

@Web Conference  
3 Mar 2021

# FAPI-SIG Community 14<sup>th</sup> Meeting

# Table of Contents

Major Topics

Status Updates from 13<sup>th</sup> Meeting

FAPI-RW

FAPI-CIBA (poll mode)

Client Policy Official Support

Future Topics Recalled

# Major Topics

# Major Topics

- Project : FAPI-CIBA (poll mode)  
PR review/revise code in progress  
KEYCLOAK-12137 OpenID Connect Client Initiated Backchannel Authentication (CIBA)

# Status Updates from 13<sup>th</sup> Meeting

## FAPI-RW

# Remaining Issues Status

17 Feb 2021

4 Issues in total

3 Resolved

1 In Progress

0 Assigned

0 Not Assigned



3 Mar 2021

3 Issues in total

3 Resolved +0

0 In Progress +0

0 Assigned +0

0 Not Assigned +0

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

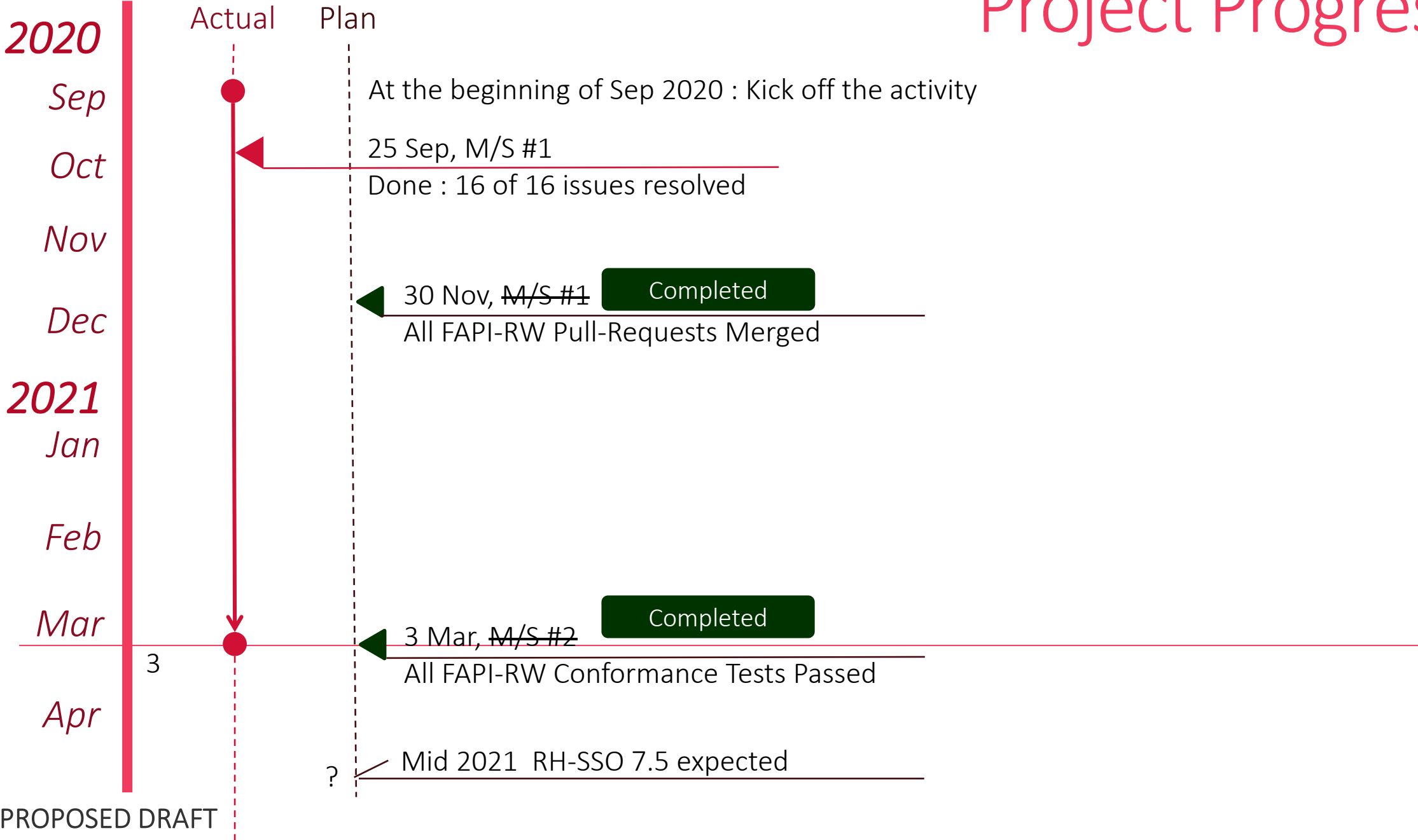
Deferred

- Follow the final version of FAPI 1.0

Deferred

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

# Project Progress



# Status Updates from 13<sup>th</sup> Meeting FAPI-CIBA (poll mode)



# Remaining Issues Status

17 Feb 2021

13 Issues in total

8 Resolved [62%]

2 In Progress

3 Assigned

0 Not Assigned



3 Mar 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

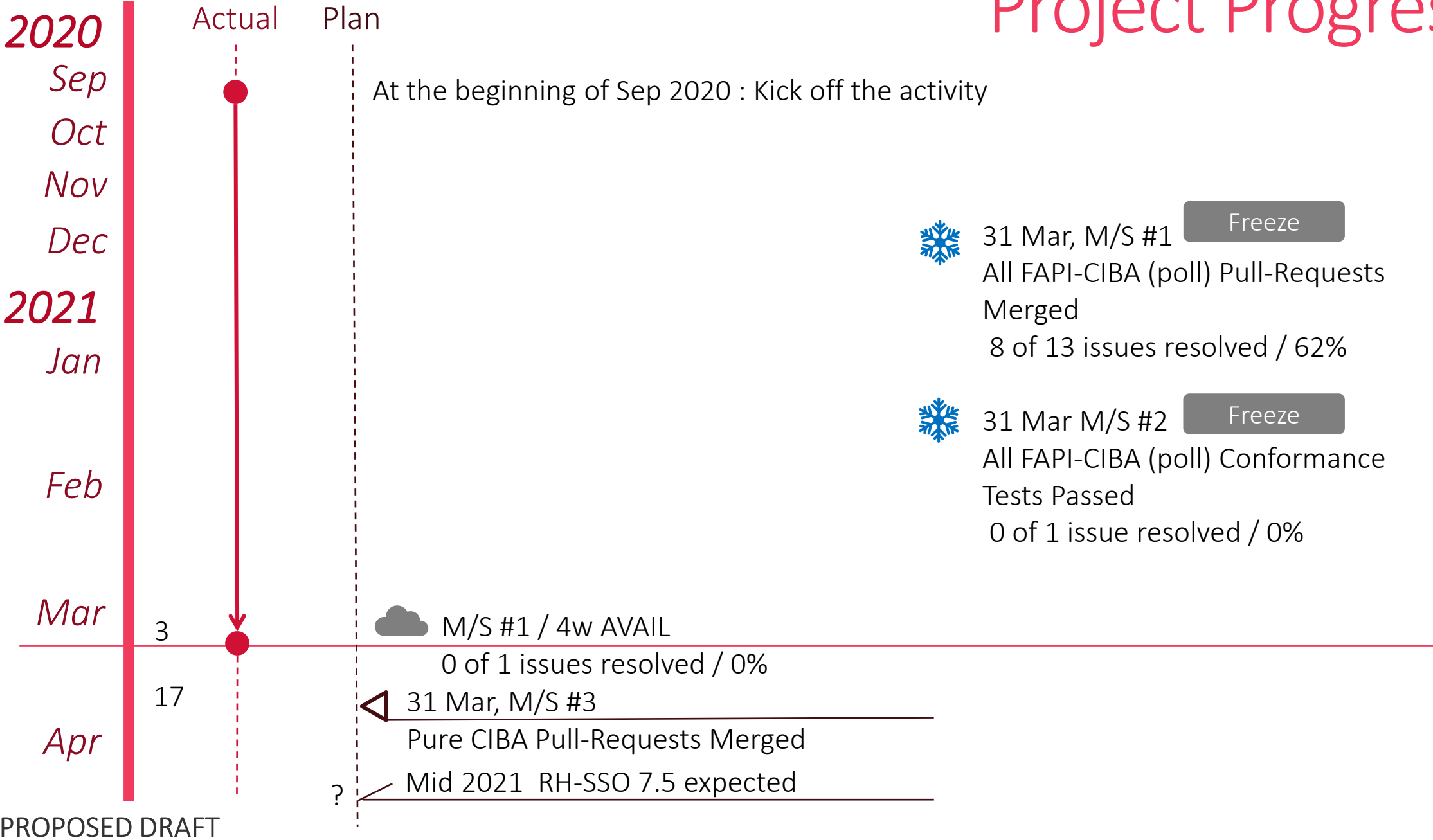
- [#53](#) encrypt/decrypt login\_hint

...



PROPOSED DRAFT

# Project Progress



# Status Updates from 13<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

17 Feb 2021

6 Issues in total

1 Resolved [17%]

1 In Progress

1 Assigned

3 Not Assigned



3 Mar 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)

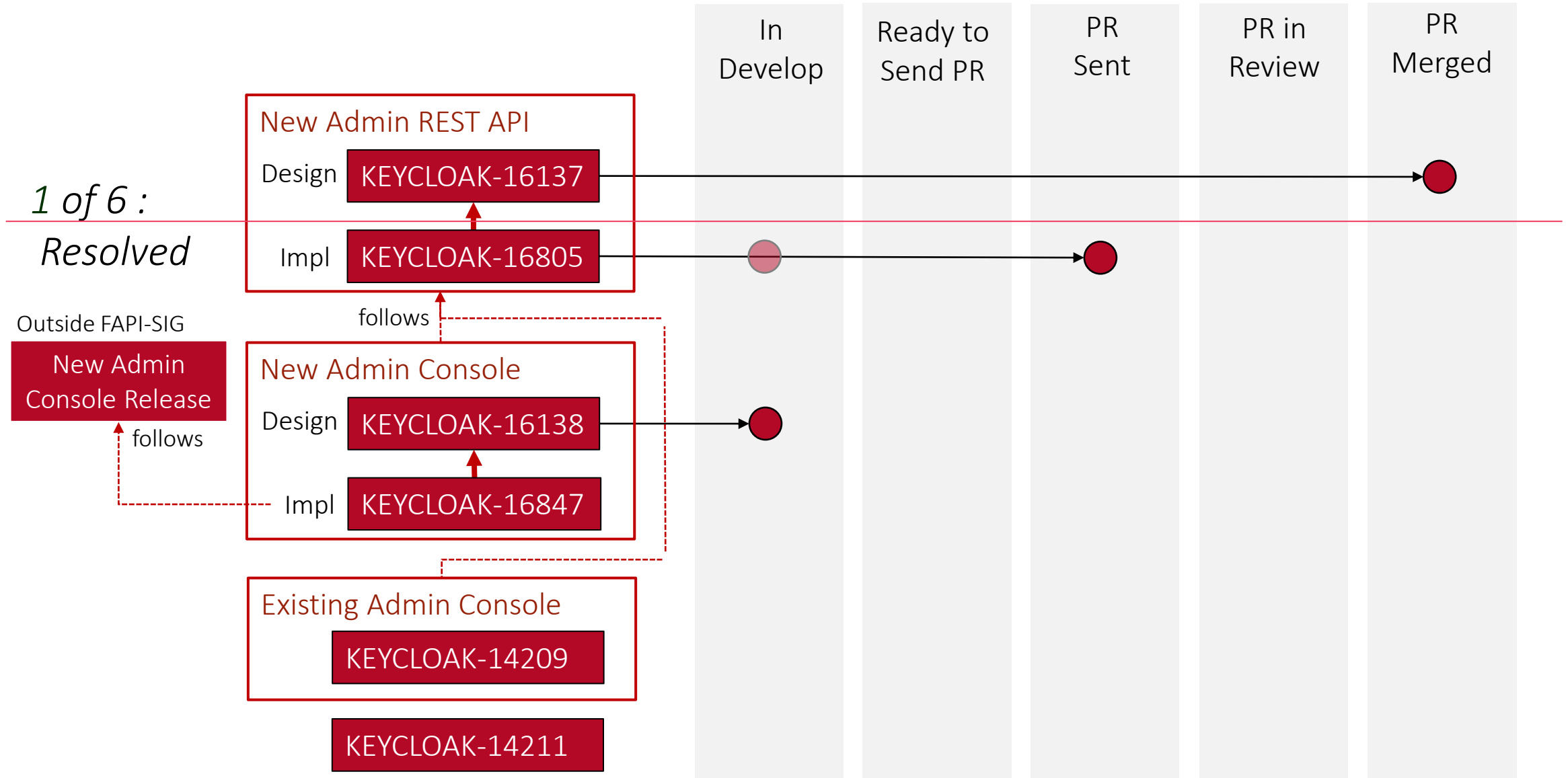
- Concept Design by RH UXD team :  
<https://marvelapp.com/prototype/6e70eh2/screen/74918976>
- KEYCLOAK-16847 Client Policy : Support New Admin Console UI (Implementation)
- KEYCLOAK-14209 Client Policy : UI on Admin Console
- KEYCLOAK-14211 Client Policy : Remove Client Policy related individual settings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

[Potential Blocking Factor]

- New Admin Console Release (not yet released)



# Issue status in detail : External Interfaces



# Issues Status - Client Registration Policies Migration

17 Feb 2021

3 Issues in total

0 Resolved [0%]

9 In Progress

0 Assigned

1 Not Assigned



3 Mar 2021

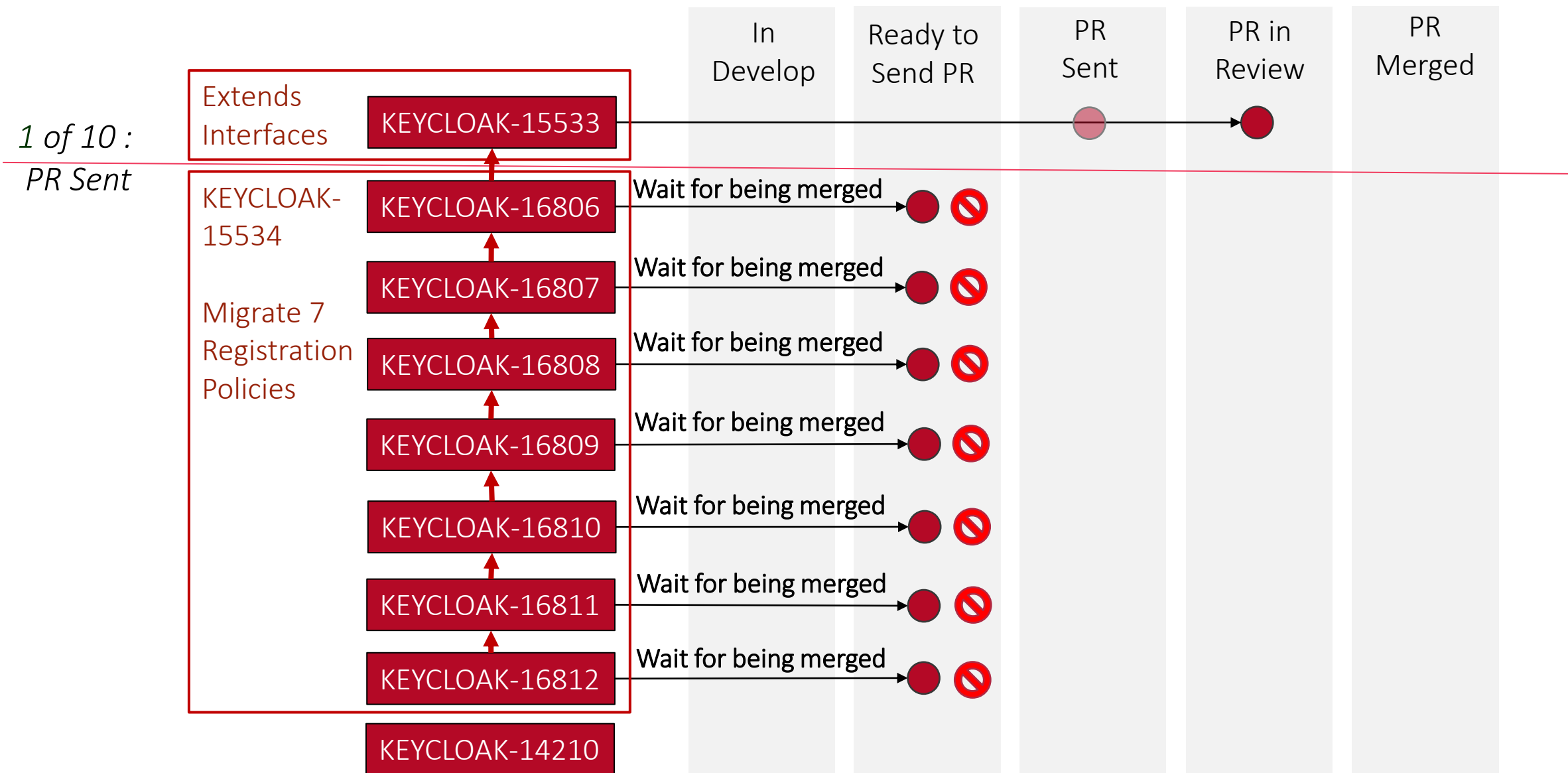
0 Resolved [0%] +0

9 In Progress +0

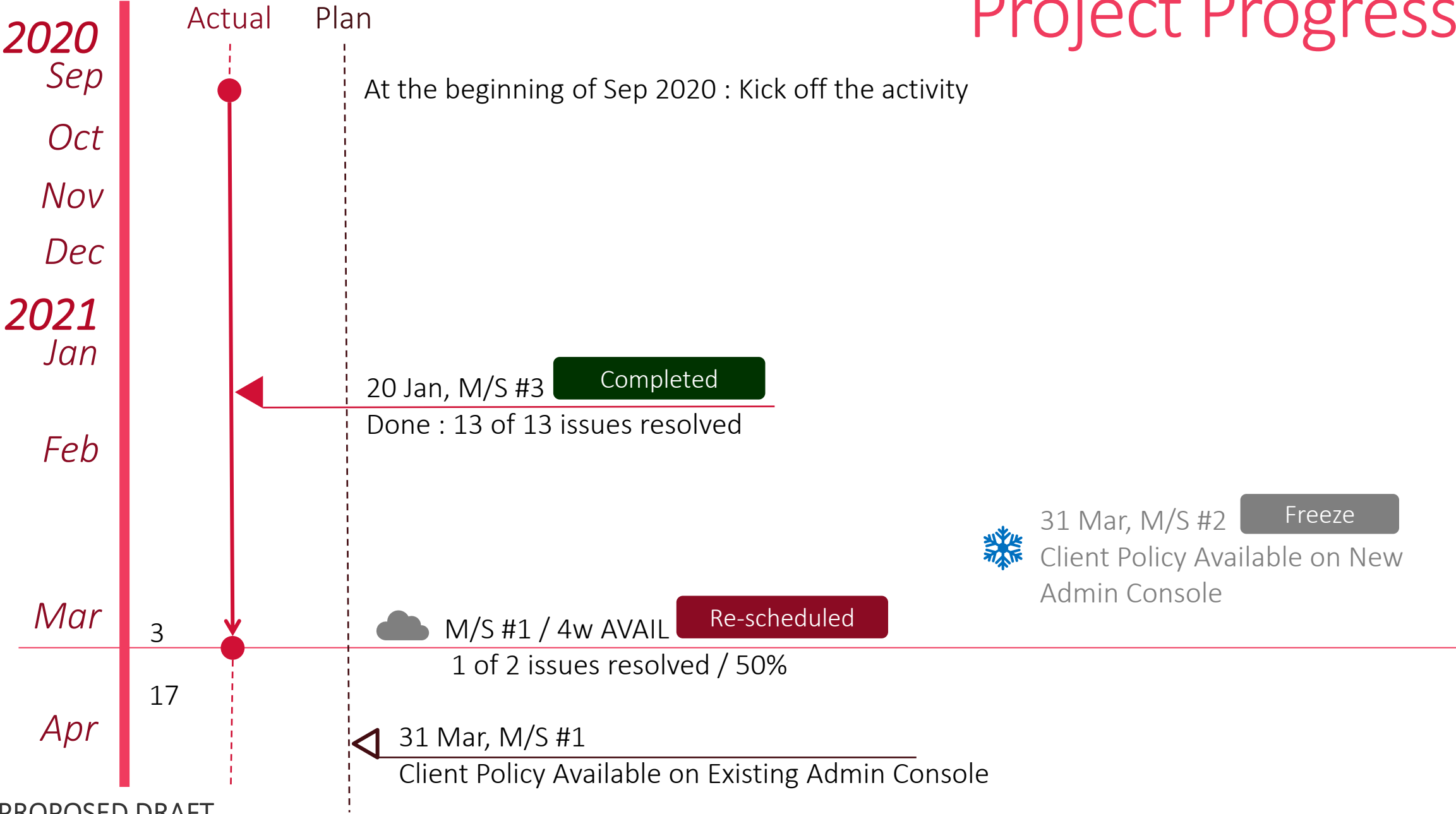
0 Assigned +0

1 Not Assigned +0

# Issue status in detail : Client Registration Policies Migration



# Project Progress



# Future Topics Recalled

# OIDC Client's Public Key Management

Refer to [https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/OIDC-Client-Keys/FAPI-SIG-Annex\\_OIDC\\_Client\\_Keys.pdf](https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/OIDC-Client-Keys/FAPI-SIG-Annex_OIDC_Client_Keys.pdf) in detail.

# Keycloak PSD2 support

- Recap the breakout session held on Fri 5 Feb 2021
  - To keycloak, contribute the interface (SPI provider) for conducting market specific client certificate verification (in this case, PSD2 market/UK OpenBanking market).
  - Keycloak should be adopted to wider range of markets and deployment so that this interface should not pertain to any specific implementation for this verification.
  - Adorsys works on preparing its design document at first.

# Keycloak PSD2 support

## ● PSD2

### Support requirements from eIDAS

TPP's QWAC verification of Client Authentication on TLS layer

#### On TLS w/Client Termination

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

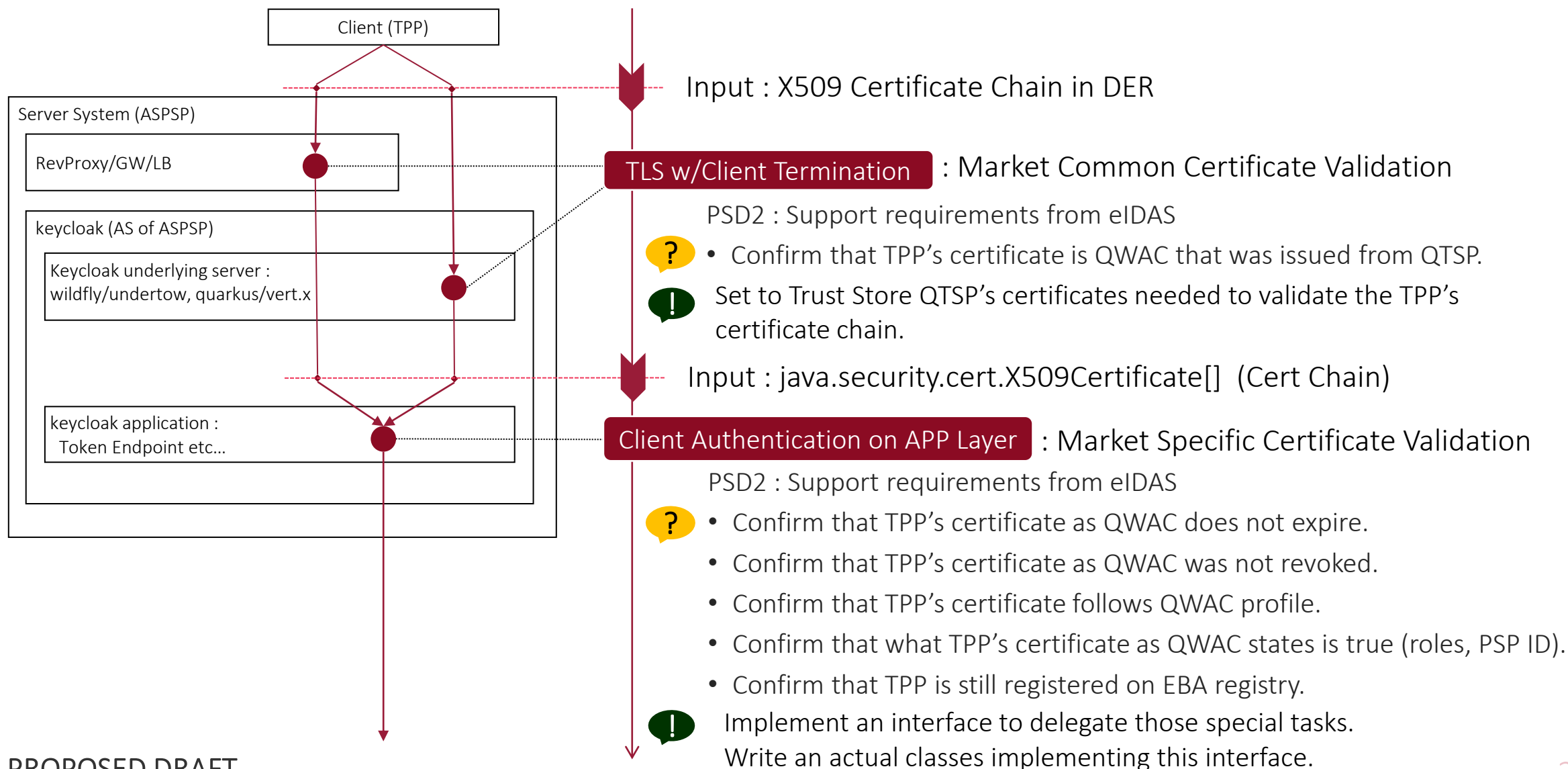
#### On Client Authentication on APP Layer

#### On Client Policies

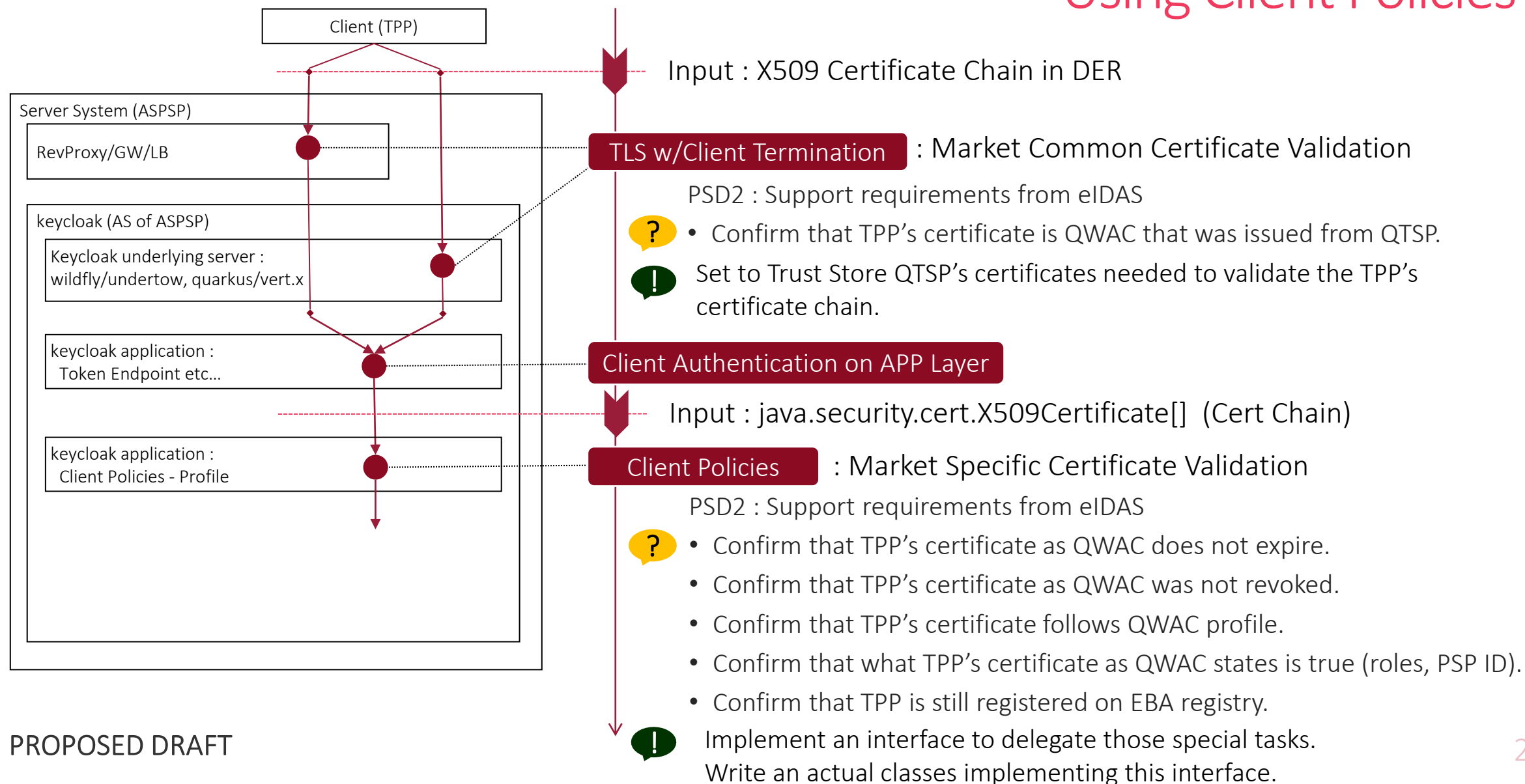
2. Confirm that TPP's certificate as QWAC does not expire.
3. Confirm that TPP's certificate as QWAC was not revoked.
4. Confirm that TPP's certificate follows QWAC profile.
5. Confirm that what TPP's certificate as QWAC states is true (roles, PSP ID).
6. Confirm that TPP is still registered on EBA registry.



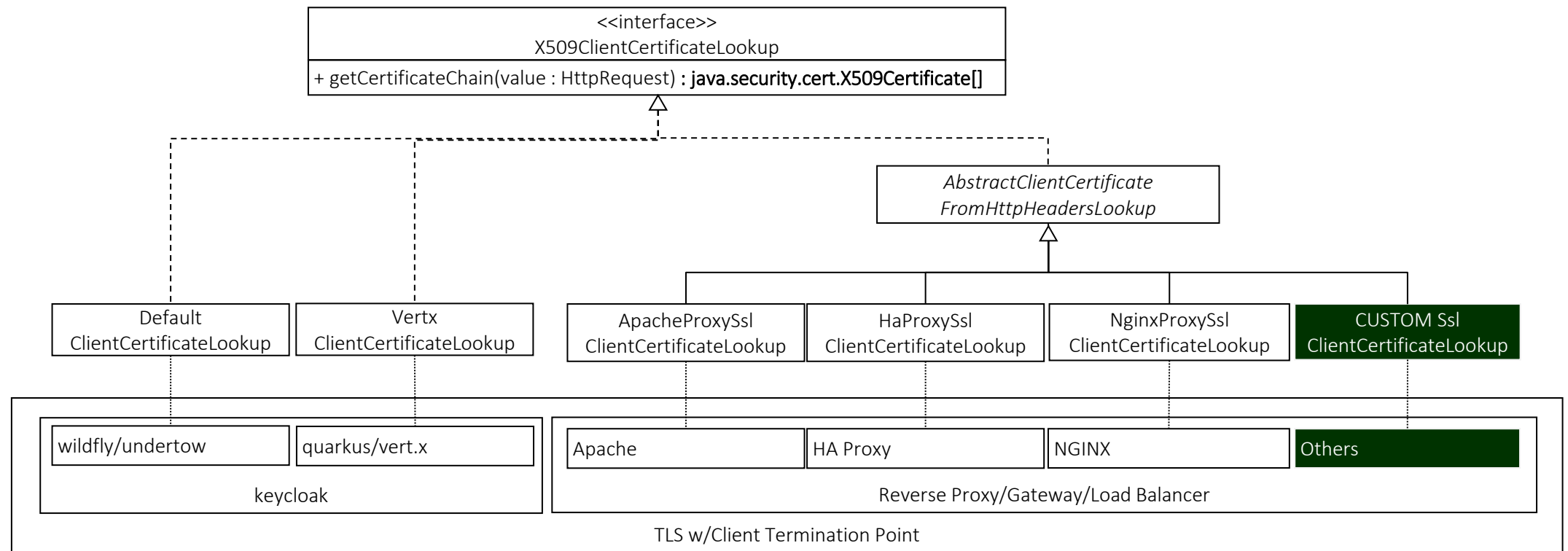
# Analysis in depth: Keycloak12 Client Certificate Handling Flow



# Analysis in depth : Keycloak12 Client Certificate Handling Flow Using Client Policies

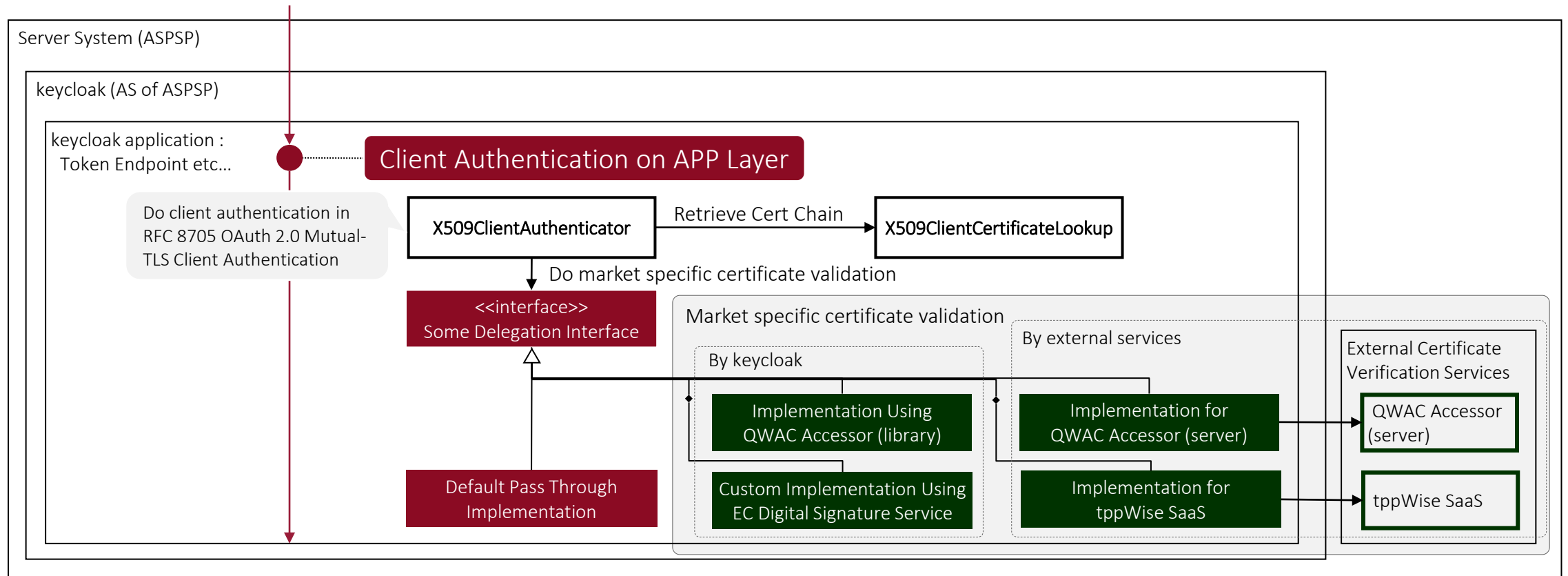


# Analysis in depth : Keycloak12 Client Certificate Acquisition from TLS w/Client Termination Point



 : We can add custom client certificate lookup provider if we use other options for Rev proxy/GW/LB.

# Simulation : Client Certificate Market Specific Verification Layout with RFC 8705 OAuth 2.0 Mutual-TLS Client Authentication

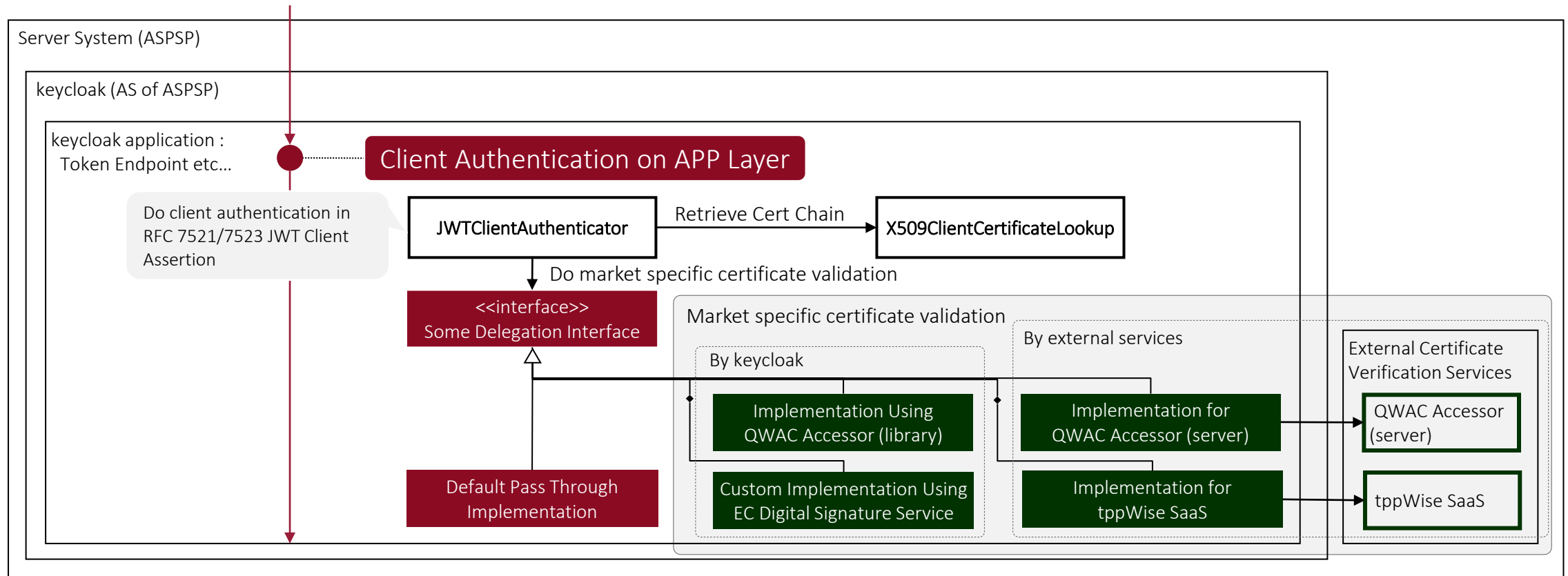


: already existed classes in keycloak12.

: newly upstreamed, included in keycloak so that they should be any OSS/proprietary solution independent.

: newly provided by OSS/proprietary solutions. Shown in the above diagram are examples (Adorsys, Banfico).

# Simulation : Client Certificate Market Specific Verification Layout with RFC 7521/7523 JWT Client Assertion

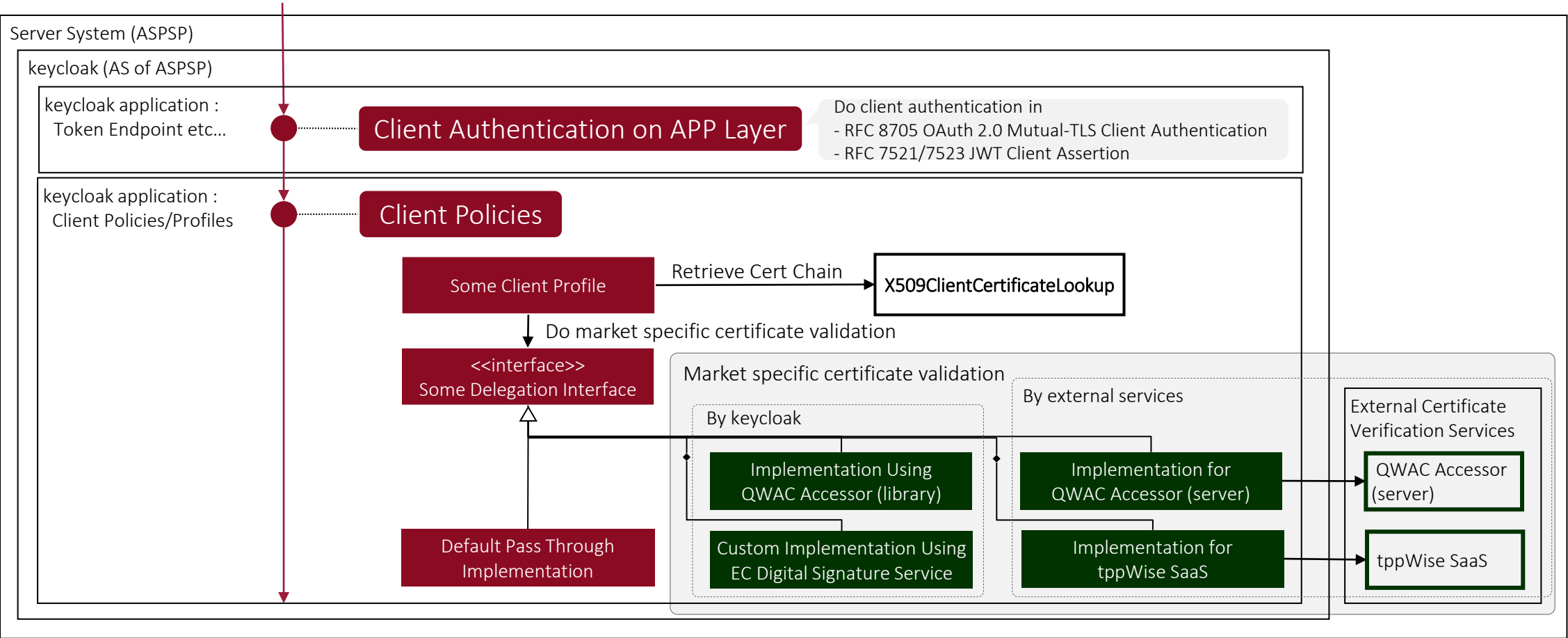





: already existed classes in keycloak12.

: newly upstreamed, included in keycloak so that they should be any OSS/proprietary solution independent.

: newly provided by OSS/proprietary solutions. Shown in the above diagram are examples (Adorsys, Banfico).

# Simulation : Client Certificate Market Specific Verification Layout Using Client Policies



-  : already existed classes in keycloak12.
-  : newly upstreamed, included in keycloak so that they should be any OSS/proprietary solution independent.
-  : newly provided by OSS/proprietary solutions. Shown in the above diagram are examples (Adorsys, Banfico).

END