

@Web Conference  
12 February 2025

# OAuth SIG Community 20<sup>th</sup> Meeting (65<sup>th</sup> from ex-FAPI-SIG)

# Table of Contents

## Ongoing

1. OID4VCI
2. DPOP
3. OpenID Federation 1.0
4. SSF
5. Token Exchange
6. Passkeys

## Keeping Watch

1. OAuth 2.0 for First-Party Applications
2. Transaction Token
3. OpenID Connect Native SSO for Mobile Apps 1.0
4. OIDC4IDA

## Community Event

KeyConf 25

Ongoing

# 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:

[1] [OID4VCI] Approaching Credential Scope based API design

<https://github.com/keycloak/keycloak/issues/32961>

Status: 6 out of all 8 issues were resolved. (75%)

■ Discussion: <https://github.com/keycloak/keycloak/discussions/17616>

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

■ Guide: [adorsys/keycloak-ssi-deployment](https://adorsys.github.io/keycloak-ssi-deployment)

# 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: 5 of 11 issues were resolved (+3 issue added, +0 newly resolved, 45.5%)

# OpenID Federation 1.0

## ■ 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>

Some SIG members are working on it.

- prepared an intermediate authority and trust anchor
- confirmed that a client can be registered to Keycloak by its trust chain.
- confirmed that removing clients that are not used by a batch does not work.

# Shared Signals Framework (SSF)

## ■ Motivation

Some major platform vendors supported/required it:

- [Apple Business Manager, Apple School Manager](#)
- [Google Cross-Account Protection \(RISC\)](#)

## ■ Standardization Body

[OpenID Foundation - Shared Signals Working Group](#)

## ■ 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-interoperability-profile-1\\_0-ID1.html](https://openid.net/specs/openid-caep-interoperability-profile-1_0-ID1.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 transmitter.

<https://github.com/thomasdarimont/keycloak/tree/poc/shared-signals/services/src/main/java/org/keycloak/protocol/ssf>

# 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:

Standard token exchange: 5 out of 25 issues were resolved.  
(+6 issue added, +2 newly resolved, 20.0%)

Federated token exchange: 0 out of 12 issues were resolved.  
(+1 issue added, +0 newly resolved, 0.0%)

Impersonation: 0 out of 4 issues were resolved  
(+1 issue added, +0 newly resolved, 0.0%)

- Documentation:

- [https://docs.google.com/document/d/1T\\_4hjf0tapLAC5Hpac8wNiEHcrAmYZDQGpj3JRJ2MBI](https://docs.google.com/document/d/1T_4hjf0tapLAC5Hpac8wNiEHcrAmYZDQGpj3JRJ2MBI)

- Discussion

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



# 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: 7 of 14 issues were resolved (no progress, 50%)

- <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/>
- passkeys futures detection: <https://featuredetect.passkeys.dev/>

# Keeping Watch

# OAuth 2.0 for First-Party Applications

## ■ Specification (IETF Internet Draft)

- <https://www.ietf.org/archive/id/draft-parecki-oauth-first-party-apps-00.html>

## ■ Status: Some SIG members would work on it.

## ■ Discussion:

<https://github.com/keycloak/keycloak/discussions/36924>

<https://github.com/keycloak/keycloak/discussions/25014>

# Transaction Token

- Specification (IETF Internet Draft in OAuth WG)
  - <https://datatracker.ietf.org/doc/draft-ietf-oauth-transaction-tokens/>
- Status: Some SIG members have PoC and would work on it.
  - <https://github.com/dteleguin/tts-demo>

# 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.

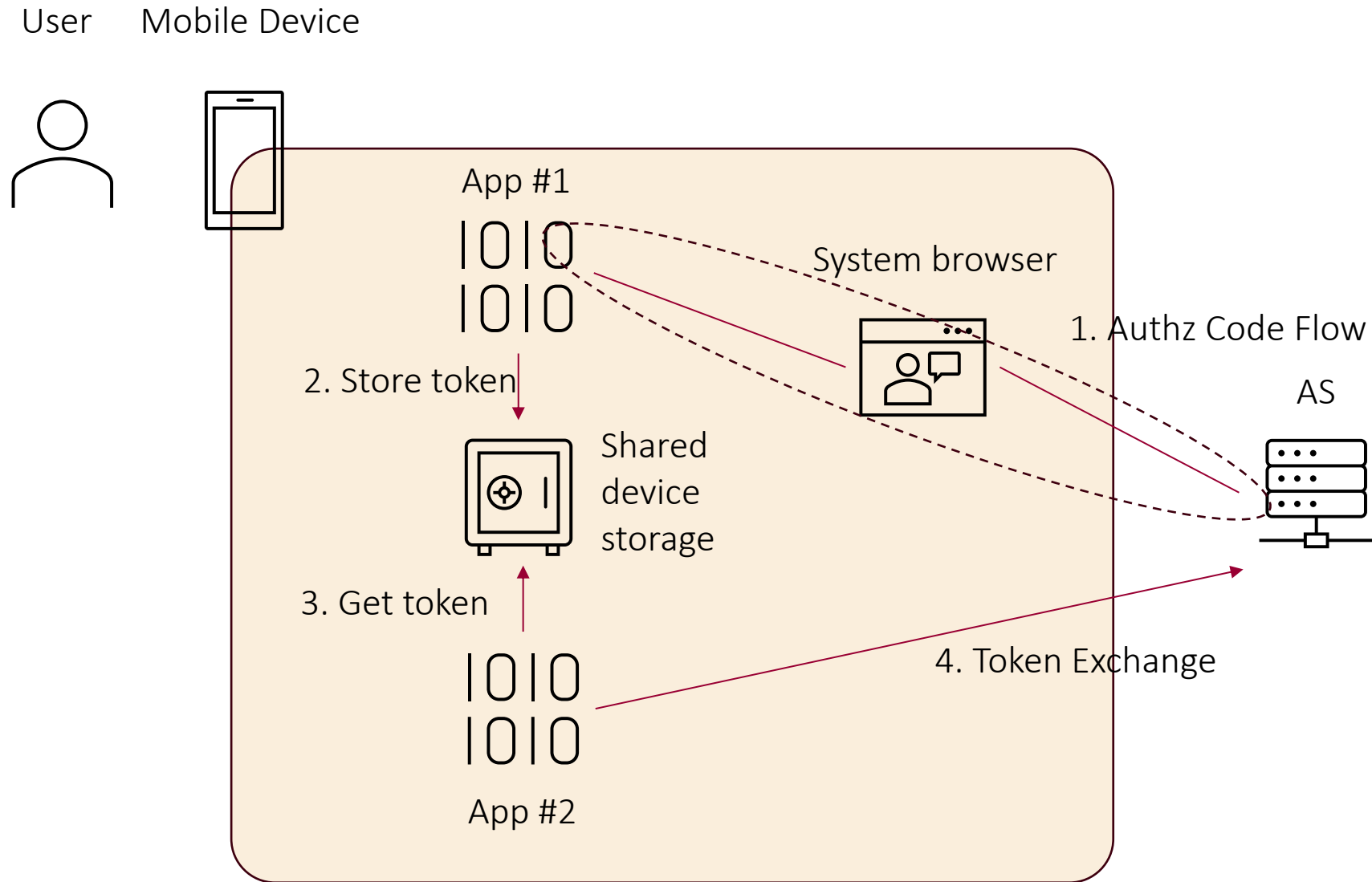
To avoid using the session cookie, use token exchange.

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 25

- Date: Just before or after OSS Summit Europe 28-29 August 2025 Amsterdam Netherlands
- Venue: Amsterdam, Netherlands 

## Discussion Items (the latest proposal by Adorsys):

- [1] Days: 2 days
- [2] Capacity: how many audiences we expect?
- [3] Conference format:
  - Including unconference session
  - Having multiple sessions in parallel: 2 rooms
- [4] Scope:
  - Enlarging its scope (e.g., not only topic about Keycloak, but standards, specifications, market trends)
- [5] Registration:
  - Requiring a registration fee: about 99 EUR



END