OpenID Foundation
July 2020 FDX Workshop
Certification Program

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/

OpenID Certification Program Overview

- A light-weight, low-cost, 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 freely available at https://openid.net/developers/certified/
- OIDF certification pricing has been widely accepted to date

Program Stats

485 certifications of 162 implementations

Total OP Certifications	372	Total RP Certifications	73
Total OP Implementations	109	Total RP Implementations	28
Total FAPI Certifications	30	Total FAPI-CIBA Certifications	8
Total FAPI Implementations	22	Total FAPI-CIBA Implementations	2
Total FAPI RP Certifications	2		
Total FAPI Implementations	1		

(As of July 2020)

OIDF FAPI Certification Program

- FAPI-RW ID1 OP testing (OBUK specific) started December 2017
- 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
- Optionally supports:
  - OpenBanking UK intent lodging
  - Australian Consumer Data Rights
  - App2app authentication/authorization
- 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

Demo

- Live demo of the conformance suite

Why use the OIDF's conformance 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

Security checks - keys

12:34:03 **FAILURE** `EnsureServerJwksDoesNotContainPrivateOrSymmetricKeys`

2 More

Jwks contains private and/or symmetric keys

private_keys


```
[
  {
    "p": "uKADG9h1fv0aWcdBArKbIuMwlsWta_3vWMGymWaA0McIFrmoYi0_MNQAqos3hKE
u1TltpzBWXBooDJz2oqptD464SGonWDK3oDawcSyH1TOmTgePlffVfn7u8",
    "kty": "RSA",
    "q": "uFhhMgTXP9u_Upv6i1C7T-YHk_jJ2e3PO9RxF74gfkPoP35N6KORVELZgaAC0q3
xr6TikTYyRL_B3PYH4KWxiW9uErV3yNGDFGxpOmhxNR6zTPxGec1gUk2mU",
    "d": "FSd7Am9oKHWMabvsV0r_aAXHORr22AQwJgfROgAbAiTYC8bJSDXK1CjzHzzQB5-
U5hsLtDNtvEpZy_LFnPEsxnOqLE8BLWFQcaFUczA8AKPIS5NHz_rywXixwa5y1KeIWXr_dyMG
eiNtP6_mABXTWFagvgVwwSMT8Ufd-Evw8PKb46yROcIub-1F9h0Ainqqaq7FovHIQDa5MuKWB
    "e": "AQAB",
    "use": "sig",
    "kid": "sig-2020-07-21T11:27:04Z",
    "qi": "jkzvNCY02KW9Bky833DCNJApkXjc4PHd5J98bAqZzLP3o3smbLWqvdvl92acP0
a-PxSuRkt6MUFitlCpgeN1n69L6326kkMfM_aTO0rhMM0gZembd4rJKgI6k",
    "dp": "lvJMWGHbfp3VA34DSv9YE2gIe9zW8ypEnB6RtRW3T_rKRDo6zzoLJhLPEKCOHa
zwQ2iWnFDK6rZ_9AAJLemFDWk0hhA0Zsngk97i10T_MXLvD3DjFkvwg2GoU",
    "alg": "PS256",
    "dq": "Dm99TPlsEagXl1R3jilIQb11onS8-b_RlpHQOVe-G6UdrrspRqpoWvzRI4FwNy
EwSdzTkSN5VEDf4XmyrDjNakG7kON8-dDOPu8uXlCHbO12hPTMYAVhIZDLE",
    "n": "hPK_VckSwJtFaGRPbBlNjTyRsnpaN9m1CCZHVfSJI3IPh8creglOHVsC2jFG6Lg
VzesHvTRi-dDRgtAFGWc_U_go2W_7MqH4zkHw_RIliGP814hIWmi-zrEH5-5Yrvo8H_f8Ohx2
rWF89BknLeeDIPDaaXHzZY0khaP7ccO3W7EzkUud9y64TEMxGY_AeMDCbDr-maycRHy54AgZk
  }
]
```


symmetric_keys


```
[]
```

Further Security checks – request object

- 'exp' already expired
- Incorrect 'aud'
- Correctly signed, but with non-permitted alg
- Correctly ignoring items outside the signed message
- With a syntactically valid, but incorrect, signature
- Valid signature but from a different client
- Valid signature but using 'alg: none'
- With nonce only outside request object
- With non-registered redirect uri

Security checks – token endpoint

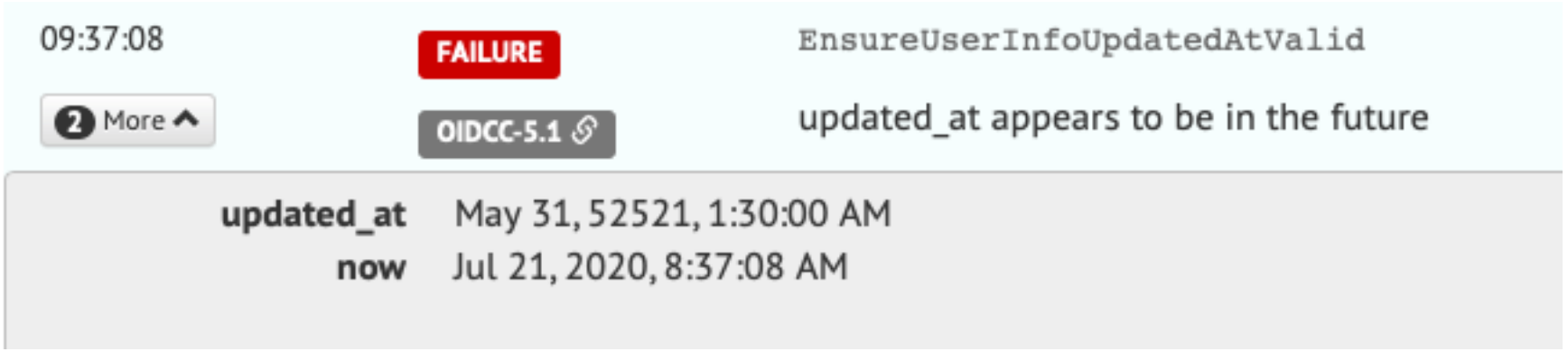
- Calling token endpoint
  - Without client authentication
  - With expired client authentication assertion
  - With client authentication assertion intended for different server (‘aud’)
  - Valid client authentication, but passing client_id for target client
  - With already-used authorization code
  - With authorization code issued to another client
  - No MTLS client cert supplied for binding access token to

Security checks – more

- Issuer
  - Configuration document location is correct
- JWKS
  - Keys too short
- Authorization code
  - Too short
  - Not enough entropy
- Calling resource server
  - With valid mtls client cert, but not the one bound to access token
- TLS 1.0/1.1 not allowed

Interoperability checks – time stamps

"Seconds since 1st Jan 1970" has been a well-known standard for years… but:



Interoperability checks - more

- The standard ‘happy’ flow
- Variants on Accept: headers
  - With/without charset
  - With q parameters
  - With multiple options
- With optional fields
  - All present
  - All missing
- Where case insensitive, testing both cases
- With allowed variants
  - ‘aud’ is an array
- Discovery document
  - Reflects what’s supported
  - Syntactically valid

Future Roadmap

- JARM testing for FAPI-RW recently added
  - Not yet part of certification program
- 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
- On the roadmap
  - FAPI 2.0
  - 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