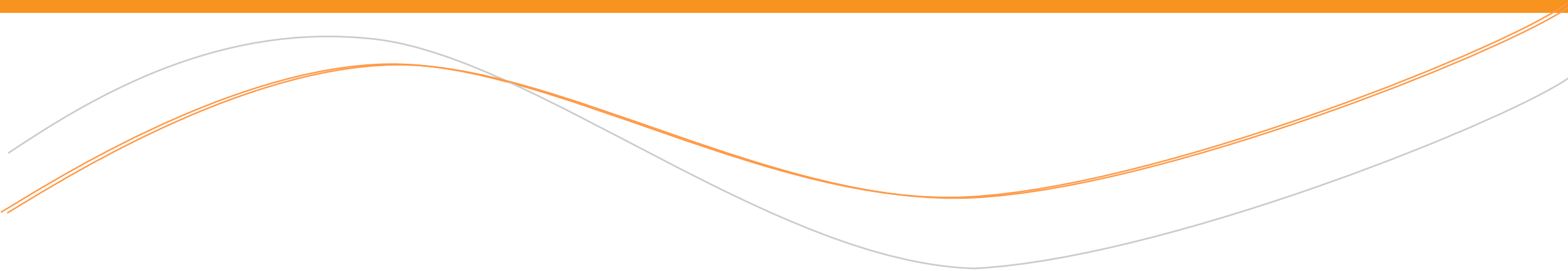


OpenID Foundation Certification Program

Joseph Heenan
Certification Technical Lead
OpenID Foundation

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/

Certification Program Success

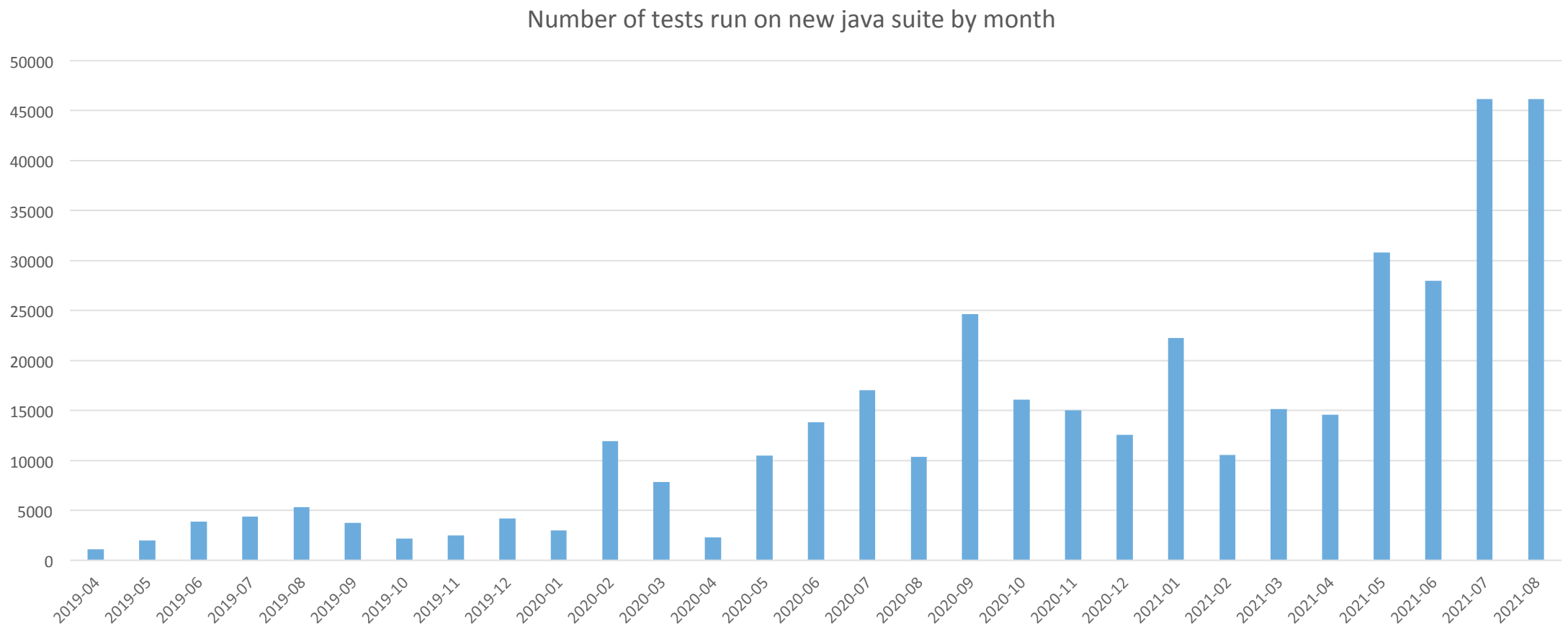
616 certifications of 200 deployments (April 2021)

Total OP Certifications	436	Total RP Certifications	94
Total OP Deployments	125	Total RP Deployments	34

Total FAPI Certifications	70	Total FAPI-CIBA Certifications	12
Total FAPI Deployments	36	Total FAPI-CIBA Deployments	3

Total FAPI RP Certifications	4
Total FAPI Deployments	2

Growth of program



FAPI Certification: Core goals

- Interoperability
- Security
- Correct deployment of certified software

However:

- FAPI tests do not test all of OpenID Connect Core
  - ‘Pretty good’ coverage of relevant parts though
  - Vendors should run OpenID Connect Core tests as well (if they support non-FAPI)

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 can be embarrassing if other people test your server & you fail
  - Anyone can test a server

A failure from a production bank system

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 `[]`

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

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

Open Banking Adoption of FAPI & FAPI Certification

- UK led the way with FAPI adoption and FAPI certification under the direction of the Open Banking Implementation Entity
  - Currently 15 UK banks have 31 FAPI certifications of 16 deployments
  - Most of the CMA9 have certified
  - OBIE require the largest 9 banks to recertify annually

- Additional jurisdictions adopting FAPI and FAPI certification
  - US – OIDF anticipates the Financial Data Exchange formally adopting FAPI and requiring FAPI certification
  - AU – OIDF coordinating with AU DSB team who have adopted FAPI as a normative standard and will be encouraging AU banks to FAPI certify
  - Brazil – Security Work Group in Brazil has adopted FAPI as part of Brazil's open banking stack and will require banks to be FAPI certified. OIDF collaborating with Security WG on Brazil-specific conformance tests
  - Other jurisdictions – OIDF working with regulators and coordinators in Europe, Bahrain and other locals to encourage and support the adoption of FAPI and FAPI conformance

What’s happened this year

- FAPI Certification program for PAR launched
  - PAR == Pushed authorization requests
- FAPI specifications from ”Implementer’s Draft” to ”Final”
  - OP & RP Certification for the final specs went live 2 months later
- FAPI OP & RP tests with Brazil ecosystem support launched
  - Also tests dynamic client registration & signed API requests/responses

Brazil OpenBanking

- Based on FAPI1-Advanced
- OIDF have worked closely with Mirow/Central Bank
- 100+ banks due to certify by end October
- Some extra restrictions compared to FAPI Advanced spec
  - Encrypted request objects required
  - PS256 for signing
  - Intent pre-lodging (similar to UK OpenBanking)
  - Intent id passed in a structured scope
  - Brazil specific ACR claim values

The next 6 months

- eKYC conformance testing
- FAPI-CIBA relying party testing
- FAPI-CIBA testing for Brazil profile
- FAPI2 Baseline testing

Wrap up

- Conformance Suite source code etc publicly available on gitlab:
  https://gitlab.com/openid/conformance-suite
- Instructions for testing/certifying:
  https://openid.net/certification/instructions/
- Production deployment:
  https://www.certification.openid.net/
  (Login with **any** google/gitlab/openid account)
- Contact the team or myself if you'd like some help:
  - joseph.heenan@oidf.org or certification@oidf.org
  - https://twitter.com/josephheenan
  - https://www.linkedin.com/in/josephheenan