Certification Program Update

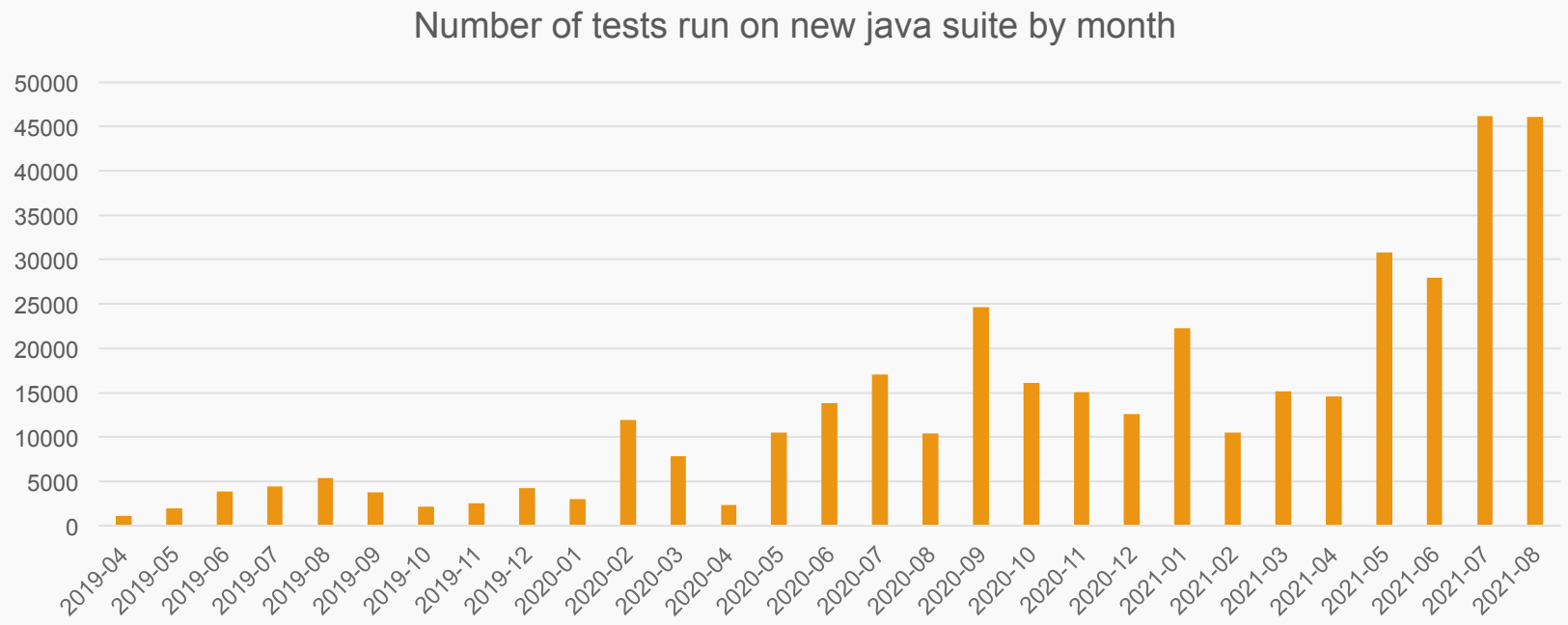
Joseph Heenan
Authlete & OIDF

December 2021
OpenID Foundation Workshop

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/

Growth of program



FAPI Certification: Core goals

- Interoperability
- Security
- Correct deployment of certified software

However:

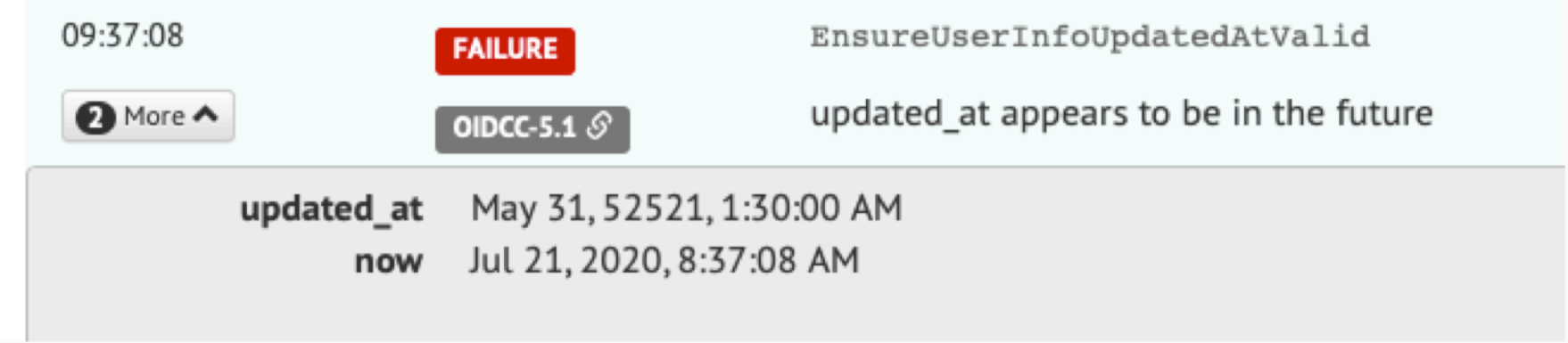
- FAPI tests do not test all of OpenID Connect Core
  - ‘Pretty good’ coverage of relevant parts though
  - Vendors should run OpenID Connect Core tests as well (if they support non-FAPI)

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

Interoperability Checks – Time Stamps

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



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

Brazil OpenBanking

- Based on FAPI1-Advanced
- OIDF have worked closely with Mirow/Central Bank
- 100+ banks certified in less than 6 months
- 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

Review of 2021

- **January:** Welcomed one new team member
- **January:** Launched FAPIRW Implementer's draft 2 OP certifications for CDR Australian Consumer Data Rights
- **January:** Launched FAPIRW Implementer's draft 2 OP with Pushed Authentication Requests (PAR) certifications
- **June:** Launched FAPI1-Advanced certifications for RP and OP
- **June:** Launched FAPI1-Advanced OP tests for Brazil OpenBanking
  - Including the first FAPI Dynamic Client Registration test
- **October:** Launched FAPI1-Advanced RP tests for Brazil OpenBanking
- **October:** Added Dynamic Client Management (RFC7592) tests for Brazil OpenBanking
- **November:** One team member moved on, recruited two new ones
- **November:** beta ekyc-ida OP tests launch

The next 6 months

- Finalizing eKYC openid provider conformance testing
- FAPI-CIBA relying party testing
- FAPI-CIBA testing for Brazil profile
- FAPI2 Baseline testing
- Improvements to submission process

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