OAuth SIG Community 2nd Meeting (47th from ex-FAPI-SIG)

@Web Conference

2 August 2023

PROPOSED DRAFT

Table of Contents

Ongoing working items of security features

- FAPI 2.0 Security Profile / FAPI 2.0 Message Signing
- DPoP
- EdDSA
- Reference Token
- Lightweight Token
- OIDC4IDA

PROPOSED DRAFT

Ongoing working items of security features

OIDF Certificate Program for FAPI 2.0

Site URL : https://openid.net/certification/

□FAPI2 Providers & Profiles

- FAPI 2.0 Security Profile Second Implementer’s Draft & Message Signing First Implementer’s Draft: 5 conformance profiles

  - FAPI2SP MTLS + MTLS
  - FAPI2SP private key + MTLS
  - FAPI2SP OpenID Connect
  - FAPI2MS JAR
  - FAPI2MS JARM

■ Specification

- FAPI 2.0 Security Profile: Implementer's Draft
  https://openid.net/specs/fapi-2_0-security-profile.html
- FAPI 2.0 Message Signing: Draft
  https://openid.bitbucket.io/fapi/fapi-2_0-message-signing.html

PROPOSED DRAFT

FAPI 2.0 Security Profile / FAPI 2.0 Message Signing

- Epic: FAPI 2.0 support

  https://github.com/keycloak/keycloak/issues/20708

  3 issues were newly resolved:

- FAPI 2.0 security profile - supporting RFC 9207 OAuth 2.0 Authorization Server Issuer Identification

  PR Merged

  https://github.com/keycloak/keycloak/issues/20584

- FAPI 2.0 security profile - not allow an authorization request whose parameters were not included in PAR request

  PR Merged

  https://github.com/keycloak/keycloak/issues/20623

- FAPI 2.0 security profile - not allow an authorization request whose parameters were not included in Request Object pushed to PAR request

  PR Merged

  https://github.com/keycloak/keycloak/issues/20710

FAPI 2.0 Security Profile / FAPI 2.0 Message Signing

- Epic: FAPI 2.0 support

  https://github.com/keycloak/keycloak/issues/20708

  2 issues remaining to complete the epic:

- FAPI 2.0 security profile - make client policy conditions called by PRE_AUTHORIZATION_REQUEST

  PR sent

  https://github.com/keycloak/keycloak/issues/22043

- Add FAPI 2.0 security profile as default profile of client policies

  PR sent

  https://github.com/keycloak/keycloak/issues/21181

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

- Epic: DPoP support
  https://github.com/keycloak/keycloak/issues/21916
  3 issues were newly resolved:
  - DPoP support
    https://github.com/keycloak/keycloak/issues/21916
    PR Merged
  - DPoP: OIDC client registration support
    https://github.com/keycloak/keycloak/issues/21918
    PR Merged
  - Adjustements to the behaviour of dpop_bound_access_tokens switch
    https://github.com/keycloak/keycloak/issues/21920
    PR Merged

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

- Epic: DPoP support

  https://github.com/keycloak/keycloak/issues/21916

  3 issues remaining to complete the epic:

  - DPoP documentation

    https://github.com/keycloak/keycloak/issues/21917

    PR sent

  - Using DPoP token type in the access-token and as token_type in introspection endpoint

    https://github.com/keycloak/keycloak/issues/21919

    In discussion

  - Fully decouple DPoP from TokenEndpoint and TokenManager if possible

    https://github.com/keycloak/keycloak/issues/21921

    In discussion

PROPOSED DRAFT

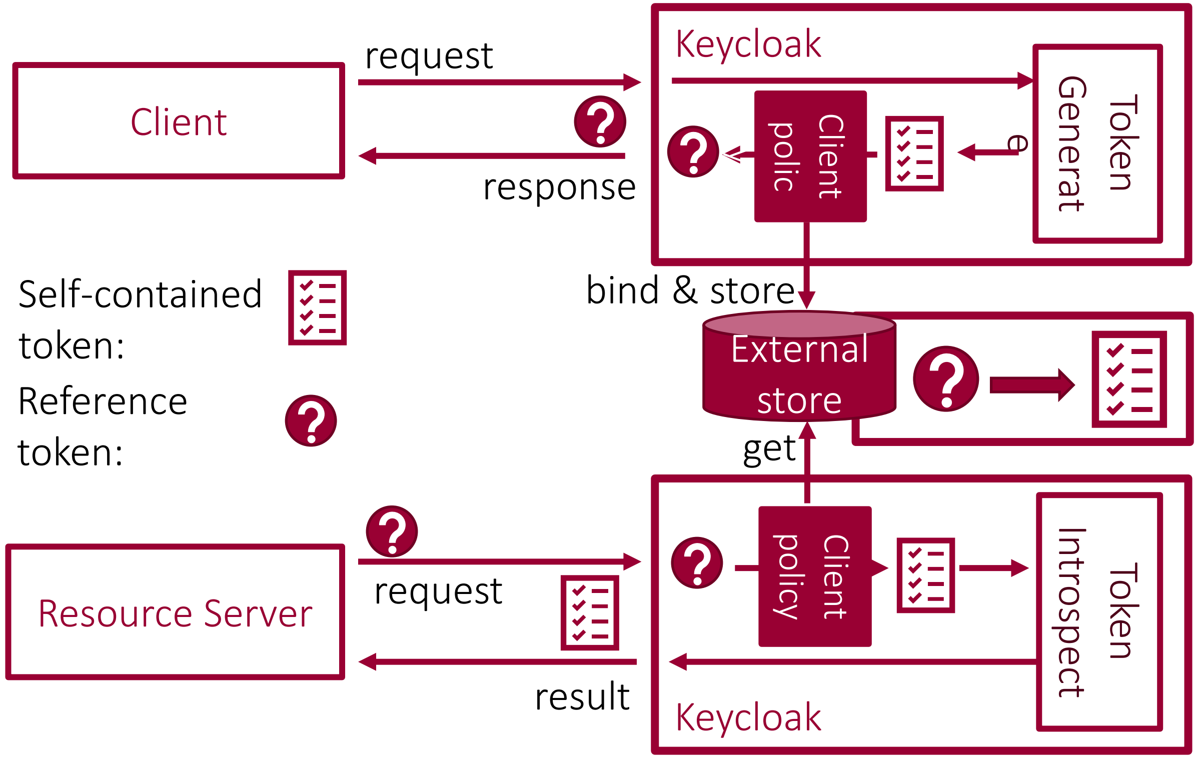
Edwards-curve Digital Signature Algorithm (EdDSA)

- Supporting EdDSA: PR sent
  https://github.com/keycloak/keycloak/issues/15714

Reference Token

- Discussion
  - Supporting reference access/refresh tokens: https://github.com/keycloak/keycloak/discussions/19649
- Implementation
  - Supporting reference access/refresh tokens: PR closed https://github.com/keycloak/keycloak/pull/19824

Out-of-Box is preferred to an external store that a user needs to prepare by themselves.



Lightweight Token

- Discussion
  - Lightweight access tokens: https://github.com/keycloak/keycloak/discussions/9713
- Implementation
  - Enhancing Light Weight Token: Draft PR sent https://github.com/keycloak/keycloak/pull/22148

OpenID Connect for Identity Assurance 1.0 (OIDC4IDA)

■ 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
  https://github.com/keycloak/keycloak/pull/21309

END