FAPI-SIG Community 5th Meeting

@Web Conference

21 Oct 2020

PROPOSED DRAFT

Table of Contents

Status Updates from 4th Meeting

- FAPI-RW
- FAPI-CIBA (poll mode)

Client Policy Official Support Reconsideration

About Client Policies Practice Guide

PROPOSED DRAFT

Status Updates from 4th Meeting FAPI-RW

Remaining Issues Status

2 Oct 2020		16 Oct 2020	
4 Issues in total			
0 Resolved	➡	0 Resolved	
0 Assigned		3 Assigned	+3
4 Not Assigned		1 Not Assigned	-3

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

✓ Not Assigned, but in progress

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

✓ Assigned

Status Updates from 4th Meeting FAPI-CIBA (poll mode)

Subtasks Status

2 Oct 2020

13 Subtasks in total

0 Resolved

0 PR sent, in review

0 Assigned

13 Not Assigned

→

16 Oct 2020

0 Resolved	
4 PR sent, in review	+4
6 Assigned	+6
3 Not Assigned	-10

Remaining Issues for FAPI-CIBA project

[Backchannel Authentication Request]

- #53 encrypt/decrypt login_hint

✓ PR sent, in review.

- #54 support login_hint_token

✓ PR sent, in review

- #55 support id_token_hint

✓ PR sent, in review

- #56 support Signed Authentication Request

✓ Assigned

- #57 support User Code

✓ PR sent, in review

Remaining Issues for FAPI-RW project

[Settings]

- #58 Realm Settings (CIBA Policy) overriden by Client Settings

✓ Assigned

[Internals]

- #59 Use Only Auth Result Cache by Infinispan For CIBA Flow Session Binding

✓ Assigned

- #60 Use Auth Result ID instead of decoupled_auth_id For CIBA Flow Session Binding

✓ Assigned

- #61 Token Request Throttling Information Not Cluster-wide Sync

0 offer to work on it

- #62 Use Security Event Token (SET) as message format between keycloak and Decoupled Auth Server

0 offer to work on it

Remaining Issues for FAPI-RW project

[Arquillian Integration Test]

- #63 Confirm CIBA Implementation Works Well in Clustering Environment

  1 offer to work on it, but not yet 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

Client Policy Official Support Reconsideration

Client Policies - Benefits

Client Policies can realize security profiles like FAPI and OAuth2 BCP in unified and extensible manner. Its benefits are as follow.

- Usability

  It can improve messy client settings.

  Security profile related client settings can be moved from Admin Console's client settings UI.

- Code Maintainability/Extensibility/Availability

  It can improve the readability of endpoint classes.

  Security profile related hardcoded codes can be moved from endpoint classes to separatable providers. Keycloak need not restart when introducing new policies.

- Backward Compatibility

  It can realize what the current Client Registration Policies do

Client Policies - Current Status and Goals

- Usability

[Current Status] No UI is supported.

[Goal] Support UI on Admin Console.

- Code Maintainability/Extensibility/Availability

[Current Status] FAPI-RW security profile related codes are partially implemented as keycloak’s body codes.

[Goal] FAPI-RW security profile related codes are totally implemented as Client Policies Executors/Conditions.

- Backward Compatibility

[Current Status] Client Registration Policies works.

[Goal] Replace Client Registration Policies with Client Policies.

Client Policies - Subtasks

[High Priority]

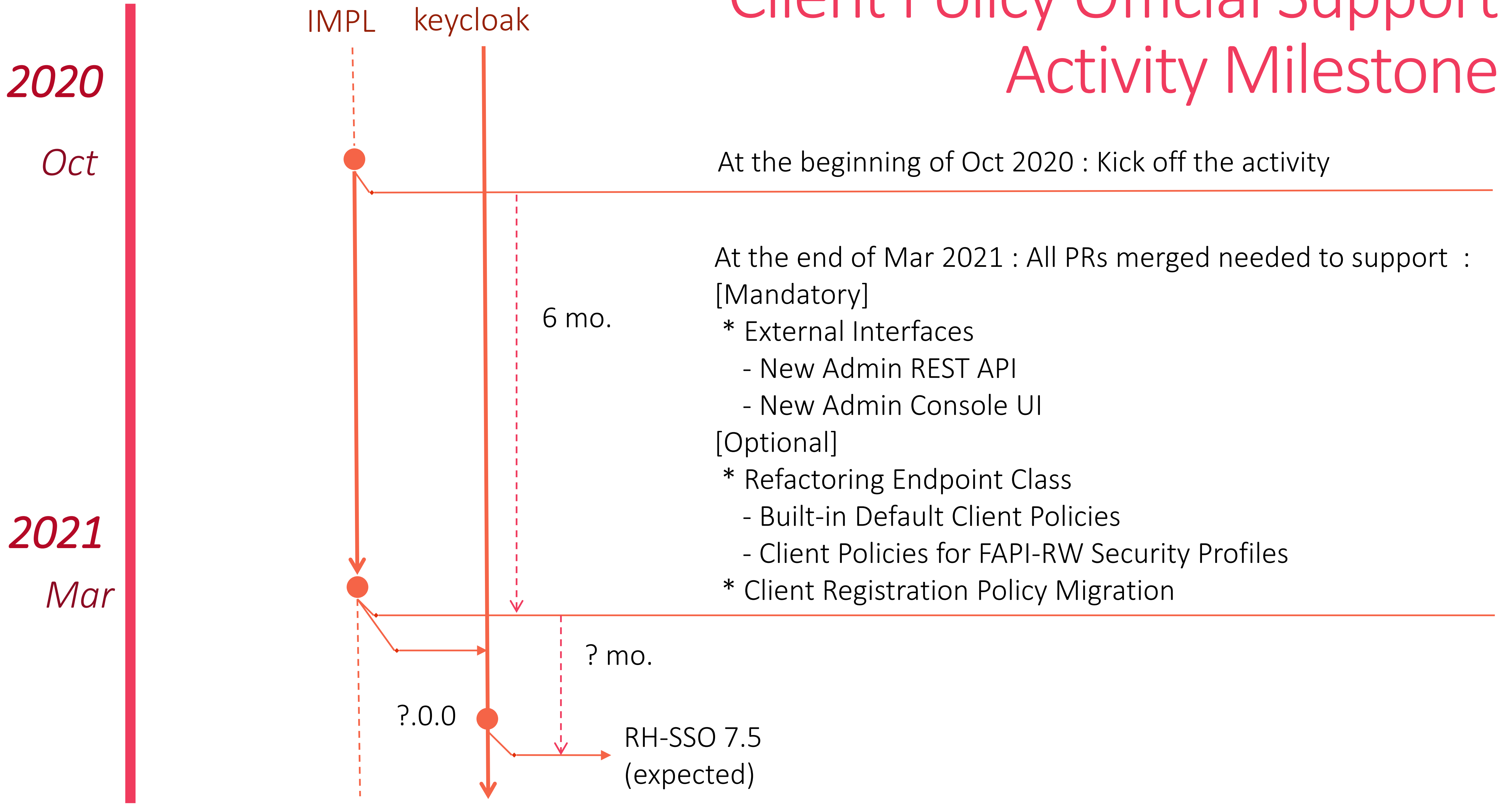
- For Usability : External Interfaces
  - New Admin REST API
  - New Admin Console UI
- For Code Maintainability/Extensibility/Availability : Refactoring Endpoint Class
  - Built-in Default Client Policies
  - Client Policies for FAPI-RW Security Profiles

[Low Priority]

- For Backward Compatibility : Client Registration Policies Migration

If new Client Policies and existing Client Registration Policies are allowed to coexist, it can be deferred.

Client Policy Official Support Activity Milestone



IMPL keycloak

2020

Oct

At the beginning of Oct 2020 : Kick off the activity

6 mo.

At the end of Mar 2021 : All PRs merged needed to support :

[Mandatory]

* External Interfaces
- New Admin REST API
- New Admin Console UI

[Optional]

* Refactoring Endpoint Class
- Built-in Default Client Policies
- Client Policies for FAPI-RW Security Profiles

* Client Registration Policy Migration

2021

Mar

? mo.

?.0.0

RH-SSO 7.5
(expected)

PROPOSED DRAFT

External Interfaces

		Admin REST API	
		Existing API	New API
Admin Console	Existing UI	-	-
	New UI	x	x

[Situation]

<API>

- Editable clear JSON representation will be introduced (e.g. User Profile) .

<UI>

- The current Client Policy lacks its UI so that it needs to be supported.
- Existing Admin Console UI will become obsolete.
- New Admin Console UI will become available (will be included in RH-SSO 7.5).

➢ **Support also new Admin REST API (clear JSON representation).**

➢ **Support only new Admin Console UI.**

New Admin REST API (Clear JSON Representation)

Clear JSON Representation has partially been introduced in User Profile.

● Design

Update the existing Client Policies’ design document.

Reference : User Profile’s design document

● Implementation

Reference : User Profile’s JIRA ticket

User Profile’s PR

[Issues not yet registered as JIRA ticket]

- Support new Admin REST API (like JSON representation in User Profile)

New Admin Console UI

New Admin Console does not appear so that we'll determine details about its design and implementation after it appears.

● Design

TBD

● Implementation

TBD

[Tickets need to be resolved and still open]

- KEYCLOAK-14209 Client Policy : UI on Admin Console
- KEYCLOAK-14211 Client Policy : Remove Client Policy related individual settings on Admin Console

Refactoring Endpoint Class

On each endpoint class, categorize processes implemented into 3 types :

1. Parse and verify requests

   : should be done by the endpoint class itself

2. Enforce and/or check requests from security perspective

   : should be done by the client policies

   2-1. based on what is common to all security profiles

   : by the built-in default client policies

   2-2. based on specific security profile

   : by the ordinal client policies

Built-in Default Client Policies

[Tickets need to be resolved and still open]

- KEYCLOAK-14208 Client Policy : Pre-set Policies

Client Policies for FAPI-RW Security Profiles

[Tickets need to be resolved and still open]

RESOLVED KEYCLOAK-14190 Client Policy - Condition : The way of creating/updating a client

- KEYCLOAK-14191 Client Policy - Condition : Author of a client - User Group
- KEYCLOAK-14192 Client Policy - Condition : Author of a client - User Role
- 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

- KEYCLOAK-14196 Client Policy - Condition : Client - Client Scope
- KEYCLOAK-14197 Client Policy - Condition : Client - Client Host
- KEYCLOAK-14198 Client Policy - Condition : Client - Client IP

Client Policies for FAPI-RW Security Profiles

- PR Sent KEYCLOAK-14199 Client Policy - Executor : Enforce more secure client authentication method when client registration
- KEYCLOAK-14200 Client Policy - Executor : Enforce Holder-of-Key Token
- PR Sent KEYCLOAK-14201 Client Policy - Executor : Enforce Proof Key for Code Exchange (PKCE)
- KEYCLOAK-14202 Client Policy - Executor : Enforce secure signature algorithm for Signed JWT client authentication
- 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
- KEYCLOAK-14206 Client Policy - Executor : Enforce more secure state and nonce treatment for preventing CSRF
- KEYCLOAK-14207 Client Policy - Executor : Enforce more secure client signature algorithm when client registration

Client Registration Policies Migration

[Tickets need to be resolved and still open]

- KEYCLOAK-14210 Client Policy : Migrate Client Registration Policies to Client Policies
- KEYCLOAK-15533 Client Policy : Extends Policy Interface to Migrate Client Registration Policies
- KEYCLOAK-15534 Client Policy : Implement Existing Client Registration Policies as Client Policies

About Client Policies Practical Guide

Brief Description of Client Policies Practical Guide

Please refer to

https://github.com/keycloak/kc-sig-fapi/blob/master/FAPI-SIG/documents/ClientPolicies/ClientPoliciesPracticalGuide.pdf

END