OpenID Certification

May 14, 2019

Dr. Michael B. Jones

Identity Standards Architect – Microsoft

What is OpenID Certification?

- OpenID Certification enables OpenID Connect and FAPI implementations to be certified as meeting the requirements of defined conformance profiles
- An OpenID Certification has two components:
  - Technical evidence of conformance resulting from testing
  - Legal statement of conformance
- Certified implementations can use the “OpenID Certified” logo

What value does certification provide?

- Technical:
  - Certification testing gives confidence that things will “just work”
  - No custom code required to integrate with implementation
  - Better for all parties
  - Relying parties explicitly asking identity providers to get certified
- Business:
  - Enhances reputation of organization and implementation
  - Shows that organization is taking interop seriously
  - Customers may choose certified implementations over others

OpenID Connect Certification Profiles

- Six conformance profiles of OpenID Providers:
  - Basic OpenID Provider
  - Implicit OpenID Provider
  - Hybrid OpenID Provider
  - OpenID Provider Publishing Configuration Information
  - Dynamic OpenID Provider
  - Form Post OpenID Provider
- Six corresponding conformance profiles of OpenID Relying Parties:
  - Basic Relying Party
  - Implicit Relying Party
  - Hybrid Relying Party
  - Relying Party Publishing Configuration Information
  - Dynamic Relying Party
  - Form Post Relying Party

New Connect Certification Profiles

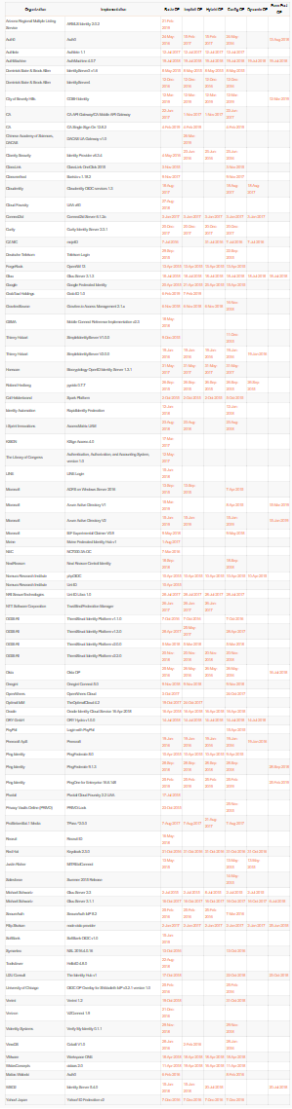
- Third Party Initiated Login for OPs and RPs
  - ***Please test these tests!***
- Four logout profiles for OPs and RPs being developed
  - RP-Initiated Logout
  - Session Management Logout
  - Front-Channel Logout
  - Back-Channel Logout
- Logout tests in alpha release
  - https://new-op.certification.openid.net:60000/
  - https://new-rp.certification.openid.net:8080/
  - Expect testing instructions this week

FAPI Certification Status

- FAPI Part 2 (Read/Write) OP certification launched April 2019
  - Two FAPI OP certifications completed to date
    - Authlete
    - ForgeRock
- FAPI Part 2 RP certification tests soon to be ready to test
- FAPI Client Initiated Back-channel Authentication (CIBA) tests for OP and RP certification also soon to come

OpenID Connect OP Certifications

- OpenID Provider certifications at https://openid.net/certification/#OPs
  - 281 profiles certified for 91 implementations by 74 organizations
- Recent additions:
  - Arizona Regional Multiple Listing Service, City of Beverly Hills, CA, Chinese Academy of Sciences, GrabTaxi Holdings, Microsoft, Ping Identity, SoftBank
- Each entry link to zip file with test logs and signed legal statement
  - ***Test results available for public inspection***



OpenID Connect RP Certifications

- Relying Party certifications at https://openid.net/certification/#RPs
  - 65 profiles certified for 26 implementations by 18 organizations
- Recent additions:
  - IBM, Ping Identity

Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic RP	Form Post RP
Brock Allen	oidc-client-js 1.3		4-Feb-2017		7-Feb-2017		
Dominick Baier	IdentityModel.OidcClient 2.0	27-Jan-2017			6-Feb-2017		
Damien Bowden	angular-auth-oidc-client 1.0.2		21-Jun-2017		11-Aug-2017		
F5 Networks	BIG-IP 13.1.0 Evergreen	7-Jul-2017					
Thierry Habart	SimpleIdentityServer V1.0.1	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017	
Janrain	IDPD 2.6.0	7-Feb-2017					
Roland Hedberg	pyoidc 0.9.4	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016	
Roland Hedberg	oidcrp 0.4.0	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	
IBM	Open Liberty 18.0.0.4	26-Oct-2018					
IBM	WebSphere Liberty 18.0.0.4	26-Oct-2018					
Tom Jones	TC.AUTHENTICATION 1.0	30-Jun-2017					
Karlsruher Institut für Technologie, SCC	oidcc 1.0.1	2-Feb-2017			2-Feb-2017		
KSIGN	KSign Trust Thing 1.0	2-Jan-2018					
KSIGN	KSign Trust Thing 1.1		3-Oct-2018				
Nomura Research Institute	phpOIDC 2016 Winter	7-Feb-2017	7-Feb-2017	7-Feb-2017	7-Feb-2017	7-Feb-2017	
Nov Matake	openid_connect rubygem v1.0.3	20-Jan-2017					
Ping Identity	PingAccess 4.2.2	26-Jan-2017					
Ping Identity	PingFederate 8.3.1	17-Jan-2017			31-Jan-2017		
Ping Identity	PingFederate 9.2.1	4-Feb-2019			4-Feb-2019		4-Feb-2019
Filip Skokan	node openid-client ^1.3.0	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016	
Filip Skokan	node openid-client ^2.0.0	12-Apr-2018	12-Apr-2018	12-Apr-2018	12-Apr-2018	12-Apr-2018	29-Jun-2018
Manfred Steyer	angular-oauth2-oidc 2.0.5		16-Aug-2017				
ZmartZone IAM	lua-resty-openidc 1.5.1	17-Nov-2017			17-Nov-2017		
ZmartZone IAM	mod_auth_openidc 2.3.1	21-Jul-2017	21-Jul-2017	21-Jul-2017	21-Jul-2017	21-Jul-2017	

FAPI OP Certifications

- FAPI OP Certifications at https://openid.net/certification/#FAPI_OPs
  - 3 profiles certified for 2 implementations by 2 organizations
- Recent additions:
  - Authlete, ForgeRock

Organization	Implementation	FAPI R/W OP w/ MTLS	FAPI R/W OP w/ Private Key
Authlete	Authlete 2.1	1-Apr-2019	1-Apr-2019
ForgeRock	ForgeRock Financial 3.1.0-credence		1-Apr-2019

A Very International Effort

- European programmers developed and operate the certification test suites:
  - Roland Hedberg, Sweden
  - Joseph Heenan, UK
  - Serkan Özkan, Turkey
  - Tomas Pazderka, Czech Republic
  - Filip Skokan, Czech Republic
  - Hans Zandbelt, Netherlands
- OpenID Connect leadership also very international:
  - Nat Sakimura, Japan
  - John Bradley, Chile
  - Michael Jones, United States

Use of Self-Certification

- OpenID Certification uses self-certification
  - Party seeking certification does their own testing
  - (rather than paying a 3rd party to do the testing)
- Simpler, quicker, less expensive, more scalable than 3rd party certification
- Results are nonetheless trustworthy because
  - Testing logs are made available for public scrutiny
  - Organization puts its reputation on the line by making a public declaration that its implementation conforms to the profile being certified to

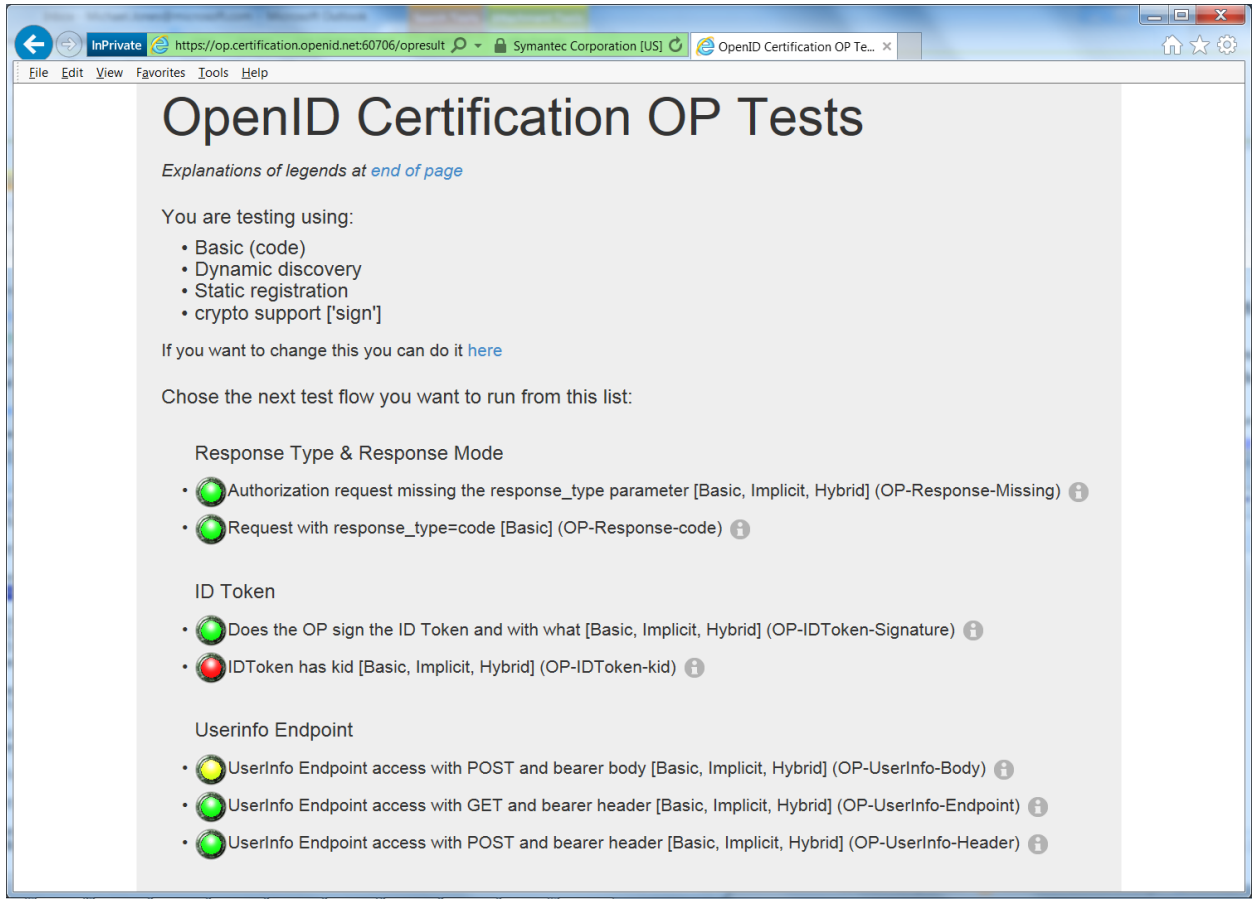
How does OpenID Certification work?

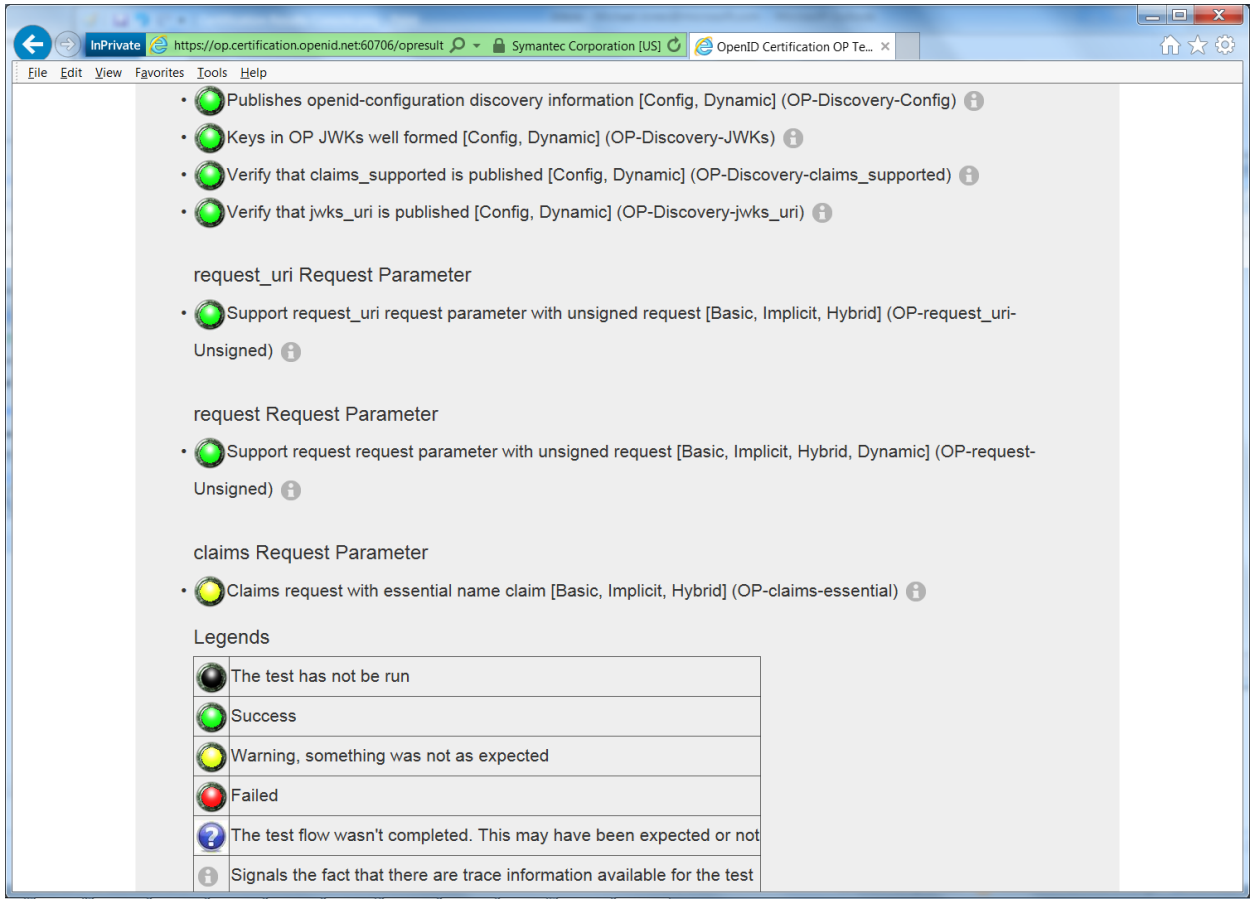
- Organization decides what profiles it wants to certify to
  - For instance, “Basic OP”, “Config OP”, and “Dynamic OP”
- Runs conformance tests publicly available at https://op.certification.openid.net/ or https://rp.certification.openid.net/ or https://www.certification.openid.net/
- Once all tests for a profile pass, organization submits certification request to OpenID Foundation containing:
  - Logs from all tests for the profile
  - Signed legal declaration that implementation conforms to the profile
- Organization pays certification fee (for profiles not in pilot mode)
- OpenID Foundation verifies application is complete and grants certification
- OIDF lists certification at https://openid.net/certification/ and registers it in OIXnet at http://oixnet.org/openid-certifications/

What does certification cost?

- Not a profit center for the OpenID Foundation
  - Fees there to help cover costs of operating certification program
- Member price
  - $200 for OpenID Connect, $500 for FAPI
    - Connect price will change to $500 in June 2019
- Non-member price
  - $999 for OpenID Connect, $2,500 for FAPI
    - Connect price will change to $2,500 in June 2019
- New profiles in pilot mode are available to members for free
- Costs described at https://openid.net/certification/fees/

Example Testing Screen





Log from a Conformance Test

Test info

Profile: {'openid-configuration': 'config', 'response_type': 'code', 'crypto': 'sign', 'registration': 'static'}
Timestamp: 2015-04-07T02:58:53Z
Test description: Keys in OP JWKs well formed [Config, Dynamic]
Test ID: OP-Discovery-JWKs
Issuer: https://stsadweb.one.microsoft.com/adfs

Test output

```
__After completing the test flow:__
[verify-base64url]
        status: OK
        description: Verifies that the base64 encoded parts of a JWK is in fact base64url encoded and not just base64 encoded
[check-http-response]
        status: OK
        description: Checks that the HTTP response status is within the 200 or 300 range
__X:==== END ====__
```

Trace output

```
0.000288 ------------ DiscoveryRequest ------------
0.000299 Provider info discover from 'https://stsadweb.one.microsoft.com/adfs'
0.000305 --> URL: https://stsadweb.one.microsoft.com/adfs/.well-known/openid-configuration
0.426715 ProviderConfigurationResponse: {
  "access_token_issuer": "http://stsadweb.one.microsoft.com/adfs/services/trust",
  "authorization_endpoint": "https://stsadweb.one.microsoft.com/adfs/oauth2/authorize/",
  "claims_parameter_supported": false,
  "claims_supported": [
    "aud",
    "iss",
    "iat",
    "exp",
    "auth_time",
    "nonce",
    "at_hash",
    "c_hash",
    "sub",
    "upn",
    "unique_name",
    "pwd_url",
    "pwd_exp",
    "ver"
  ],
  "grant_types_supported": [
    "authorization_code",
    "refresh_token",
    "client_credentials",
    "urn:ietf:params:oauth:grant-type:jwt-bearer",
    "implicit",
    "password"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "issuer": "https://stsadweb.one.microsoft.com/adfs",
  "jwks_uri": "https://stsadweb.one.microsoft.com/adfs/discovery/keys",
  "request_parameter_supported": false,
  "request_uri_parameter_supported": true,
  "require_request_uri_registration": true,
  "response_modes_supported": [
    "query",
    "fragment",
    "form_post"
  ],
  "response_types_supported": [
    "code",
    "id_token",
    "code id_token",
    "token id_token"
  ],
  "scopes_supported": [
    "logon_cert",
    "profile",
    "user_impersonation",
    "aza",
    "vpn_cert",
    "full_access",
    "email",
    "openid"
  ],
  "subject_types_supported": [
    "pairwise"
  ],
  "token_endpoint": "https://stsadweb.one.microsoft.com/adfs/oauth2/token/",
  "token_endpoint_auth_methods_supported": [
    "client_secret_post",
    "client_secret_basic",
    "private_key_jwt",
    "windows_client_authentication"
  ],
  "token_endpoint_auth_signing_alg_values_supported": [
    "RS256"
  ],
  "version": "3.0",
  "webfinger_endpoint": "https://stsadweb.one.microsoft.com/adfs/.well-known/webfinger"
}
0.846957 JWKS: {
  "keys": [
    {
      "alg": "RS256",
      "e": "AQAB",
      "kid": "f-5GWKyaV6fDdnKB7A3b0llXZ0E",
      "kty": "RSA",
      "n": "ygUNL9XXanKy_fQ1X0SMt9LRKpH3Xup11k5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW0lI8FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS_2C
      "use": "sig",
      "x5c": [
        "MIIFrjCCBJagAwIBAgIKEzgGLwABAACESDANBgkqhkiG9w0BAQUFADCBgDETMBEGCgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCWlpY3Jvc29
      ],
      "x5t": "f-5GWKyaV6fDdnKB7A3b0llXZ0E"
    }
  ]
}
0.847706 ==== END ====
```

Result

PASSED

Certification of Conformance

- Legal statement by certifier stating:
  - Who is certifying
  - What software
  - When tested
  - Profile tested
- Commits reputation of certifying organization to validity of results

OpenID

CERTIFICATION OF CONFORMANCE
TO OPENID CONNECT CONFORMANCE PROFILE

Name of Entity ("Implementer") Making this Certification: Ping Identity Corporation

Software or Service ("Deployment") Name & Version #: PingFederate Summer 2015 Release

OpenID Connect Conformance Profile: Basic OpenID Provider

Conformance Test Suite Software: op.certification.openid.net as of April 10, 2015

Test Date: April 10, 2015

1. Certification: Implementer has tested the Deployment (including by successfully completing the validation testing using the Conformance Test Suite Software) and verified that it conforms to the OpenID Connect Conformance Profile, and hereby certifies to the OpenID Foundation and the public that the Deployment conforms to the OpenID Connect Conformance Profile as set forth above.
2. Maintenance: If subsequent changes to the Deployment, or other information or testing, indicates that the Deployment is not in conformance, Implementer will either correct the nonconformance (and update this Certification if necessary) or revoke this Certification.
3. Incorporation of Terms: The Terms and Conditions for Certification of Conformance to an OpenID Connect Conformance Profile, located at www.openid.net/certification, are incorporated by reference in this Certification, and Implementer agrees to be bound by such Terms and Conditions.

Implementer's Address Information	
Address:	1001 17th Street,Suite 100
City, State/Province, Postal Code	Denver, CO 80202
Country	USA
Implementer's Authorized Contact Information	
Name:	Brian Campbell
Title:	Distinguished Engineer
Phone:	720.317.2061
Email:	bcampbell@pingidentity.com

Authorized Signature:

Name: David Wasserman

Title: Assoc. Gen. Counsel

Date: Apr. 10, 2015

How does certification relate to interop testing?

- OpenID Connect held 5 rounds of interop testing – see http://osis.idcommons.net/
  - Each round improved implementations and specs
  - By the numbers: 20 implementations, 195 members of interop list, > 1000 messages exchanged
- With interop testing, by design, participants can ignore parts of the specs
- Certification raises the bar:
  - Defines set of conformance profiles that certified implementations meet
  - Assures interop across full feature sets in profiles

Can I use the certification sites for interop testing?

- Yes – please do!
- The OpenID Foundation is committed to keeping the conformance test sites up and available for free to all
- Many projects using conformance testing for regression testing
  - Once everything passes, you're ready for certification!
- Test software is open source Python using Apache 2.0 license
  - Some projects have deployed private instances for internal testing
  - Available as a Docker container

Favorite Comments on OpenID Certification

- Eve Maler – VP of Innovation at ForgeRock
  - "You made it as simple as possible so every interaction added value."
- Jaromír Talíř – CZ.NIC
  - "We used and still are using certification platform mainly as testing tool for our IdP. Thanks to this tool, we have fixed enormous number of bugs in our platform an even some bugs in the underlying library."
- Brian Campbell – Distinguished Engineer at Ping Identity
  - "The process has allowed us to tighten up our implementation and improve on the already solid interoperability of our offerings in the OpenID Connect ecosystem."
- William Denniss – Google
  - "We have built the RP tests into the continuous-integration testing pipeline for AppAuth."

Certification Won Two Awards in 2018

OpenID CERTIFIED

Identity Innovation Award

European Identity Award

What's next for OpenID Certification?

- Additional Connect profiles being developed:
  - Third Party Initiated Login
  - RP-Initiated Logout, Session Management, Front-Channel Logout, Back-Channel Logout
  - Refresh Token Behaviors
- Additional FAPI profiles being developed:
  - FAPI RP
  - FAPI CIBA OP
  - FAPI CIBA RP
- Certification for additional specifications is anticipated:
  - E.g., HEART, MODRNA, iGov, EAP, etc.

Call to Action

- Certify your OpenID Connect and FAPI implementations now
- Help us test the new tests
- Join the OpenID Foundation and/or the OpenID Connect working group

Where can I learn more?

- Certification instructions and current results:
  - https://openid.net/certification/
- Frequently asked questions:
  - https://openid.net/certification/faq/

- My blog:
  - http://self-issued.info/
- Or drop me an e-mail:
  - mbj@microsoft.com