

@Web Conference  
5 Oct 2022

# FAPI-SIG Community 39<sup>th</sup> Meeting

# Table of Contents

Supporting security profiles

- PR for UK OpenBanking
- PR for Open Banking Brazil FAPI 1.0 Implementer's Draft 3 (ID3)
- PR for DPoP
- PR for extending Client Policies for Solid-OIDC

Proposal : Extend FAPI-SIG's scope and rename FAPI-SIG

# Supporting Security Profiles

# PR for UK OpenBanking




Intent support before issuing tokens (UK OpenBanking)

Issue: <https://github.com/keycloak/keycloak/issues/12883>

PR: <https://github.com/keycloak/keycloak/pull/13068>

**-> The PR has been merged.**

It was confirmed that keycloak incorporating PR can pass conformance tests of UK OpenBanking (all 2 conformance profiles).

#	 Security Profile Specification	 Conformance Profile of Certified OpenID Provider	 Conformance Test Plan	Test Status	Base Version
1	UK Open Banking	UK-OB Adv. OP w/ MTLS	FAPI1-Advanced-Final	Passed	18.0.0
2	UK Open Banking	UK-OB Adv. OP w/ Private Key	FAPI1-Advanced-Final	Passed	18.0.0

# PR for Open Banking Brazil FAPI 1.0 Implementer's Draft 3 (ID3)

Pluggable Features of Token Manager

Issue: <https://github.com/keycloak/keycloak/issues/12065>

PR: <https://github.com/keycloak/keycloak/pull/12551>

ID2: When token refresh, an authorization server may return a refreshed refresh token.

ID3: When token refresh, an authorization server does not return a refresh token.

-> Keycloak does not pass the test checking this point.

It was confirmed that keycloak incorporating PR can pass conformance tests of Open Banking Brazil FAPI 1.0 ID3.

# PR for DPoP (Demonstration of Proof of Possession)

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

Issue: <https://issues.redhat.com/browse/KEYCLOAK-15169>

PR: <https://github.com/keycloak/keycloak/pull/8895>

PR is still Draft status.

Its specification is still Internet Draft.

<https://datatracker.ietf.org/doc/html/draft-ietf-oauth-dpop-11>

# PR for extending Client Policies for W3C Solid-OIDC

Pre-authorization hook for client policies

Issue: <https://github.com/keycloak/keycloak/issues/9017>

PR: <https://github.com/keycloak/keycloak/pull/9018>

Motivation: supporting W3C Solid-OIDC

<https://solid.github.io/solid-oidc/>

“The Solid OpenID Connect (Solid-OIDC) specification defines how resource servers verify the identity of relying parties and end users based on the authentication performed by an OpenID provider. Solid-OIDC builds on top of OpenID Connect 1.0 for use within the Solid ecosystem.”

# Proposal : Extend FAPI-SIG's scope and rename FAPI-SIG



# Proposal : Extend FAPI-SIG's scope

## [OAuth]

OAuth 2.1 (Internet Draft), OAuth 2.0 for Native Apps (RFC 8252)

OAuth 2.0 for Browser-Based Apps (Internet Draft)

## [OIDC]

eKYC & Identity Assurance (<https://openid.net/wg/ekyc-ida/>)

OpenID Connect for Identity Assurance 1.0

## [Others]

Preparation for existing algorithms being compromised

Edwards-Curve Digital Signature Algorithm (EdDSA) (RFC 8032)

Ed25519 : 128-bit security level Curve25519

Ed448 : 224-bit security level Curve448

# Proposal : Rename FAPI-SIG

Candidates:

Security SIG

IAM Security SIG

API Security SIG

Secure Digital Identity SIG

etc...

END