

@Web Conference
6 August 2025

OAuth SIG Community 26th Meeting (71st from ex-FAPI-SIG)

Table of Contents

- New Support
 1. Workload Identity - Transaction Token, SPIFEE
 2. FiPA
 3. SSF
 4. OIDFED
 5. Attestation-Based Client Auth
 6. MCP
- Refinement
 7. OID4VCI
 8. Token Exchange
 9. DPOP
 10. Passkeys
 11. FAPI 2.0
- Community Event

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

- Event: IETF 123 Madrid

<https://events.oauth.net/2025/07/ietf-123-madrid-ASzyJKU1TnAV>

- OAuth 2.0 Dynamic Client Registration with Trusted Issuer Credentials
<https://datatracker.ietf.org/doc/draft-kasselman-oauth-dcr-trusted-issuer-token/>
- OAuth Client Registration on First Use with SPIFFE
<https://datatracker.ietf.org/doc/draft-kasselman-oauth-spiFFE/>

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. [Updating the discussion \(#38796\)](#)

- 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
- CAEP: https://openid.net/specs/openid-caep-1_0-ID2.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>

■ Status: No update.

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](#))

■ Status:

The slack channel was created (<https://cloud-native.slack.com/archives/C096PUDTC3U>).

■ Epic issue: OpenID Federation implementation ([#40509](#))

5. OAuth 2.0 Attestation-Based Client Authentication

■ Motivation

- OpenID4VC HAIP adopts it as one option of wallet authentication methods.
- It might be useful in FiPA context.

■ Specification (Internet Draft)

<https://www.ietf.org/archive/id/draft-ietf-oauth-attestation-based-client-auth-05.html>

■ Discussion: Support for OAuth 2.0 Attestation-Based Client Authentication ([#40413](#))

■ Status: Some SIG members would work on it ([#39287](#)), which is related to OID4VCI.

6. Model Context Protocol (MCP)

■ Motivation:

- Keycloak can be used as an authorization server in AI agent industry.

■ Specification (regarding Authorization):

<https://modelcontextprotocol.io/specification/draft/basic/authorization>

- Protocol Revision: 2024-11-05, 2025-03-26, **2025-06-18 (latest)**, Draft (in progress)

■ Epic Issue: MCP Authorization specification support ([#41251](#))

Status: 0 out of all 2 issues were resolved. (+2 created, 0%)

1 PR sent ([#41440](#)).

Refinement

7. 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%)

7. OpenID Verifiable Credentials Issuance (OID4VCI)

■ Epic issues:

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

Status: 19 out of all 28 issues were resolved. (+1 created, +13 resolved, 68%)

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

Status: 3 out of all 4 issues were resolved. (+1 resolved, 75%)

■ Topics:

- OIDF's OID4VCI conformance test targets Draft 15.
- OIDF's OID4VCI conformance test assumes [OpenID4VC High Assurance Interoperability Profile \(HAIP\)](#). Now Implementer's Draft 1 (HAIP draft 3).
- OpenID for Verifiable Credential Issuance - [draft 16](#) was released.

8. Token Exchange - Internal/External

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

- Status: In progress

- Epic issues:

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

 - Status: 6 out of all 23 issues were resolved. (+7 created, +3 resolved, 26%)

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

 - Status: 0 out of all 5 issues were resolved. (no progress, 0%)

9. 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: 11 of 15 issues were resolved. (+1 resolved, 73%)

10. 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: 24 of 27 issues were resolved. (+6 added, +7 resolved, 89%)

■ 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/>

11. FAPI 2.0

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

The final version of FAPI 2.0 Message Signing will be published in Aug 2025.

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

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

The PRs sent. ([#41120](#), [#41609](#))

- Epic Issue: FAPI 2.0 Message Signing final version support ([#41311](#))

Status: 1 of 3 issues were resolved. (+3 added, +1 resolved, 30%)

Community Event

Events

2025

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)

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: Closed.

Note:

- BarCamp “Keycloak Maintainers and Friends in Amsterdam” on 29 August just after KeyConf 25 in Backbase HQ.



END