

@Web Conference  
7 August 2024

# OAuth SIG Community 14<sup>th</sup> Meeting (59<sup>th</sup> from ex-FAPI-SIG)

# Table of Contents

## Ongoing working items of security features

1. OID4VCI
2. DPOP
3. Token Exchange

## Proposal/Backlog

1. OpenID Federation 1.0
2. OpenID Connect Native SSO for Mobile Apps 1.0
3. Passkeys
4. OIDC4IDA

## Community Event

Keyconf 24

# Ongoing working items of security features

# OpenID Connect for Verifiable Credentials (OID4VCs)

■ Goal: Keycloak can work as an issuer of VCs. (currently it is an **experimental** feature)

- Phase 1: supported as an experimental feature
- Phase 2: supported as a preview feature
- Phase 3: supported officially

Completed by KC 25

In Progress

■ Epic issue

- <https://github.com/keycloak/keycloak/issues/25936>

■ Status: 22 out of all 25 issues were resolved. (+3 new issues, +1 resolved)

Keycloak **25** starts supporting passkeys as an **experimental** feature.

■ Discussion

- <https://github.com/keycloak/keycloak/discussions/17616>

■ Design

- <https://github.com/keycloak/keycloak-community/blob/main/design/OID4VCI.md>

# OpenID Connect for Verifiable Credentials (OID4VCs)

## ■ Current focus points

- Key Binding
- Verifiable Presentation (VP) verification (originally, a verifier's capability)

## ■ Guide

- <https://github.com/adorsys/keycloak-ssi-deployment/>

## ■ Breakout sessions

21<sup>st</sup> : 17 Jul (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/21st>)

22<sup>nd</sup> : 24 Jul (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/22nd>)

23<sup>rd</sup> : 31 Jul (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/23rd>)

# Demonstrating Proof-of-Possession (DPoP)

- Goal: Officially supported (currently it is a **preview** feature)

- Status: In progress

Keycloak **23** starts supporting DPoP as a **preview** feature.

- Epic issue

- <https://github.com/keycloak/keycloak/issues/22311>

- Status: 2 of 3 issues were resolved (+2 issues resolved)

- Remaining issue: Fully decouple DPoP from TokenEndpoint and TokenManager if possible

- Issue: <https://github.com/keycloak/keycloak/issues/21921>

Due to other contributions, DPoP is decoupled from TokenEndpoint, and

There is the only one remaining part of DPoP in TokenManager.

# Token Exchange

- Goal: Officially supported (currently it is a **preview** feature)

- Status: In progress

Keycloak (unknown version) supported token exchange as a **preview** feature.

- Epic issue

- <https://github.com/keycloak/keycloak/issues/31546>

- Status: 0 out of all 7 issues were resolved.

- Discussion

- <https://github.com/keycloak/keycloak/discussions/26502>

- Resources:

- Specification: RFC 8693 OAuth 2.0 Token Exchange
- Keycloak's implementation
  - [https://www.keycloak.org/docs/latest/securing\\_apps/index.html#\\_token-exchange](https://www.keycloak.org/docs/latest/securing_apps/index.html#_token-exchange)

# Proposal/Backlog



# OpenID Federation 1.0

## ■ Motivation

Establishing trust between Entities like OPs and RPs by means of a trusted third party called a Trust Anchor, whose main purpose is to issue statements about Entities.  
(Ex. even if an RP has not yet been registered to an OP)

## ■ Motivation

- Enabling Automatic Registration of Clients 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.

## ■ Specification (Implementer's Draft)

- [https://openid.net/specs/openid-federation-1\\_0.html](https://openid.net/specs/openid-federation-1_0.html)

## ■ Discussion

- <https://github.com/keycloak/keycloak/discussions/31027>

## ■ Adopters

- Italian government (Sistema Pubblico di identità Digitale (SPID) / Carta di Identità Elettronica (CIE))  
<https://docs.italia.it/italia/spid/spid-cie-oidc-docs/it/versione-corrente/index.html>
- Global Assured Identity Network (GAIN) PoC  
<https://openid.net/cg/gain-poc/proof-of-concept/>

# OpenID Federation 1.0

## ■ Reference Implementation:

- KeyCloak for the European Open Science Cloud:

<https://github.com/eosc-kc/keycloak-oidc-federation>

- Thomas Darimont (forked eosc-kc implementation):

<https://github.com/thomasdarimont/keycloak-oidc-federation/tree/update/keycloak-25.0.x>

## ■ Resources:

Connect2id:

<https://connect2id.com/learn/openid-federation>

<https://connect2id.com/learn/openid-federation-metadata-policies>

Sphereon: API specifications

<https://app.swaggerhub.com/apis/SphereonInt/OpenIDFederationAPI/1.0.0-d35>

OpenID Foundation: conformance suite (conformance test development in progress)

<https://gitlab.com/openid/conformance-suite/>

# Passkeys (Multi-Device FIDO Credentials)

■ Status: Goal: Officially supported (currently it is a **preview** feature)

■ Status: In progress

Keycloak **23** starts supporting passkeys as a **preview** feature.

■ Discussion

- <https://github.com/keycloak/keycloak/discussions/16201>

■ Epic Issue: 6 of 11 issues were resolved (no progress)

- <https://github.com/keycloak/keycloak/issues/23656>

■ 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/>

# OpenID Connect Native SSO for Mobile Apps 1.0

## ■ Overview:

SSO in mobile apps: Share user authentication information among mobile applications installed on the same device.

Current BCP recommends to use a session cookie on a system browser, but some problems:

- The session cookie could be deleted by a user.
- The session cookie could not be shared if a user uses private browsing.

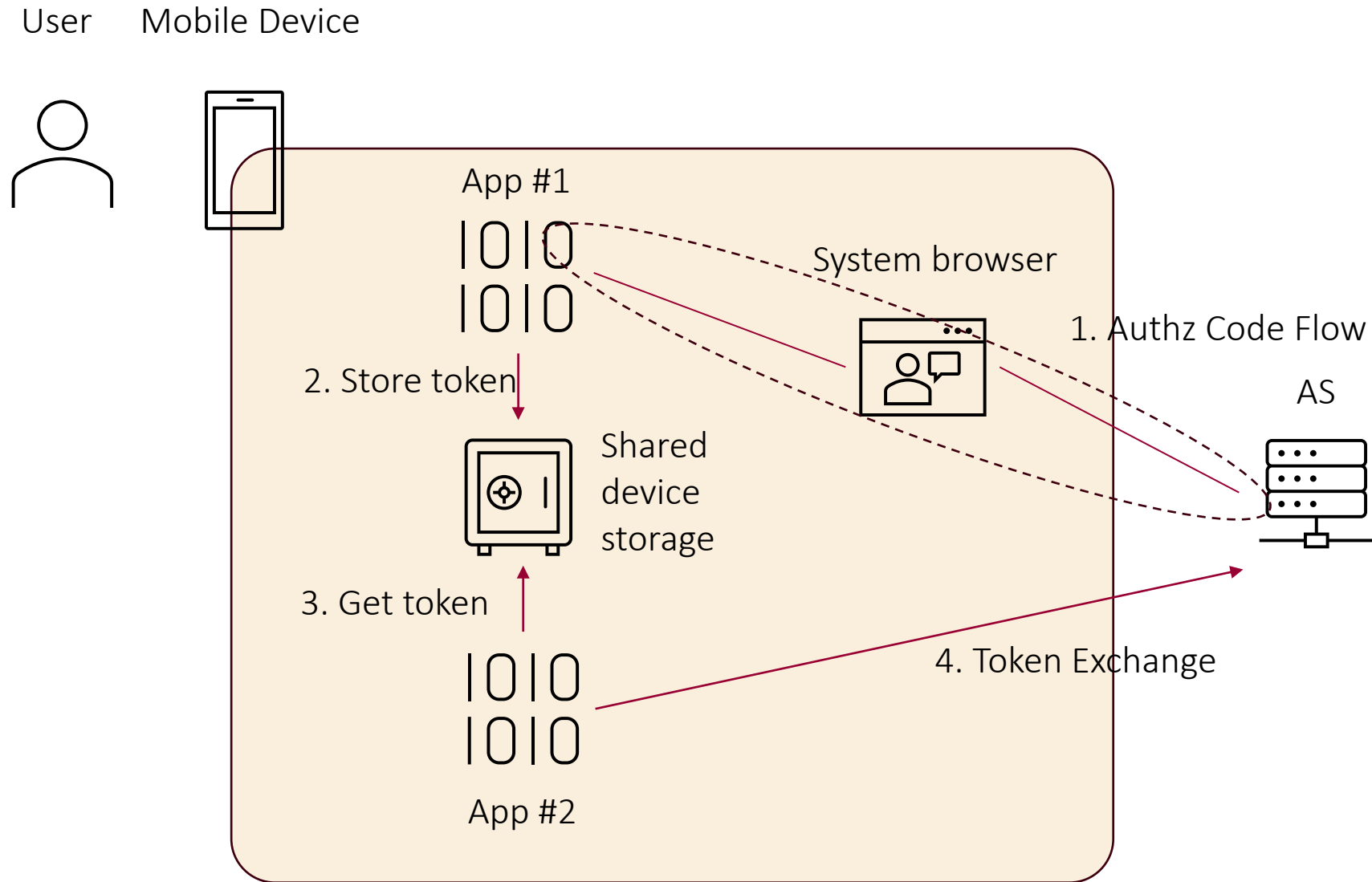
To avoid using the session cookie, use token exchange.

It could be one of use-cases of Token Exchange.

## ■ Specification (Implementer's Draft)

- [https://openid.net/specs/openid-connect-native-sso-1\\_0.html](https://openid.net/specs/openid-connect-native-sso-1_0.html)

# OpenID Connect Native SSO for Mobile Apps 1.0



# OpenID Connect for Identity Assurance 1.0 (OIDC4IDA)

## ■ Status: In progress

Waiting for discussion and review.

## ■ Specification

- OpenID Connect for Identity Assurance 1.0

Draft

[https://openid.net/specs/openid-connect-4-identity-assurance-1\\_0.html](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html)

## ■ Discussion

- Support for OIDC extensions: OIDC4IDA

<https://github.com/keycloak/keycloak/discussions/21270>

## ■ Implementation

- implement oidc4ida


Draft PR sent

Draft PR: <https://github.com/keycloak/keycloak/pull/21309>

# Community Event

# Keyconf 24

**Tickets sold out!**

- Date and Time: 10 AM to 4 PM, September 19th Thursday
- Venue: ARCOTEL Kaiserwasser, Vienna/Austria 
- Website : <https://keyconf.dev/>
- CfP
  - Schedule:
  - CfP Closes: 31 July
  - CfP Notifications: 19 August



# Proposal - KeyConf 25 as KubeCon EU 2025 London

## ■ Motivation

- Making Keycloak widely known (KubeCon draws a large number of attendees)
- Sponsors became also widely known by a wide range of peoples

## ■ Schedule: Apr 1-4 London

- Application form open : mid Aug
- Application deadline: mid Nov

## ■ Option: Half day or 1 day

## ■ Sponsors

At least 3 sponsors are required, but we can submit an application for the co-hosted event even if we cannot find any sponsors. CNCF can search sponsors.

- Gold: 9,500 USD - 2 free tickets, sponsor's logo shown on CNCF pages
- Platinum: 25,000 USD - 4 free tickets , sponsor's logo shown on CNCF pages
- Diamond: 35,000 USD - 5 free tickets, sponsor's logo shown on CNCF pages, Keynote speech

# Proposal - KeyConf 25 as KubeCon EU 2025 London

## ■ Speaker

A speaker of co-located event can attend KubeCon EU for free (no need to buy a ticket).

There are three types of the speaker:

[1] In normal session

[2] In Keynote speech

<a> As a sponsor

<b> As not a sponsor

A program committee of the co-located event can determine a speaker in [1] from CfPs (using the same mechanism as KubeCon, namely, sessionize).

Only Diamond sponsor can be a speaker in [2]-<a>.

A program committee of the co-located event can determine a speaker in [2]-<b>.



END