

@Web Conference
5 June 2024

OAuth SIG Community 12th Meeting (57th from ex-FAPI-SIG)

Table of Contents

Ongoing working items of security features

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

Community Event

Keyconf 24

Ongoing working items of security features

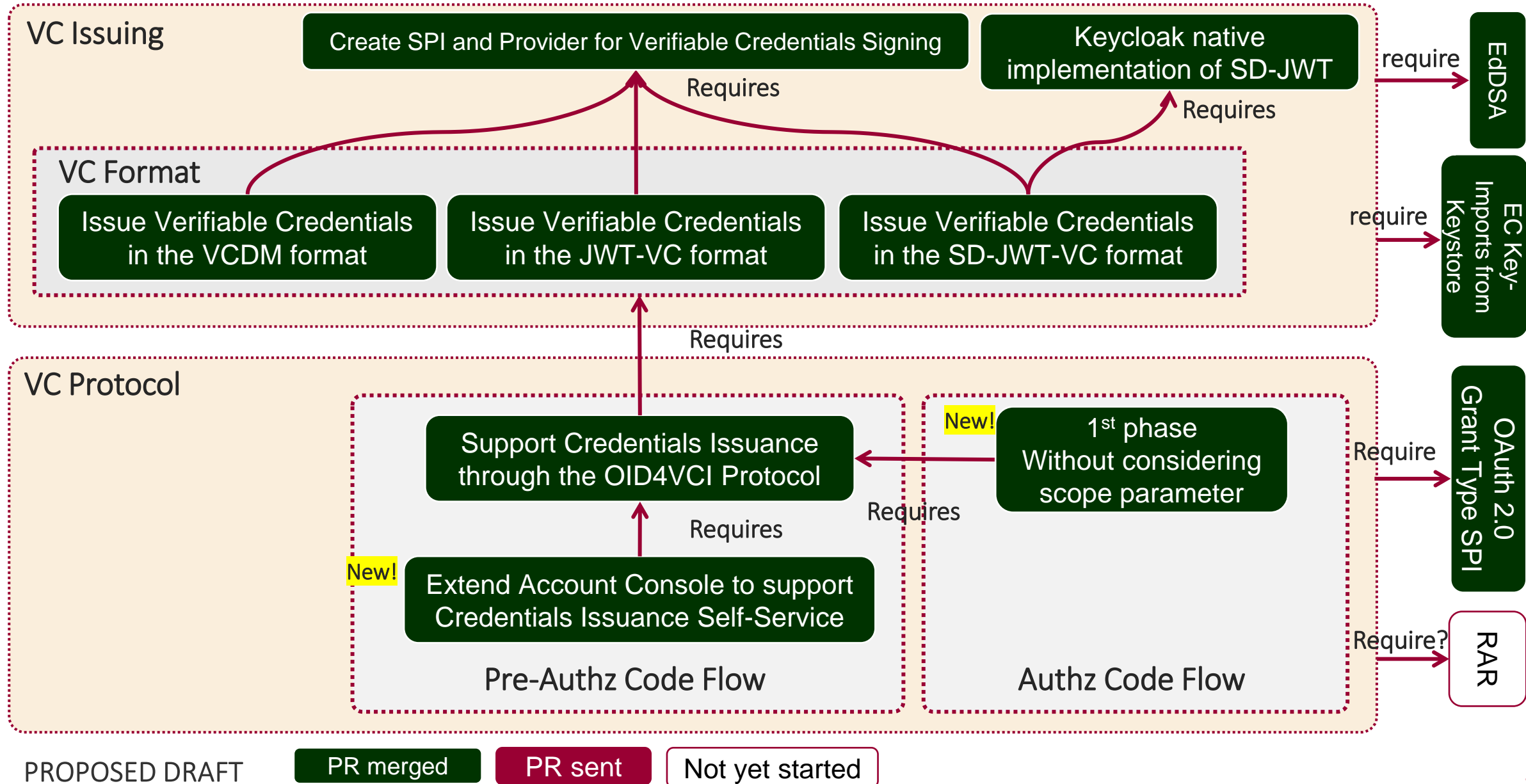
OpenID Connect for Verifiable Credentials (OID4VCs)

Completed

- Immediate goal: Keycloak can work as an issuer of VCs.
- Epic issue : Support OpenID for Verifiable Credentials(OID4VC)
 - <https://github.com/keycloak/keycloak/issues/25936>
- Status: 17 out of all 17 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>
- Breakout sessions
 - 17th : 8 May (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/17th>)
 - 18th : 15 May (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/18th>)
 - 19th : 22 May (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/19th>)
 - 20th : 29 May (<https://github.com/keycloak/kc-sig-fapi/tree/main/OAuth-SIG/Breakouts/OID4VCs/20th>)

PROPOSED DRAFT

OpenID Connect for Verifiable Credentials (OID4VCs)



OpenID Connect for Verifiable Credentials (OID4VCs)

■ Follow-up: toward preview feature

- VC issuance in Authz code flow with considering scope parameter

Issue: <https://github.com/keycloak/keycloak/issues/29725>

In Progress

- VC issuance with considering authorization_details parameter

- RFC 9396 OAuth 2.0 Rich Authorization Requests (RAR)

- OAuth 2.0 Attestation-Based Client Authentication

- [Internet Draft] OAuth 2.0 Attestation-Based Client Authentication

- Additional Parameters : Authorization Endpoint

- issuer_state

- Additional Parameters : Token Endpoint

- c_nonce / c_nonce_expires_in

and some bug fixes...

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>

6 of 11 issues were resolved, 1 PR was merged. **Updated!**

■ Implementation

- Passkeys: Supporting WebAuthn Conditional UI

Merged

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

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)

Nothing
Progress

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

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) **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

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

- Date and Time: 10 AM to 4 PM, September 19th Thursday
- Venue: ARCOTEL Kaiserwasser, Vienna/Austria 
- Web-site (registration) : <https://www.eventbrite.de/e/keyconf24-tickets-887467387847>
- Program Proposal
 - 9:00-10:00 Registration and Welcome Coffee
 - 10:00-10:30 Keynote speeches and sessions :
Keynote speeches (from sponsors) 7 min x 4 (Red Hat, Adorsys, Banfico, Hitachi)
 - 10:30-12:00 Sessions : 30 min x 3
 - 12:00-13:00 Lunch Break
 - 13:00-14:30 Sessions (or unconferences) : 30 min x 3
 - 14:30-15:00 Coffee Break
 - 15:00-16:00 Sessions (or unconferences) : 30 min x 2

Keyconf 24

■ Call for Sessions (CfS)

Form:

<https://forms.office.com/e/pgBuPzbgqP>

CfS Contents:

Full Name, Email Address, Company, Speaker Job Title, Session Title, Session Overview/Description, Consent to the processing of your personal data in accordance with the GDPR

Schedule:

CfS Closes: 31 July

CfS Notifications: 19 August



END