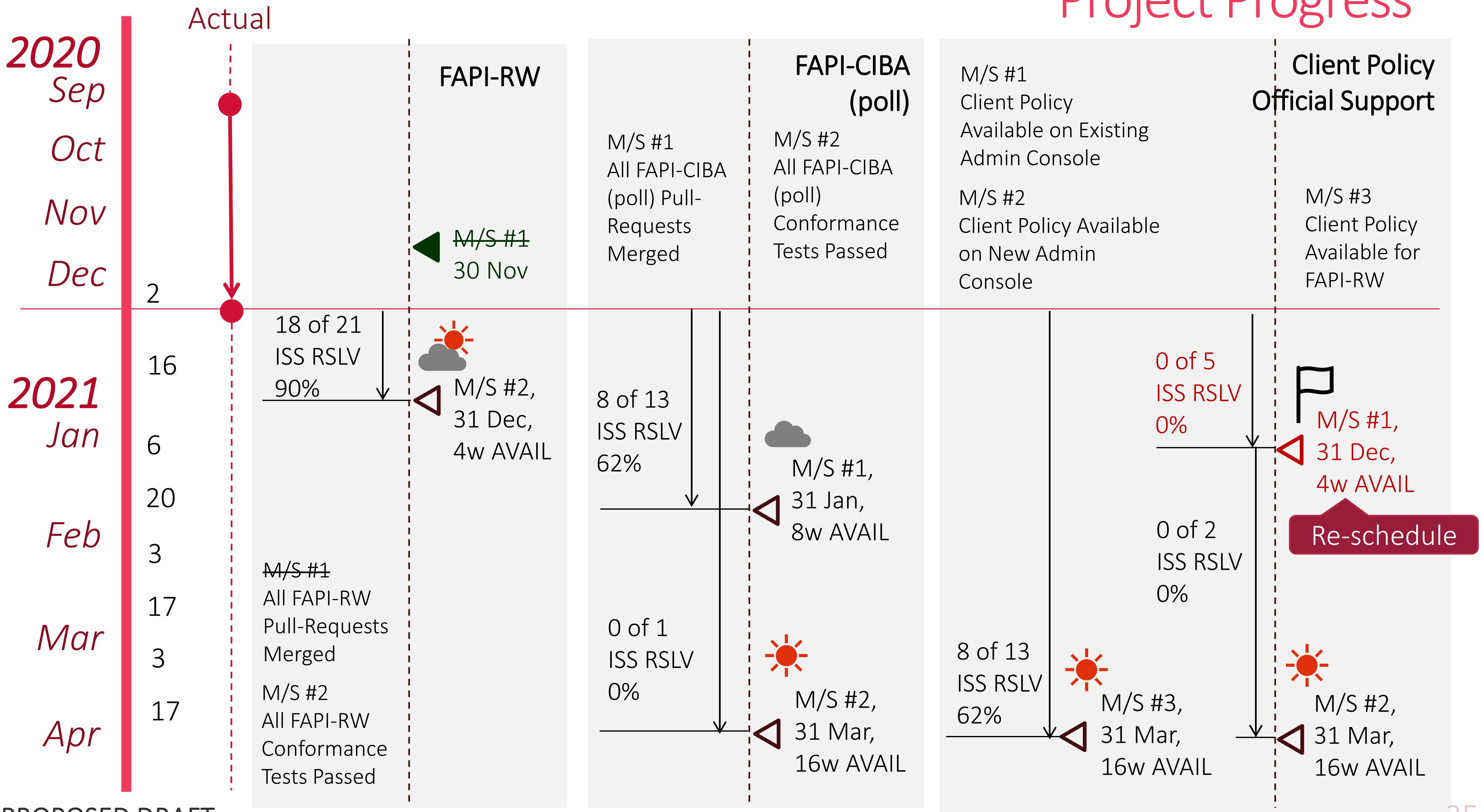
◁ 31 Mar, M/S #2
Client Policy Available on New Admin Console

M/S #3
Client Policy Available for FAPI-RW

PROPOSED DRAFT

Project Progress

Project Progress



Actual

2020
Sep
Oct
Nov
Dec
2
16
2021
Jan
6
20
Feb
3
17
Mar
3
17
Apr

FAPI-RW

~~M/S #1~~
30 Nov

18 of 21
ISS RSLV
90%

M/S #2,
31 Dec,
4w AVAIL

~~M/S #1~~
All FAPI-RW
Pull-Requests
Merged

M/S #2
All FAPI-RW
Conformance
Tests Passed

FAPI-CIBA (poll)

M/S #1
All FAPI-CIBA
(poll) Pull-Requests
Merged

M/S #2
All FAPI-CIBA
(poll)
Conformance
Tests Passed

8 of 13
ISS RSLV
62%

M/S #1,
31 Jan,
8w AVAIL

0 of 1
ISS RSLV
0%

M/S #2,
31 Mar,
16w AVAIL

Client Policy Official Support

M/S #1
Client Policy
Available on Existing
Admin Console

M/S #2
Client Policy Available
on New Admin
Console

M/S #3
Client Policy
Available for
FAPI-RW

0 of 5
ISS RSLV
0%

M/S #1,
31 Dec,
4w AVAIL

Re-schedule

0 of 2
ISS RSLV
0%

8 of 13
ISS RSLV
62%

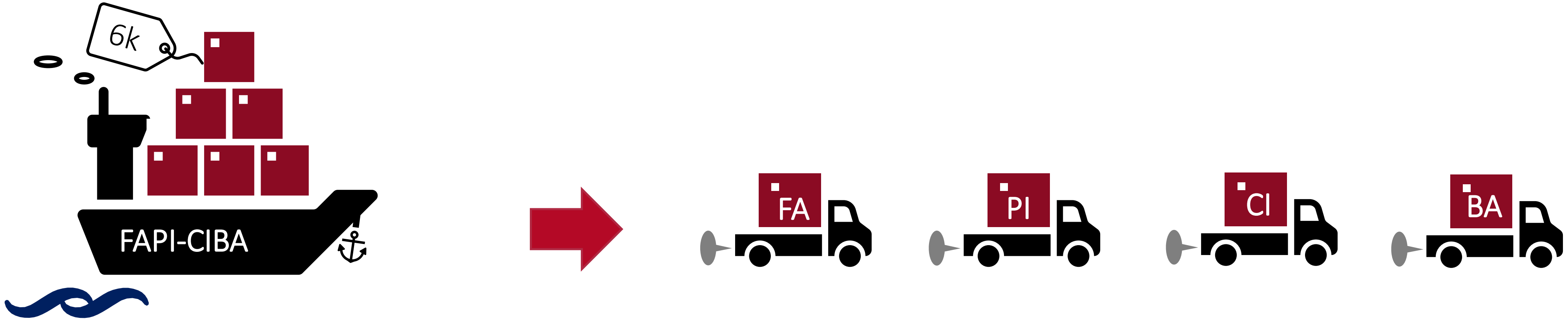
M/S #3,
31 Mar,
16w AVAIL

M/S #2,
31 Mar,
16w AVAIL

PROPOSED DRAFT

Follow-up Tasks

FAPI-CIBA : one-by-one small PRs Instead of one big PR



The PR for FAPI-CIBA (poll) support will be about 6ksteps. It is hard for the keycloak development team to review this PR.

Therefore, I would like to break down this big PR into several PRs as follows.

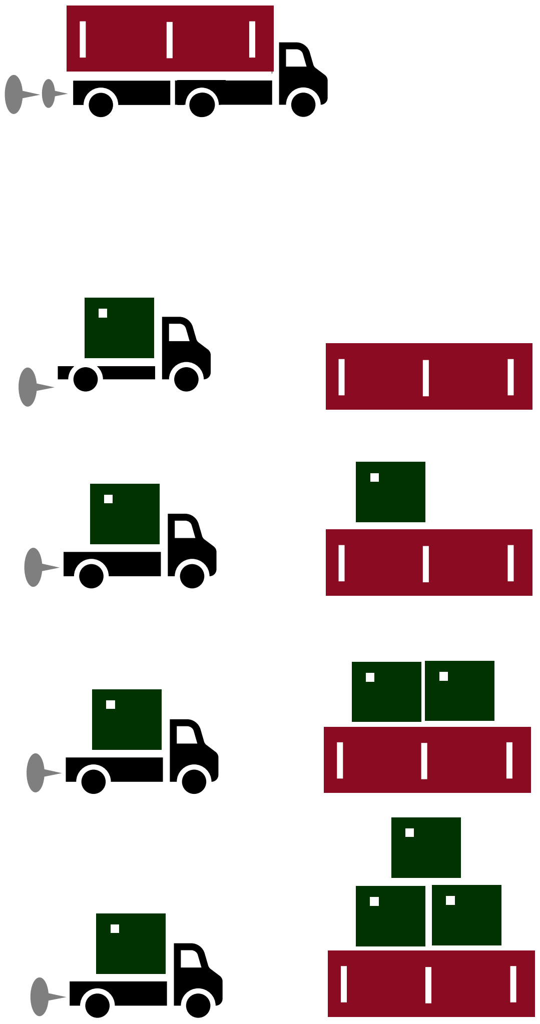
- Pure CIBA : KEYCLOAK-12137 OpenID Connect Client Initiated Backchannel Authentication (CIBA)

  At first, send the PR for CIBA support not conforming with FAPI-CIBA (poll mode)

- FAPI-CIBA : KEYCLOAK-11846 OpenID Connect Financial-grade API: Client Initiated Backchannel Authentication Profile

  After merging the Pure CIBA PR, send PRs implementing features needed for FAPI-CIBA (poll mode) consecutively

CIBA-FAPI : one-by-one small PRs Instead of one big PR

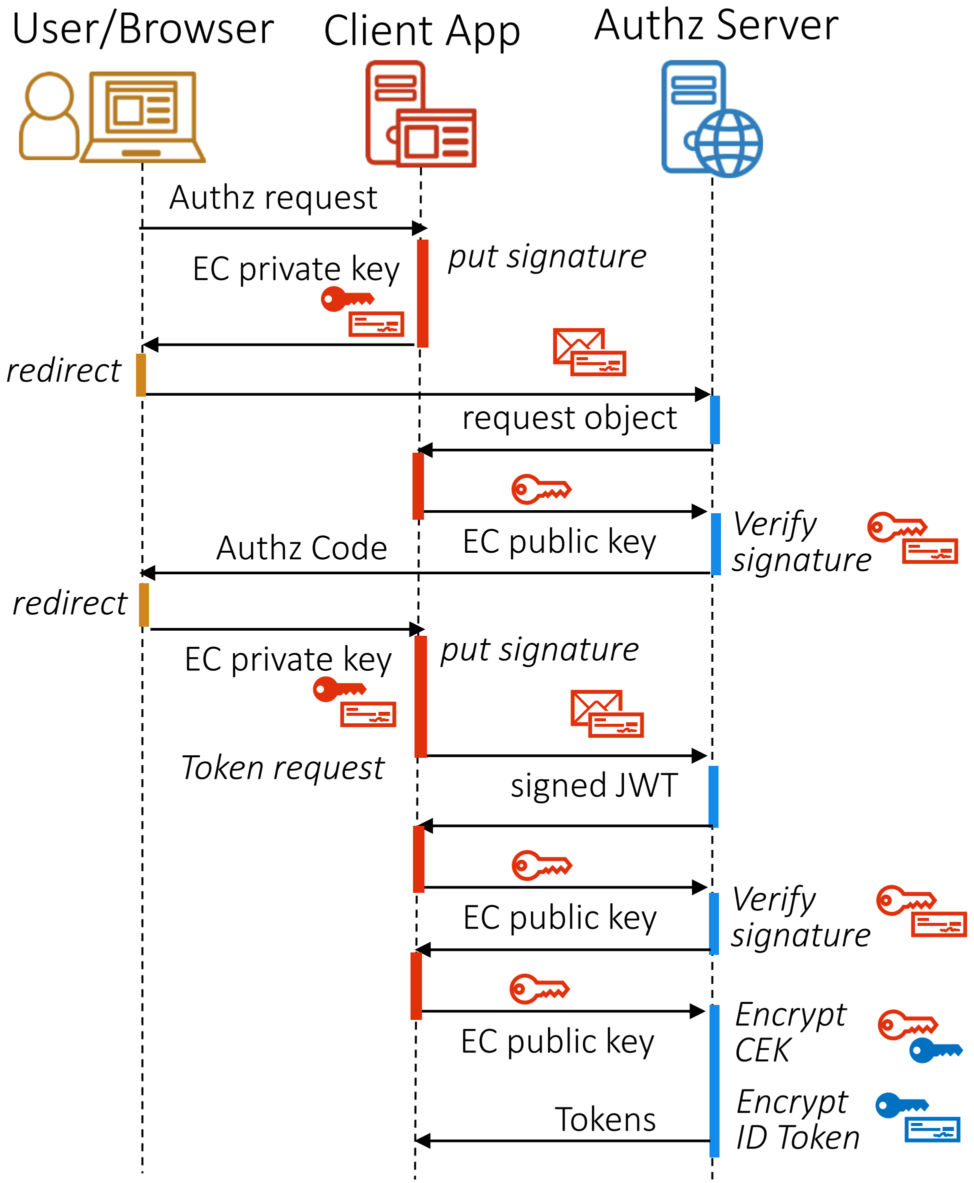


- Pure CIBA
  - CIBA Implementation based on its prototype (tnorimat/ciba-prototype)
  - #59 Use Only Auth Result Cache by Infinispan For CIBA Flow Session Binding
  - #60 Use Only Auth Result Cache on Communication with Decoupled Auth Server
  - #61 Token Request Throttling Information Not Cluster-wide 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

OIDC Client’s Public Key Management



[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

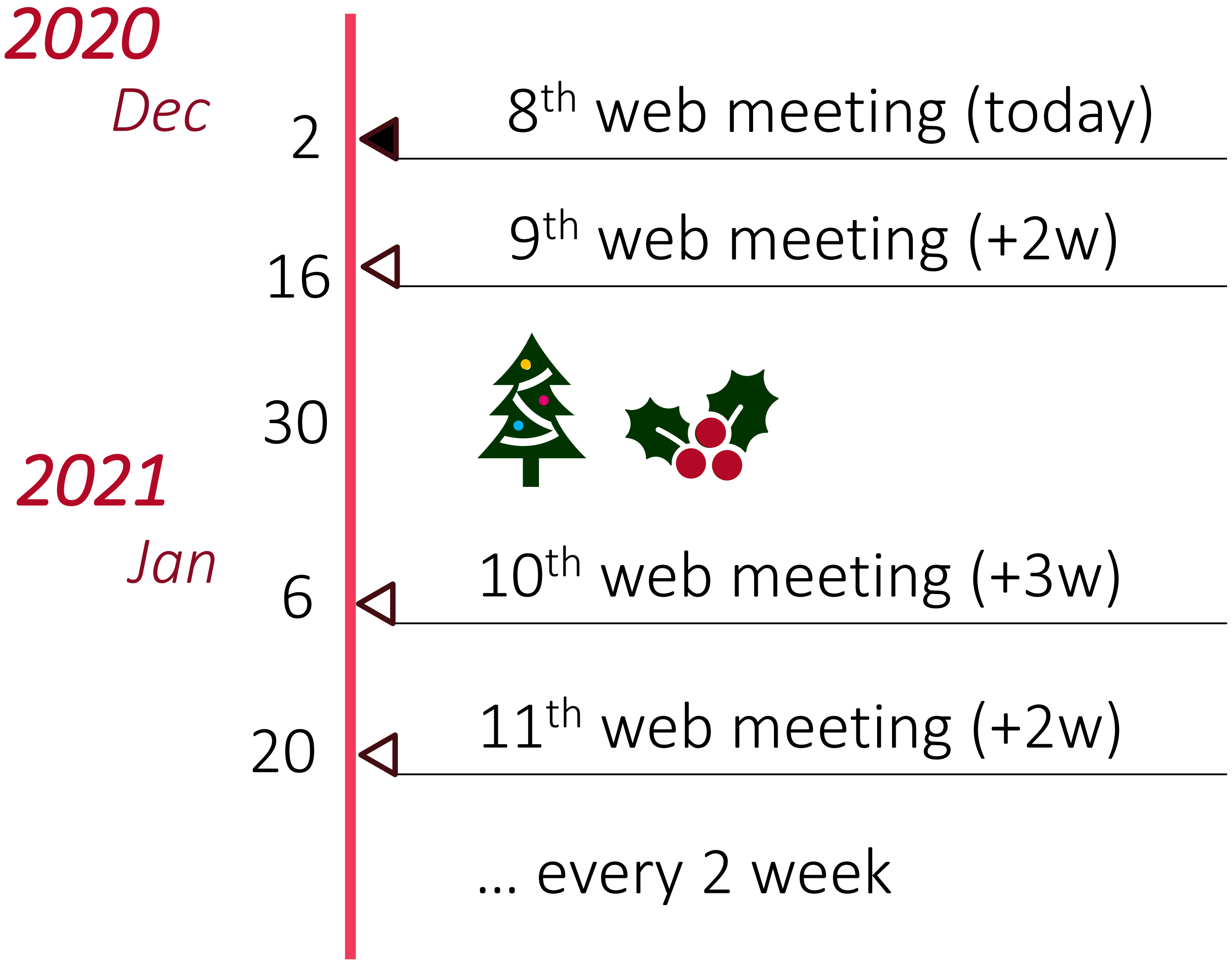
[JIRA Ticket]

KEYCLOAK-10462 Improve support for setting keys for OIDC clients

PROPOSED DRAFT

Meeting Schedule Proposal

Meeting Schedule Proposal



2020

Dec

2 — 8th web meeting (today)

16 — 9th web meeting (+2w)

30

2021

Jan

6 — 10th web meeting (+3w)

20 — 11th web meeting (+2w)

… every 2 week

END