SIG Meeting: 2025-04-09 22nd Meeting (67th from Ex FAPI-SIG)

Meeting Slides

- Date: Wed 9 April 2025
- Time:
  11:00 - 12:00 UTC in 1 hour
  07:00 - 08:00 EDT (UTC-4)
  12:00 - 13:00 BST (UTC+1)
  13:00 - 14:00 CEST (UTC+2)
  14:00 - 15:00 EEST (UTC+3)
  16:30 - 17:30 IST (UTC+5:30)
  20:00 - 21:00 JST (UTC+9)
  21:00 - 22:00 AEST (UTC+10)

Agenda

Agenda Items to discuss

Attendees

- Takashi Norimatsu
- Francis Pouatcha
- Thomas Darimont
- Vinod Anandan
- Dmitry Telegin
- Ingrid Kamga
- Marek Posolda
- Ogen Bertrand
- Rodrick Awambeng
- Stefan Wiedenmann

Notes

Notes by Topic

General

- Takashi presents current state of efforts
- Next OAuth SIG meeting will be held on Wednesday 7 May 2025.

Transaction Token, SPIFEE for Workload Identity

- In workload identity event (by cyberark) as KubeCon Europe 2025 London co-located event, some demo was done by Red Hat staff.
- Continue working on it. plan to do some demo in KeyConf 25 Amsterdam.

OAuth 2.0 for First-Party Applications (FiPA)

- Did some Poc (sd-jwt).
- Plan to create a discussion about it.

Shared Signals Framework (SSF)

- Some maintainers (Stian, Alexander) requests to investigate implementation option for SSF event processing. They are afraid that implementing them onto Keycloak directly adds complexity to Keycloak.
- Created a quarkus-based slide-car app outside keycloak, and now investigating better way: Valkey
  https://valkey.io/topics/streams-intro/

OpenID Federation 1.0

bucchi submitted the article to Medium:
https://bucchi.medium.com/building-trust-with-openid-federation-trust-chain-on-keycloak-f8ac021add3a
Which draft version? -> Implementer's Draft 4 (draft 36) (https://openid.net/specs/openid-federation-1_0-ID4.html)

OpenID Verifiable Credentials Issuance (OID4VCI)

remaining option issue
https://github.com/keycloak/keycloak/issues/32967
not planned (front end issue)
all mandatory issues were resolved.
the latest: ID2 draft 15 but need to consider interoperability with other entities.
comment: better to mention which draft version used.
create issue to follow the latest event.

OpenID Foundation conformance test: parameter settings - HAIP
fistly check metadata comply with ID2 draft 15.

Adorsys will look at how to move to draft 15.

OIDF OpenID4VCI conformance tests update:

FYI, we'll probably release the first version of OpenID4VCI Issuer conformance tests in the next few days.
https://gitlab.com/openid/conformance-suite/-/merge_requests/1608

We'll use ID2 draft15 as a base
https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

An we focus on the constraints given by https://openid.github.io/oid4vc-haip/openid4vc-high-assurance-interoperability-profile-wg-draft.html#section-4

Token Exchange

26.2 release: this or next week?
fine-graind admin permission supported from 26.2.

Demonstrating Proof-of-Possession (DPoP)

Passkeys

RH team will work on it.
(testing framework, etc)

FAPI 2.0

KeycloakCon Japan 2025

KeyConf 25 Amsterdam

BarCamp will be planned on 29 August, the next day of KeyConf 25 Amsterdam.

Who can attend the BarCamp? The same as Keycloak DevDay 2025 post event, inviting only speakers of KeyConf 25?

BackBase HQ office basically is OK to be used for BarCamp, but do not have several rooms.

Changes in Audience validation of JWT client authentication

Due to the changed rules for audience validation for private_key_jwt and client_secret_jwt in the OIDC Core specification to fix a security issue, we have to make the audience validation more strict => only issuer URL is allowed in the audience.

This can me relaxed with a new jwt authenticator config property and a server-side configuration.

Previously, we allowed the following URLs:

- issuerUrl
- tokenUrl
- tokenIntrospectionUrl
- parEndpointUrl
- (ciba) backchannelAuthenticationUrl

Issue: https://github.com/keycloak/keycloak/issues/38751
See: https://github.com/keycloak/keycloak/pull/38754

Related: https://openid.net/notice-of-a-security-vulnerability/
Also: https://nat.sakimura.org/2025/04/08/openid-foundation-workshop-recap/#Major_Changes_from_FAPI_2_Implementers_Draft_to_Final

-> Major Changes from FAPI 2 Implementers Draft to Final:
Change related to audience value in private key JWT client authentication (addressing security vulnerability)

Recordings

https://us06web.zoom.us/rec/share/gZm5b0W_9KfjnOL9ZWSv9qWMai8a6aMiWxcktBFZ1MZzYjdLpzHJu48tdw-yeudy.AecP3zFRKwWIyqMT