OAuth SIG OID4VC Breakout 17th Session

@Web Conference
08th May 2024

Table of Contents

PROPOSED DRAFT

- Immediate Goal: Keycloak can work as an issuer of VCs

- Status: 8 out of 11 issues were resolved.

- 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
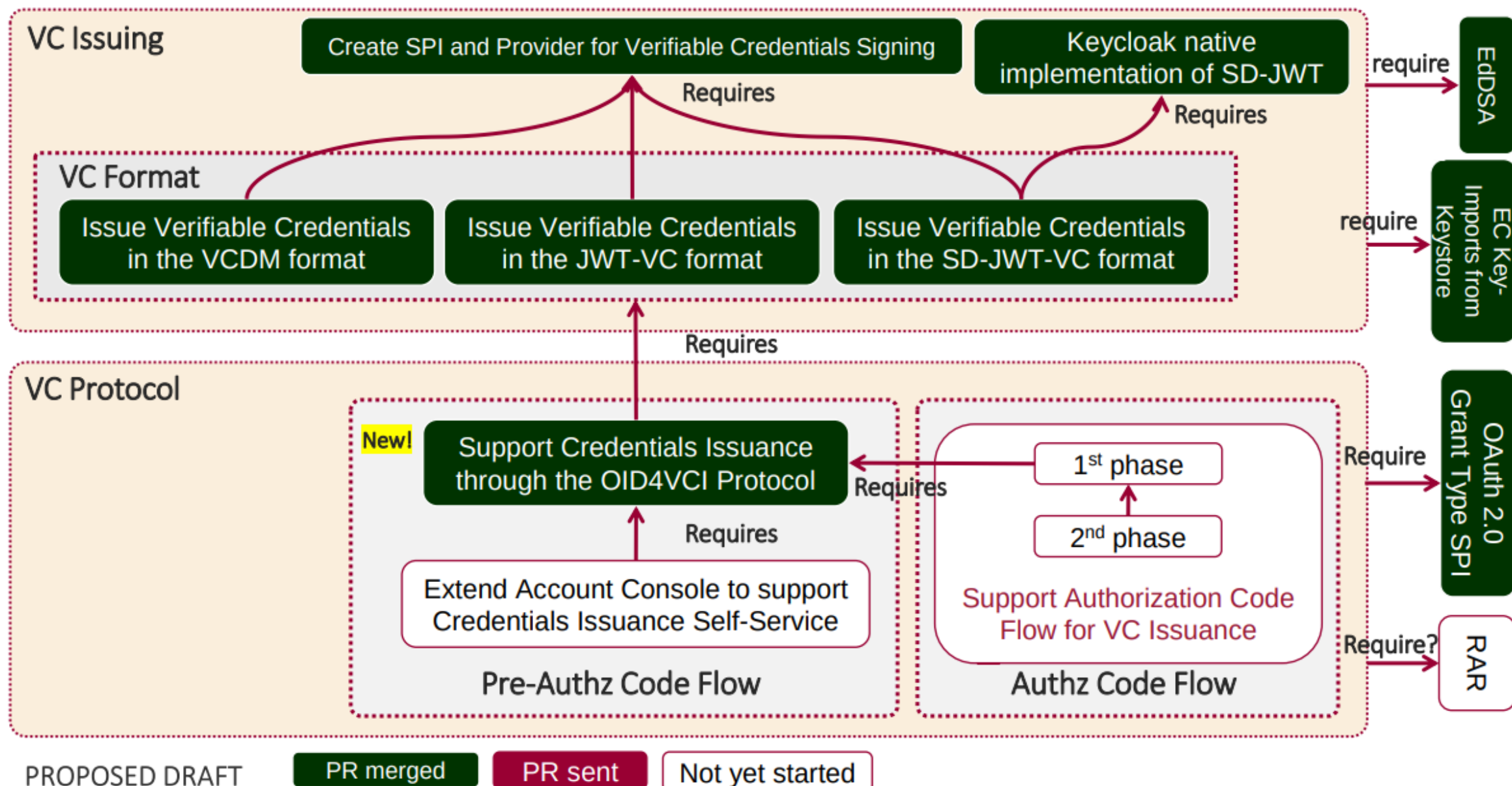
- **Main Issue**

https://github.com/keycloak/keycloak/issues/25936

- ⊘ **Create SPI and Provider for Verifiable Credentials Signing** #25937
- ⊘ **Support Credentials Issuance through the OID4VCI Protocol** #25940
- ⊘ **Issue Verifiable Credentials in the JWT-VC format** #25941
- ⊘ **Issue Verifiable Credentials in the SD-JWT-VC format** #25942
- ⊘ **Issue Verifiable Credentials in the VCDM format** #25943
- ⊘ **Keycloak native implementation of SD-JWT** #25638
- ⊘ **Support EC Key-Imports for the JavaKeystoreKeyProvider** #26936
- ⊘ **Grant urn:ietf:params:oauth:grant-type:pre-authorized_code enabled even if oid4vc_vci feature is disabled** #28968
- ⊙ **Extend Account Console to support Credentials Issuance Self-Service** #25945
- ⊙ **Support Authorization Code Flow for VC Issuance** #26328
- ⊙ **JWSBuilder when used directly with AsymmetricSignatureSignerContext produces non compliant ECDSA signed JWT** #29309

- **Merged Pull Request: #26238**
- **Active Issues: #25945, #26328**
- **New Issue: #29309**

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

New!

Support Credentials Issuance through the OID4VCI Protocol

Requires

1st phase

2nd phase

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 |

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
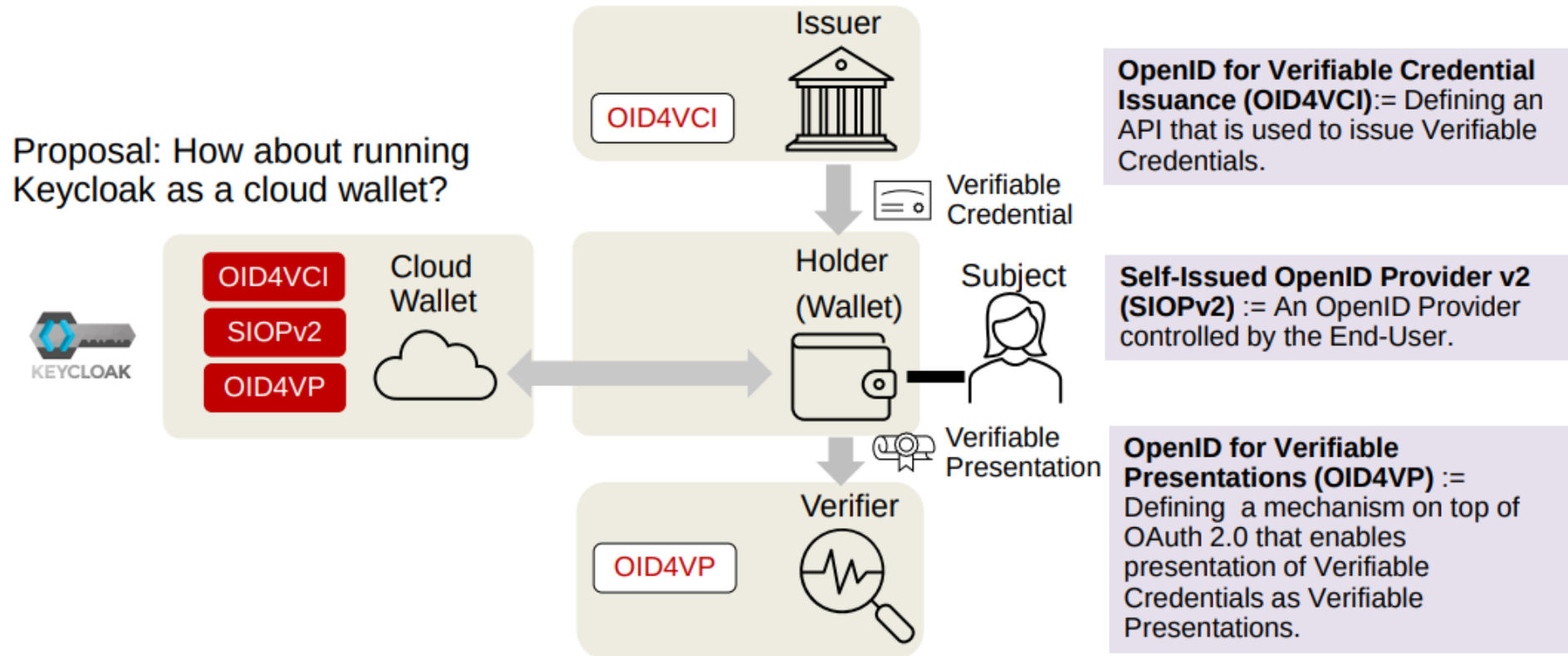 - https://github.com/keycloak/keycloak/issues/9225

Proposal: Keycloak as Cloud Wallet

Keycloak's community is working on supporting OID4VCI.
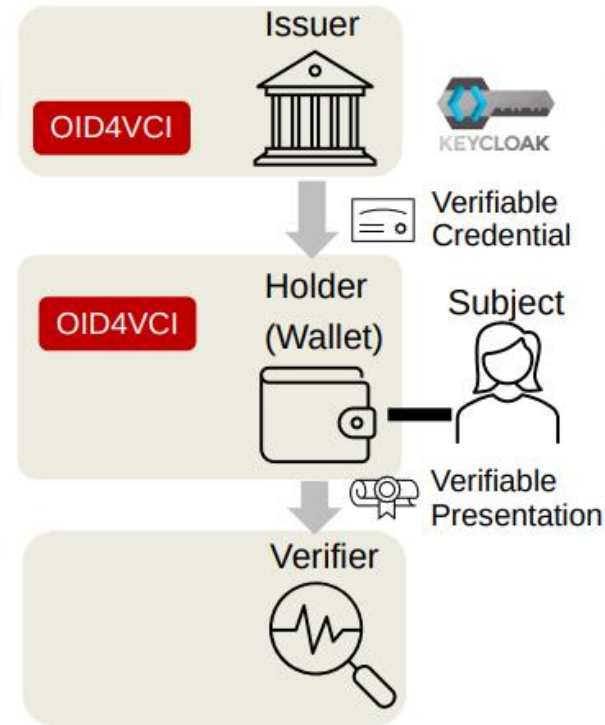
OpenID for Verifiable Credential Issuance (OID4VCI):= Defining an API that is used to issue Verifiable Credentials.

Proposal: Keycloak as Cloud Wallet

Proposal: How about running Keycloak as a cloud wallet?

KEYCLOAK

Cloud Wallet — OID4VCI, SIOPv2, OID4VP

Issuer — OID4VCI

Verifiable Credential

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.

Open Floor