

@Web Conference  
17 Feb 2021

# FAPI-SIG Community 13<sup>th</sup> Meeting

# Table of Contents

Major Topics

Status Updates from 12<sup>th</sup> Meeting

FAPI-RW

FAPI-CIBA (poll mode)

Client Policy Official Support

Future Topics Recalled

# Major Topics

# Major Topics

- Project : Client Policy Official Support  
PR sent

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

# Status Updates from 12<sup>th</sup> Meeting

## FAPI-RW

# 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

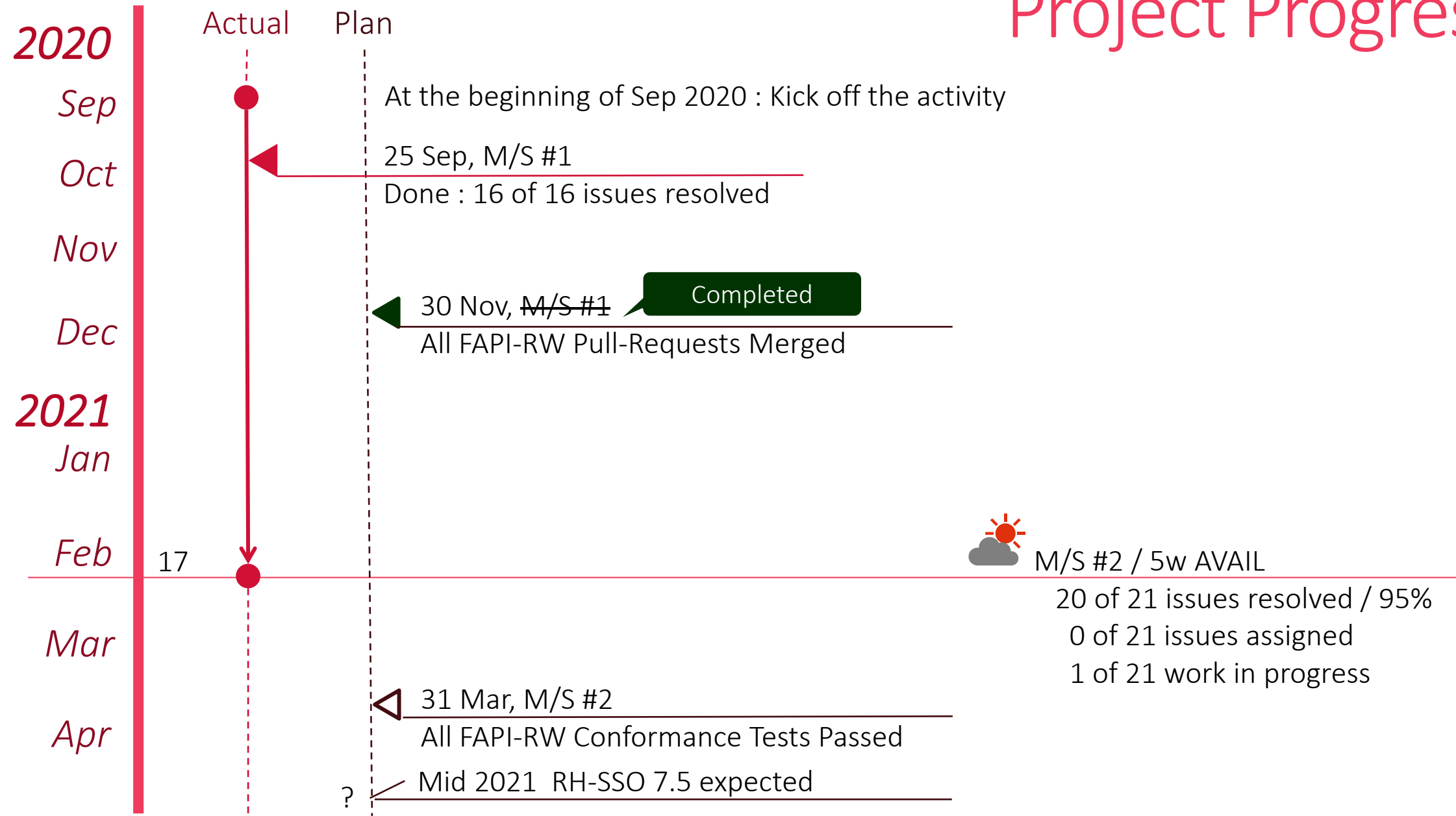
- #45 Integrating FAPI-RW conformance tests run into keycloak's CI/CD pipeline

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 12<sup>th</sup> Meeting FAPI-CIBA (poll mode)



# Remaining Issues Status

3 Jan 2021

13 Issues in total

8 Resolved [62%]

2 In Progress

3 Assigned

0 Not Assigned



17 Feb 2021

8 Resolved [62%] +0

2 In Progress +0

3 Assigned +0

0 Not Assigned +0

# Remaining Issues Details

- #56 support Signed Authentication Request  
In Review
- #58 Realm Settings (CIBA Policy) overridden 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

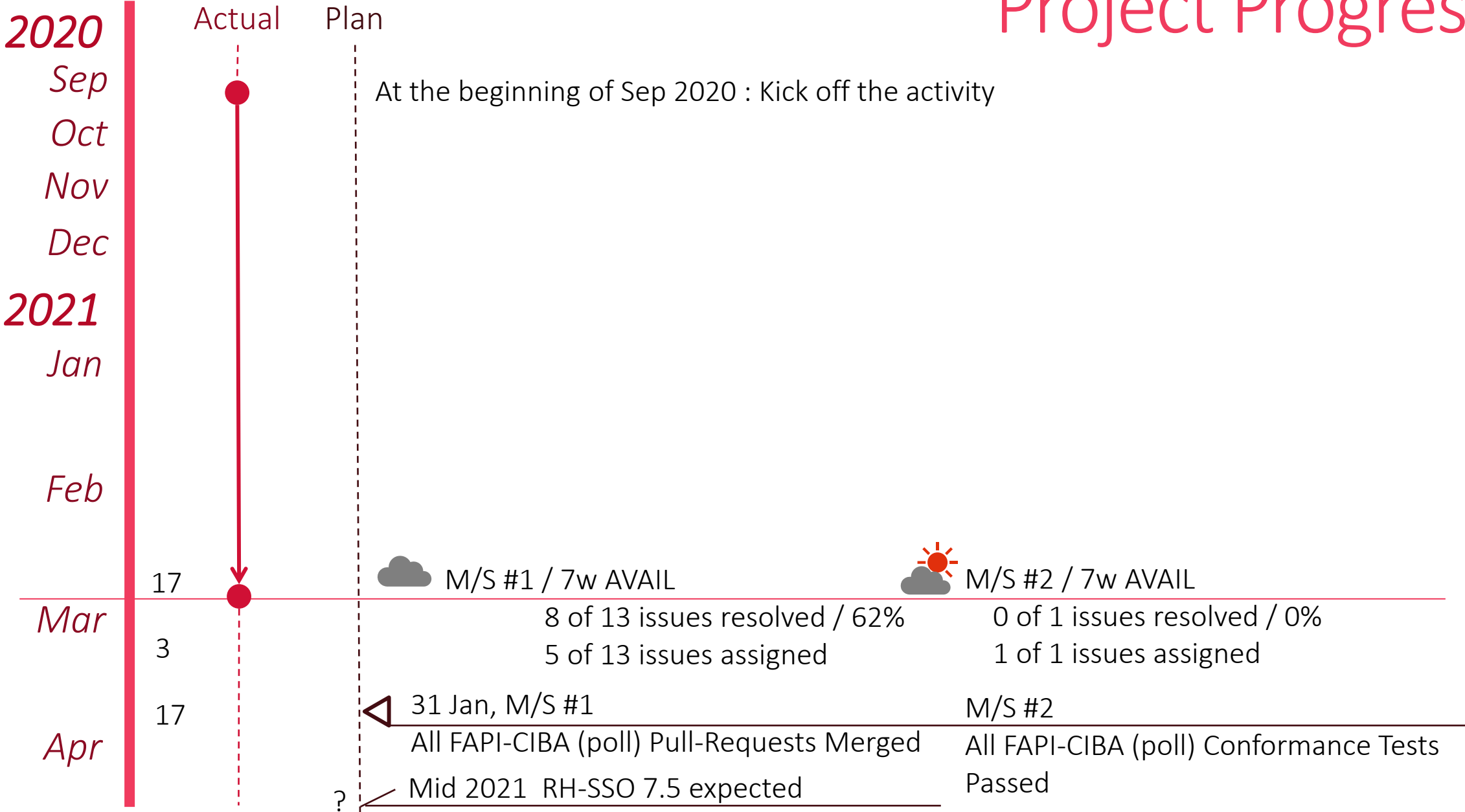
- [#53](#) encrypt/decrypt login\_hint

...



PROPOSED DRAFT

# Project Progress



# Status Updates from 12<sup>th</sup> 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

6 Issues in total

1 Resolved [17%]

1 In Progress

1 Assigned

3 Not Assigned



17 Feb 2021

1 Resolved [17%] +0

1 In Progress +0

1 Assigned +0

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)

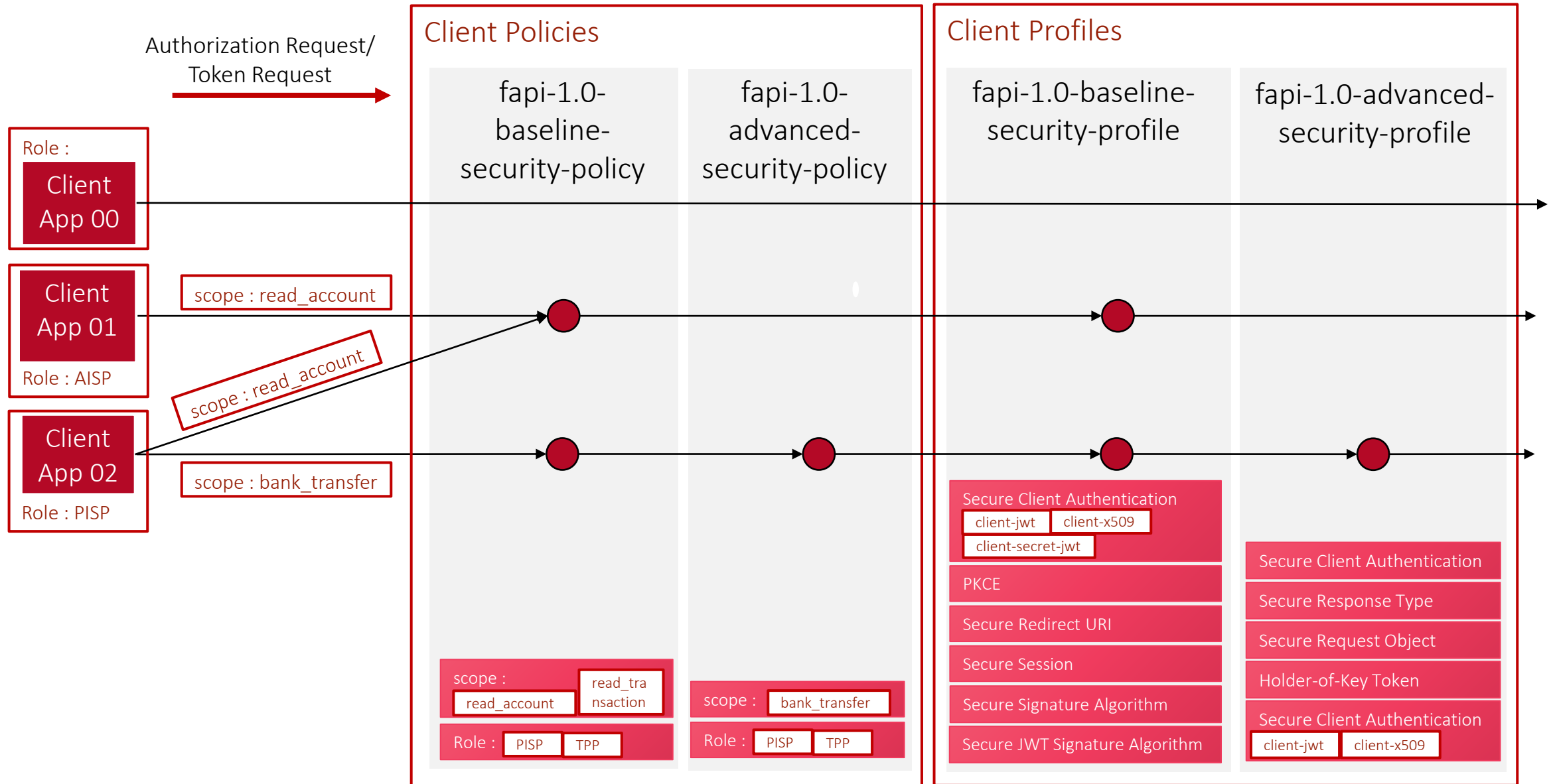


# JSON Representation for Client Profiles/Policies

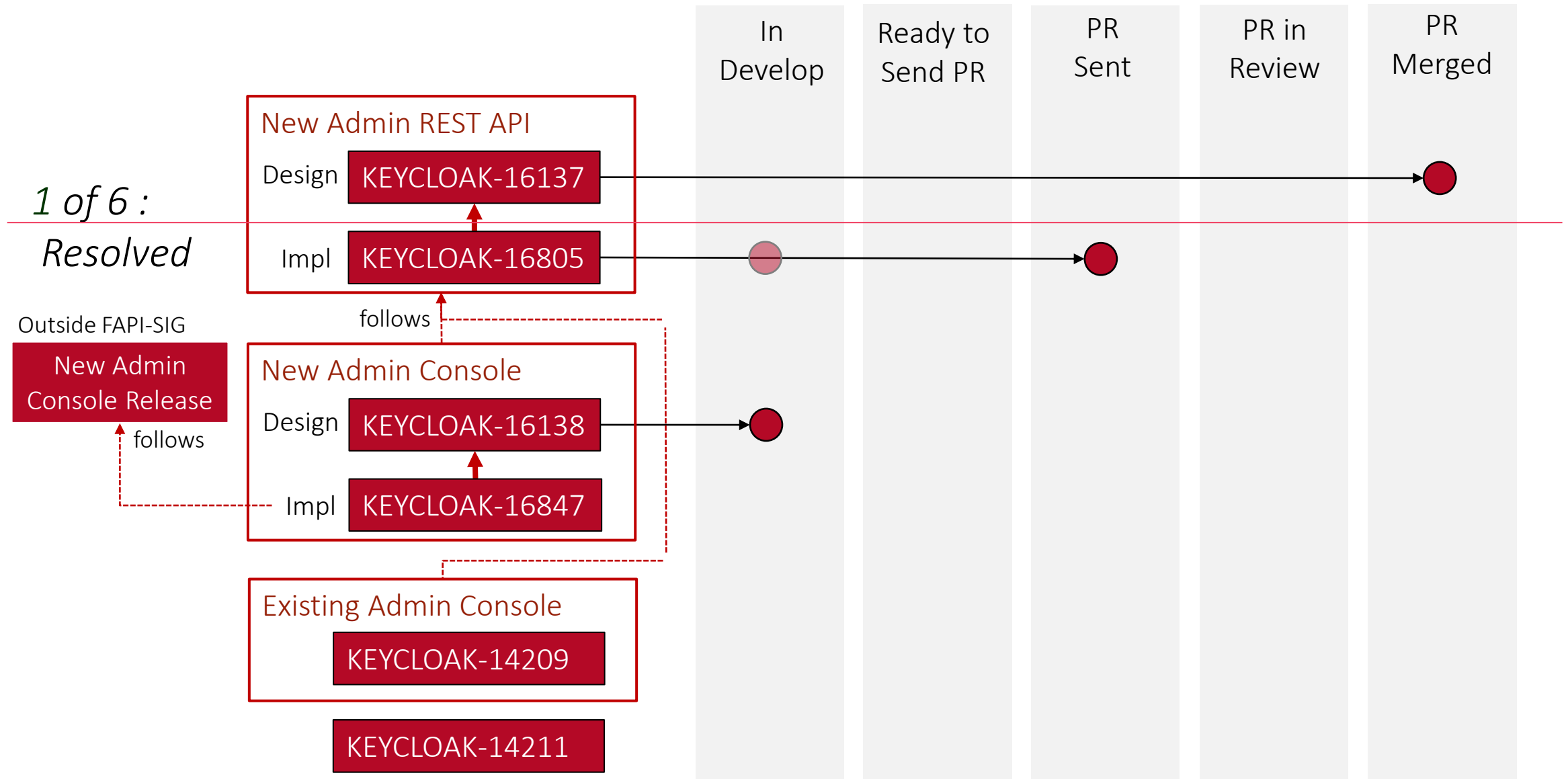
```
"profiles" : [ {  
  "name" : "fapi-1.0-baseline-security-profile",  
  "description" : "FAPI 1.0 Baseline Security Profile",  
  "builtin" : false,  
  "executors" : [ {  
    "secure-client-authn-executor" : {  
      "client-authns" : ["client-secret-jwt", "client-jwt", "client-x509" ],  
      "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", "TPP" ]  
  }, {  
    "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", "TPP" ]  
  }, {  
    "clientscopes-condition" : {  
      "type" : "Optional",  
      "scope" : [ "bank_transfer" ] }  
  } ],  
  "profiles" : [ "fapi-1.0-baseline-security-profile",  
    "fapi-1.0-advanced-security-profile" ] }
```

# Client Profiles/Profiles : how to work



# Issue status in detail : External Interfaces



# Issues Status - Client Registration Policies Migration

3 Jan 2021

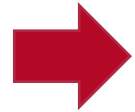
3 Issues in total

0 Resolved [0%]

9 In Progress

0 Assigned

1 Not Assigned



17 Feb 2021

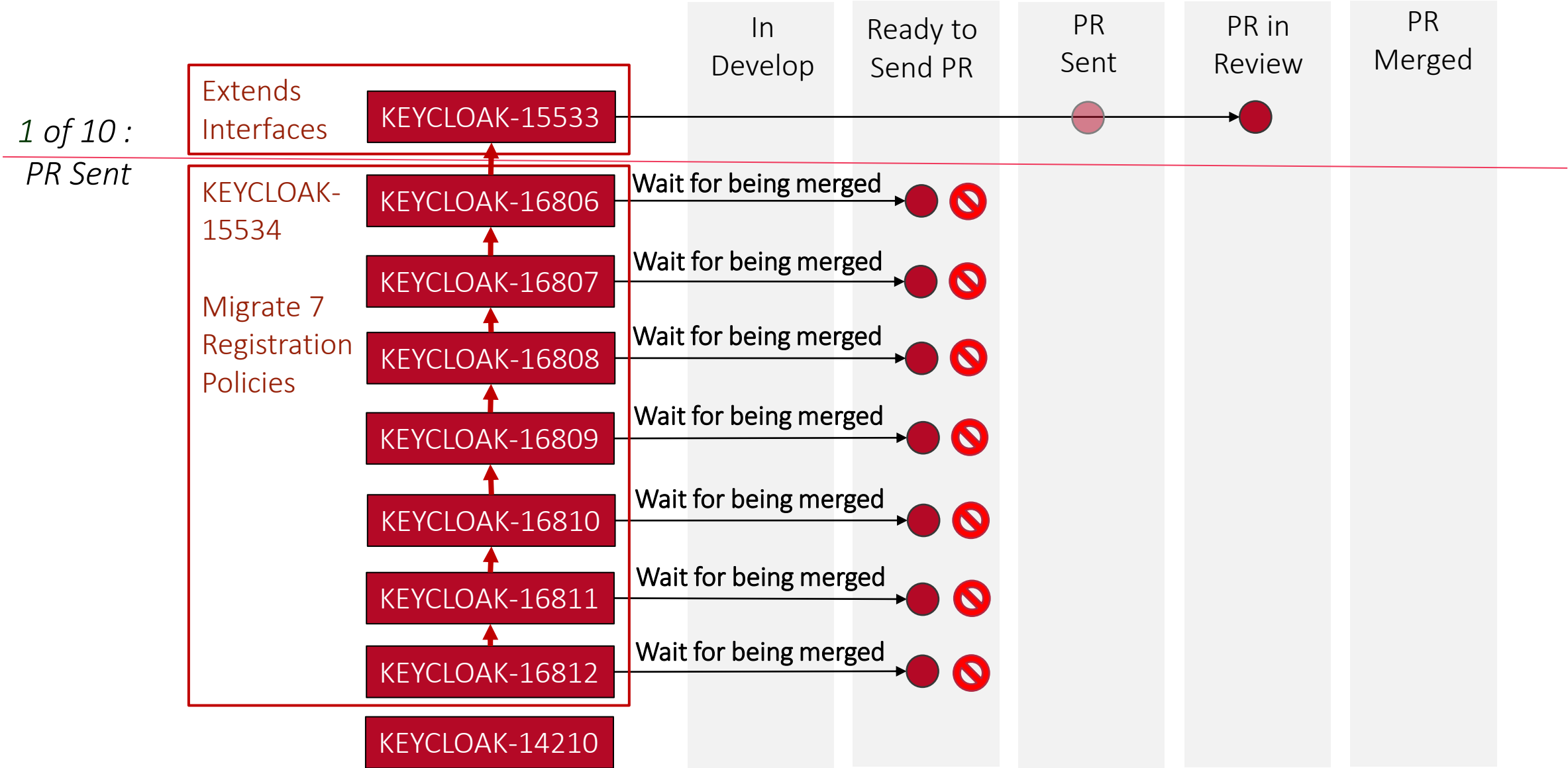
0 Resolved [0%] +0

9 In Progress +0

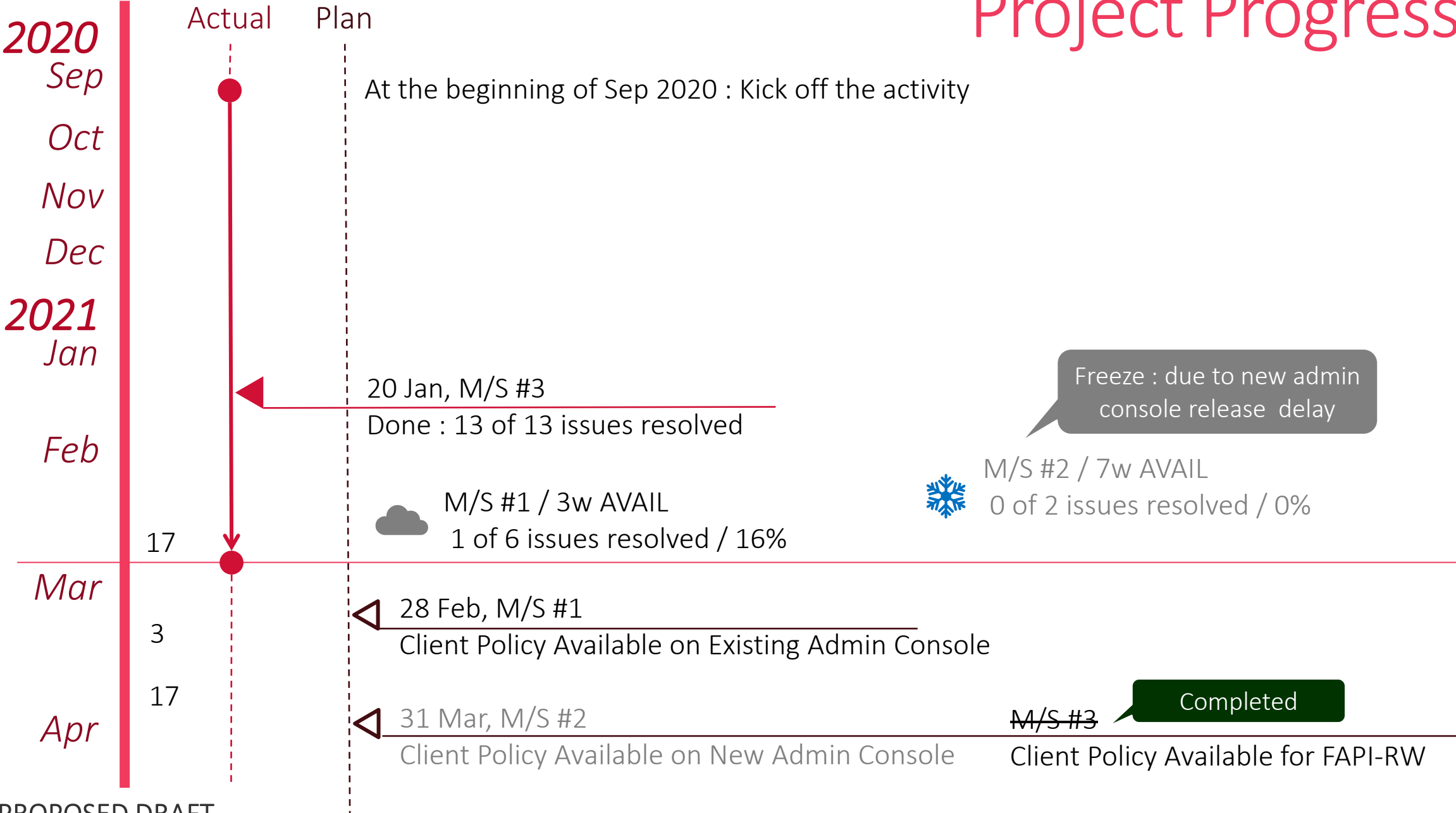
0 Assigned +0

1 Not Assigned +0

# Issue status in detail : Client Registration Policies Migration

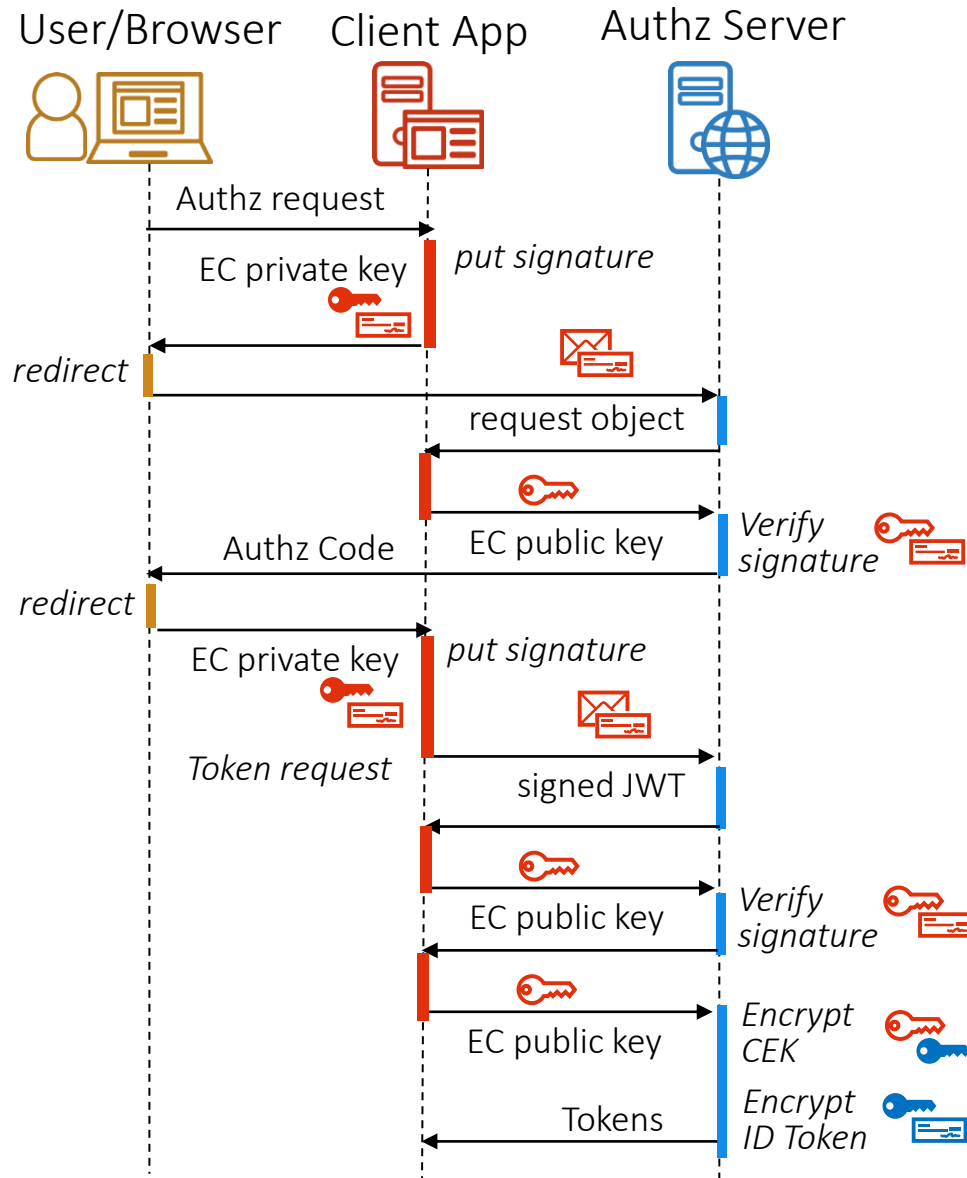


# Project Progress



# Future Topics Recalled

# 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