FAPI-SIG Community 45th Meeting

@Web Conference

3 May 2023

PROPOSED DRAFT

Table of Contents

Ongoing working items of security features

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

#1 Specification Internet Draft v16

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

#2 Design In review

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

#3 Issue

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

#4 PR (Draft) In review

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

Takashi re-reviewed the design and PR, and try to write 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.

#1 Discussion

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

#2 Issue

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

#3 Design

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

#4 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.

#1 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

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

Enlarging a scope of FAPI-SIG and renaming FAPI-SIG

Enlarging a scope of FAPI-SIG and renaming FAPI-SIG

Our proposal in the previous meeting:

OAuth SIG, OAuth Families SIG, OAuth protocols SIG - This SIG supports to Keycloak any kind of specification of OAuth2 and OpenID Connect.

➡

Many Keycloak maintainer including Stian preferred OAuth SIG.

➡

How about the following?

Name: OAuth SIG

Scope: Supporting to Keycloak any kind of specification of OAuth2 and OpenID Connect.

Keycloak use case
by Agence du Numérique en Santé, France

END