

@Web Conference
7 Sep 2022

FAPI-SIG Community 38th 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

Proposal : Extend FAPI-SIG's scope

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>

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>

Proposal : Extend FAPI-SIG's scope

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

END