FAPI-SIG Community 13th Meeting

@Web Conference

17 Feb 2021

PROPOSED DRAFT

Table of Contents

PROPOSED DRAFT

Major Topics

Major Topics

- Project : Client Policy Official Support
  PR sent

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

Status Updates from 12th Meeting FAPI-RW

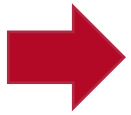
PROPOSED DRAFT

Remaining Issues Status

3 Jan 2021

4 Issues in total

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



17 Feb 2021

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

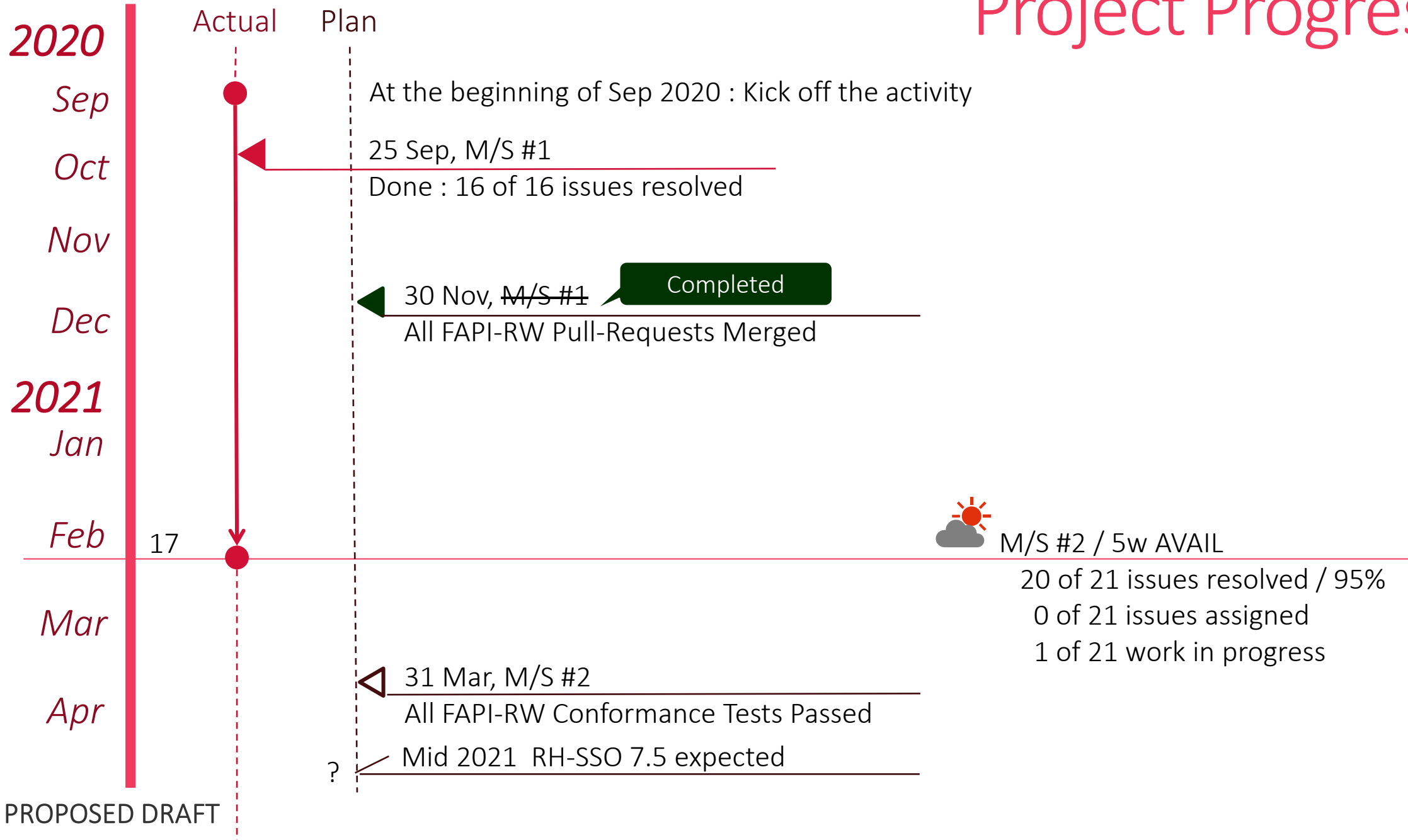
- #45 Integrating FAPI-RW conformance tests run into keycloak's CI/CD pipeline

  FAPI-RW conformance test run automation completed. Integrating this automation onto keycloak codebase remains open.

- Follow the final version of FAPI 1.0

  Not yet published so that we can not start working on.

Project Progress



Status Updates from 12th Meeting FAPI-CIBA (poll mode)

Remaining Issues Status

3 Jan 2021		17 Feb 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

- #56 support Signed Authentication Request

  In Review
- #58 Realm Settings (CIBA Policy) overriden 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

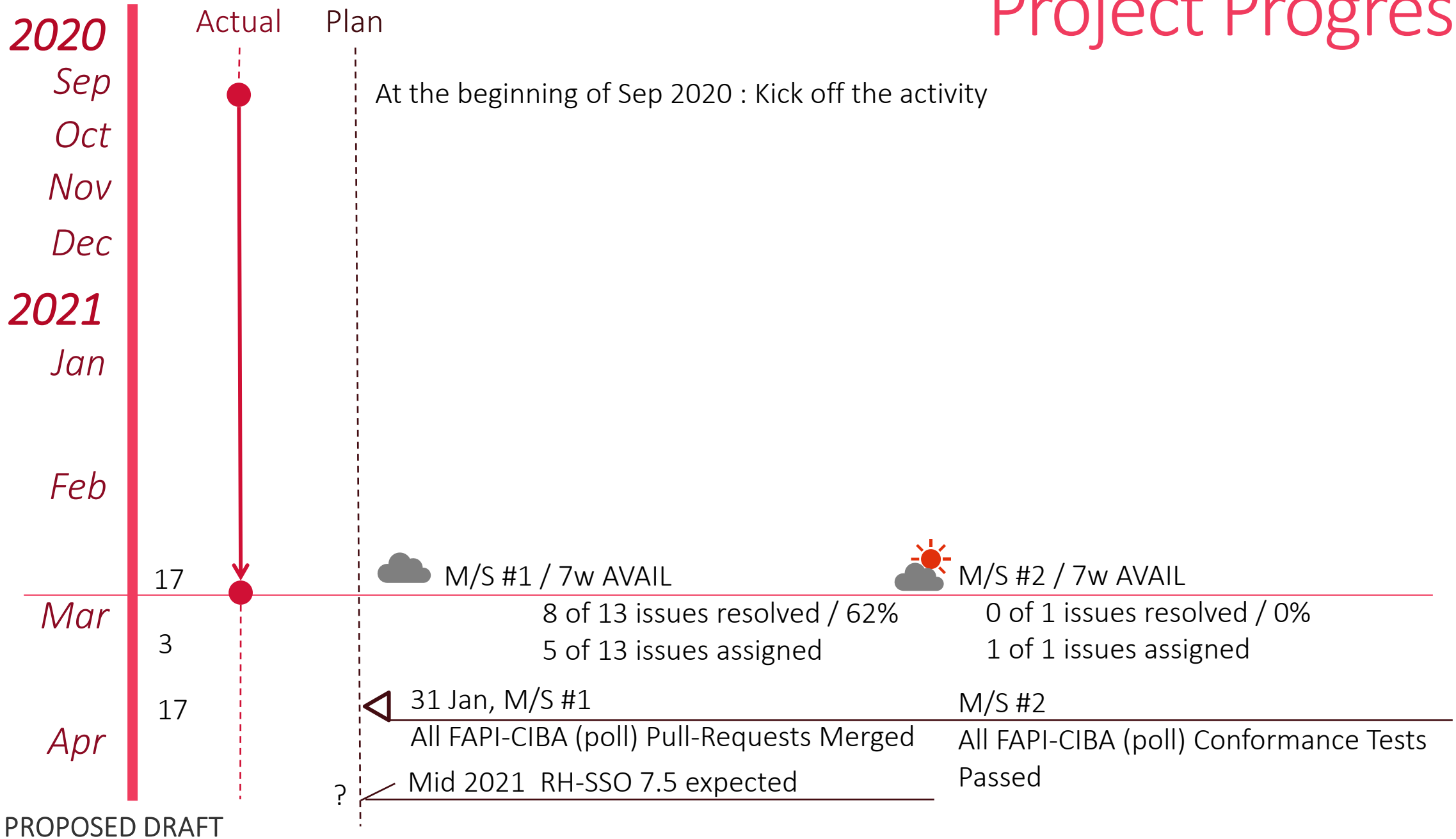
- FAPI-CIBA
  - #54 support login_hint_token

- FAPI-CIBA
  - #53 encrypt/decrypt login_hint

• • •

PROPOSED DRAFT

Project Progress



Status Updates from 12th 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 Jan 2021		17 Feb 2021	
6 Issues in total			
1 Resolved [17%]	→	1 Resolved [17%]	+0
1 In Progress		1 In Progress	+0
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)

PR Sent 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]

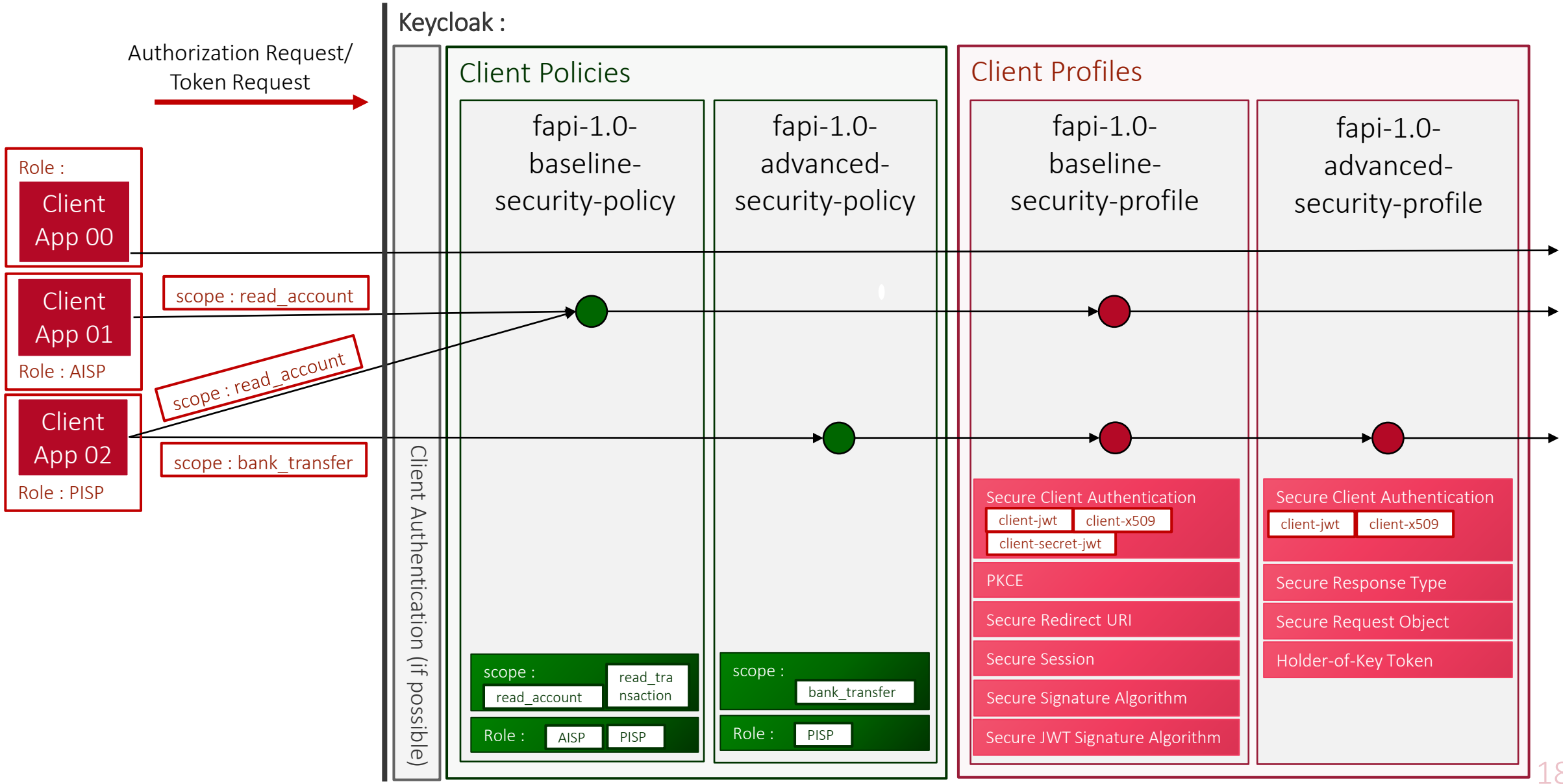
- New Admin Console Release (not yet released)

JSON Representation for Client Profiles/Policies

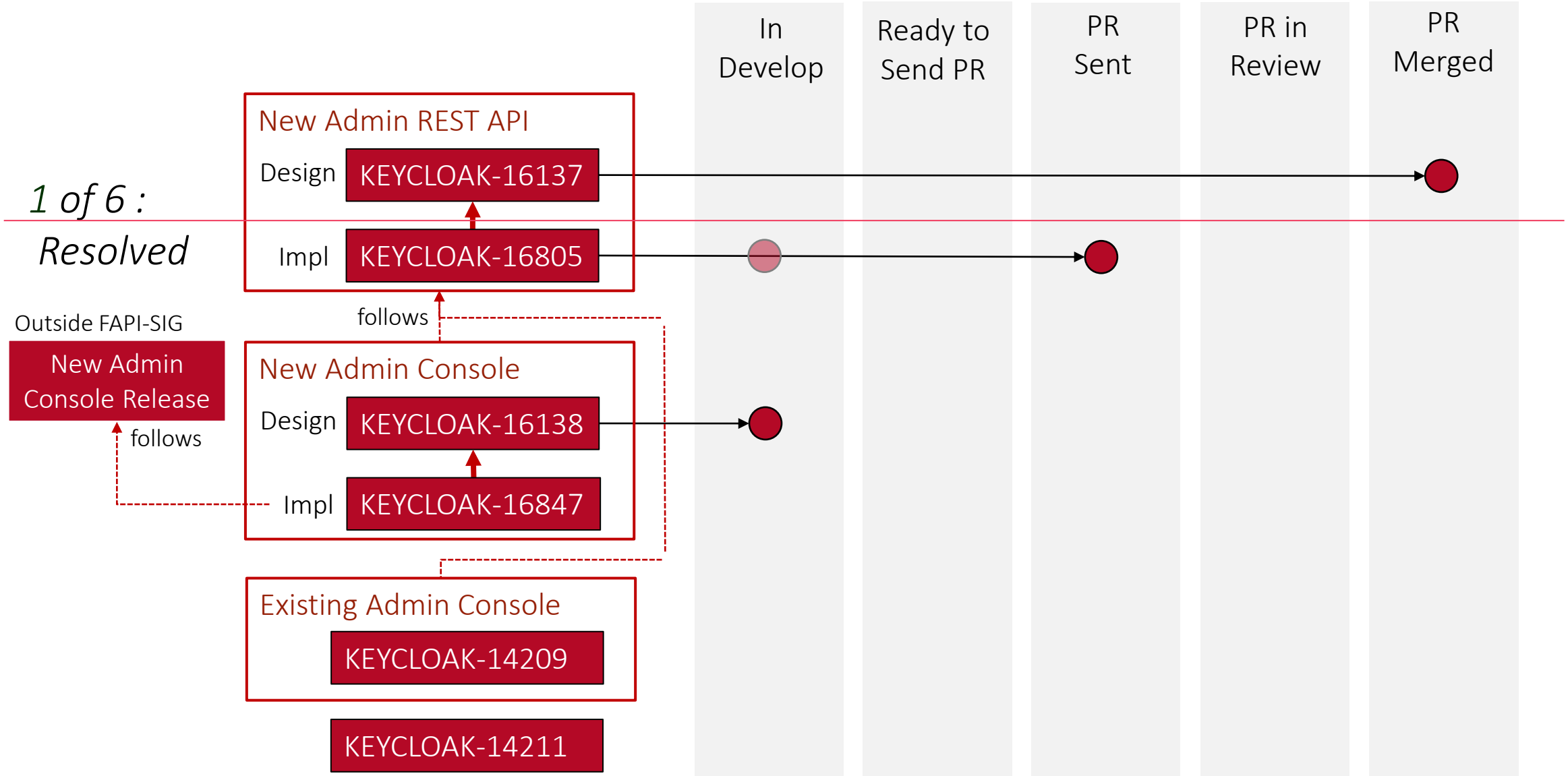
```
"profiles" : [  {
     "name" : "fapi-1.0-baseline-security-profile”,
     “description” : “FAPI 1.0 Baseline Security Profile",
     "builtin" : false,
     "executors" : [ {
        "secure-client-authn-executor" : {
         "client-authns" : ["client-secret-jwt", "client-jwt", "client-x509" ],
         "is-augment" : false }
       }, { "pkce-enforce-executor" : { "is-augment" : true }
       }, { "secure-redirecturi-enforce-executor" : { }
       }, { "secure-session-enforce-executor" : { }
       }, { "securesignalg-enforce-executor" : { }
       }, { "securesignalgjwt-enforce-executor" : { }
       } ]
   }, {
     "name" : "fapi-1.0-advanced-security-profile",
     "description" : "FAPI 1.0 Advanced Security Profile
                      (additional requirements of Baseline)",
     "builtin" : false,
     "executors" : [ {
       "secure-client-authn-executor" : {
         "client-authns" : [ "client-jwt", "client-x509" ],
         "is-augment" : false }
     }, { "holder-of-key-enforce-executor" : { "is-augment" : true }
     }, { "secure-reqobj-executor" : { }
     }, { "secure-responsetype-executor" : { }
     } ] } ] }
```

```
"policies" : [ {
     "name" : "fapi-1.0-baseline-security-policy",
     "builtin" : true,
     "enable" : true
     "conditions" : [ {
       "client-accesstype-condition" : { "type" : [ "confidential" ] }
     }, { "clientroles-condition" : { "roles" : [ "AISP", “PISP" ]
     }, {
       "clientscopes-condition" : {
         "type" : "Optional",
         "scope" : [ "read_account", "read_trasactions" ] }
     } ],
     "profiles" : [ "fapi-1.0-baseline-security-profile" ]
   }, {
     "name" : "fapi-1.0-advanced-security-policy",
     "builtin" : false,
     "enable" : true
     "conditions" : [ {
       "client-accesstype-condition" : { "type" : [ "confidential" ] }
     }, { "clientroles-condition" : { "roles" : [ "PISP" ]
     }, {
       "clientscopes-condition" : {
         "type" : "Optional",
         "scope" : [ "bank_transfer" ] }
     } ],
     “profiles” : [  "fapi-1.0-baseline-security-profile”,
                     "fapi-1.0-advanced-security-profile" ] }]
```

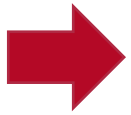
Client Profiles/Policies : how to work



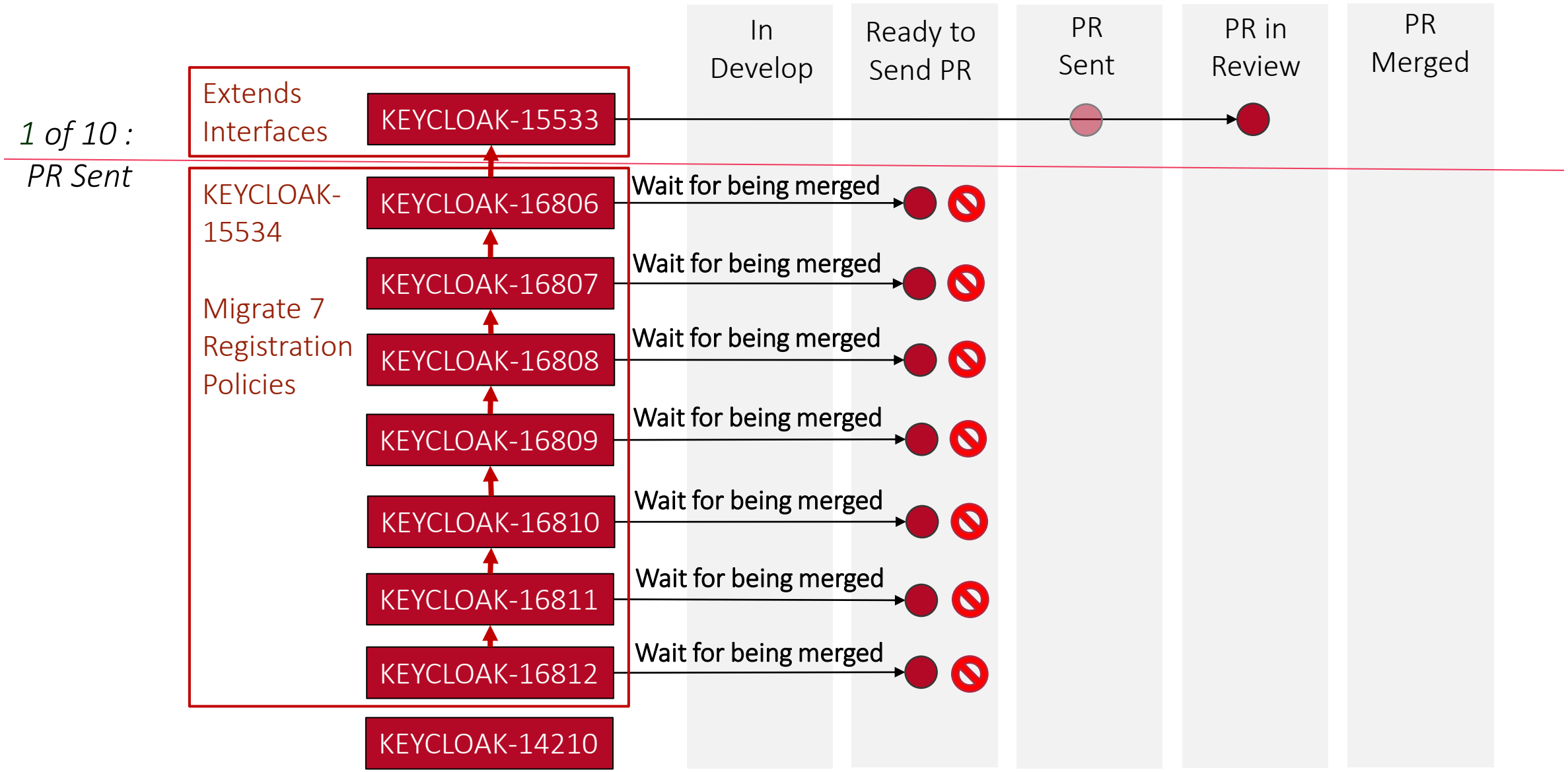
Issue status in detail : External Interfaces



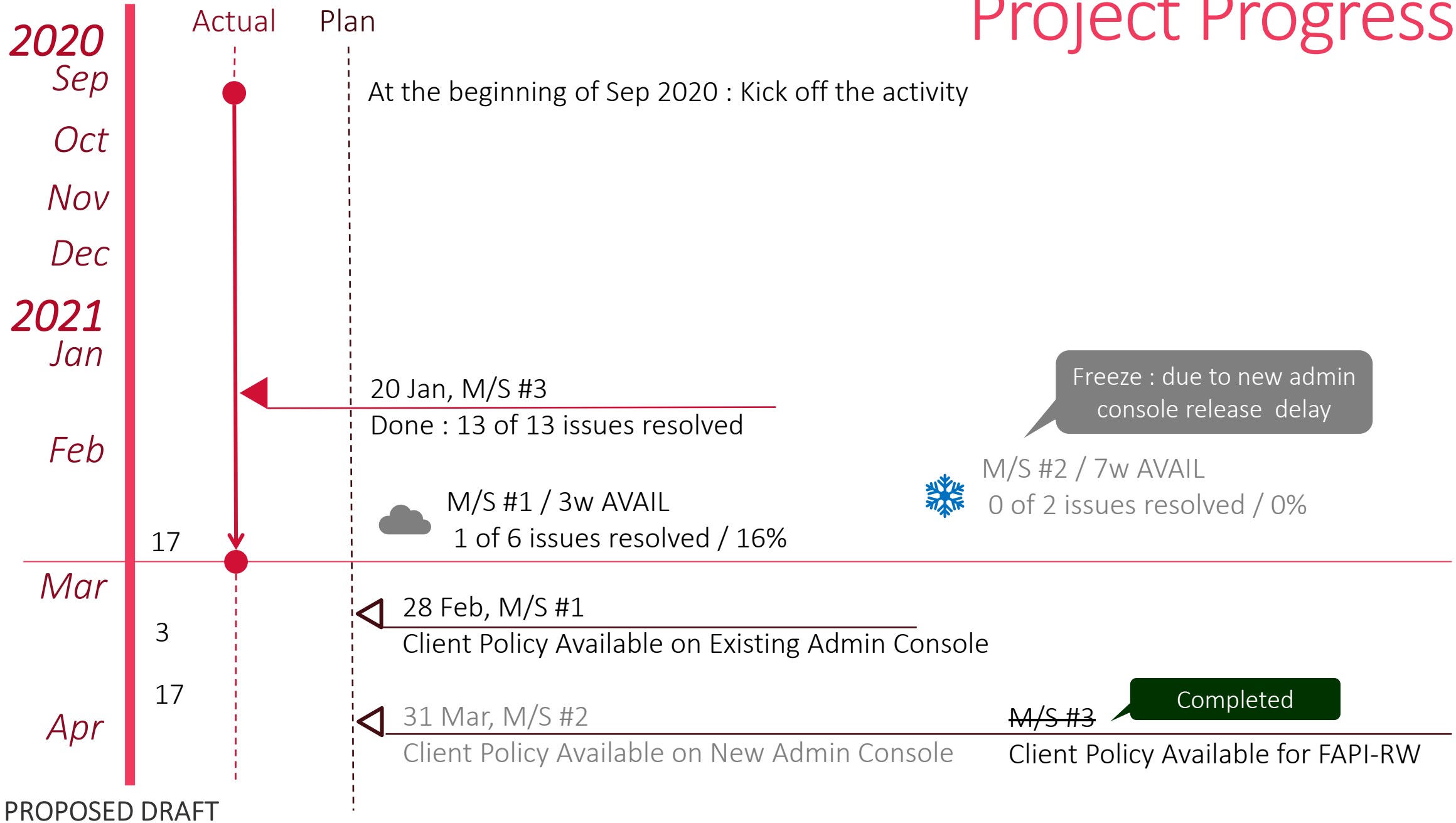
Issues Status - Client Registration Policies Migration

3 Jan 2021		17 Feb 2021	
3 Issues in total			
0 Resolved [0%]		0 Resolved [0%]	+0
9 In Progress		9 In Progress	+0
0 Assigned		0 Assigned	+0
1 Not Assigned		1 Not Assigned	+0

Issue status in detail : Client Registration Policies Migration

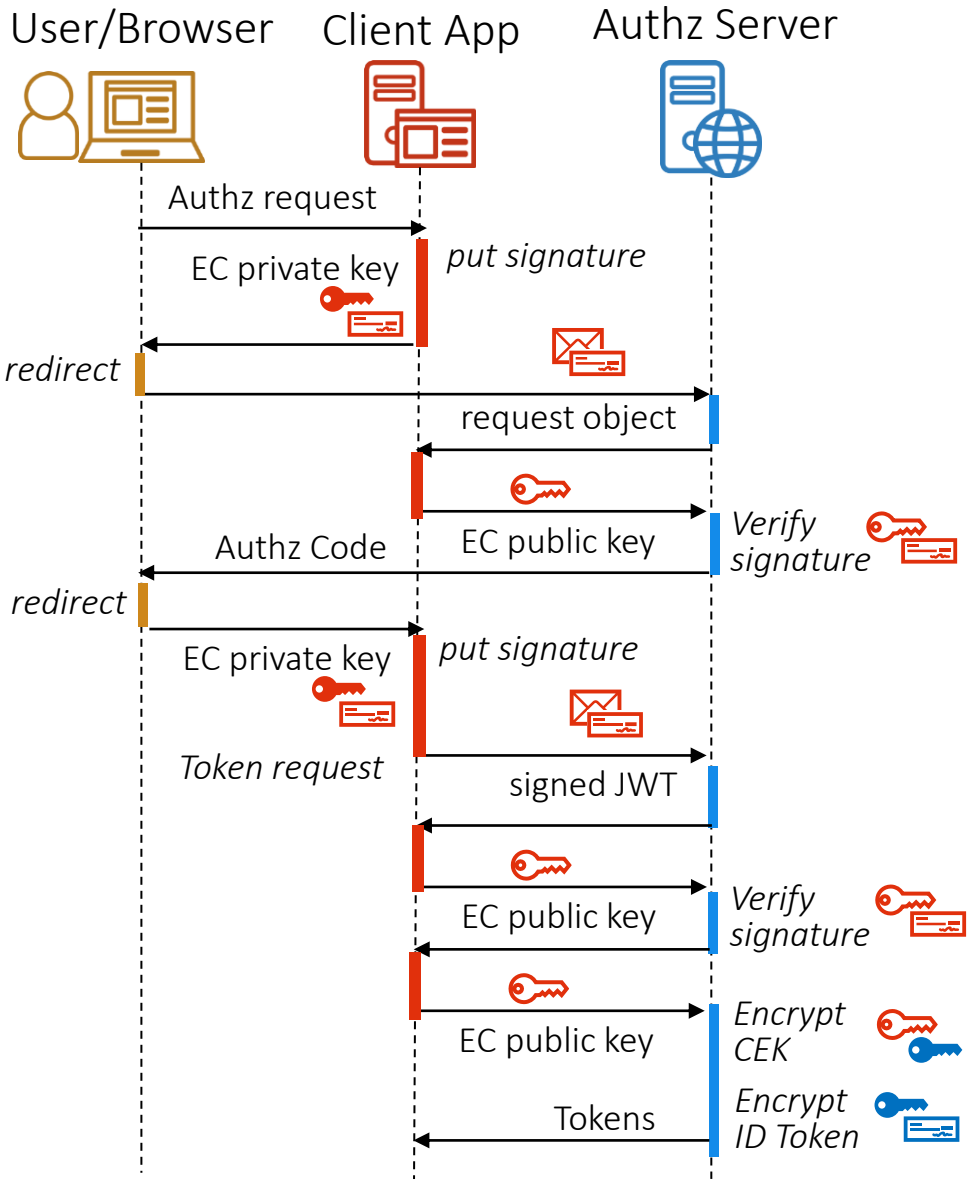


Project Progress



Future Topics Recalled

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

END