

@Web Conference  
2 July 2025

# OAuth SIG Community 25<sup>th</sup> Meeting (70<sup>th</sup> from ex-FAPI-SIG)

# Table of Contents

- New Support
  1. Workload Identity - Transaction Token, SPIFEE
  2. FiPA
  3. SSF
  4. OIDFED
  5. FIDO2 conformance test
  6. Attestation-Based Client Auth
  7. MCP
- Refinement
  8. OID4VCI
  9. Token Exchange
  10. DPOP
  11. Passkeys
  12. 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](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)
- 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/>



# 6. 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](#))

# 7. 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>

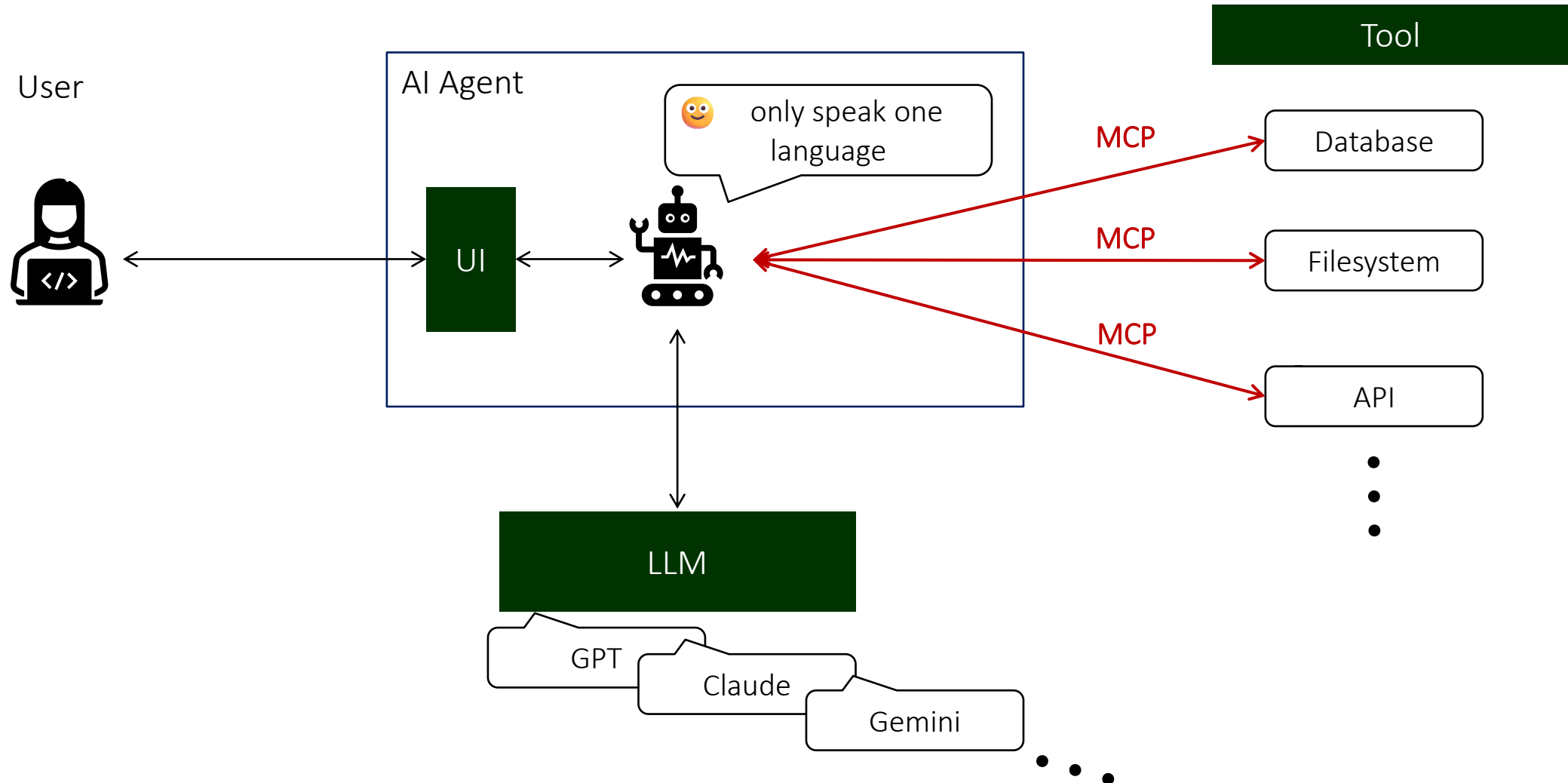
- Protocol Revision: 2024-11-05, 2025-03-26, **2025-06-18 (latest)**, Draft (in progress)

## ■ Discussion:

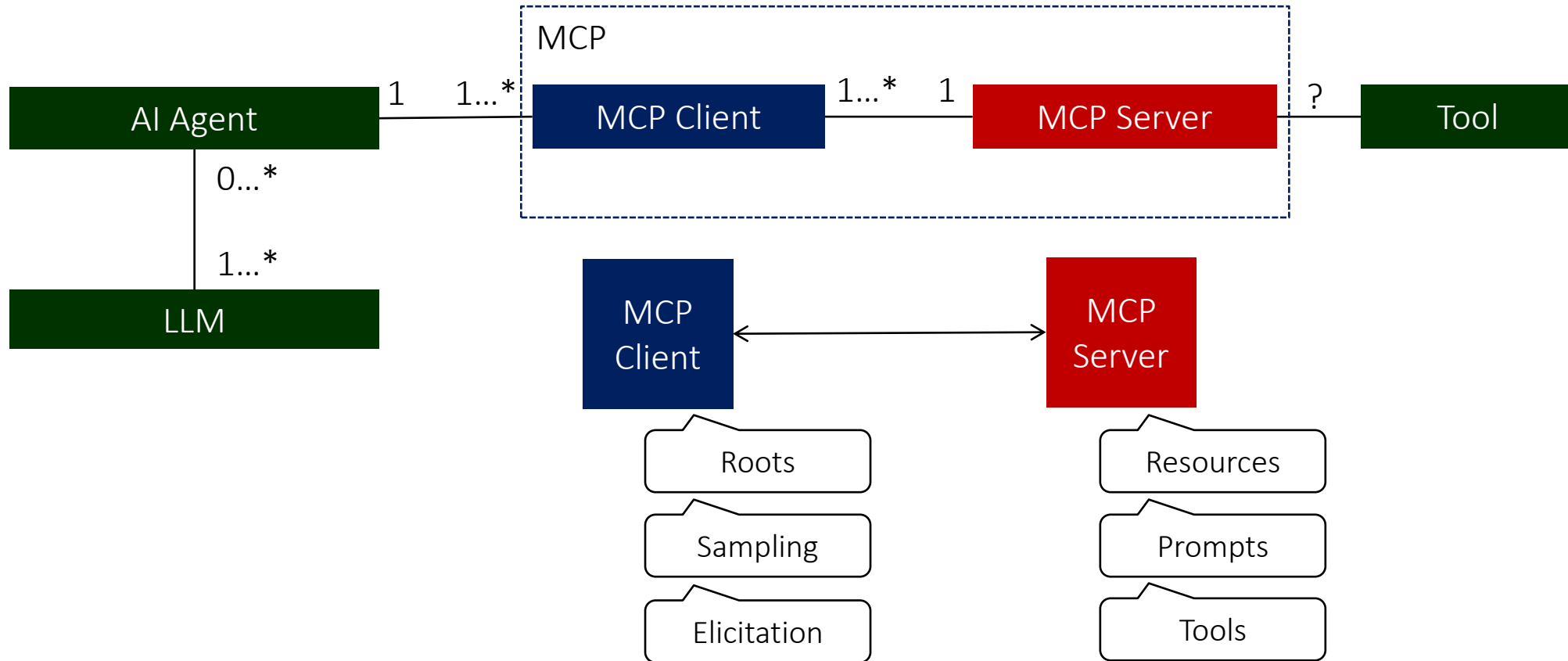
- Keycloak MCP Server ([#39995](#))

This talk is based on this version.

# 7. Model Context Protocol (MCP)



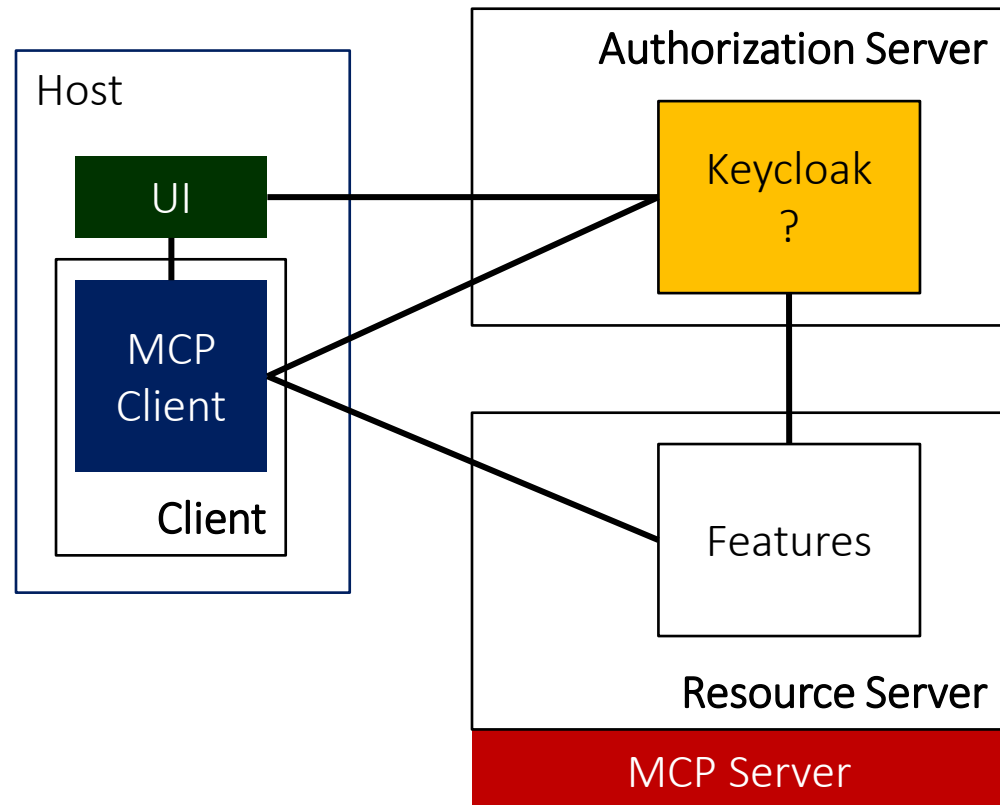
# 7. Model Context Protocol (MCP)



- Single endpoint  
(Ex. <https://example.com/mcp>)
- Support GET and POST

# 7. Model Context Protocol (MCP)

OAuth 2.0 Context:

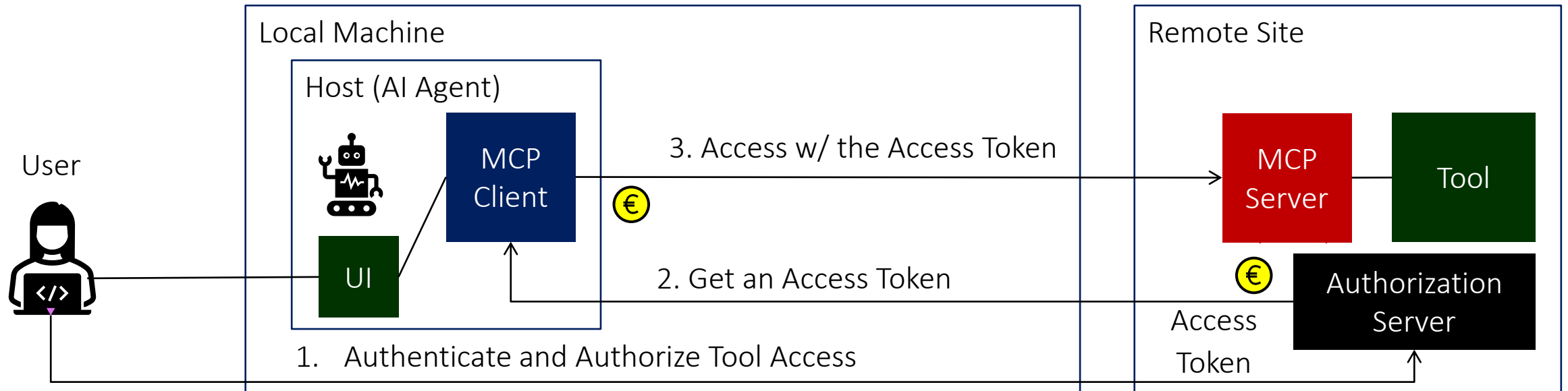


Roles:

MCP	OAuth2
MCP Client	Client
MCP Server	Resource Server
Authorization Server	Authorization Server
User	Resource Owner

\*: AuthN := Authentication, AuthZ := Authorization

# 7. Model Context Protocol (MCP)



# 7. Model Context Protocol (MCP)

## Authentication and Authorization in MCP

### **Server Metadata Discovery:**

- Advertising an Authorization Server's metadata to a Client
- Advertising a Resource Server's metadata to a Client

### **Dynamic Client Registration:**

- Dynamically registering a Client to an Authorization Server

### **Authorization:**

- Granting to a Client an access to a resource in a Resource Server
- Explicitly specifying a target resource in a Resource Server

# 7. Model Context Protocol (MCP)

	Authorization Server	MCP Server	MCP Client
Server Metadata Discovery (MUST)			
RFC 8414 OAuth 2.0 Authorization Server Metadata	X		X
RFC 9728 OAuth 2.0 Protected Resource Metadata		X	X
Dynamic Client Registration (SHOULD)			
RFC 7591 OAuth 2.0 Dynamic Client Registration Protocol	X		X
Authorization (MUST)			
The OAuth 2.1 Authorization Framework	X		X
RFC 8707 Resource Indicators for OAuth 2.0			X



# 7. Model Context Protocol (MCP)

Two pain points Keycloak faces to comply with MCP

1. Server Metadata Discovery – Authorization Server  
RFC 8414 OAuth 2.0 Authorization Server Metadata
2. Token Audience Binding  
RFC 8707 Resource Indicators for OAuth 2.0

# 7. Model Context Protocol (MCP)

## Issue 1: Server Metadata Discovery – Authorization Server

Keycloak's issuer URL (issuer metadata):

`https://keycloak.example.com/realms/mcp-tools`

well-known URI crafted the URL by following RFC 8414:

`https://keycloak.example.com/.well-known/oauth-authorization-server/realms/mcp-tools`

Actual Keycloak's well-known URI:

`https://keycloak.example.com/realms/mcp-tools/.well-known/oauth-authorization-server`

→ Keycloak needs to follow RFC 8414 for well-known URI

■ Discussion: Complying with RFC 8414 about Well-Known URI for Authorization Server Metadata ([#40809](#))

But, according to [the merged PR](#), which allows to use OIDC Discovery specified server metadata, Keycloak might not need to follow RFC 8414 defining well-known endpoint URI for MCP in the next version of MCP.

# 7. Model Context Protocol (MCP)

## Issue 2: Token Audience Binding

P1: binding an access token with its audience represented in **resource** parameter

MCP spec says “MCP servers MUST validate that access tokens were issued specifically for them as the intended audience, according to RFC 8707 Section 2.”

→ Keycloak needs to create an access token that can prove its intended audience, which is specified by the **resource** parameter sent from an MCP client.

P2: consistency check of **resource** parameters

MCP spec says “MCP clients MUST include the **resource** parameter in both authorization requests and token requests.”

→ Keycloak needs to check whether the **resource** parameters of an authorization request and token request are consistent.

- Discussion: Support for RFC 8707 OAuth2 Resource Indicators ([#35743](#))

- Draft PR: Add support for RFC 8707 OAuth2 Resource Indicators ([#35711](#))

# 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%)

# 1. OpenID Verifiable Credentials Issuance (OID4VCI)

## ■ Epic issues:

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

Status: 6 out of all 27 issues were resolved. (+2 resolved, 22%)

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

Status: 2 out of all 4 issues were resolved. (no progress, 50%)

## ■ 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.

## 2. Token Exchange - Internal/External

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

- Status: In progress

- Epic issues:

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

    - Status: 3 out of all 17 issues were resolved. (+1 resolved, 18%)

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

    - Status: 0 out of all 5 issues were resolved. (no progress, 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: 10 of 15 issues were resolved. (+1 resolved, 67%)
  - PR sent ([#35441](#)), Issue in progress (DPoP nonce [#39042](#))



# 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: 17 of 21 issues were resolved. (+4 added, +7 resolved, 81%)

■ 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

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 on 29 August just after KeyConf 25 on Backbase HQ.



END