OpenID Foundation
May 2020 Workshop
Certification Update

Who Am I?

- Joseph Heenan, CTO at fintechlabs.io
- OpenID Certification Team lead developer
- Software engineer & architect with over 25 years' experience
- Active contributor to the OpenID Connect FAPI/CIBA/FAPI-CIBA specifications
- 20+ years of mobile app experience
- Assisted many of the largest UK banks with achieving compliance to the OpenID specification

https://www.linkedin.com/in/josephheenan/

OIDF FAPI Certification Program

- FAPI-RW ID2 OP testing launched April 2019
- FAPI-RW ID2 RP testing launched in June 2019
- FAPI-CIBA ID1 OP testing launched September 2019
- All tests (optionally) support OpenBanking UK intent lodging
- Visit https://openid.net/certification/instructions/ for details

FAPI-RW Certification: Core goals

- Interoperability
- Security
- Correct deployment of certified software

However:

- FAPI tests do not test all of OpenID Connect Core or OAuth
  - ‘Pretty good’ coverage of relevant parts though
  - Vendors should run OpenID Connect Core tests as well

FAPI-RW Certification: Reasons to test

- Reduced support costs
  - If your implementation is interoperable it will “just work” for third parties
- Evidence of compliance to show government regulators
- Evidence of compliance may reduce insurance costs, chances of security breach, etc.
- It will be embarrassing if other people test your server & you fail
  - Anyone can test a server

FAPI-RW Certification: app2app

- App2app testing has been fully supported since April 2019
- Tests need to be repeated for each OS (i.e. Android & iOS)
- Tend to show new problems due to issues in the mobile app code
- FAPI App2app certifications free until end of June 2020
- See my upcoming Identiverse presentation for more about app2app
- https://openid.net/2019/10/21/guest-blog-implementing-app-to-app-authorisation-in-oauth2-openid-connect/

OIDF FAPI Conformance Suite

- New suite written in Java
- Originally developed for UK OpenBanking by my team at fintechlabs.io
  - Based on initial prototype done by Justin Fletcher/Tristan Lewis for ONC
- Donated by UK OpenBanking Implementation Entity to OpenID Foundation
  - OB UK send participants to OIDF for FAPI certification

Major differences vs current python certification suite

- Mutual TLS client authentication
- Signed request objects
- Certificate Bound access tokens
- Browser automation
- API & “native” docker
- Simplified UI
- All configuration editable
- Automated public regression test
- Automated regression testing of all source code changes
  - Tests against Authlete & node oidc-provider
- Predictable fixed redirect URIs
- Two registered clients are required (to verify certificate binding etc)
- Easily extensible to support further profiles
- A “test” can make multiple checks
- Test results private by default

OpenID Connect Certification in Java

- Launching in pilot mode today
  - OP 3rd party login/logout tests coming soon
- Already tested against a number of OPs / RPs
  - New bugs in OPs were found…
- Additional checks compared to python
  - Tests refresh tokens, if supported
  - Form post testing is more comprehensive
  - ‘sub’ consistency checked more consistently
- Please test; any feedback would be greatly appreciated
- Email certification@oidf.org for help
- Python tests to be retired later in 2020

OpenID

Logged in as joseph.john.heenan@gmail.com

Tokens | Logout

Test Plan OpenID Connect Core: Basic Certification Profile Authorization server test

Server metadata location discovery

Client Registration Type dynamic_client

Configure Test

Please see OpenID Foundation Certification Instructions.

Form | JSON

Test Information

alias

description

publish: No

Server

discoveryUrl

login_hint

Client

client_name

Second client

client_name

Create Test Plan

Future Roadmap

- JARM testing for FAPI-RW recently added
  - Not yet part of certification programme
- PAR (Pushed Authentication Request)
  - Additional option in FAPI-RW tests
  - Tests available soon
  - PAR specification is still new, certification program won't launch until spec is stable
- To be confirmed
  - FAPI 2
  - CIBA
  - eKYC

Wrap up

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

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

- Contact me if you'd like some help:
  - joseph.heenan@oidf.org or certification@oidf.org
  - https://twitter.com/josephheenan
  - https://www.linkedin.com/in/josephheenan