OAuth-SIG Community 1st Meeting (46th from ex-FAPI-SIG)

@Web Conference

7 June 2023

PROPOSED DRAFT

Table of Contents

OIDF Certificate Program Updates

OIDF Certificate Program Updates

Site URL : https://openid.net/certification/

- FAPI OpenID Providers (OP) & Profiles
  - FAPI OP - KSA Open Banking: 2 conformance profiles
  - FAPI OP - Brazil Open Insurance: 9 conformance profiles
- FAPI2 Providers & Profiles
  - FAPI 2.0 Security Profile Second Implementer's Draft & Message Signing First Implementer's Draft: 5 conformance profiles
    - FAPI2SP MTLS + MTLS
    - FAPI2SP private key + MTLS
    - FAPI2SP OpenID Connect
    - FAPI2MS JAR
    - FAPI2MS JARM
  - Australia FAPI 2.0 ConnectId Implementer's Draft: 2 conformance profiles

Ongoing working items of security features

FAPI 2.0 Security Profile / FAPI 2.0 Message Signing

- Specification
  - FAPI 2.0 Security Profile: Implementer's Drafts
    https://openid.net/specs/fapi-2_0-security-profile.html
  - FAPI 2.0 Message Signing: Draft
    https://openid.bitbucket.io/fapi/fapi-2_0-message-signing.html
- PRs for passing all 5 conformance profiles' tests of FAPI 2.0
  - FAPI 2.0 security profile - Reject Implicit Grant executor does not return an appropriate error
    https://github.com/keycloak/keycloak/pull/20638 Merged
  - FAPI 2.0 security profile - not allow an authorization request whose parameters were not included in PAR request
    https://github.com/keycloak/keycloak/pull/20678 Merged
  - FAPI 2.0 security profile - not allow an authorization request whose parameters were not included in Request Object pushed to PAR request
    https://github.com/keycloak/keycloak/pull/20741 Review required
  - FAPI 2.0 security profile - supporting RFC 9207 OAuth 2.0 Authorization Server Issuer Identification
    https://github.com/keycloak/keycloak/pull/20621 Review required

OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)

- Specification **Internet Draft v16**

  URL: https://datatracker.ietf.org/doc/id/draft-ietf-oauth-dpop.html

- Design **In review**

  URL: https://github.com/keycloak/keycloak-community/pull/254

- Issue

  URL: https://issues.redhat.com/browse/KEYCLOAK-15169

- PR (Draft) **In review**

  URL: https://github.com/keycloak/keycloak/pull/8895

Takashi re-reviewed the design and PR, and proposed arquillian integration tests for the PR.

If tests are added, hopefully, the PR will be re-submitted official and other maintainers review it.

Reference token

Some use cases requires a reference type access token instead of an ordinary assertion type access token.

- Discussion

  URL: https://github.com/keycloak/keycloak/discussions/19649/

- Issue

  URL: https://github.com/keycloak/keycloak/issues/19650

- Design

  URL: https://github.com/keycloak/kc-sig-fapi/blob/main/FAPI-SIG/meetings/42nd/presentations/FAPI-SIG_42nd_MTG_agenda.pdf

- PR

  URL: https://github.com/keycloak/keycloak/pull/19824

➡ I received some feedback comments on the architecture of this feature, so am reconsidering the architecture.

Tracking OAuth MTLS RFC

Keycloak supported Internet draft version OAuth MTLS, not RFC version OAuth MTLS.

There are difference between Internet draft version and RFC version.

Confidential client does not need to user OAuth MTLS certification bound refresh token.

■ Discussion

URL: https://github.com/keycloak/keycloak/discussions/19704

[proposal]

Keycloak makes a refresh token certificate bound, so a client cannot do token refresh if the bound certificate with the refresh token and an access token expires.

➡

Keycloak does not make a refresh token certificate bound , so a client can do token refresh even if the bound certificate with an access token expires.

Keyconf 23

Keyconf 23

Date and Time: 10 AM - 4 PM, June 16, 2023

Venue: Level39, 1 Canada Square, Canary Wharf, London, UK

Web page: https://www.eventbrite.co.uk/e/keyconf-23-tickets-621079815447

(tickets sold out)

Program:

- Recently added features in Keycloak in past years that make Keycloak a strong performer in the IAM market - Marek Posolda / Red Hat
- OpenID FAPI work in the last 12 months - Vinod Anandan / Citibank
- Keycloak in Open Banking or consent-driven open data ecosystem - Kannan Rasappan / Banfico & Francis Pouatcha / Adorsys
- OpenID FAPI presentation (any demo or theme) - Takashi Norimatsu / Hitachi
- Roadmap on possible ideas for the future work of Keycloak - Marek Posolda / Red Hat
- Workshops on potential uses cases

END