@Web Conference

6 March 2024

OAuth SIG Community 9th Meeting

(54th from ex-FAPI-SIG)

PROPOSED DRAFT

Table of Contents

KubeCon + CloudNativeCon Europe 2024

Completed working items of security features

1. OAuth 2.1
2. OAuth 2.0 Grant Type SPI

Ongoing working items of security features

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

Community Event

Keyconf 24

OSS Summit Europe 2040

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

OAuth 2.1

Completed

- Status : Completed

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 #25637 Completed
- Supporting OAuth 2.1 for confidential clients #25314 Completed
- Client policies : executor for enforcing DPoP #25315 Completed
- Supporting OAuth 2.1 for public clients #25316 Completed

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

OAuth 2.0 Grant Type SPI

Completed

- Status: Completed
- Discussion
  - https://github.com/keycloak/keycloak/discussions/26249
- Issue
  - https://github.com/keycloak/keycloak/issues/26250
- PR
  - https://github.com/keycloak/keycloak/pull/26251

OAuth 2.0 Grant Type SPI

Token Endpoint.java

Switch-case ➡ Provider

```
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();
    }
```

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

Ongoing working items of security features

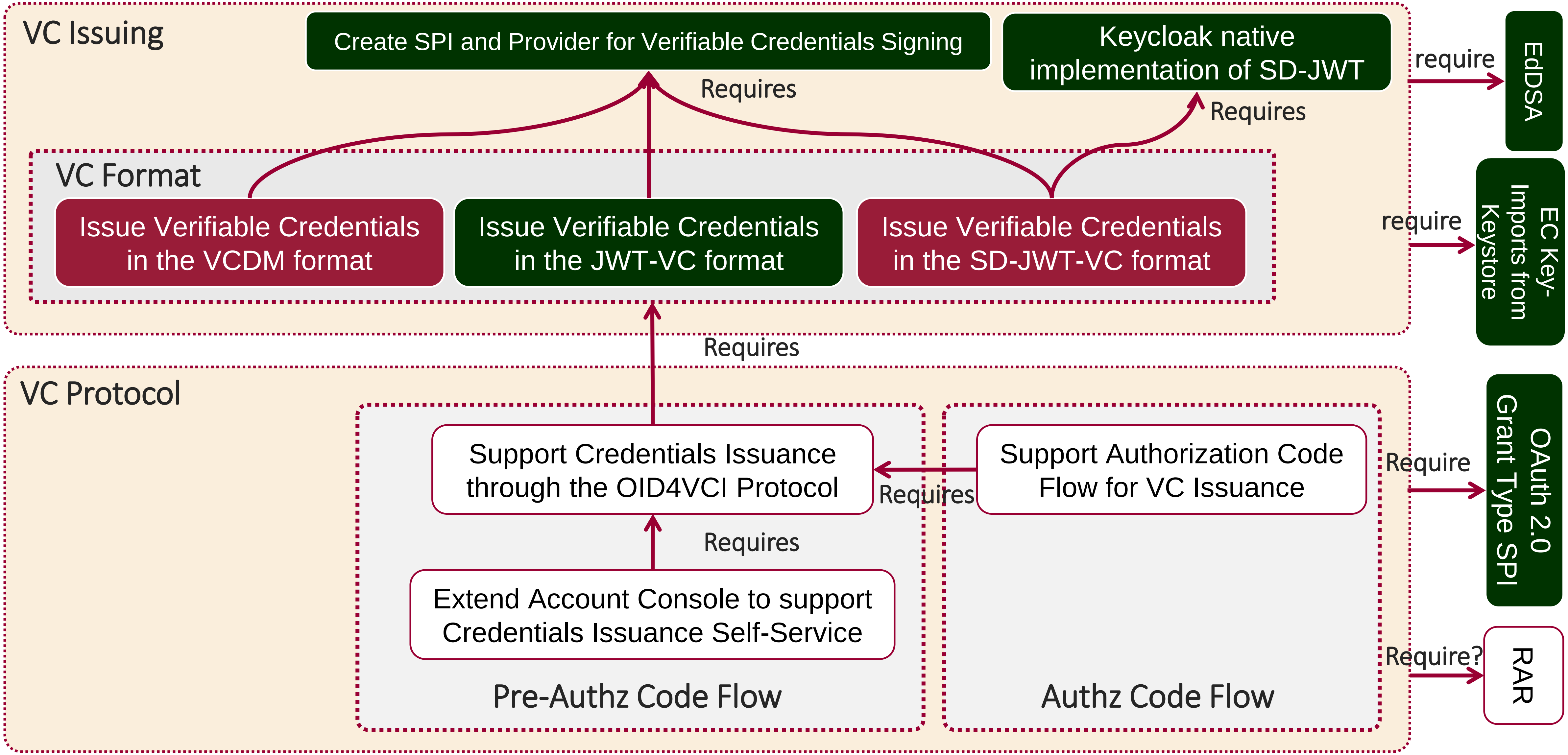
OpenID Connect for Verifiable Credentials (OID4VCs)

In Progress

- ■ Immediate goal: Keycloak can work as an issuer of VCs.
- ■ Status: 4 out of all 9 issues were 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)


VC Issuing
Create SPI and Provider for Verifiable Credentials Signing
Keycloak native implementation of SD-JWT
Requires
Requires
require
EdDSA
VC Format
Issue Verifiable Credentials in the VCDM format
Issue Verifiable Credentials in the JWT-VC format
Issue Verifiable Credentials in the SD-JWT-VC format
require
EC Key-Imports from Keystore
Requires
VC Protocol
Support Credentials Issuance through the OID4VCI Protocol
Requires
Support Authorization Code Flow for VC Issuance
Require
OAuth 2.0 Grant Type SPI
Requires
Extend Account Console to support Credentials Issuance Self-Service
Pre-Authz Code Flow
Authz Code Flow
Require?
RAR

PROPOSED DRAFT

🟩 PR merged

🟥 PR sent

□ Not yet started

OpenID Connect for Verifiable Credentials (OID4VCs)

■Breakout sessions

8th : 14 Feb (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/8th)

9th : 21 Feb (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/9th)

10th : 28 Feb (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/9th)

■Follow-up

- RFC 9396 OAuth 2.0 Rich Authorization Requests (RAR)
- [Internet Draft] OAuth 2.0 Attestation-Based Client Authentication

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

Passkeys (Multi-Device FIDO Credentials)

In 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
  - Refactoring JavaScript code of WebAuthn's authenticators to follow the current Keycloak's JavaScript coding convention

    In Progress

    https://github.com/keycloak/keycloak/pull/27239
  - Passkeys: Supporting WebAuthn Conditional UI

    In Progress

    https://github.com/keycloak/keycloak/pull/24305

PROPOSED DRAFT

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/

Improvements

- Rename Resident key to Discoverable Credential — Completed
  https://github.com/keycloak/keycloak/pull/27104
- Add New User Registration Option on WebAuthn Authentication UI — Completed
  https://github.com/keycloak/keycloak/pull/27106
- Add EdDSA/Ed25519 to WebAuthn Signature algorithms — Completed
  https://github.com/keycloak/keycloak/pull/27108
- Replace Security Key with Passkey in WebAuthn UIs and their documents — Completed
  https://github.com/keycloak/keycloak/pull/27151

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

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, Berlin, or other major city / Germany?
- Sponsor: ?
- Program: ?
- Cost: ? 6,000 - 10,000 EUR? (We already had some sponsors)

Keyconf 24

How about holding the conference just before or after the other major conference the same as Keyconf 23?

■Proposal

[1] Tech Show Frankfurt

https://www.techshowfrankfurt.de/

May Wed 22 - Thr 23, 2024, Frankfurt, Germany

Candidate date: Tur 21

[2] Open Source Summit Europe 2024

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

Sep Mon 16 - Wed 18, 2024, Vienna, Austria

Candidate date: Fri 20

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

OSS Summit Europe 2024

- Web Site: https://events.linuxfoundation.org/open-source-summit-europe/
- Date: 16 - 18 September 2024
- Venue: TBD, Vienna, Austria
- CFP Closes: Tuesday, April 30, 12:00 AM PDT (UTC-7) / 09:00 CEST (UTC+2)

END