OpenID Foundation Workshop for SAMA

FAPI RP Conformance Testing & Certification

February 27, 2023
Workshop Agenda

- OpenID Foundation Overview
- Brief Introduction to FAPI
  - KSA FAPI Profile
- OIDF Certification Program Overview
- Conformance Testing Demonstration
- Q&A Session
OpenID Foundation Overview
OpenID Foundation Overview

Non-profit, international standardization organization founded in 2007
- An expert and unbiased resource providing strategic guidance on the digital identity landscape and how public and private entities can build sustainable digital identity solutions to benefit users and all ecosystem participants.

Focused on the development of open internet identity and security standards to ensure robust global deployments while enabling interoperability
- Committed to serving all digital users with secure and privacy preserving digital identity protocols

All OpenID standards are developed within Foundation working groups
- Global community of experts that develop and validate standards through an open, consensus-based processes
- OIDF standards are actively maintained, and evolve as needed to support existing and new use cases

OpenID Certification Program ensures compliant, secure and interoperable deployments
- Self-certification to reduce cost and complexity
- All certifications are public and low cost to facilitate transparency & ecosystem adoption
- Sometimes mandated to support government policy & regulation
Non-Profit & Government Members
Current Working Groups

- 10 Foundation working groups (WGs) focused on developing OpenID standards as defined in their charters.
- WGs meet mostly online to share information and develop specification documentation using issue tracking systems, git repositories and mailing lists.
- Global community of experts that develop and validate proven standards through open, consensus-based processes.
Brief Introduction to FAPI
FAPI: Financial General-Purpose High-security API protection protocol based on OAuth 2.0 family of specifications. Now just called FAPI.
FAPI WG Founded in June 2016

- Originally was targeting the financial use-cases.
  - There were only 3 people in the room then ...

- Lots of request to generalise it so that it can be used in other industrial verticals such as healthcare and transportation

- It is for everybody that needs to secure

- Now just called FAPI as there are many non-financial use-cases adopting FAPI that require a high security protocol
One of the Most Successful OpenID Protocols after Connect

Projected FAPI Adoption

- FDX Recommending FAPI
- Live, CMA9+ are going through the Certification
  - Live July 2021
- Adopted FAPI 1.0 ID2 with GOST Cryptographic algorithm
- Banking association guideline recommends FAPI
  - Launched on July 2020

OpenID®
OIDF Certification Program Overview
OpenID Certification Program Overview

- A light-weight, low-cost, self-certification program to serve members, drive adoption and promote high-quality implementations
  - Identity Providers launched in early 2015
  - Relying Parties launched in late 2016
  - Financial-grade profiles launched in 2019
- Each certification makes it easier for those that follow and helps make subsequent deployments more trustworthy, interoperable and secure
- All certified implementations are openly listed at [https://openid.net/developers/certified/](https://openid.net/developers/certified/)

OIDF certification is a success with 2191 certifications of 629 deployments to date!
# FAPI Certifications

[Permalink](https://openid.net/certification/#FAPI_OPs)

## Certified Financial-grade API (FAPI) OpenID Providers

Financial-grade API (FAPI) 1.0 Final

These deployments have achieved certification for the Financial-grade API (FAPI) 1.0 Final profile, as published March 2021:

There are separate profiles depending on whether MTLS or private_key_jwt client authentication is used, and certifiers can run OpenBanking, Australian Consumer Data Rights or Brazil OpenBanking specific versions of the tests to show their compliance/support for the extra security requirements of those ecosystems. Please see the certification instructions for further details.

### FAPI 1 Advanced Final (Generic)

<table>
<thead>
<tr>
<th>Organization</th>
<th>Implementation</th>
<th>FAPI Adv. OP w/ MTLS</th>
<th>FAPI Adv. OP w/ MTLS, PAR</th>
<th>FAPI Adv. OP w/ Private Key</th>
<th>FAPI Adv. OP w/ Private Key, PAR</th>
<th>FAPI Adv. OP w/ MTLS, JARM</th>
<th>FAPI Adv. OP w/ Private Key, JARM</th>
<th>FAPI Adv. OP w/ MTLS, PAR, w/ Private Key, JARM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloudentity</td>
<td>Cloudentity</td>
<td>16-Aug-2021 [view]</td>
<td>16-Aug-2021 [view]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FinansysTech</td>
<td>FinansysTech Auth Server 1.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[OpenID Certified](https://openid.net/certified)
Why Use the OIDF’s Certification Program?

- OIDF tests are developed with close support of relevant working group
  - Tests are updated based on requests from working group

- Testers get direct support from the OIDF certification team
  - Domain experts familiar with all the specs
  - Team have access to OIDF/OAuth2 spec authors when necessary

- Internationally recognized, award winning

- Tests are maintained and updated by OIDF when:
  - new versions of underlying specs published
  - new potential security vulnerabilities are found
  - new interoperability problems are found
  - testers find failures difficult to interpret

- Issues found by testers are raised back to the relevant OIDF working groups
  - Specs can be improved / clarified / disambiguated as necessary
Ecosystem Wide Benefits

- For “Open” initiatives to succeed, they must:
  - Interoperate
  - Be scalable
  - Be secure

- Must test both sides of the connection
  - The ‘sharing’ party (the bank / authorization server)
  - The ‘receiving’ party (the fintech / OAuth2 client)

- Ecosystems can only scale if they are interoperable
  - An ecosystem with 40 full participants will have 1,560 distinct connections
  - Vital that conformance happens before go live
  - Retrofitting interoperability and security is time consuming and disruptive

- OIDF can engage at the ecosystem / regulatory level
Certification Program Resources

Conformance Suite source code etc publicly available on gitlab:
https://gitlab.com/openid/conformance-suite

Instructions for testing/certifying:
https://openid.net/certification/instructions/

Notes notes about the KSA/SAMA tests:
OP testing: https://openid.net/certification/fapi_op_testing/#ksa
RP testing: https://openid.net/certification/fapi_rp_testing/#ksa

Production deployment:
https://www.certification.openid.net/
(Login with any google/gitlab/openid account)

Contact the OIDF certification team if you require help: certification@oidf.org
KSA FAPI Profile Overview

- Aligns the generic FAPI tests to the KSA specific specification:
  - Pushed authentication requests (PAR) are mandatory
  - JWT Secured Authorization Response Mode (JARM is not used)
  - Client credentials grant is used to obtain an access token
    - scope=accounts
  - account-access-consents is used to create a ConsentId prior to test running
    - Only one permission is requested: ReadAccountsBasic
  - ConsentId is passed in request object to PAR endpoint in a parameterized scope
  - accounts endpoint is expected to be used for resource endpoint tests
FAPI Certification: SAMA Status

- KSA FAPI Profile OP certifications opened, Wednesday, February 8, 2023.

- KSA FAPI Profile RP certifications are open as of today, Tuesday, February 28, 2023
FAPI Certification: Pre-testing steps

- Two registered OAuth2 clients are required

- Tester needs to be able to create & register client credentials
  - Or be provided with them in the correct format

- Recommended that tester has existing domain knowledge
  - TLS certificates, JWKS manipulation, OAuth2, FAPI
  - For first run, a developer or highly-technical tester is desirable
1. Configure your systems to support FAPI correctly
2. Create a sandbox system identical to your production system
3. Create OAuth clients in your sandbox are per certification instructions
4. Create test configurations in conformance suite for FAPI tests
5. Run FAPI tests
6. Check test results all pass (or only have ‘warnings’)
7. Check any screenshots (tests marked ‘REVIEW’) match description in test
8. If your server supports both private_key_jwt and MTLS client authentication, you must run the tests for both
9. Pay certification fee
10. Complete PDF attestation document for FAPI
11. Prepare submission & submit certification as per instructions
Conformance Testing Demonstration

Visit: OpenID.net