OAuth SIG Community 5th Meeting

(50th from ex-FAPI-SIG)

@Web Conference

1 November 2023

PROPOSED DRAFT

Table of Contents

KubeCon + CloudNativeCon North America 2023

KubeCon + CloudNativeCon North America 2023

- Web Site: https://events.linuxfoundation.org/kubecon-cloudnativecon-north-america/
- Program: https://events.linuxfoundation.org/kubecon-cloudnativecon-north-america/program/schedule/
- Date: 6 - 9 November 2023
- Venue: McCormick Place West, Chicago, Illinois, United States of America
- Keycloak related sessions:
  - *Maintainer track: 10 Years of Keycloak - What's Next for Cloud-Native Authentication and OIDC?*
    Alexander Schwartz, Red Hat & Takashi Norimatsu, Hitachi, Ltd.
  - *Contribfest: Keycloak - Accelerate New Features, Squash Bugs and Learn to Contribute*
    Alexander Schwartz & Michal Hajas, Red Hat.
  - *Session: Challenge to Implementing "Scalable" Authorization with Keycloak*
    Yoshiyuki Tabata, Hitachi, Ltd.
  - *Session: Beyond Passwords: Keycloak's Contributions to Identity and Access Management and Security*
    Soojin Lee, Megazone

Ongoing working items of security features

Edwards-curve Digital Signature Algorithm (EdDSA)

- Specification
  - RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA)
  - RFC 8037 CFRG Elliptic Curve Diffie Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)
- Discussion
  - Supporting EdDSA
    https://github.com/keycloak/keycloak/discussions/15713
- Implementation
  - Supporting EdDSA PR sent
    Issue: https://github.com/keycloak/keycloak/issues/15714
    PR: https://github.com/keycloak/keycloak/pull/17215

Working for resolving review comments.

Lightweight Token

- Discussion
  - Lightweight access tokens:
    https://github.com/keycloak/keycloak/discussions/9713
- Implementation
  - Enhancing Light Weight Token: Merged
    Issue: https://github.com/keycloak/keycloak/issues/21183
    PR: https://github.com/keycloak/keycloak/pull/22148

Three follow-up issues are still open.

- Supporting a reference/lightweight access token
  Epic Issue: https://github.com/keycloak/keycloak/issues/21186

OpenID Connect for Identity Assurance 1.0 (OIDC4IDA)

- 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

Waiting for discussion and review.

Passkeys (Multi-Device FIDO Credentials)

- 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/
- Discussion

  https://github.com/keycloak/keycloak/discussions/16201
- Implementation

  Epic Issue: https://github.com/keycloak/keycloak/issues/23656

  3 of 4 issues were resolved

  Authentication by passkeys can be used as a preview feature.

  Login-less authentication with WebAuthn Conditional UI can also be used as a preview feature.

OpenID4VC High Assurance Interoperability Profile with SD-JWT VC

- Discussion

  https://github.com/keycloak/keycloak/discussions/17616

- Design

  https://github.com/keycloak/keycloak-community/pull/350

- Implementation (by FIWARE)

  https://github.com/FIWARE/keycloak-vc-issuer

The first breakout meeting was held on 19 Oct.

- At first, we try to make Keycloak an Issuer.
- FIWARE's extension for OID4VCI is used to realize flows described in the discussion
- To do so, we list up what we need to implement to keycloak side.

  e.g, RAR support, OAuth 2.0 Attestation-Based Client Authentication, etc…

New topics

Token Exchange

- Token Exchange:
  https://www.keycloak.org/docs/latest/securing_apps/index.html#_token-exchange

Token Exchange is Technology Preview and is not fully supported.
This feature is disabled by default.

How to get the "Token-Exchange" feature out of preview?

END