FAPI-SIG Community Meeting

@Web Conference

7 Aug 2020

Hitachi (mainly I) has developed features required for FAPI security profile support (e.g. Proof Key for Code Exchange, OAuth 2.0 Mutual-TLS Certificate-Bound Access Tokens, supporting secure signature algorithms etc.).

Major features have already been supported but there are still some issues need to be resolved for passing FAPI conformance tests in order for keycloak to become Certified Financial-grade API (FAPI) OpenID Providers.

We Hitachi began to collaborate with Japanese community member (Wada-san@NRI), and he developed test environment, and we registered issues in keycloak-fapi repository (https://github.com/jsoss-sig/keycloak-fapi).

We have listed up tasks as issues in FAPI conformance tests and keycloak's JIRA tickets.

Brief Story

Agenda

- Clarifying the objectives of FAPI-SIG
- Clarifying how to go forward FAPI-SIG activities
- Proposing work items
  - For FAPI 1.0
  - Beyond FAPI 1.0

Clarifying the objectives of FAPI-SIG

1. Make keycloak pass the conformance test of Certified Financial-grade API (FAPI) OpenID Providers.

   FAPI R/W OP w/ MTLS , FAPI R/W OP w/ Private Key

2. Make keycloak pass the conformance test of Certified Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) OpenID Providers.

   FAPI-CIBA OP poll w/ MTLS, FAPI-CIBA OP poll w/ Private Key,

   FAPI-CIBA OP poll w/ MTLS, FAPI-CIBA OP poll w/ Private Key

etc...

[MTLS] :RFC 8705 OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens Client

Private_key_jwt : section 9 Authentication on OIDC

Clarifying how to go forward FAPI-SIG activities

Do as open source community activities.

All activities are public.

Sometimes have a meeting to discuss activities.

etc..

Proposing work items :
For FAPI 1.0:

Scope - Implement and contribute features for FAPI 1.0

Part 1 : Read Only API Security Profile (FAPI-RO)

Part 2 : Read and Write API Security Profile (FAPI-RW)

Part 3 : Client Initiated Backchannel Authentication Profile (CIBA)

Part 4 : JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

Scope - Run and pass conformance tests for FAPI 1.0

Part 1 : Read Only API Security Profile (FAPI-RO)

Part 2 : Read and Write API Security Profile (FAPI-RW)

-> conformance test for Certified Financial-grade API (FAPI) OpenID Providers (both FAPI R/W OP w/ MTLS and FAPI R/W OP w/ Private Key)

Part 3 : Client Initiated Backchannel Authentication Profile (CIBA)

-> conformance test for Certified Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) OpenID Providers (FAPI-CIBA OP poll w/ MTLS, FAPI-CIBA OP poll w/ Private Key, FAPI-CIBA OP poll w/ MTLS, FAPI-CIBA OP poll w/ Private Key)

Part 4 : JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

-> no conformance test (but coming soon)

Current Status - Implement and contribute features for FAPI 1.0

Part 1 : Read Only API Security Profile (FAPI-RO)

Part 2 : Read and Write API Security Profile (FAPI-RW)

-> In progress (on final stage)

Part 3 : Client Initiated Backchannel Authentication Profile (CIBA)

-> In progress (design document PR has been merged)

Part 4 : JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

-> Open

Current Status - Run and pass conformance tests for FAPI 1.0

Part 1 : Read Only API Security Profile (FAPI-RO)

Part 2 : Read and Write API Security Profile (FAPI-RW)

-> In progress (run and analyze its result on Aug 2018 against keycloak 6)

Part 3 : Client Initiated Backchannel Authentication Profile (CIBA)

-> open (but no implementation)

Part 4 : JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

-> open (but no implementation and conformance test)

Current Status In Details

FAPI-RO and FAPI-RW

Ran and analyzed its result for conformance tests of both FAPI R/W OP w/ MTLS and FAPI R/W OP w/ Private Key on https://github.com/jsoss-sig/keycloak-fapi.

To pass both tests, 27 issues need to be resolved, 11 are still open, 16 have been closed.

9 of 11 open issues will be closed by resolving 11 of keycloak JIRA tickets :

KEYCLOAK-11254 to 11262 - 9 tickets will be resolved by Client Policies

KEYCLOAK-11263 - 1 ticket is still open

KEYCLOAK-14380 - 1 ticket was resolved

Client Policies related JIRA tickets :

KEYCLOAK-13933, 14189 to 14209 - 22 tickets are in progress as Client Policies

Current Status In Details

FAPI-RO and FAPI-RW

[Client Policies]

PR merged :

KEYCLOAK-14189 : merged

PR sent :

KEYCLOAK-14190

ready and will send PR :

KEYCLOAK-14191 - 14193, 14195 - 14207

open :

KEYCLOAK-14194, 14208 - 14209

Current Status In Details

FAPI-RO and FAPI-RW

Ran and analyzed its result for conformance tests of both FAPI R/W OP w/ MTLS and FAPI R/W OP w/ Private Key on https://github.com/jsoss-sig/keycloak-fapi.

To pass both tests, 27 issues need to be resolved, 11 are still open, 16 have been closed.

2 of 11 open issues are still not treated, no JIRA tickets :

Issue#12, #22

https://github.com/jsoss-sig/keycloak-fapi/issues?q=is%3Aissue+is%3Aopen+label%3Aundetermined

Current Status In Details

FAPI-RO and FAPI-RW

Problems : Ran and analyzed its result for conformance tests of both FAPI R/W OP w/ MTLS and FAPI R/W OP w/ Private Key but version of this conformance tests became obsolete.

[conformance test release]

Dec 2017 : FAPI-RW Implementer’s Draft ver1 (OpenBanking specific) for OpenID Provider

Apr 2019 : FAPI-RW Implementer’s Draft ver2 for OpenID Provider

Analyzed result is for Implementer’s Draft ver1

Current active conformance test is Implementer’s Draft ver2

-> **need to re-run and analyze the result for Implementer’s Draft ver2 conformance test against latest keycloak.**

Current Status In Details

FAPI-CIBA

[Implementation & Contribution]

Its design document has been merged.

Its Proof-of-Concept codes has been prepared. Now try to revise these codes to comply with the merged design document.

[conformance test run & feedback]

Nothing started. Waiting for implementation.

Tasks

FAPI-RO and FAPI-RW

[implementation & contribution]

Work for remaining JIRA tickets

- KEYCLOAK-11263, 14194, 14208 - 14209

Work for remaining issues

- https://github.com/jsoss-sig/keycloak-fapi/issues?q=is%3Aissue+is%3Aopen+label%3Aundetermined

[conformance test run & feedback]

- Re-run and analyze the result for Implementer's Draft ver2 conformance test against latest keycloak.

Proposing work items :
Beyond FAPI 1.0:

Items

Integrating FAPI conformance test run into keycloak’s CI/CD pipeline

Implement and contribute security profiles

- RFC 8252 OAuth 2.0 for Native Apps
- OAuth 2.0 for Browser-Based Apps
- OAuth 2.1
- FAPI-RW App2App

Items

- Ecosystem specific
  - UK Open Banking (In service)
    - verifying TPP’s certificate (eIDAS consideration)
    - dynamic client registration (SSA consideration)
  - Australia Consumer Data Right (launched on July 2020)
    - security profiles based on FAPI 1.0