

@Web Conference
6 September 2024

OAuth SIG Community 17th Meeting (62nd from ex-FAPI-SIG)

Table of Contents

Ongoing

1. OID4VCI
2. DPOP
3. OpenID Federation 1.0
4. SSF

Standing Still

1. Token Exchange
2. 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)

■ Epic issue:

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

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

Status: 0 out of all 11 issues were resolved. (no progress, 0%)

Some SIG members are working on some tickets (2 in progress, 1 resolved).

[2] Pre-authorized-code flow of OID4VCI Implementation Shift to Scope-Based Approach within OpenID Connect Protocol

<https://github.com/keycloak/keycloak/issues/32772>

Status: 0 out of all 3 issues were resolved. (no progress, 0%)

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

■ 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/)

■ Breakout sessions

27th : 9 Oct (<https://cloud-native.slack.com/archives/C05KR0TL4P8/p1728911695051919>)

28th : 16 Oct (<https://cloud-native.slack.com/archives/C05KR0TL4P8/p1729077599586509>)

29th : 23 Oct (<https://cloud-native.slack.com/archives/C05KR0TL4P8/p1729682195485119>)

30th : 30 Oct (<https://cloud-native.slack.com/archives/C05KR0TL4P8/p1730291024363319>)

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 6 issues were resolved (+2 issue added)

- Make sure DPoP is passing with official OIDC testsuite

<https://github.com/keycloak/keycloak/issues/31970>

Some SIG members are working on it.

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

■ 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
- CAEP: https://openid.net/specs/openid-caep-interoperability-profile-1_0-ID1.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 transmitter.

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

Standing Still

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: 3 out of all 9 issues were resolved. (+2 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

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 13 issues were resolved (+2 open issues, +1 resolved)

- <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.

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.

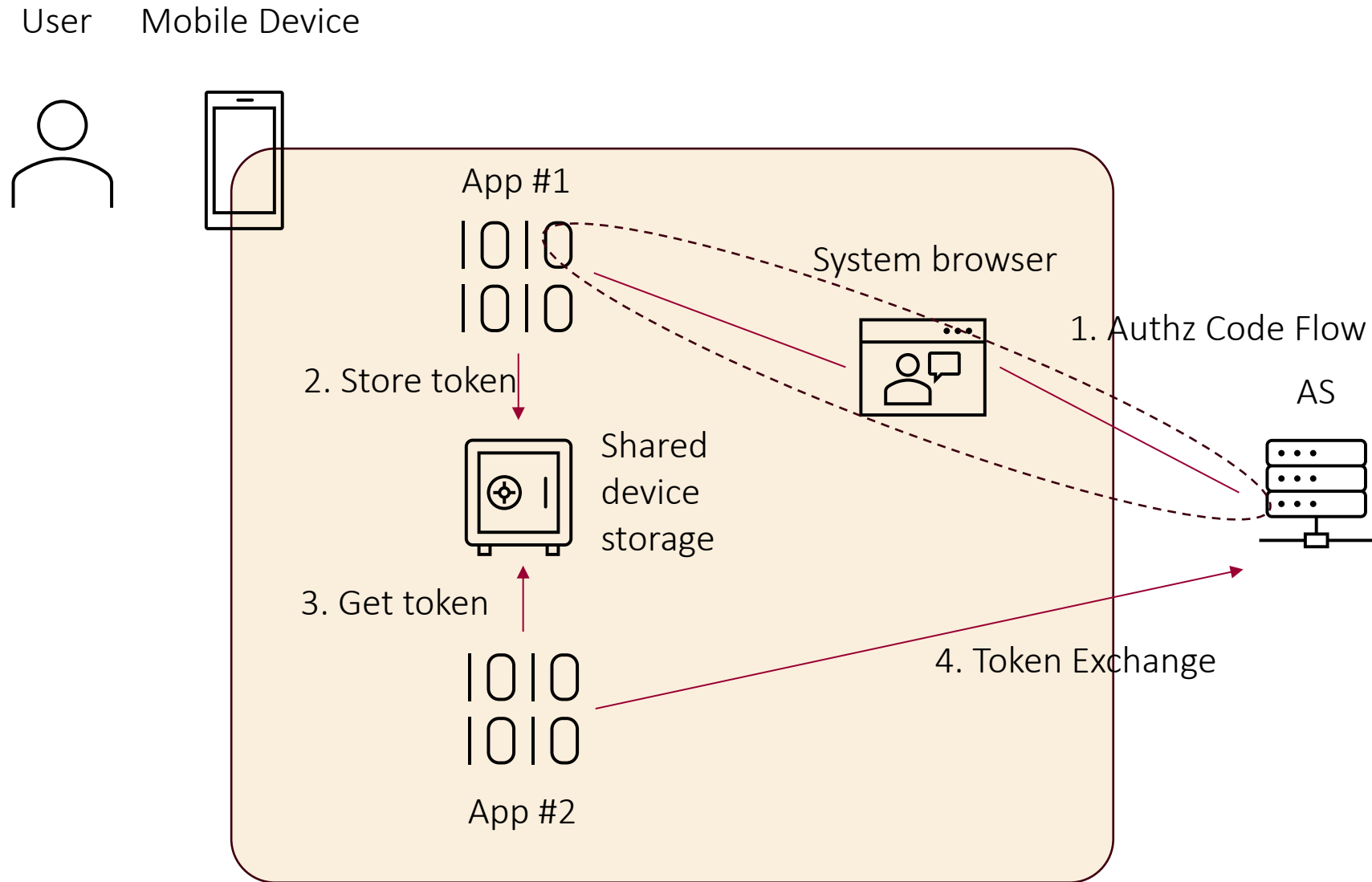
To avoid using the session cookie, use token exchange.

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

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

■ 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

Options:

1. Day just before or after OSS Summit Europe (25-27 Aug, Amsterdam, Netherlands)

<https://events.linuxfoundation.org/open-source-summit-europe/>

- Date: Friday 22 or Thursday 28 Aug 2025
- Venue: Amsterdam, Netherlands 
 - Option A: OSS Summit Europe co-located event
 - ✓ Audience : OSS Summit Europe attendee only?
 - Option B: Standalone Event (like KeyConf 24 Vienna)
 - ✓ Registration Fee: free or required?
(e.g., Keycloak Dev Day requires about 100 EUR)

2. Standalone Event

- Date and Time: Sep or Oct 2025 ? / 1 Day ?
- Venue: Athens, Greece / Bucharest, Romania / Cardiff, Wales / Dublin, Ireland / Oslo, Norway / Prague, Czech Republic / Zurich, Switzerland etc.



END