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

<table>
<thead>
<tr>
<th>Certification Type</th>
<th>Number</th>
<th>Certification Type</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total OP Certifications</td>
<td>372</td>
<td>Total RP Certifications</td>
<td>73</td>
</tr>
<tr>
<td>Total OP Implementations</td>
<td>109</td>
<td>Total RP Implementations</td>
<td>28</td>
</tr>
<tr>
<td>Total FAPI Certifications</td>
<td>30</td>
<td>Total FAPI-CIBA Certifications</td>
<td>8</td>
</tr>
<tr>
<td>Total FAPI Implementations</td>
<td>22</td>
<td>Total FAPI-CIBA Implementations</td>
<td>2</td>
</tr>
<tr>
<td>Total FAPI RP Certifications</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total FAPI Implementations</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(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 for OPs - to be launched shortly
  - FAPI-RW ID2 OP using PAR (Pushed Authentication Requests – to be launched shortly
  - App2app authentication/authorization

Visit [https://openid.net/certification/instructions/](https://openid.net/certification/instructions/) for details
Recent changes – python suite decommissioned

- All tests (OP, RP, OpenID Connect, FAPI, CIBA, etc) are all on:
  
  https://www.certification.openid.net/

- Single Java code base

- Python tests have been reimplemented in java
  - The new tests have been tested by a large number of new and already certified OPs and RPs

- Old servers have been decommissioned
  - op.certification.openid.net & rp.certification.openid.net are no more
Recent changes – new tests

- Request object is not accepted as a private_key_jwt client authentication assertion

- Servers must accept valid PKCE
  - No requirement to implement PKCE
  - If no PKCE support, must ignore unrecognized parameters as per RFC6749

- Requests succeed with scopes in either order
  - e.g. scope=openid profile vs scope=profile openid

- Above we all added for both OpenID Connect and FAPI Ops

- For OpenID Connect, OPs can now certify without supporting alg: none
Upcoming changes – PAR (Pushed Authentication Requests)

- IETF Standard from OAuth2 Working Group


- An evolution of FAPI-RW’s request object endpoint

- Avoids passing authorization request details via the front channel
  - Better for privacy
  - Avoids any size limits on URLs

- Working Group Last Call was August 2020

- Australian CDR planning to go live with PAR from Nov 2020

- Certification program for FAPI-RW with PAR expected Nov 2020
Upcoming changes – Australian CDR

- Based on FAPI-RW

- 4 or 5 banks (OPs) live, 3 RPs live
  - Many of banks are now going through FAPI conformance testing

- Minor changes compared to base FAPI-RW spec
  - private_key_jwt must be used
  - x-v header must be sent to resource server endpoint
  - Refresh tokens must be supported
  - Returned id_tokens must be encrypted
  - For ACR claims, a CDR specific value is used, “urn:cds.au:cdr:2”

- Development of CDR version of FAPI RP tests under discussion
Upcoming changes – FAPI-Advanced Final

- Final of the FAPI specs will be going for vote shortly

- Relatively few normative changes

- New names
  - FAPI-R -> FAPI Baseline
  - FAPI-RW -> FAPI Advanced

- Expected to go to ‘final’ 5th January 2021

- Tests for the new version will be added in due course
  - Implementers Draft 2 versions of the tests will be retained
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 (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 will be embarrassing if other people test your server & you fail
  - Anyone can test a server
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 - issuer

3.3. Authorization Server Metadata Validation

The "issuer" value returned MUST be identical to the authorization server's issuer identifier value into which the well-known URI string was inserted to create the URL used to retrieve the metadata. If these values are not identical, the data contained in the response MUST NOT be used.

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:05:56</td>
<td>SUCCESS</td>
<td>CheckDiscEndpointDiscoveryUrl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>discoveryUrl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>actual  <a href="https://fapidev-as.authlete.net/.well-known/openid-configuration">https://fapidev-as.authlete.net/.well-known/openid-configuration</a></td>
</tr>
<tr>
<td>15:05:56</td>
<td>SUCCESS</td>
<td>CheckDiscEndpointIssuer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>issuer is consistent with the discovery endpoint</td>
</tr>
</tbody>
</table>
Security checks - keys

```json
private_keys
[
  {
    "p": "ukAGd9h1v80wcdsArKbiuwwlS4ta_3WWMgymWaA0McIFroMY0_MNQAzqosJ3Keui1lcp2eXbod4Ja2qKt0D464S00mK43oDawc5yH07oTg9P1lByY7zu8",
    "kty": "RSA",
    "q": "ufh1hmgTY9Up_u-upv6i1C7T-YHk_jj2e3P09Rxf74gfkhPoP35N6K0RVEZgaAC0qJ2R6tIkyRcL3B3yH4KwX1w3u6rV3yNNGF6xp0mhx9N6ZTPXGe19jUk2M",
    "d": "Fs5d7mm9oKWM4AbvsvV0r_aAXMORr22AQWjgfrQ9AbpAIYcyBbJSUXKICJzhzQ5BE5hltDNcvEp2Y_LFnhPESxnxOqLE88LWFQcaFucza8AKPIS5NhZ_rwxykAxwaSy1KeIWXr_dyMG
    e1N.mpABKj2FWfAgvyVw5M78Ufd-Ew8PKb46yR0Ub-1F9hBAinnaq7FovH1Qa5MuKwB
    "e": "AQAB",
    "use": "sig",
    "kid": "sig-2020-07-21T11:27:04Z",
    "qi": "jzkwVNC02W9h9y833DCNJAgpxjc4Phd5J98baqZzLP3o3smBLWqvdvL92acP0a-FxSuKt6MUf1tClp6n1n69L632kKmfu_aTM0rNhM0zEmbd4r3KgI6k",
    "dp": "llvJMGw9hbfp3V1A3Dsva9Y2ge1e9w8ype8687W34rRkRdo6zzolJhLPKCOHozw2Q1wFmKFGkZ.9AAJLemFDkWh0AhhA0ZsngK9711oT_MXLV0d3JFkvwg2G0u",
    "alg": "PS256",
    "dq": "Dm99PTPlsEagX11R3jilIQb1on58-b_RLPHQQVe-G6U6rrspRqpoWvzRI4FwMv9EySdxT5k5VEdF4mXyrbjNakG7k0N3-oD0BPuxIChb012hPMTMYahvIZDLE",
    "n": "hPv_WcKs5w4TfaGRPBhB1NjyRspna9m1C2HvF5JIIHp8cregl0HV5s2jF6GLyZes5HvTR1-3DGrtaFGWc_U_goZwL7MqV4H2kHRI1lGPs814hlWmlz-zeEH5-5Yrvo88F_t80hX2
    rWF8s98BknLeeDIPaAXH2zZYKhaP7cc03w7EzkUud9y64temxG_YeMDCbDr-maycRhY54AgZh
  }
]
```

symmetric_keys
[]
```
Security checks – JWS request objects processing

08:45:05 SUCCESS
Signed the request object

08:45:05 SUCCESS
BuildAuthorizationObject.setValueRedirectToAuthorizationEndpoint

08:45:05 SUCCESS
Sending to authorization endpoint

redirect_to_authorization...https://review-.../api/authorization?request=eyJraWRQI...
Security checks – objects ‘signed’ with alg ‘none’
Further Security checks – request object

- ‘exp’ already expired
- Incorrect ‘aud’
- Correctly signed, but with non-permitted alg
- With a syntactically valid, but incorrect, signature
- Valid signature but from a different client
- 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 – continued

- **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**
- **Insecure ciphers not allowed**
- **And many more…**
Interoperability checks – time stamps

“Seconds since 1st Jan 1970” has been a well-known standard for years... but:
Interoperability checks - continued

- 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
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