

@Web Conference
3 September 2025

OAuth SIG Community 27th Meeting (72nd from ex-FAPI-SIG)

Table of Contents

New Support

1. Workload/Agent Identity
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

New Support

1. Workload/Agent Identity

■ Specification

- Transaction Tokens (v6)
<https://www.ietf.org/archive/id/draft-ietf-oauth-transaction-tokens-06.html>
- SPIFEE
<https://github.com/spiffe/spiffe/tree/main>
- OAuth Client Registration on First Use with SPIFFE
<https://datatracker.ietf.org/doc/draft-kasselman-oauth-spiffe/>
- OAuth 2.0 Dynamic Client Registration with Trusted Issuer Credentials
<https://datatracker.ietf.org/doc/draft-kasselman-oauth-dcr-trusted-issuer-token/>
- OAuth SPIFFE Client Authentication
<https://datatracker.ietf.org/doc/draft-schwenkschuster-oauth-spiffe-client-auth/>

1. Workload/Agent Identity

■ Status

- Transaction Tokens: Some SIG members have PoC and would work on it.
<https://github.com/dteleguin/tts-demo>
- SPIFEE: Some IBM staff have PoC and would work on it.
<https://github.com/spiffe/spiffe/tree/main>
- Agent Identity: Keycloak and SPIRE for Agent Identity
<https://github.com/christian-posta/keycloak-agent-identity>
- Epic? Issue: Support authenticating clients with SPIFFE/SPIRE
<https://github.com/keycloak/keycloak/issues/41907>
<https://github.com/stianst/playground/tree/main/demos/spiffe>

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

■ Specification

- OAuth 2.0 for First-Party Applications (v1)
<https://www.ietf.org/archive/id/draft-ietf-oauth-first-party-apps-01.html>

■ Discussion

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

■ Status

- User Authentication by SD-JWT VC in FiPA flow: In progress.

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

- OpenID Shared Signals Framework Specification 1.0 (SSF)
https://openid.net/specs/openid-sharedsignals-framework-1_0.html
- OpenID Continuous Access Evaluation Profile 1.0 (CAEP) (draft 03, ID2)
https://openid.net/specs/openid-caep-1_0-ID2.html
- OpenID RISC Profile Specification 1.0 (RISC) (draft 02)
https://openid.net/specs/openid-risc-1_0-02.html

3. Shared Signals Framework (SSF)

■ Discussion

- Support RISC and CAEP events / Shared Signals and Events ([#14217](#))

■ Topic

- Some SIG members have PoC and would work on it.
<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

- OpenID Federation 1.0 (draft 43)
https://openid.net/specs/openid-federation-1_0.html

■ Discussion

- Support for OpenID Federation 1.0 ([#31027](#))
- Slack channel (<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

- OAuth 2.0 Attestation-Based Client Authentication (I-D v6)
<https://www.ietf.org/archive/id/draft-ietf-oauth-attestation-based-client-auth-06.html>

■ Discussion

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

■ Issue

- [OID4VCI] Understand key attestations as additional information to jwt proofs or as per new attestation proof type (for Key binding) ([#39287](#))

6. Model Context Protocol (MCP)

■ Motivation

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

■ Specification

- Model Context Protocol: Base Protocol – Authorization (Draft)
<https://modelcontextprotocol.io/specification/draft/basic/authorization>
- Protocol Revision: 2024-11-05, 2025-03-26, **2025-06-18 (latest)**, Draft (in progress)

■ Discussion

- Complying with RFC 8414 about Well-Known URI for Authorization Server Metadata ([#40809](#))
- Support for RFC 8707 OAuth2 Resource Indicators ([#35743](#))

■ Epic Issue

- MCP Authorization specification support ([#41251](#))
Status: 0 out of all 2 issues were resolved. (no progress, 0%) 1 PR sent ([#41440](#)).

Refinement

7. OpenID Verifiable Credentials Issuance (OID4VCI)

■ Motivation

- Possible use-cases: German National EUDI Wallet

<https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/en/start/>

■ Specifications

- OpenID for Verifiable Credential Issuance - draft 16

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-16.html

- OpenID for Verifiable Credential Issuance - draft 17

https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

■ Discussion

- OpenID for Verifiable Credential Issuance ([#17616](#))
- [OID4VCI] Realm based scope credential approach ([#39265](#))

7. OpenID Verifiable Credentials Issuance (OID4VCI)

■ Epic issue

- [OID4VCI] Implementing Support for OID4VCI ID2 draft 16 ([#41569](#))

Status: 21 out of all 21 issues were resolved. (100%)

- Open Pull requests

<https://github.com/keycloak/keycloak/pulls?q=is%3Apr+is%3Aopen+OID4VCI>

8. Token Exchange – External to Internal

■ Epic issue

- External to internal token exchange ([#38335](#))

Status: 3 out of all 10 issues were resolved. (30%)

9. Demonstrating Proof-of-Possession (DPoP)

■ Epic issue

- DPoP: promote from preview to supported ([#22311](#))

Status: 14 of 16 issues were resolved. (+1 added, +3 resolved, 88%)

It seems that Keycloak 26.4 (end of Sep) support DPoP as officially supported feature.

10. Passkeys

■ Discussion

- Support for passkeys ([#16201](#))

■ Epic Issue

- Passkeys support ([#23656](#))

Status: 26 of 26 issues were resolved. (+2 resolved, 100%)

It seems that Keycloak 26.4 (end of Sep) support Passkeys as officially supported feature.

■ 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

■ Specifications

- FAPI 2.0 Security Profile (Final)
https://openid.net/specs/fapi-security-profile-2_0-final.html
- FAPI 2.0 Message Signing (draft 02)
https://openid.net/specs/fapi-message-signing-2_0-02.html

■ Epic Issues

- FAPI 2.0 Security Profile final version support ([#38769](#))
Status: 2 of 4 issues were resolved. (+1 resolved, 75%) The PRs sent. ([#41120](#))
- FAPI 2.0 Message Signing final version support ([#41311](#))
Status: 1 of 3 issues were resolved. (no progress, 30%)

■ Topic

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

Community Event

Events

2025

August

Completed



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)

2026

March



23 - 26 KubeCon + CloudNativeCon Europe 2025 (RAI Amsterdam Convention Centre, Amsterdam, Netherlands)



23 KeycloakCon Europe 2025 (RAI Amsterdam Convention Centre, Amsterdam, Netherlands)
- CNCF hosted co-located event

July



29 - 30 KubeCon + CloudNativeCon Japan 2025 (Pacifico Yokohama, Yokohama, Japan)



? KeycloakCon Japan 2025 (Pacifico Yokohama, Yokohama, Japan)
- CNCF hosted co-located event

October



7 - 9 Open Source Summit Europe 2025 (Prague, Czech Republic)



? KeyConf 26 (Prague, Czech Republic)



END