OAuth SIG Community 11ˢᵗ Meeting

(56ᵗʰ from ex-FAPI-SIG)

@Web Conference

2 May 2024

Table of Contents

Ongoing working items of security features

  1. OID4VCI

  2. Passkeys

  3. DPoP

  4. Token Exchange

  5. OIDC4IDA

Proposal

  Keycloak as Cloud Wallet

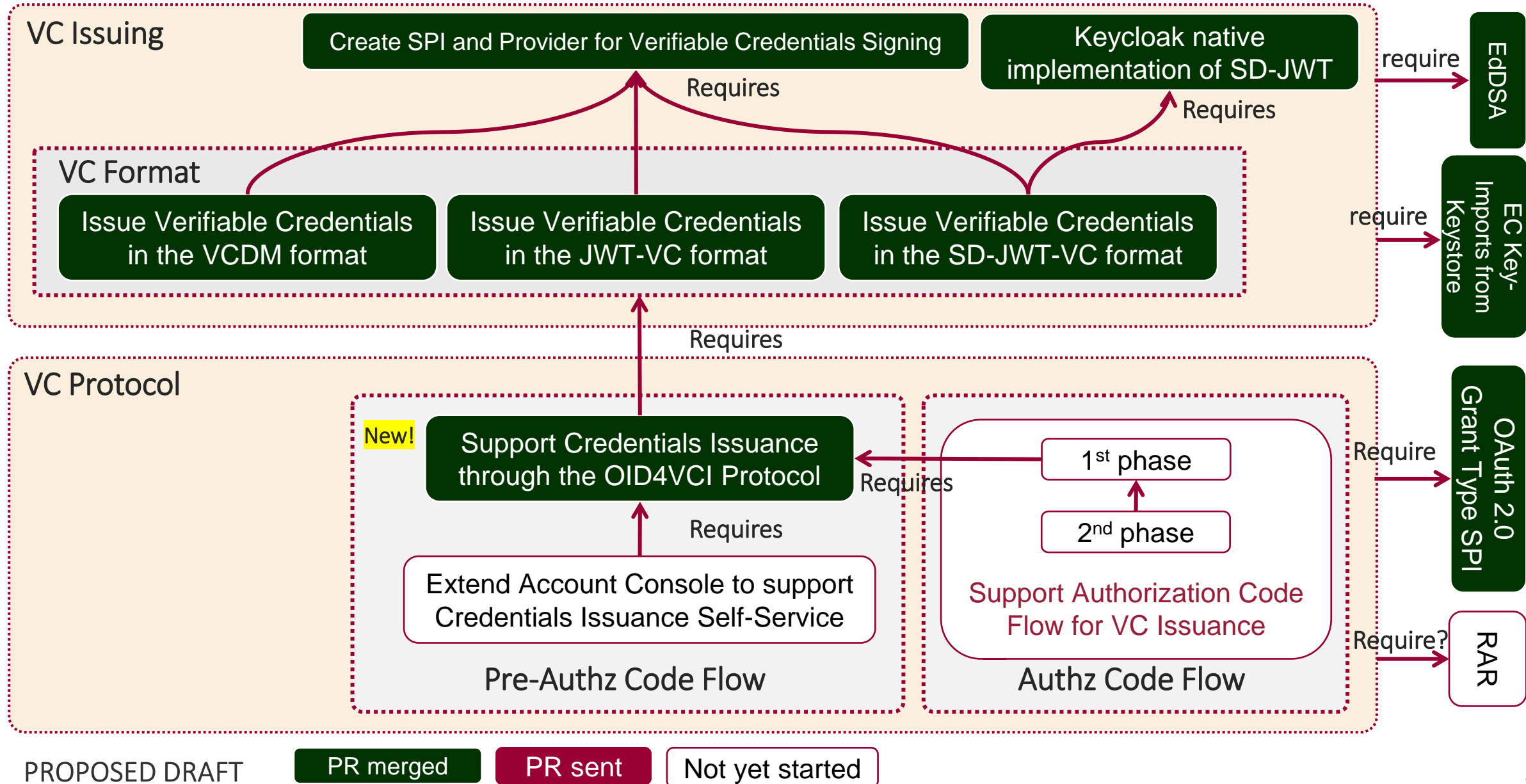Community Event

  Keyconf 24

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: 7 out of all 9 issues were resolved. 1 PR was newly merged.

    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

OpenID Connect for Verifiable Credentials (OID4VCs)

VC Issuing

Create SPI and Provider for Verifiable Credentials Signing

Keycloak native implementation of SD-JWT → require → EdDSA

Requires ↑ ↑ *Requires*

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

Requires

New! Support Credentials Issuance through the OID4VCI Protocol ← *Requires* — 1st phase ← 2nd phase

Support Authorization Code Flow for VC Issuance

Requires ↑

Extend Account Console to support Credentials Issuance Self-Service

Pre-Authz Code Flow

Authz Code Flow

Require → OAuth 2.0 Grant Type SPI

Require? → RAR

OpenID Connect for Verifiable Credentials (OID4VCs)

■Breakout sessions

14th : 10 April (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/14th)

15th : 17 April (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/15th)

16th : 24 April (https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/16th)

■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: 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

2 of 6 issues were resolved, 1 PR was submitted and its review seems to be completed **Updated!**

■ Implementation

- Passkeys: Supporting WebAuthn Conditional UI
  https://github.com/keycloak/keycloak/pull/24305

In Progress

A lot of people were requested to support passkeys officially in several conferences.
(e.g., KubeCon EU 2024, OSW 2024, etc...)

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/

OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)

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

Token Exchange

- 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!
- 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

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
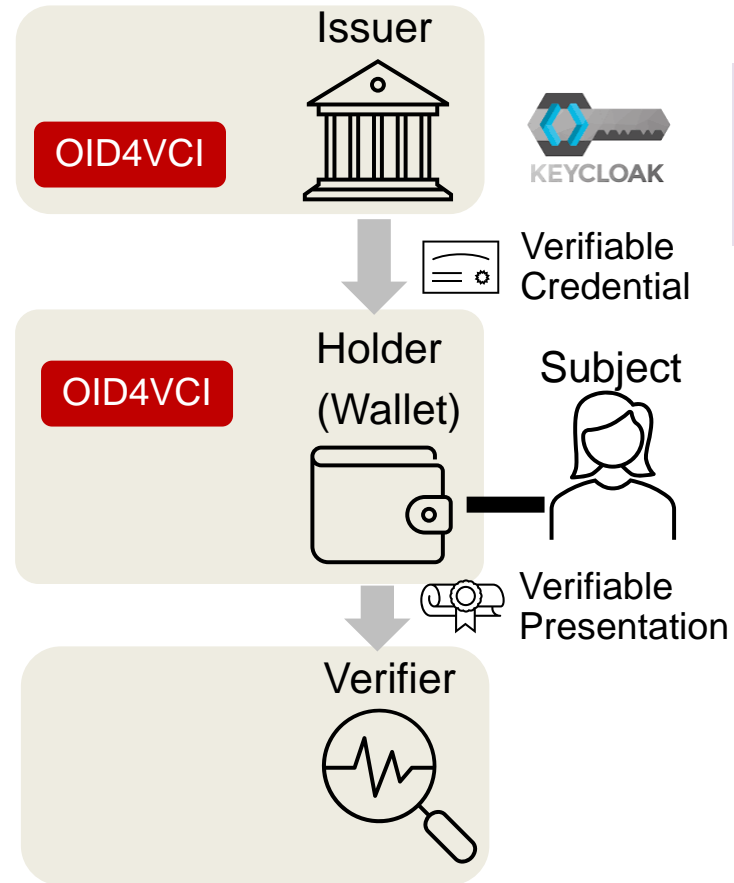 - Support for OIDC extensions: OIDC4IDA
    https://github.com/keycloak/keycloak/discussions/21270
- ■ Implementation
  - implement oidc4ida **Draft PR sent**
    Draft PR: https://github.com/keycloak/keycloak/pull/21309

PROPOSED DRAFT

Proposal

Keycloak as Cloud Wallet

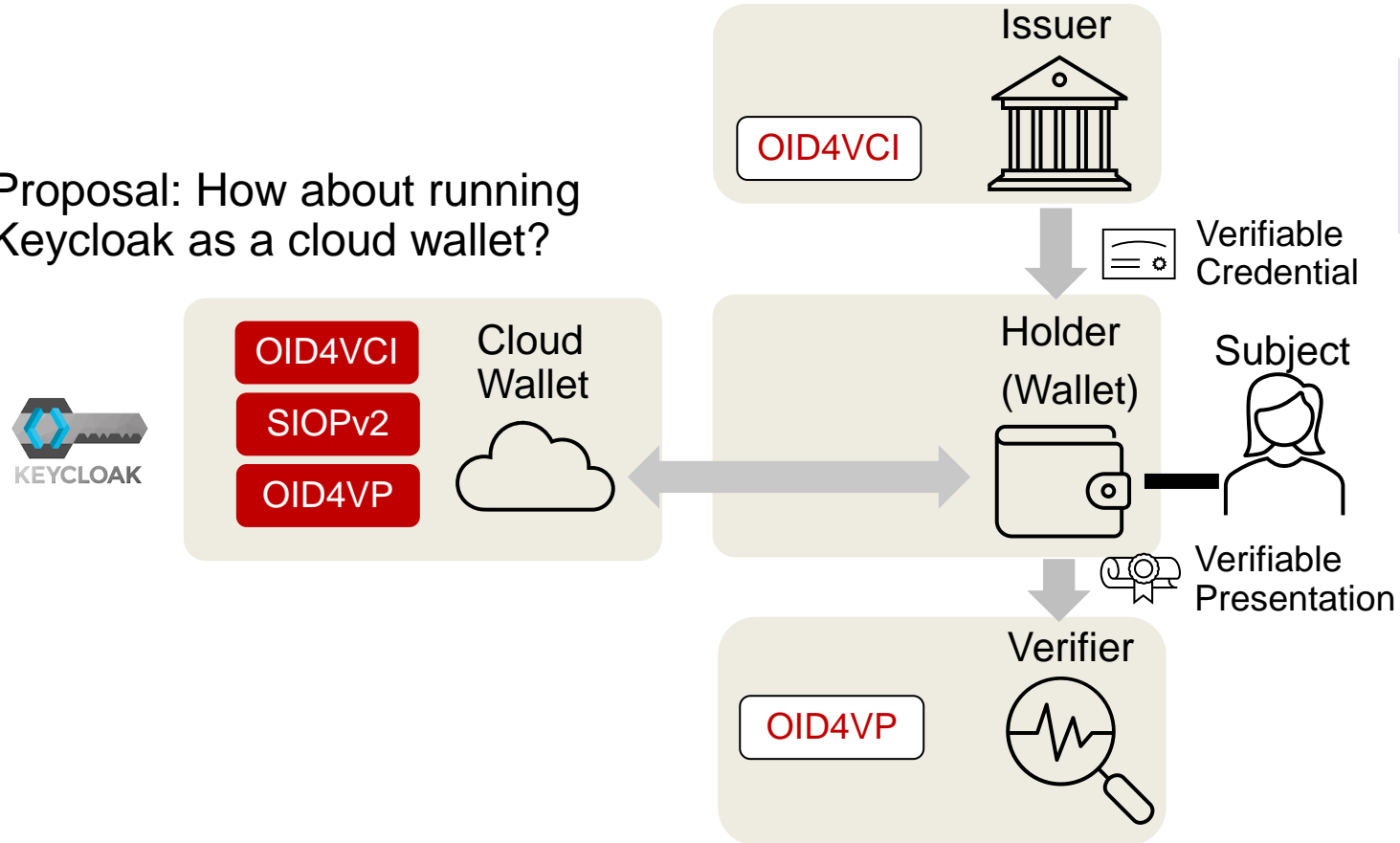Keycloak's community is working on supporting OID4CI.

OpenID for Verifiable Credential Issuance (OID4VCI):= Defining an API that is used to issue Verifiable Credentials.

Keycloak as Cloud Wallet

Proposal: How about running Keycloak as a cloud wallet?

Issuer

OID4VCI

Verifiable Credential

Cloud Wallet

OID4VCI
SIOPv2
OID4VP

KEYCLOAK

Holder (Wallet)

Subject

Verifiable Presentation

Verifier

OID4VP

OpenID for Verifiable Credential Issuance (OID4VCI):= Defining an API that is used to issue Verifiable Credentials.

Self-Issued OpenID Provider v2 (SIOPv2) := An OpenID Provider controlled by the End-User.

OpenID for Verifiable Presentations (OID4VP) := Defining a mechanism on top of OAuth 2.0 that enables presentation of Verifiable Credentials as Verifiable Presentations.

Community Event

Keyconf 24

- Date and Time: 10 AM to 4 PM, September 19th Thursday

- Venue: ARCOTEL Kaiserwasser, Vienna/Austria 🇦🇹

- Sponsor: Adorsys, Banfico, Hitachi (also welcome other sponsors)

- Program: TBD (how to gather proposals of a talk, who select them, etc…)

- Budget: TBD, but about 6,000 - 10,000 EUR in total

FYI: co-located event

Open Source Summit Europe 2024

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

- Date: September 16th Monday - 18th Wednesday

- Venue: Austria Center Vienna, Vienna/Austria 🇦🇹

END