OpenID Foundation
October 2020 OAuth2 Security Workshop
Certification Program Update

Joseph Heenan
Certification Technical Lead
OpenID Foundation

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 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/ 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
- Draft Status : https://tools.ietf.org/html/draft-ietf-oauth-par
- 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

RFC 8414 OAuth 2.0 Authorization Server Metadata June 2018

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.

15:05:56	SUCCESS	CheckDiscEndpointDiscoveryUrl
1 More		discoveryUrl
	actual	https://fapidev-as.authlete.net/.well-known/openid-configuration
15:05:56	SUCCESS	CheckDiscEndpointIssuer
	OIDCD-4.3	issuer is consistent with the discovery endpoint
	OIDCD-7.2	

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


```
[]
```

Security checks – JWS request objects processing

08:45:05 SUCCESS SignRequestObject

More

Signed the request object

claims {"aud":"https:\/\/review-as.authlete.net\/","scope":"openid payments","claims":{"id_token":{"acr":{"value":"urn:mace:incommon:iap:silver","essential":true}}},"iss":"52480754053","response_type":"code id_token","redir
d.net\/test\/a\/authlete-review\/callback","state":"YgilSWUb7O","exp":1593762[illegible]05,"nonce":"6Q14G3gkX9","client_id":"52480754053"}

header {"kid":"fapi-jwt-assertion-20180817-1","alg":"PS256"}

request_object eyJraWQiOiJmYXBpLWp3dC1hc3NlcnRpb24tMjAxODA4MTctMSIsImFsZyI6IlBTMjU2In0.eyJhdWQiOiJodHRwczpcL1wvcmV2aWV3LWFzLmF1dGhsZXRlLm5ldFwvIiwic2NvcGUiOiJvcGVuaWQgcGF5bWVudHMiLCJ
p7InZhbHVlIjoidXJuOm1hY2U6aW5jb21tb246aWFwOnNpbHZlciIsImVzc2VudGlhbCI6dHJ1ZX19fSwiaXNzIjoiNTI0ODA3NTQwNTMiLCJyZXNwb25zZV90eXBlIjoiY29kZSBpZF90b2tlbiIsInJlZGlyZWN0X3VyaSI6Im
Glvbi5vcGVuaWQubmV0XC90ZXN0XC9hXC9hdXRobGV0ZS1yZXZpZXdcL2NhbGxiYWNrIiwic3RhdGUiOiJZZ2lsU1dVYjdPIiwiZXhwIjoxNTkzNzYyNjA1LCJub25jZSI6IjZRMTRHM2drWDkiLCJjbGllbnRfaWQiOiI1MjQ
4jXwu5IQPi8pQTWEZnh2nZBolsysOXFsknafQoJ66RbJcc87LgAavlENayPCB6RgN-ARQETzmEcGgT1edmweQS2tMr2hfSJwdhwoVk9bpSRCsm6ltganb0_lzeozjlc60PMdsU7BxF4r0I0mVcTNHj-qs1p68hFFhRQTVmB
EcI5J42g4hsxhmQeAXuQg9-4hRbOltQzvsWCjc015YOFFQSYu0GtRzJyy7DOD16Y7cIlVCFvlsXFJzVuJ8teM-N3q9KZdO3c_hIncNJNx1sotWw3JuRuNFQ

VIEW ON JWT.IO

key {"kty":"RSA","d":"ZHPB6jX2Np7cUjFu2iiYlT1YPdJ6KSyyPjEWT72TYOX6O-0a48Ez3m5OnOy_bCwD3F7_WAL0wbWXWFsRt6DmCqW-MGxG38klMQwV4dhgI6lEYyfhvBazJyQJeqHwKE5VIezgyBJyGkK9GHUqq3k3s-h
uv3ex-LGqhLT_BWX4Y1fowAgUvDLcaLj-_tRonKF4oJRiz6oMO4KTJJofhXzptY0T_K0u8bx7Y7JN-W7fC8havmG5bnKetsLQYHcn7ddWtOA_6Qxjxb6SMIr1bNWeGVA5p15NMHcIfsNmSK03Y-Xic5eiuBhwQ","e":"AQAB","
"PS256","n":"9sLLHll-BiuwlvupyiAOaTR-ChAjuwQhThxtSD5wgL9AG2YJlamxo52ZEhTdNKomGRw3woihBRk8okPSd1YZCkFuOc7iF1sUsxDA0APbdeAzZdwGcqvPlEqoz8HsnormZFTP9tG451Z_cMd20_cCufGqi6XBp
p5Zkb42AACsT9GuxB-Qrrpp1hkCJdSvXhAwlvX2jOxXQORJZkW2ST0DpCTbtAoPEW0aoCIkwWjV08qTSBduA14eIl9xPACfElosTDEbL1bR6BGxoILSJTe4U5Lz4Us7l8TWhO_OaQsyxSLFxXOy13KMQ"}

08:45:05 SUCCESS BuildRequestObjectByValueRedirectToAuthorizationEndpoint

More

Sending to authorization endpoint

redirect_to_authoriza... https://review-www.authlete.net/api/authorization?request=eyJraWQiOiJmYXBpLWp3dC1hc3NlcnRpb24tMjAxODA4MTctMSIsImFsZyI6IlBTMjU2In0.eyJhdWQiOiJodHRwczpcL1wvcmV2aWV3LWFzLmF1dGhsZX
GF5bWVudHMiLCJjbGFpbXMiOnsiaWRfdG9rZW4iOnsiYWNyIjp7InZhbHVlIjoidXJuOm1hY2U6aW5jb21tb246aWFwOnNpbHZlciIsImVzc2VudGlhbCI6dHJ1ZX19fSwiaXNzIjoiNTI0ODA3NTQwNTMiLCJyZXNwb25zZ
yZWN0X3VyaSI6Imh0dHBzOlwvXC93d3cuY2VydGlmaWNhdGlvbi5vcGVuaWQubmV0XC90ZXN0XC9hXC9hdXRobGV0ZS1yZXZpZXdcL2NhbGxiYWNrIiwic3RhdGUiOiJZZ2lsU1dVYjdPIiwiZXhwIjoxNTkzNzYyNjA1
bnRfaWQiOiI1MjQ4MDc1NDA1MyJ9.cXkddTzTxeu9pkPoZI-x4jXwu5IQPi8pQTWEZnh2nZBolsysOXFsknafQoJ66RbJcc87LgAavlENayPCB6RgN-ARQETzmEcGgT1edmweQS2tMr2hfSJwdhwoVk9bpSRCsm6ltganb0
p68hFFhRQTVmBqtz9O-gGULv5yLgJ3zSl9tUbYouu6gtHxxl9EcI5J42g4hsxhmQeAXuQg9-4hRbOltQzvsWCjc015YOFFQSYu0GtRzJyy7DOD16Y7cIlVCFvlsXFJzVuJ8teM-N3q9KZdO3c_hIncNJNx1sotWw3JuRuNFQ&
ps://www.certification.openid.net/test/a/authlete-review/callback&scope=openid%20payments&nonce=OatMLfEthj&response_type=code%20id_token

08:45:05 REDIRECT fapi-rw-id2-ensure-different-nonce-inside-and-outside-request-object

More

Redirecting to authorization endpoint

08:45:05 REVIEW ExpectRequestDifferentNonceInsideAndOutsideErrorPage

More

OIDCC-6.1

If the server does not return an invalid_request error back to the client, it must either show an error page (saying the request object is invalid as the 'nonce' value in the request object ar
nshot of the error page) or must successfully authenticate and but return the nonce from inside the request object.

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

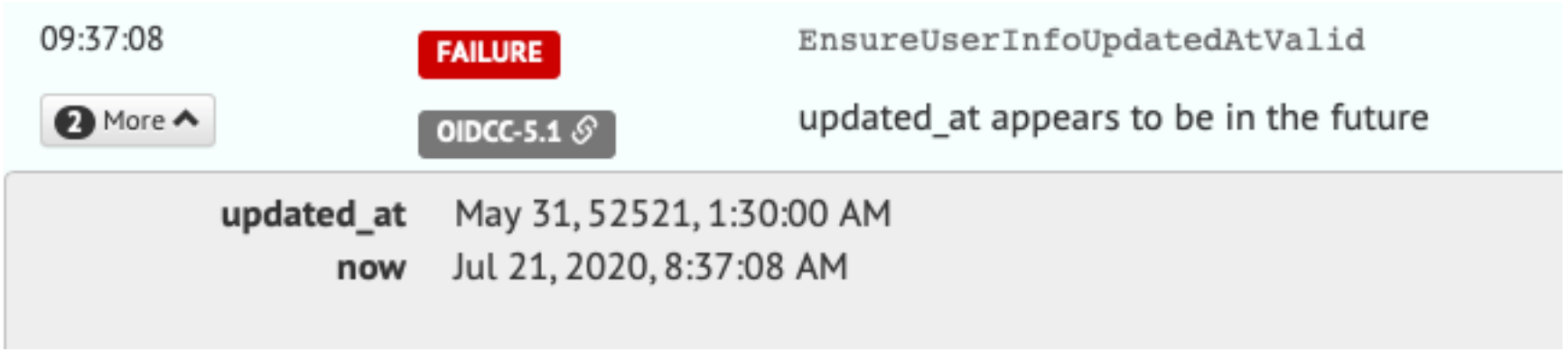
- Calling token endpoint
  - Without client authentication
  - With expired client authentication assertion
  - With client authentication assertion intended for different server (‘aud’)
  - Valid client authentication, but passing client_id for target client
  - With already-used authorization code
  - 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