

@Web Conference  
4 June 2025

# OAuth SIG Community 24<sup>th</sup> Meeting (69<sup>th</sup> from ex-FAPI-SIG)

# Table of Contents

## New Support

1. Workload Identity - Transaction Token, SPIFEE
2. FiPA
3. SSF
4. OpenID Federation 1.0
5. FIDO2 conformance test

## Refinement

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

## Community Event

KeycloakCon Japan

KeyConf 25 Amsterdam

# New Support

# 1. Workload Identity - Transaction Token, SPIFEE

- Specification (IETF Internet Draft in OAuth WG)

<https://www.ietf.org/archive/id/draft-ietf-oauth-transaction-tokens-05.html>

- 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](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-01.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](#))

Enable user authentication by presentation of an SD-JWT identity credential with OAuth 2.0 for First-Party Applications (FiPA) ([#38796](#))

# 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](https://openid.net/specs/openid-sharedsignals-framework-1_0-ID3.html)
- CAEP: [https://openid.net/specs/openid-caep-1\\_0-ID2.html](https://openid.net/specs/openid-caep-1_0-ID2.html) (updated)
- RISC: [https://openid.net/specs/openid-risc-profile-specification-1\\_0.html](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](https://openid.net/specs/openid-federation-1_0.html)

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

PoC: dynamically registering a wallet by OpenID Federation

CNCF Blog:

<https://www.cncf.io/blog/2025/04/25/building-trust-with-openid-federation-trust-chain-on-keycloak/>

KeycloakCon Japan: <https://keycloakconjapan2025.sched.com/event/23463>

# 5. FIDO2 Conformance Test

Running FIDO2 conformance test against Keycloak:

- Functional Certification
- Conformance Self-Validation Testing
- Specification: FIDO2
- Type: Server

<https://fidoalliance.org/certification/functional-certification/>



# Refinement

# 1. OpenID Verifiable Credentials Issuance (OID4VCI)

- Goal: Keycloak can work as an issuer of VCs. (currently it is an **experimental** feature)
- Status: In progress
- Possible use-cases: German National EUDI Wallet  
<https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/en/start/>
- Design:  
<https://github.com/keycloak/keycloak-community/blob/main/design/OID4VCI.md>
- Guide: [adorsys/keycloak-ssi-deployment](#)
- Discussions:
  - OpenID for Verifiable Credential Issuance ([#17616](#))
  - [OID4VCI] Realm based scope credential approach ([#39265](#))
- Epic issue: [OID4VCI] Approaching Credential Scope based API design ([#32961](#))  
Status: 8 out of all 8 issues were resolved. (100%) -> **Close it?**

# 1. OpenID Verifiable Credentials Issuance (OID4VCI)

## ■ Epic issues:

[OID4VCI] Implementing support for OID4VCI ID2 Draft 15 ([#39273](#))

Status: 4 out of all 27 issues were resolved. (+8 added, +4 resolved, 15%)

[WIP] [OID4VCI] Support: Authorization Code Flow ([#39261](#))

Status: 2 out of all 4 issues were resolved. (+2 resolved, 50%)

## 2. Token Exchange - Internal/Internal

- Goal: Officially supported (currently it is a **preview** feature)
- Status: Completed (Keycloak 26.2)
- Epic issues:
  - Support for standard Token-Exchange ([#31546](#)) -> Closed

## 2. Token Exchange - Internal/External

- Goal: support as **preview** feature(?)

- Status: In progress

- Epic issues:

  - Federated token exchange ([#38335](#))

    - Status: 2 out of all 17 issues were resolved. (+3 added, 12%)

  - Subject impersonation token exchange ([#38336](#))

    - Status: 0 out of all 5 issues were resolved. (0%)

# 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: 9 of 15 issues were resolved. (+3 added, +1 resolved, 60%)

## 4. Passkeys

■ Goal: Officially supported (currently it is a **preview** feature since KC 23)

■ Status: In progress

■ Discussion: Support for passkeys ([#16201](#))

■ Epic Issue: Passkeys support ([#23656](#))

Status: 10 of 18 issues were resolved. (+4 added, 56%)

■ 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](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://openid.net/specs/fapi-2_0-security-profile-ID2.html)

[https://www.keycloak.org/docs/latest/release\\_notes/index.html#fapi-2-drafts-support](https://www.keycloak.org/docs/latest/release_notes/index.html#fapi-2-drafts-support)

Need to follow the final version.

■ Epic Issue: FAPI 2.0 Security Profile final version support ([#38769](#))



# Community Event

# Events

2025

June



13 KeycloakCon Japan 2025 (Hilton Odaiba Hotel, Tokyo, Japan)



16 - 17 KubeCon + CloudNativeCon Japan 2025 (Hilton Odaiba Hotel, Tokyo, Japan)  
- Keycloak session in Maintainer Track

August




25 - 27 Open Source Summit Europe 2025 (RAI Amsterdam Convention Centre, Amsterdam, Netherlands)



28 KeyConf 25 (Van der Valk Hotel Amsterdam Zuidas - RAI, Amsterdam, Netherlands)


# KeycloakCon Japan

- Date: 13 June 2025, 1:00 - 8:00 PM (just before KubeCon Japan 2025, Tokyo, Japan)
- Venue: Hilton Tokyo Odaiba (Tokyo, Japan) 

As CNCF-hosted co-located event of KubeCon + CloudNativeCon Japan 2025.

- Web Site: <https://events.linuxfoundation.org/keycloakcon-japan/>
- Registration: Open. This event is free to attend.
- Schedule: Published.  
<https://events.linuxfoundation.org/keycloakcon-japan/program/schedule/>

# KeyConf 25

- Date: 28 August 2025 (just after OSS Summit Europe 2025, Amsterdam, Netherlands)
- Venue: Van der Valk Hotel Amsterdam Zuidas - RAI, Amsterdam, Netherlands 
- Web Site: <https://keyconf.dev/>
- Registration: Open.
- CfP: Open.

## Note:

- BarCamp on 29 August just after KeyConf 25 on Backbase HQ.



END