Overview of the FAPI Profiles

Dave Tonge
FAPI WG Co-Chair
CTO Moneyhub

20 April 2021

FAPI 1?
FAPI 2?
FAPI 1.0 Part 2???

What are all these profiles
(and why naming things is hard)

Final Specifications

Financial-grade API 1.0 – Part 1: Baseline Security Profile

Financial-grade API 1.0 – Part 2: Advanced Security Profile

Why?

- Based on OAuth 2.0 and OpenID Connect suite of standards, but with less optionality and the requirement to use modern security best practices.
- Clear point-by-point specifications that implementers can use as a “check list”
- Exhaustive conformance tests to allow implementers to ensure their software is secure and interoperable

Implementers Drafts

Financial-grade API: Client Initiated Backchannel Authentication Profile

Why? To enable “decoupled” authorization flows.

Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

Why? To enable signed responses from the AuthZ endpoint without requiring OpenID Connect.

Working Group Last Call

Financial-grade API 2.0: Baseline Security Profile

Financial-grade API 2.0: Attacker Model

Why?

FAPI 2.0 has a broader scope than FAPI 1.0. It aims for complete interoperability at the interface between client and authorization server as well as interoperable security mechanisms at the interface between client and resource server. It also has a more clearly defined attacker model to aid formal analysis.

Working Group Drafts

Financial-grade API 2.0: Advanced Security Profile

Grant Management for OAuth 2.0

Simple HTTP Message Integrity Protocol

Why?

Preventing the wheel from being re-invented by jurisdictions implementing FAPI.

Relevant IETF Drafts

- RFC8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
- OAuth JAR - JWT Secured Authorization Request (JAR)
- OAuth PAR - Pushed Authorization Requests
- OAuth RAR - Rich Authorization Requests
- OAuth DPoP - Demonstrating Proof-of-Possession at the Application Layer
- OAuth 2.0 Authorization Server Issuer Identifier in Authorization Response

Thank you

Please join the WG:

https://openid.net/wg/fapi/

Dave Tonge
FAPI WG Co-Chair
CTO Moneyhub