FAPI-SIG Community 23rd Meeting

@Web Conference

21 Jul 2021

PROPOSED DRAFT

Table of Contents

Major Topics

Status Updates from 22nd Meeting

Working Items Status

PROPOSED DRAFT

Major Topics

Major Topics

- FAPI-CIBA

  Ran conformance tests against KC14 and listed up what need to be done to pass tests.

- Open Banking Brasil FAPI

  Several PRs has been sent by keycloak dev team.

Status Updates from 22nd Meeting
FAPI 2.0

Components of FAPI 2.0 Advanced

Completed Client Policies for PAR

- ✓ KEYCLOAK-18653 Client Policy - Endpoint : support Pushed Authorization Request Endpoint

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18653

  GH PR: https://github.com/keycloak/keycloak/pull/8240

Components of FAPI 2.0 Advanced

Grant Management requires RAR so that RAR need to be done at first

In Progress OAuth 2.0 Rich Authorization Requests (RAR)

- Design Document : https://github.com/keycloak/keycloak-community/pull/266
- Implementation : (WIP) https://github.com/tnorimat/keycloak/pull/24

In Progress Grant Management for OAuth 2.0

- Design Document : https://github.com/keycloak/keycloak-community/pull/265
- Implementation : (WIP) https://github.com/tnorimat/keycloak/pull/23

Status Updates from 22nd Meeting FAPI-CIBA

FAPI-CIBA Support

Completed Client Policies for CIBA

- ✓ KEYCLOAK-18654 Client Policy - Endpoint : support Token Request by CIBA Backchannel Authentication

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18654

  GH PR: https://github.com/keycloak/keycloak/pull/8242

Completed FAPI-CIBA requirements support

- ✓ KEYCLOAK-18123 Client Policy - Executor : Enforce Backchannel Authentication Request satisfying high security level

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18123

  GH PR: https://github.com/keycloak/keycloak/pull/8238

FAPI-CIBA Support

Completed Secure Signing Algorithm for CIBA

- ✓ KEYCLOAK-18683 Client policy executor for check Backchannel signed request algorithms matching FAPI compliant algorithms

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18683

  GH PR: https://github.com/keycloak/keycloak/pull/8252

Pass conformance test : Mandatory 7 Issues

Completed “auth_time” claim in ID token

- ✓ KEYCLOAK-18826 FAPI-CIBA-ID1 conformance test : ID Token needs to include "auth_time" claim

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18826

  GH PR: https://github.com/keycloak/keycloak/pull/8277

Completed Backchannel Authentication endpoint allowed as “aud” claim in signed authentication request

- ✓ KEYCLOAK-18827 FAPI-CIBA-ID1 conformance test : Client JWT authentication should allow Backchannel Authentication endpoint as audience

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18827

  GH PR: https://github.com/keycloak/keycloak/pull/8283

Completed Signed authentication request’s claim checks

- ✓ KEYCLOAK-18828 FAPI-CIBA-ID1 conformance test : Additional checks of signed authentication request

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18828

  GH PR: https://github.com/keycloak/keycloak/pull/8294

Pass conformance test : Mandatory 7 Issues

Completed Condition evaluated on backchannel authentication and token requests

- KEYCLOAK-18829 FAPI-CIBA-ID1 conformance test : ClientRolesCondition needs to be evaluated on CIBA backchannel authentication request and token request

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18829

  GH PR: https://github.com/keycloak/keycloak/pull/8278

Completed Holder-of-Key token for CIBA token request

- KEYCLOAK-18830 FAPI-CIBA-ID1 conformance test : HolderOfKeyEnforcerExecutor needs to be executed on CIBA token request

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18830

  GH PR: https://github.com/keycloak/keycloak/pull/8293

Completed Status code when user authentication is not completed

- KEYCLOAK-18831 FAPI-CIBA-ID1 conformance test : need to return 400 if user authentication is not successfully completed

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18831

  GH PR: https://github.com/keycloak/keycloak/pull/8285

Pass conformance test : Mandatory 7 Issues

Completed Status code when client authentication is not completed

- ✓ KEYCLOAK-18832 FAPI-CIBA-ID1 conformance test : need to return 401 error=invalid_client if client authentication is not successfully completed on Backchannel Authentication endpoint

  JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18832

  GH PR: https://github.com/keycloak/keycloak/pull/8295

Pass conformance test : Optional 3 Issues

Open Confidential client is only allowed for CIBA

KEYCLOAK-18833 FAPI-CIBA-ID1 : need to only accept confidential client on Backchannel Authentication endpoint

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18833

GH PR: not yet

Open Change profiles depending on scope value

KEYCLOAK-18834 Client Policies : ClientScopesCondition needs to be evaluated on CIBA backchannel authentication request and token request

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18834

GH PR: not yet

In Progress Provide default profile the same as FAPI1-Baseline/Advanced

KEYCLOAK-18863 Global client profile for FAPI CIBA

JIRA Ticket: https://issues.redhat.com/browse/KEYCLOAK-18863

GH PR: not yet

Status Updates from 22nd Meeting Open Banking Brasil FAPI

Specifications

In Progress Open Banking Brasil Financial-grade API Security Profile 1.0

Specification : Implementer's Draft 1

JIRA Ticket (Epic) : KEYCLOAK-18629 OpenBanking Brasil support

Not Yet Open Banking Brasil Financial-grade API Dynamic Client Registration 1.0

Specification : Implementer's Draft 1

JIRA Ticket (Epic) : NA

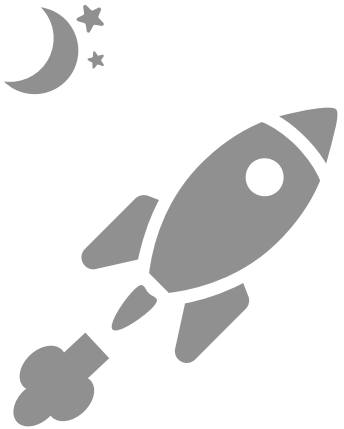
Current Keycloak's Status

In Progress OpenBanking Brazil support

JIRA Ticket [Epic] : https://issues.redhat.com/browse/KEYCLOAK-18629

Listed up all works needed to be done. 20 in total.

15 resolved/closed. 4 open. 1 PR sent.



Working Items Status

Working Items

[Security Features]

<Common>

In Progress OIDC Client's Public Key Management

Hitachi

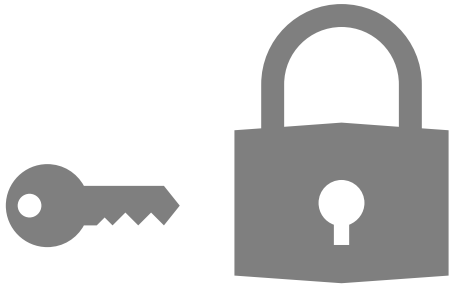
1st phase -> 2nd phase

[Security Features]

<SPA/Native App>

In Progress OAuth 2.0 Demonstration of Proof-of-Possession (DPoP)

Backbase



Working Items

[Security Features]

<High Level Security>

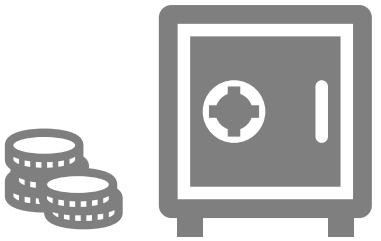
- FAPI 2.0 (baseline/advanced)

In Progress Rich Authorization Request (RAR) — Adorsys

In Progress Grant Management API — Adorsys

- FAPI-CIBA

In Progress Other requirements support — Hitachi



Working Items

[Market Specific Features]

<PSD2>

- Following eIDAS regulations

In Progress QWAC verification

Adorsys

- Consent Management

<UK OpenBanking>

- Onboarding
  - Software Statement Support
  - Software Statement Assertion (SSA) Verification

Working Items

[Market Specific Features]

<Open Banking Brasil>

In Progress OB-BR FAPI

Red Hat

Roadmap

	2020 Sep	2021 Apr
Security		
Common Client Policies	• Implemented as Preview • New Admin REST API support	• Migrate Client Registration Policy • Move Preview to Official Support -> leads to FAPI 1.0 Official Support
High Level Security		
FAPI 1.0	• Supported ID2 ver • Passed ID2 conformance test	• Support Final ver • Pass Final ver conformance test
FAPI 2.0		• Start design and implementation PAR, RAR, Grant Management API
FAPI-CIBA	• Supported Pure CIBA (poll mode) as Preview	• Support FAPI-CIBA (poll mode) • Pass conformance test
SPA/Native App DPoP		• Start design and implementation

PROPOSED DRAFT

Roadmap

Market Specific	2020 Sep	2021 Apr
PSD2	• Discussed QWAC verification	• Start design and implementation QWAC verification
UK OpenBanking		• Start design and implementation (?) Onboarding
Open Banking Brasil		• Support OBB FAPI

END