OpenID Foundation
FAPI Certification Program
April 2020 Workshop

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
  - All OB UK spec versions supported
    - ensure you have version number in API URLs as per OB spec
- Visit https://openid.net/certification/instructions/ for details

FAPI-RW Certification: Core goals

- Interoperability
- Security
- Correct deployment of certified software

However:

- Does 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 will be free until end of June 2020

FAPI-RW Certification: Tips

- Pick an authorization server vendor that is FAPI certified
  - Doesn't guarantee your deployment will pass, but it really helps
- Run certification early and before production deployment
  - It is very rare to pass first time
  - Conformance testing can be part of your Continuous Integration
- Design for interoperability
- Follow the instructions
  - https://openid.net/certification/fapi_op_testing/
  - Keys need to be in the right format, some example of conversions are here:
  - https://josephheenan.blogspot.com/2018/01/obtaining-keys-to-on-boardregister-tpp.html

Demos

- Walkthrough of FAPI-RW OB testing
- Demo of app2app testing
- Demo of RP testing

Future roadmap

- OpenID Connect Core tests
  - Being ported from python hardness into same framework as FAPI
  - Improved UX & coverage compared to the python tests
  - Launching Summer 2020
- 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
- FAPI 2.0
  - TBC

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.html
  (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