OAuth SIG Community 8th Meeting

(53rd from ex-FAPI-SIG)

@Web Conference

7 February 2024

PROPOSED DRAFT

Table of Contents

KubeCon + CloudNativeCon Europe 2024

Completed working items of security features

1. Lightweight Token
2. EdDSA

Ongoing working items of security features

1. OAuth 2.1
2. OID4VCs
3. Token Exchange
4. OAuth 2.0 Grant Type SPI
5. Passkeys
6. OIDC4IDA

Community Event

Keyconf 24

KubeCon + CloudNativeCon Europe 2024

KubeCon + CloudNativeCon Europe 2024

- Web Site: https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/
- Program: https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/program/schedule/
- Date: 19 - 22 March 2024
- Venue: Paris Expo Porte de Versailles, Paris, France
- Keycloak related sessions:
  - *Maintainer track: The Leading Edge of AuthN and AuthZ by Keycloak*
    Takashi Norimatsu, Hitachi, Ltd. & Thomas Darimont, Codecentric AG
  - *Session: OAuth2 Token Exchange for Microservice API Security*
    Ahmet Soormally & Letz Yaara, Tyk
  - *Session: The Hard Life of Securing a Particle Accelerator*
    Antonio Nappi & Sebastian Lopienski, CERN

Completed working items of security features

Lightweight Token

Completed

- Status: Completed
  3 mandated issues have been resolved.
- Epic Issue
  - https://github.com/keycloak/keycloak/issues/21186
- Discussion
  - https://github.com/keycloak/keycloak/discussions/9713

Edwards-curve Digital Signature Algorithm (EdDSA) Completed

- Status: Completed
- 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

Ongoing working items of security features

OAuth 2.1 In Progress

- 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 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

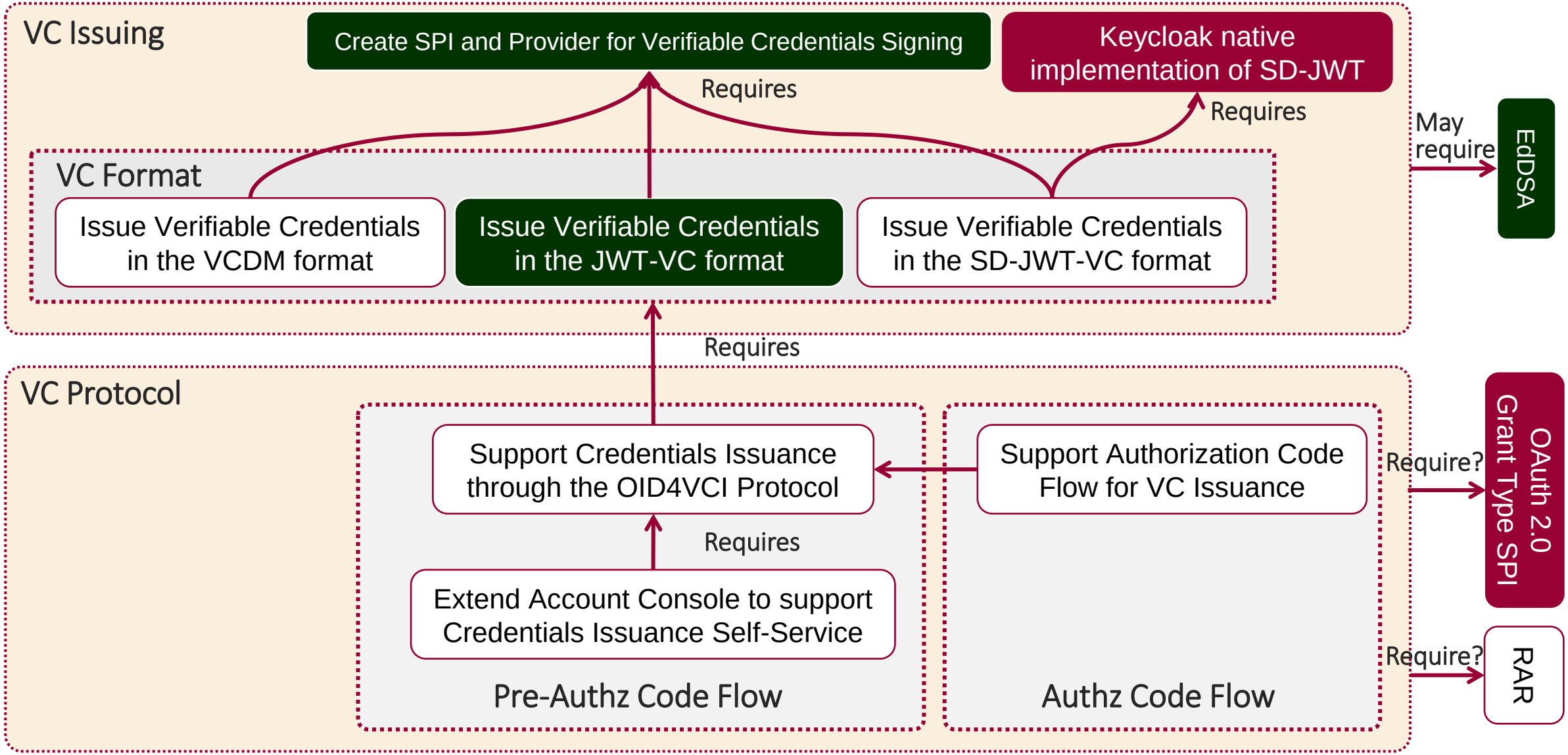
OpenID Connect for Verifiable Credentials (OID4VCs)

In Progress

- Immediate goal: Keycloak can work as an issuer of VCs.
- Status: 2 out of all 8 issues is resolved.

  Holding its breakout sessions weekly.
- 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
- Epic issue : Support OpenID for Verifiable Credentials(OID4VC)
  - https://github.com/keycloak/keycloak/issues/25936
- Prototype implementation (by FIWARE)
  - https://github.com/wistefan/keycloak/tree/add-vci
  - https://github.com/wistefan/keycloak/tree/remove-libs

OpenID Connect for Verifiable Credentials (OID4VCs)



PROPOSED DRAFT

PR merged | PR sent | Not yet started

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/4th)
  - 5th : 17 Jan (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/5th)
  - 6th : 24 Jan (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/6th)
  - 7th : 31 Jan (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/7th)
- Follow-up
  - RFC 9396 OAuth 2.0 Rich Authorization Requests (RAR)

Recall: Rich Authorization Request (RAR)

- Status : stopped?
- Discussion
  - https://github.com/keycloak/keycloak/discussions/8532
- Design
  - https://github.com/keycloak/keycloak-community/pull/325
- Epic Issue
  - https://github.com/keycloak/keycloak/issues/9225

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)
- Breakout sessions: 17 Jan
  - The current Keycloak does not fully comply with its RFC.
  - One option is to newly implement Token Exchange feature as a SPI provider to fully comply with the RFC.
- Resources:
  - Specification: RFC 8693 OAuth 2.0 Token Exchange
    - https://datatracker.ietf.org/doc/html/rfc8693
  - Keycloak's implementation
    - https://www.keycloak.org/docs/latest/securing_apps/index.html#_token-exchange

OAuth 2.0 Grant Type SPI In Progress

- Status: In progress
- Discussion
  - https://github.com/keycloak/keycloak/discussions/26249
- Issue
  - https://github.com/keycloak/keycloak/issues/26250
- Implementation
  - https://github.com/keycloak/keycloak/pull/26251

OAuth 2.0 Grant Type SPI

Token Endpoint.java

```
switch (action) {
        case AUTHORIZATION_CODE:
           return codeToToken();
        case REFRESH_TOKEN:
           return refreshTokenGrant();
        case PASSWORD:
           return resourceOwnerPasswordCredentialsGrant();
        case CLIENT_CREDENTIALS:
           return clientCredentialsGrant();
        case TOKEN_EXCHANGE:
           return tokenExchange();
        case PERMISSION:
           return permissionGrant();
        case OAUTH2_DEVICE_CODE:
           return oauth2DeviceCodeToToken();
        case CIBA:
           return cibaGrant();
      }
```

Switch-case → Provider

- Authorization Code Grant Type Provider
- Token Refresh Grant Type Provider
- Resource Owner Password Credentials Grant Type Provider
- Client Credentials Grant Type Provider
- Token Exchange Grant Type Provider
- Permission Grant Type Provider
- Device Grant Type Provider
- CIBA Grant Type Provider

PROPOSED DRAFT

Passkeys (Multi-Device FIDO Credentials)

Nothing Progress

- 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

  2 of 4 issues were resolved
- Implementation

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

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

Passkeys (Multi-Device FIDO Credentials)

Nothing Progress

- 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/

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

Community Event

Keyconf 24

- Objective: How about holding a community meeting Keyconf 24 in 2024?
- Date and Time: 1 day the same as Keyconf 23?
- Venue: Frankfurt/Germany?, Cardiff/Wales?　(Tokyo/Japan is difficult…)
- Sponsor: ?
- Program: ?
- Cost: ? 6,000 - 10,000 EUR?

Keyconf 24 as co-hosted event

- Proposal: How about holding a community meeting Keyconf 24 as the following co-hosted event?
- Event: Open Source Summit Europe
  - https://events.linuxfoundation.org/open-source-summit-europe/
- Date and Venue: 16-18 September 2024, Vienna, Austria
- Co-hosted Event Proposals due for OSS EU 2024 : Monday, April 8
- Requirement: a minimum of three potential sponsors
  - https://events.linuxfoundation.org/wp-content/uploads/2024/01/sponsor-oss-eu24_011224a.pdf
  - https://docs.google.com/presentation/d/1S3tjdLdF-BxfbZnPck3W099dqMyyhWlCmv1vAQ-E2Go/edit#slide=id.g1e60a6b4a21_0_16

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

END