OAuth SIG Community 7th Meeting

(52nd from ex-FAPI-SIG)

@Web Conference

3 January 2024

Table of Contents

Completed working items of security features

   DPoP

   FAPI 2.0

Ongoing working items of security features

   Passkeys

   OAuth 2.1

   Lightweight Token

   EdDSA

   OIDC4IDA

Emerging working items of security features

   OID4VCs

   Token Exchange

Community Event

   Keycloak Dev Day 24

   Keyconf 24

PROPOSED DRAFT

Completed working items of security features

DPoP `Completed`

■ Status: Completed

Keycloak 23 supported DPoP as a preview feature.

Blog: https://www.keycloak.org/2023/11/keycloak-2300-released

This working item was completed for a moment though there still be the task to make DPoP officially supported.

FAPI 2.0 `Completed`

■ Status: Completed

Keycloak 23 supported the following FAPI 2.0 specifications:
- FAPI 2.0 Security Profile Second Implementer's Draft
- FAPI 2.0 Message Signing First Implementer's Draft

Blog: https://www.keycloak.org/2023/11/keycloak-2300-released

■ Conformance Test

Keycloak 23 passed the conformance tests for FAPI 2.0 specifications above.

Results: https://github.com/keycloak/kc-sig-fapi?tab=readme-ov-file#passed-conformance-tests-per-keycloak-version

This working item was completed for a moment.

The item would be re-opened when the FINAL version of these FAPI 2.0 specifications are released.

Ongoing working items of security features

Passkeys (Multi-Device FIDO Credentials)

- Status: In progress

Keycloak 23 start supporting passkeys as a preview feature.

- Discussion

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

- Implementation

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

2 of 4 issues were resolved

Issue - Conditional UI : https://github.com/keycloak/keycloak/issues/24264

Ongoing PR : https://github.com/keycloak/keycloak/issues/23659

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/
- passkeys.io : https://www.passkeys.io/

OAuth 2.1

■ Status : In progress

Epic issue: https://github.com/keycloak/keycloak/issues/25141

1 of 4 issues is resolved. Others are in progress.

- Client policies: executor for validate and match a redirect URI `Draft PR sent`
- Supporting OAuth 2.1 for confidential clients `Draft PR sent`
- Client policies : executor for enforcing DPoP `Completed`
- Supporting OAuth 2.1 for public clients `Draft PR sent`

■ Discussion

https://github.com/keycloak/keycloak/discussions/24043

Lightweight Token

■ Status: Completed partially
3 of 4 follow-up issues are in progress.
Epic Issue: https://github.com/keycloak/keycloak/issues/21186
Ongoing PR: https://github.com/keycloak/keycloak/issues/23724 `PR sent`
■ 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

Edwards-curve Digital Signature Algorithm (EdDSA)

- ■ Status: In progress
  Working for resolving review comments.
- ■ 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
    Issue: https://github.com/keycloak/keycloak/issues/15714
    PR: https://github.com/keycloak/keycloak/pull/17215 **PR sent**

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

PROPOSED DRAFT

Emerging working items of security features

OpenID Connect for Verifiable Credentials (OID4VCs)

■ Immediate goal

Keycloak can work as an issuer of VCs.

■ 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

https://github.com/wistefan/keycloak/tree/add-vci

■ Working repository

https://github.com/wistefan/keycloak

OpenID Connect for Verifiable Credentials (OID4VCs)

■Breakout sessions

2nd : 27 Nov (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/2nd)

3rd : 13 Dec (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/3rd)

4th : 20 Dec (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/3rd)

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?

Community Event

Keycloak DevDay 2024 Germany

Site: https://keycloak-day.dev/

Announcement: https://www.keycloak.org/2023/12/keycloak-dev-day-24

22 Feb 2024, Frankfut, Germany

Keyconf 24

How about holding a community meeting Keyconf 24 in 2024?

Date and Time: 1 day the same as Keyconf 23?

Venue: ?

Sponsor: ?

Program: ?

Ex. event: Keyconf 23

Date and Time: 10 AM - 4 PM, June 16, 2023

Venue: Level39, 1 Canada Square, Canary Wharf, London, UK

Web page: https://www.eventbrite.co.uk/e/keyconf-23-tickets-621079815447

      (tickets sold out)

Program:

- Recently added features in Keycloak in past years that make Keycloak a strong performer in the IAM market - Marek Posolda / Red Hat
- OpenID FAPI work in the last 12 months - Vinod Anandan / Citibank
- Keycloak in Open Banking or consent-driven open data ecosystem - Kannan Rasappan / Banfico & Francis Pouatcha / Adorsys
- OpenID FAPI presentation (any demo or theme) - Takashi Norimatsu / Hitachi
- Roadmap on possible ideas for the future work of Keycloak - Marek Posolda / Red Hat
- Workshops on potential uses cases

Ex. event: Keyconf 19

Keyconf 19

Host: UK Research and Innovation, Science and Technology Facilities Council, Hartree Centre

Date: 12 and 13 Jun 2019 (2 days)

Venue: STFC Hartree Centre, Sci-Tech Daresbury, Warrington, United Kingdom

Web site: https://www.hartree.stfc.ac.uk/Pages/KeyConf.aspx (dead link)

Participants: about 20 people (including Stian, Marek and me)

Registration Fee: nothing

Program: 12 talks and 4 unconferences

PROPOSED DRAFT

END