@Web Conference

3 July 2024

OAuth SIG Community 13th Meeting

(58th from ex-FAPI-SIG)

PROPOSED DRAFT

Table of Contents

Ongoing working items of security features

1. OID4VCI
2. Passkeys
3. DPoP
4. Token Exchange
5. OIDC4IDA

Proposal

OpenID Connect Native SSO for Mobile Apps 1.0

Community Event

Keyconf 24

PROPOSED DRAFT

Ongoing working items of security features

OpenID Connect for Verifiable Credentials (OID4VCs)

- Goal: Keycloak can work as an issuer of VCs.
  - Phase 1: supported as an experimental feature Completed by KC 25
  - Phase 2: supported as a preview feature In Progress
  - Phase 3: supported officially
- Epic issue : Support OpenID for Verifiable Credentials(OID4VC)
  - https://github.com/keycloak/keycloak/issues/25936
- Status: 22 out of all 21 issues were resolved. (+5 new issues, +4 resolved)
- Discussion: OpenID for Verifiable Credential Issuance
  - https://github.com/keycloak/keycloak/discussions/17616
- Design: OpenID Verifiable for Credential Issuance
  - https://github.com/keycloak/keycloak-community/blob/main/design/OID4VCI.md
- Breakout sessions

No sessions.

Passkeys (Multi-Device FIDO Credentials)

Nothing Progress

- Status: Goal: Officially supported (currently it is a preview feature)
- Status: In progress

  Keycloak 23 start supporting passkeys as a preview feature.
- Discussion
  - https://github.com/keycloak/keycloak/discussions/16201
- Epic Issue
  - https://github.com/keycloak/keycloak/issues/23656

  6 of 11issues were resolved, 1 PR was merged.
- 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/

PROPOSED DRAFT

DPoP

In Progress

- Goal: Officially supported (currently it is a preview feature)
- Status: In progress
- Follow-up Epic
  - https://github.com/keycloak/keycloak/issues/22311

  0 of 3 issues were resolved.

- [DPoP] token_type on UserInfoEndpoint expects Bearer instead of DPoP
  - Issue: https://github.com/keycloak/keycloak/issues/30181
  - PR: https://github.com/keycloak/keycloak/pull/29967

PR Sent

- Support DPoP dynamically for all grant-types
  - Issue: https://github.com/keycloak/keycloak/issues/30179
  - PR: https://github.com/keycloak/keycloak/pull/29967

PROPOSED DRAFT

Token Exchange

In Progress

- Goal: Officially supported (currently it is a preview feature)
- Status: In progress
- Discussion: When token-exchange will become productive feature from preview feature
  - https://github.com/keycloak/keycloak/discussions/23937
  - https://github.com/keycloak/keycloak/discussions/26502 (gathering use-cases) Updated!
- Concerns
  - Authorization: Fine-grained authorization is used, and it is a preview feature

    ➡ How about implementing a SPI provider for authorization?
    - implementing a SPI provider for authorization
    - implementing a provider for fine-grained authorization
    - implementing a provider for some authorization scheme officially supported (client policy?)
- Resources:
  - Specification: RFC 8693 OAuth 2.0 Token Exchange
  - Keycloak's implementation
    - https://www.keycloak.org/docs/latest/securing_apps/index.html#_token-exchange

PROPOSED DRAFT

OpenID Connect for Identity Assurance 1.0 (OIDC4IDA) Nothing Progress

- 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

Proposal

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:

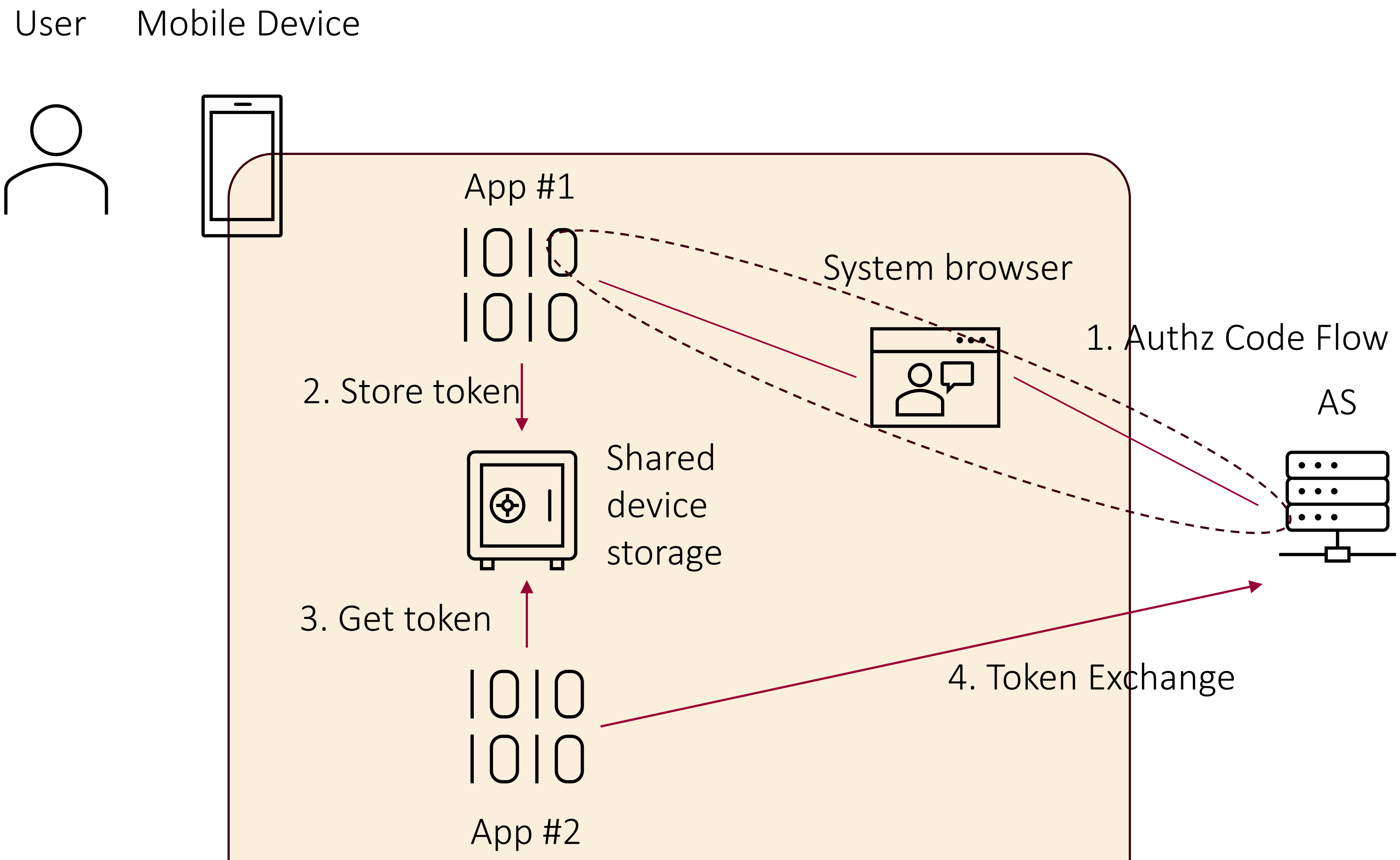
- The session cookie could be deleted by a user.
- The session cookie could not be shared if a user uses private browsing.

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



PROPOSED DRAFT

Community Event

Keyconf 24 **Tickets sold out!**

- Date and Time: 10 AM to 4 PM, September 19th Thursday
- Venue: ARCOTEL Kaiserwasser, Vienna/Austria 🇦🇹
- Web-site (registration) : https://www.eventbrite.de/e/keyconf24-tickets-887467387847
- CfP
  - Form: https://forms.office.com/e/pgBuPzbgqP
  - Schedule:

    CfP Closes: 31 July

    CfP Notifications: 19 August

END