@Web Conference

19 March 2025

OAuth SIG Community 21st Meeting

(66th from ex-FAPI-SIG)

PROPOSED DRAFT

Table of Contents

New Support

1. Workload Identity - Transaction Token, SPIFEE
2. FiPA
3. SSF
4. OpenID Federation 1.0

Refinement

1. OID4VCI
2. Token Exchange
3. DPoP
4. Passkeys
5. FAPI 2.0

Community Event

KeyConf 2025 Japan

KeyConf 25 Amsterdam

New Support

1. Workload Identity - Transaction Token, SPIFEE

- Specification (IETF Internet Draft in OAuth WG)
  https://datatracker.ietf.org/doc/draft-ietf-oauth-transaction-tokens/
- Status - Transaction Token: Some SIG members have PoC and would work on it.

  https://github.com/dteleguin/tts-demo
- Status - SPIFEE: Some IBM staff have PoC and would work on it.
  https://github.com/maia-iyer/spire-demos/tree/main/keycloak_token_exchange

2. OAuth 2.0 for First-Party Applications (FiPA)

- Specification (IETF Internet Draft)
  https://www.ietf.org/archive/id/draft-ietf-oauth-first-party-apps-00.html
- Status: Some SIG members would work on it.
- Discussion:

  Support for native login experiences with OAuth 2.0 First-Party Applications (#25014)

  Refactoring Authenticators to Support an API-Based Authentication Approach (#36924)

3. Shared Signals Framework (SSF)

- Motivation

  Some major platform vendors supported/required it:

  - Apple Business Manager, Apple School Manager
  - Google Cross-Account Protection (RISC)

- Adopters

  A lot (Cisco, Okta, etc.), but not officially announced (maybe SSF is for internal use?)

- Specification (Implementer's Draft)

  - SSF: https://openid.net/specs/openid-sharedsignals-framework-1_0-ID3.html
  - CAEP: https://openid.net/specs/openid-caep-interoperability-profile-1_0-ID1.html
  - RISC: https://openid.net/specs/openid-risc-profile-specification-1_0.html

- Discussion: Support RISC and CAEP events / Shared Signals and Events (#14217)

  Some SIG members are working on it.

  - PoC for a receiver: https://github.com/identitytailor/keycloak-ssf-support

4. OpenID Federation 1.0

■ Motivation

- Enabling automatic client Registration within the European ecosystem: Payment Service Directive (PSD), Payment Services Regulation (PSR), Financial Data Access (FIDA)
- In research & education field, eduGAIN’s OpenID Federation profile support.
- Adopters: Italy’s digital identity system (SPID),
  Greece’s academic network (GRNET) in the future?

■ Specification (Implementer's Draft)

https://openid.net/specs/openid-federation-1_0.html

■ Discussion: Support for OpenID Federation 1.0 (#31027)

Some SIG members are working on it.

- prepared an intermediate authority and trust anchor
- confirmed that a client can be registered to Keycloak by its trust chain.
- an article about it will be posted in Medium soon.

PROPOSED DRAFT

Refinement

1. OpenID Verifiable Credentials Issuance (OID4VCI)

- Goal: Keycloak can work as an issuer of VCs. (currently it is an **experimental** feature)
- Possible use-cases: German National EUDI Wallet

  https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/en/start/
- Epic issue: [OID4VCI] Approaching Credential Scope based API design (#32961)

  Status: 8 out of all 8 issues were resolved. (+2 resolved, 100%)

  Current other open issues:

  - Limit Client capabilities to OpenID Connect or OpenID4VCI (#32967, no PR)
  - Extend AbstractOIDCProtocolMapper for credentials (#32957, PR #37687)
- Discussion: OpenID for Verifiable Credential Issuance (#17616)
- Design: https://github.com/keycloak/keycloak-community/blob/main/design/OID4VCI.md
- Guide: adorsys/keycloak-ssi-deployment

PROPOSED DRAFT

2. Token Exchange

- Goal: Officially supported (currently it is a **preview** feature)
- Status: In progress
- Epic issue: Support for standard Token-Exchange (#31546)
- Status:

  Standard (internal - internal): KC 26.2 (Mar/Apr)

  33 out of 34 issues were resolved (+9 issue added, +28 newly resolved, 97.0%)

  Federated (internal - external): KC 26.4 (Sep/Oct) or later?

  1 out of 13 issues were resolved (+1 issue added, +1 newly resolved, 8.0%)

  Documentation:

  https://docs.google.com/document/d/1T_4hjf0tapLAC5Hpac8wNiEHcrAmYZDQGpj3JRJ2MBI
- Discussion: Token-Exchange Use-cases (#26502)

3. Demonstrating Proof-of-Possession (DPoP)

- Goal: Officially supported (currently it is a **preview** feature since KC 23)
- Status: In progress
- Epic issue: DPoP: promote from preview to supported (#22311)

Status: 7 of 11 issues were resolved (+1 newly resolved, 64%)

Need urgent consideration:

[Resolved] DPoP: Refresh token created with DPoP can be refreshed without proof (#36475)

[PR sent] DPoP: User Info Endpoint authorization type mismatch (#36476)

4. Passkeys (Multi-Device FIDO Credentials)

- Status: Goal: Officially supported (currently it is a **preview** feature since KC 23)
- Status: In progress
- Discussion: Support for passkeys (#16201)
  - Epic Issue: 8 of 14 issues were resolved (#23656, +1 resolved, 57%)
- Resources
  - FIDO Alliance : https://fidoalliance.org/white-paper-multi-device-fido-credentials/
  - Apple : https://developer.apple.com/passkeys/
  - Google : https://developers.google.com/identity/passkeys/
  - passkeys.dev : https://passkeys.dev/
  - passkeys.io : https://www.passkeys.io/
  - passkeys futures detection: https://featuredetect.passkeys.dev/

5. FAPI 2.0

The final version of FAPI 2.0 Security Profile was published in Feb 2025.

https://openid.net/specs/fapi-security-profile-2_0-final.html

The current (since KC23) Keycloak’s FAPI 2.0 support is for its implementer’s draft version 2.

https://openid.net/specs/fapi-2_0-security-profile-ID2.html

https://www.keycloak.org/docs/latest/release_notes/index.html#fapi-2-drafts-support

Need to follow the final version.

- Clarify the difference.
- Clarify what we should do.
- Work for that if needed.

Community Event

KeyConf 2025 Japan

- Date: 13 June 2025, 12:30 - 8:00 PM (just before KubeCon Japan 2025, Tokyo, Japan)
- Venue: TBA (Tokyo, Japan) 🇯🇵

Hosted by Cloud Native Security Japan (CNSJ), under CNCF Japan Chapter
https://community.cncf.io/events/details/cncf-cloud-native-security-japan-presents-keyconf-2025-japan/

Registration: not yet open
CfP: open
https://sessionize.com/keyconf-2025-japan/

KeyConf 25

- Date: 28 August 2025 (just after OSS Summit Europe 2025, Amsterdam, Netherlands)
- Venue: Amsterdam, Netherlands 🇳🇱

Discussion Items:

How about holding a BarCamp on 29 August just after KeyConf 25?

Attendee: up to 20 people expected.

Venue: Backbase HQ?

END