OpenID®

CERTIFIED

OpenID Certification Program

Award Presentation for IDnext 2018

March 28, 2018

Michael B. Jones

Microsoft Identity Standards Architect /
OpenID Foundation Board Secretary

OpenID Connect Background

- OpenID Connect is a simple identity layer on top of OAuth 2.0
  - Its use of JSON/REST makes it easy to build and deploy
- OpenID Connect won the European Identity award for best new standard in 2012
  - Widespread global adoption since then demonstrated this was a forward-looking recognition of successes to come
  - The go-to protocol for new federation deployments since then
- But a standard is only as good as its implementations
  - OpenID Foundation wanted to see high-quality, interoperable implementations become the norm

What is OpenID Certification?

- OpenID Foundation created the OpenID Certification program to encourage high-quality OpenID Connect implementations
  - Enables OpenID Connect 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
- See http://openid.net/certification/

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

How is OpenID Certification Innovative?

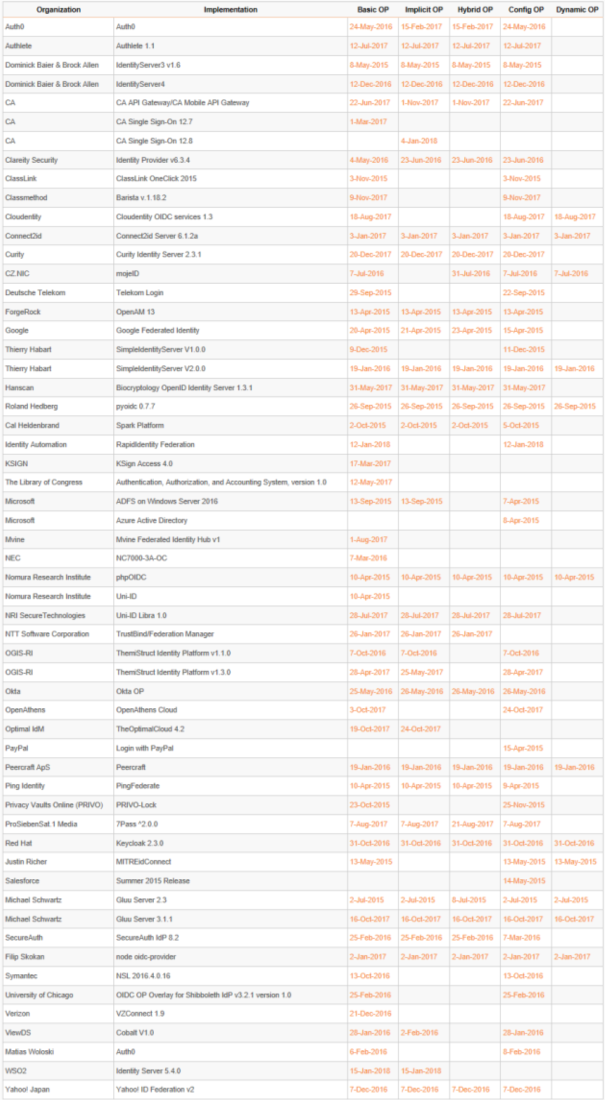
- OpenID Certification program uses ***self-certification***
  - Party seeking certification does their own testing
  - (rather than paying a 3rd party to do the testing)
- Simpler, quicker, less expensive, more scalable than 3rd party certification
  - Certification tools can be used by anyone for free at any time
  - Certification applications only $200 for members, $999 for non-members
- Results are nonetheless trustworthy because:
  - Testing logs are made available for public scrutiny
  - Organization puts its reputation on the line with a public declaration that its implementation meets the certification requirements

Expectations Greatly Exceeded!

- Certification program is now a huge marketplace force for quality and interoperability
- Numerous problems found and fixed before deployment
  - Including potential security vulnerabilities that were avoided
- Most serious Connect implementations are certified or soon will be
  - Certification has become the norm!
- Certified implementations used globally by billions of people daily
  - If you have an Android phone, use Deutsche Telekom, CZ.NIC, AOL, Google services, NTT, or Yahoo! Japan, or use Ping Federate or Microsoft ADFS, you’re using a certified OpenID Connect implementation

Who has achieved OP Certification?

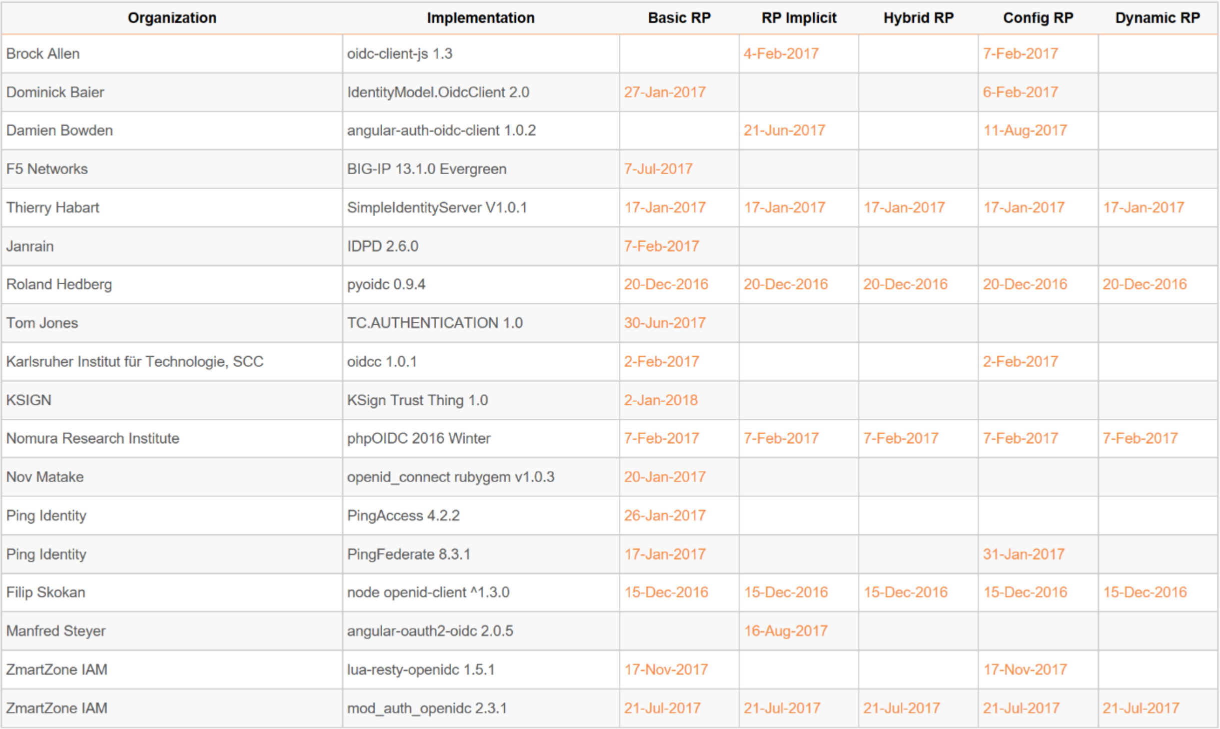
- OpenID Provider certifications at http://openid.net/certification/#OPs
  - 174 profiles certified for 57 implementations by 49 organizations
- Recent additions:
  - Auth0, CA, Classmethod, Cloudentity, Connect2id, Curity, Hanscan, Identity Automation, KSIGN, Library of Congress, Mvine, NRI, NTT, OpenAthens, Optimal Idm, ProSiebenSat.1, Michael Schwartz, Filip Skokan, WSO2
- Each entry link to zip file with test logs and signed legal statement
  - ***Test results available for public inspection***



Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP
Auth0	Auth0	24-May-2016	15-Feb-2017	15-Feb-2017	24-May-2016	
Authlete	Authlete 1.1	12-Jul-2017	12-Jul-2017	12-Jul-2017	12-Jul-2017	
Dominick Baier & Brock Allen	IdentityServer3 v1.6	8-May-2015	8-May-2015	8-May-2015	8-May-2015	
Dominick Baier & Brock Allen	IdentityServer4	12-Dec-2016	12-Dec-2016	12-Dec-2016	12-Dec-2016	
CA	CA API Gateway/CA Mobile API Gateway	22-Jun-2017	1-Nov-2017	1-Nov-2017	22-Jun-2017	
CA	CA Single Sign-On 12.7	1-Mar-2017				
CA	CA Single Sign-On 12.8		4-Jan-2018			
Clareity Security	Identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016	
ClassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015	
Classmethod	Barista v.1.18.2	9-Nov-2017			9-Nov-2017	
Cloudentity	Cloudentity OIDC services 1.3	18-Aug-2017			18-Aug-2017	18-Aug-2017
Connect2id	Connect2id Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017
Curity	Curity Identity Server 2.3.1	20-Dec-2017	20-Dec-2017	20-Dec-2017	20-Dec-2017	
CZ.NIC	mojeID	7-Jul-2016		31-Jul-2016	7-Jul-2016	7-Jul-2016
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015	
ForgeRock	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015	
Google	Google Federated Identity	20-Apr-2015	21-Apr-2015	23-Apr-2015	15-Apr-2015	
Thierry Habart	SimpleIdentityServer V1.0.0	9-Dec-2015			11-Dec-2015	
Thierry Habart	SimpleIdentityServer V2.0.0	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016
Hanscan	Biocryptology OpenID Identity Server 1.3.1	31-May-2017	31-May-2017	31-May-2017	31-May-2017	
Roland Hedberg	pyoidc 0.7.7	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015
Cal Heldenbrand	Spark Platform	2-Oct-2015	2-Oct-2015	2-Oct-2015	5-Oct-2015	
Identity Automation	RapidIdentity Federation	12-Jan-2018			12-Jan-2018	
KSIGN	KSign Access 4.0	17-Mar-2017				
The Library of Congress	Authentication, Authorization, and Accounting System, version 1.0	12-May-2017				
Microsoft	ADFS on Windows Server 2016	13-Sep-2015	13-Sep-2015		7-Apr-2015	
Microsoft	Azure Active Directory				8-Apr-2015	
Mvine	Mvine Federated Identity Hub v1	1-Aug-2017				
NEC	NC7000-3A-OC	7-Mar-2016				
Nomura Research Institute	phpOIDC	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015
Nomura Research Institute	Uni-ID	10-Apr-2015				
NRI SecureTechnologies	Uni-ID Libra 1.0	28-Jul-2017	28-Jul-2017	28-Jul-2017	28-Jul-2017	
NTT Software Corporation	TrustBind/Federation Manager	26-Jan-2017	26-Jan-2017	26-Jan-2017		
OGIS-RI	ThemiStruct Identity Platform v1.1.0	7-Oct-2016	7-Oct-2016		7-Oct-2016	
OGIS-RI	ThemiStruct Identity Platform v1.3.0	28-Apr-2017	25-May-2017		28-Apr-2017	
Okta	Okta OP	25-May-2016	26-May-2016	26-May-2016	26-May-2016	
OpenAthens	OpenAthens Cloud	3-Oct-2017			24-Oct-2017	
Optimal IdM	TheOptimalCloud 4.2	19-Oct-2017	24-Oct-2017			
PayPal	Login with PayPal				15-Apr-2015	
Peercraft ApS	Peercraft	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016
Ping Identity	PingFederate	10-Apr-2015	10-Apr-2015	10-Apr-2015	9-Apr-2015	
Privacy Vaults Online (PRIVO)	PRIVO-Lock	23-Oct-2015			25-Nov-2015	
ProSiebenSat.1 Media	7Pass ^2.0.0	7-Aug-2017	7-Aug-2017	21-Aug-2017	7-Aug-2017	
Red Hat	Keycloak 2.3.0	31-Oct-2016	31-Oct-2016	31-Oct-2016	31-Oct-2016	31-Oct-2016
Justin Richer	MITREidConnect	13-May-2015			13-May-2015	13-May-2015
Salesforce	Summer 2015 Release				14-May-2015	
Michael Schwartz	Gluu Server 2.3	2-Jul-2015	2-Jul-2015	8-Jul-2015	2-Jul-2015	2-Jul-2015
Michael Schwartz	Gluu Server 3.1.1	16-Oct-2017	16-Oct-2017	16-Oct-2017	16-Oct-2017	16-Oct-2017
SecureAuth	SecureAuth IdP 8.2	25-Feb-2016	25-Feb-2016	25-Feb-2016	7-Mar-2016	
Filip Skokan	node oidc-provider	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017
Symantec	NSL 2016.4.0.16	13-Oct-2016			13-Oct-2016	
University of Chicago	OIDC OP Overlay for Shibboleth IdP v3.2.1 version 1.0	25-Feb-2016			25-Feb-2016	
Verizon	VZConnect 1.9	21-Dec-2016				
ViewDS	Cobalt V1.0	28-Jan-2016	2-Feb-2016		28-Jan-2016	
Matias Woloski	Auth0	6-Feb-2016			8-Feb-2016	
WSO2	Identity Server 5.4.0	15-Jan-2018	15-Jan-2018			
Yahoo! Japan	Yahoo! ID Federation v2	7-Dec-2016	7-Dec-2016	7-Dec-2016	7-Dec-2016	

Who has achieved RP Certification?

- Relying Party certifications at http://openid.net/certification/#RPs
  - 44 profiles certified for 18 implementations by 16 organizations
- Recent additions:
  - Brock Allen, Damien Bowden, F5 Networks, Janrain, Karlsruher Institut für Technologie, Tom Jones, KSIGN, Manfred Steyer, NRI, ZmartZone IAM



Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic 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
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				
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	
Filip Skokan	node openid-client ^1.3.0	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016
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

A Very International Effort

- European programmers developed and operate the certification test suite:
  - Roland Hedberg, Sweden
  - Hans Zandbelt, Netherlands
  - Filip Skokan, Czech Republic
- OpenID Connect leadership also very international:
  - Nat Sakimura, Japan
  - John Bradley, Chile
  - Michael Jones, United States

Thank you for this opportunity!

- You can learn more here:
  - Certification instructions and current results:
    - http://openid.net/certification/
  - Frequently asked questions:
    - http://openid.net/certification/faq/
  - My blog:
    - http://self-issued.info/
  - Or drop me an e-mail:
    - mbj@microsoft.com

BACKUP SLIDES

Current Conformance Profiles

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

How does OpenID Certification work?

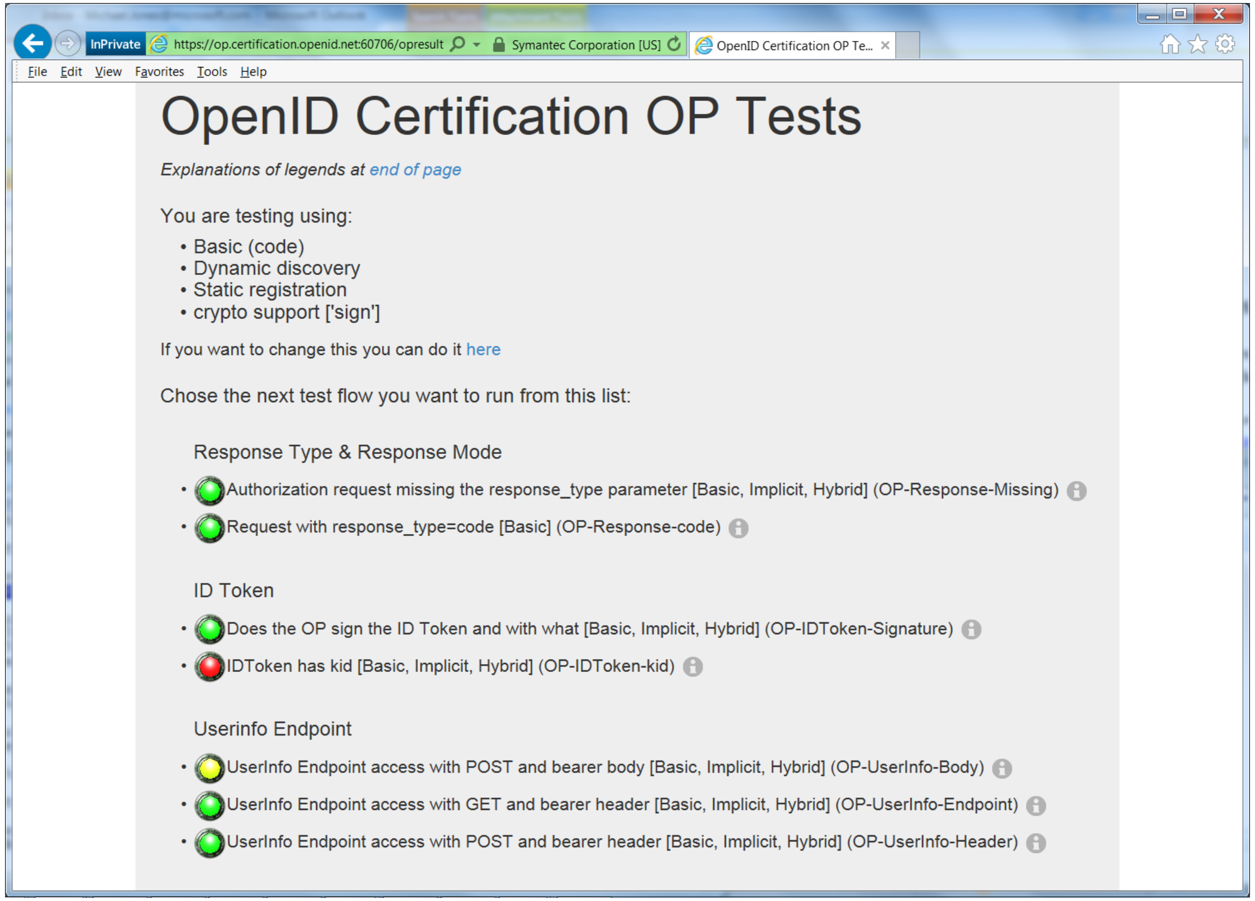
- Organization decides what profiles it wants to certify to
  - For instance, “Basic OP”, “Config OP”, and “Dynamic OP”
- Runs conformance tests publicly available at http://op.certification.openid.net/ or http://rp.certification.openid.net/
- Once all tests for a profile pass, organization submits certification 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 http://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 per new deployment
- Non-member price
  - $999 per new deployment
  - $499 per new deployment of an already-certified implementation
- Covers as many profiles as you submit within calendar year
- New profiles in pilot mode are available to members for free
- Costs described at http://openid.net/certification/fees/

Example Testing Screen

OpenID® CERTIFIED


InPrivate
https://op.certification.openid.net:60706/opresult
Symantec Corporation [US]
OpenID Certification OP Te...
File Edit View Favorites Tools Help

OpenID Certification OP Tests

Explanations of legends at end of page

You are testing using:

- Basic (code)
- Dynamic discovery
- Static registration
- crypto support ['sign']

If you want to change this you can do it here

Chose the next test flow you want to run from this list:

Response Type & Response Mode

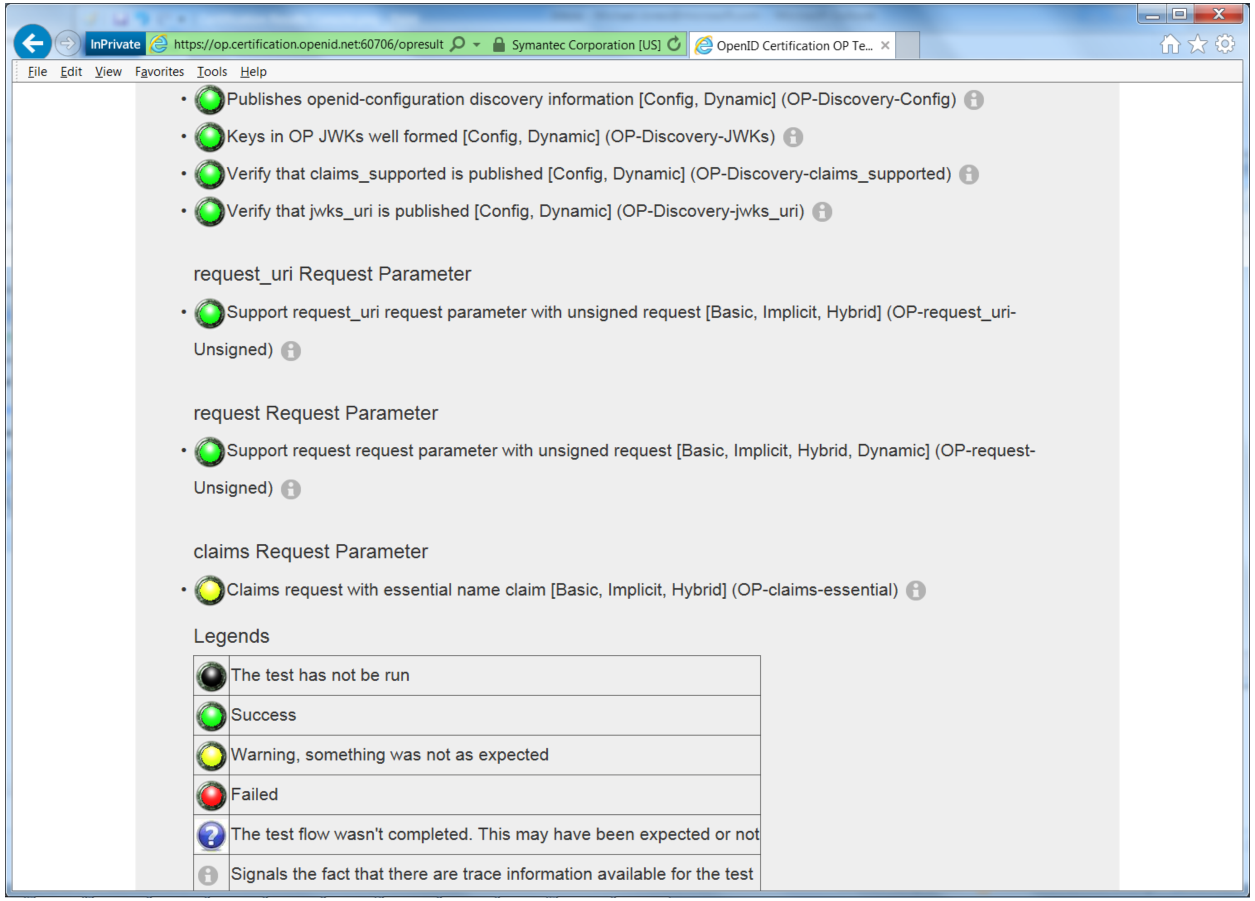
- 🟢 Authorization request missing the response_type parameter [Basic, Implicit, Hybrid] (OP-Response-Missing) ⓘ
- 🟢 Request with response_type=code [Basic] (OP-Response-code) ⓘ

ID Token

- 🟢 Does the OP sign the ID Token and with what [Basic, Implicit, Hybrid] (OP-IDToken-Signature) ⓘ
- 🔴 IDToken has kid [Basic, Implicit, Hybrid] (OP-IDToken-kid) ⓘ

Userinfo Endpoint

- 🟡 UserInfo Endpoint access with POST and bearer body [Basic, Implicit, Hybrid] (OP-UserInfo-Body) ⓘ
- 🟢 UserInfo Endpoint access with GET and bearer header [Basic, Implicit, Hybrid] (OP-UserInfo-Endpoint) ⓘ
- 🟢 UserInfo Endpoint access with POST and bearer header [Basic, Implicit, Hybrid] (OP-UserInfo-Header) ⓘ


InPrivate
https://op.certification.openid.net:60706/opresult
Symantec Corporation [US]
OpenID Certification OP Te...
File Edit View Favorites Tools Help

- 🟢 Publishes openid-configuration discovery information [Config, Dynamic] (OP-Discovery-Config) ⓘ
- 🟢 Keys in OP JWKs well formed [Config, Dynamic] (OP-Discovery-JWKs) ⓘ
- 🟢 Verify that claims_supported is published [Config, Dynamic] (OP-Discovery-claims_supported) ⓘ
- 🟢 Verify that jwks_uri is published [Config, Dynamic] (OP-Discovery-jwks_uri) ⓘ

request_uri Request Parameter

- 🟢 Support request_uri request parameter with unsigned request [Basic, Implicit, Hybrid] (OP-request_uri-Unsigned) ⓘ

request Request Parameter

- 🟢 Support request request parameter with unsigned request [Basic, Implicit, Hybrid, Dynamic] (OP-request-Unsigned) ⓘ

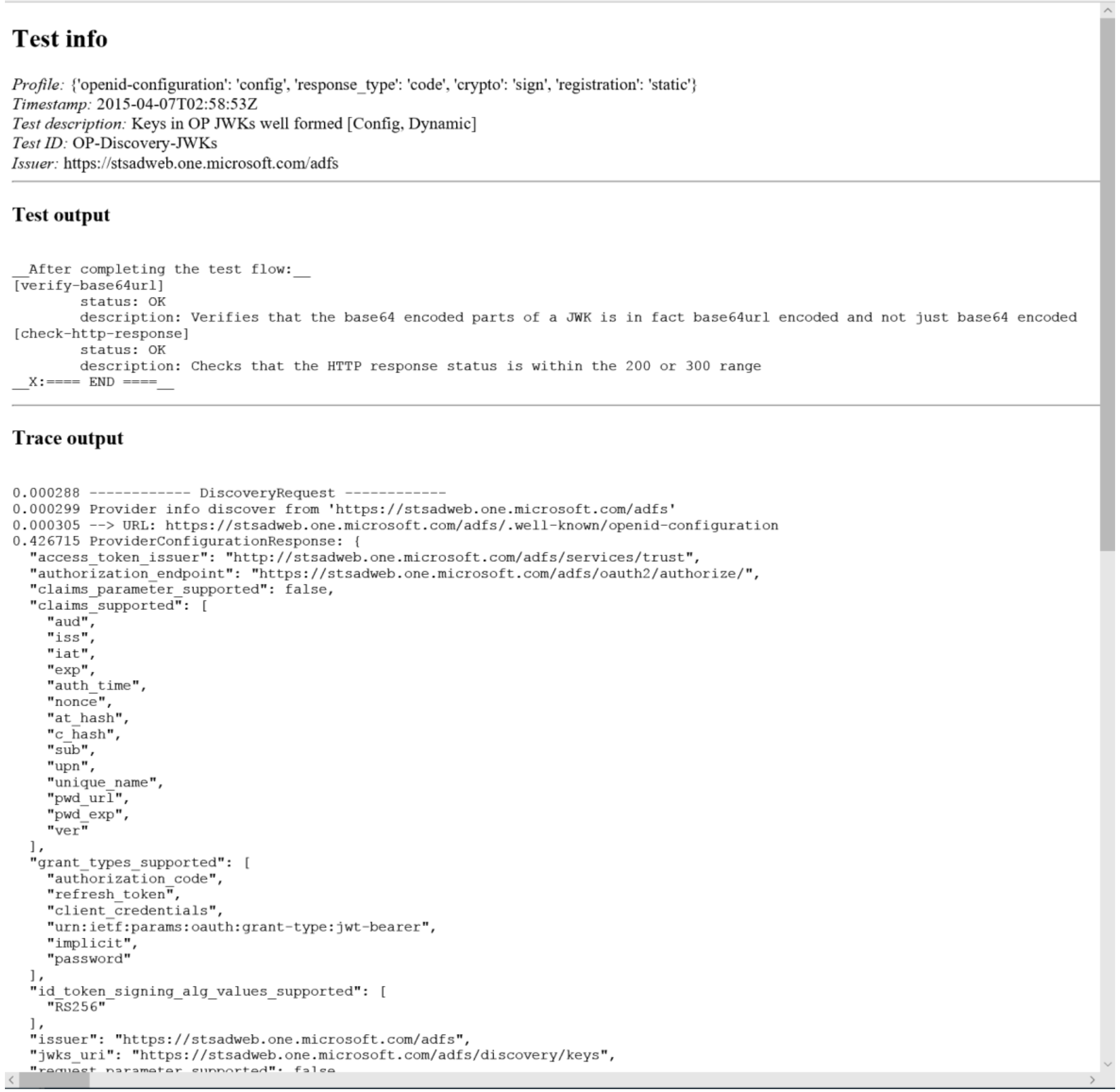
claims Request Parameter

- 🟡 Claims request with essential name claim [Basic, Implicit, Hybrid] (OP-claims-essential) ⓘ

Legends

⚫	The test has not be run
🟢	Success
🟡	Warning, something was not as expected
🔴	Failed
❓	The test flow wasn't completed. This may have been expected or not
ⓘ	Signals the fact that there are trace information available for the test

Log from a Conformance Test



Test info

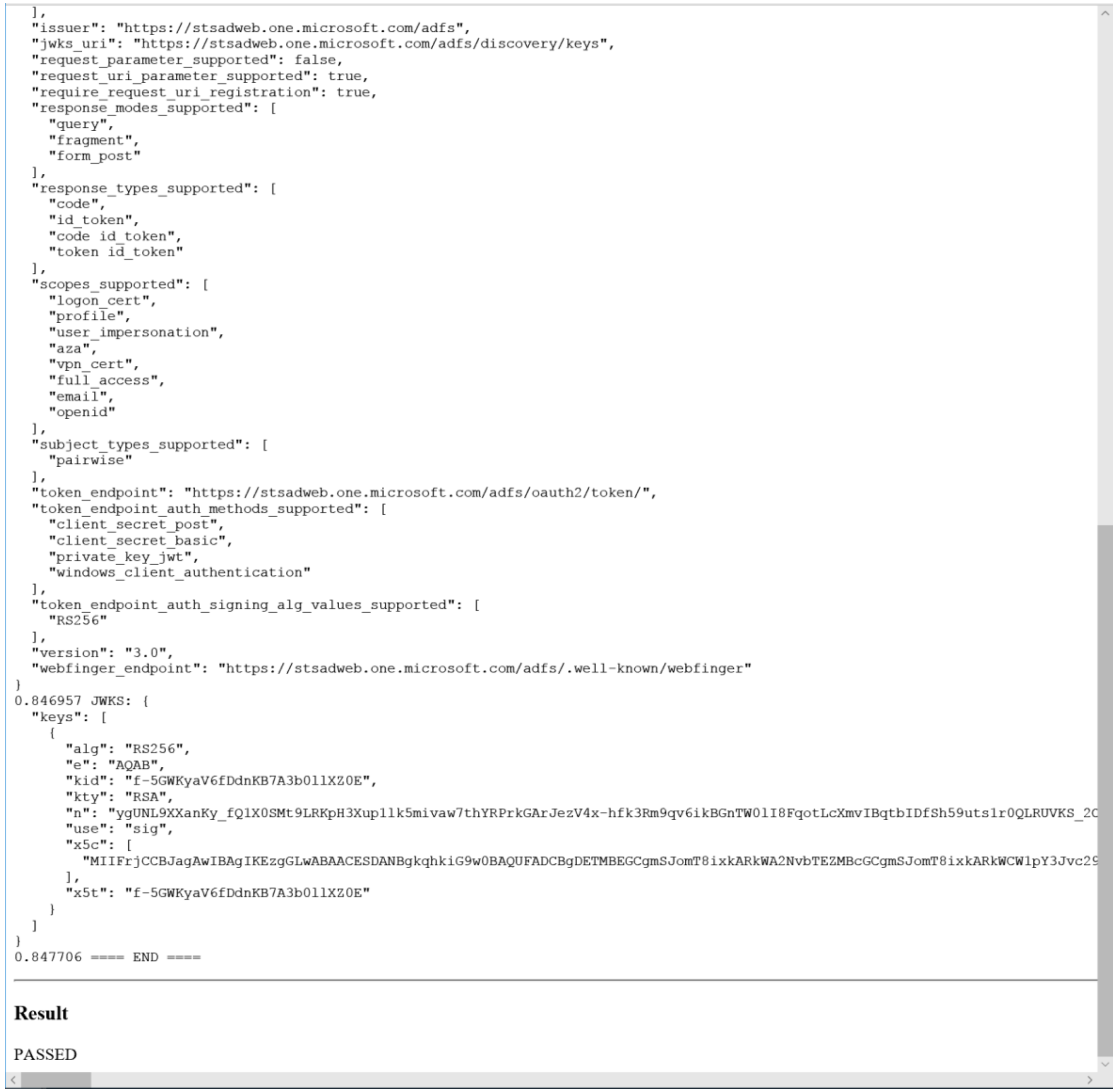
Profile: {'openid-configuration': 'config', 'response_type': 'code', 'crypto': 'sign', 'registration': 'static'}
Timestamp: 2015-04-07T02:58:53Z
Test description: Keys in OP JWKs well formed [Config, Dynamic]
Test ID: OP-Discovery-JWKs
Issuer: https://stsadweb.one.microsoft.com/adfs

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
```



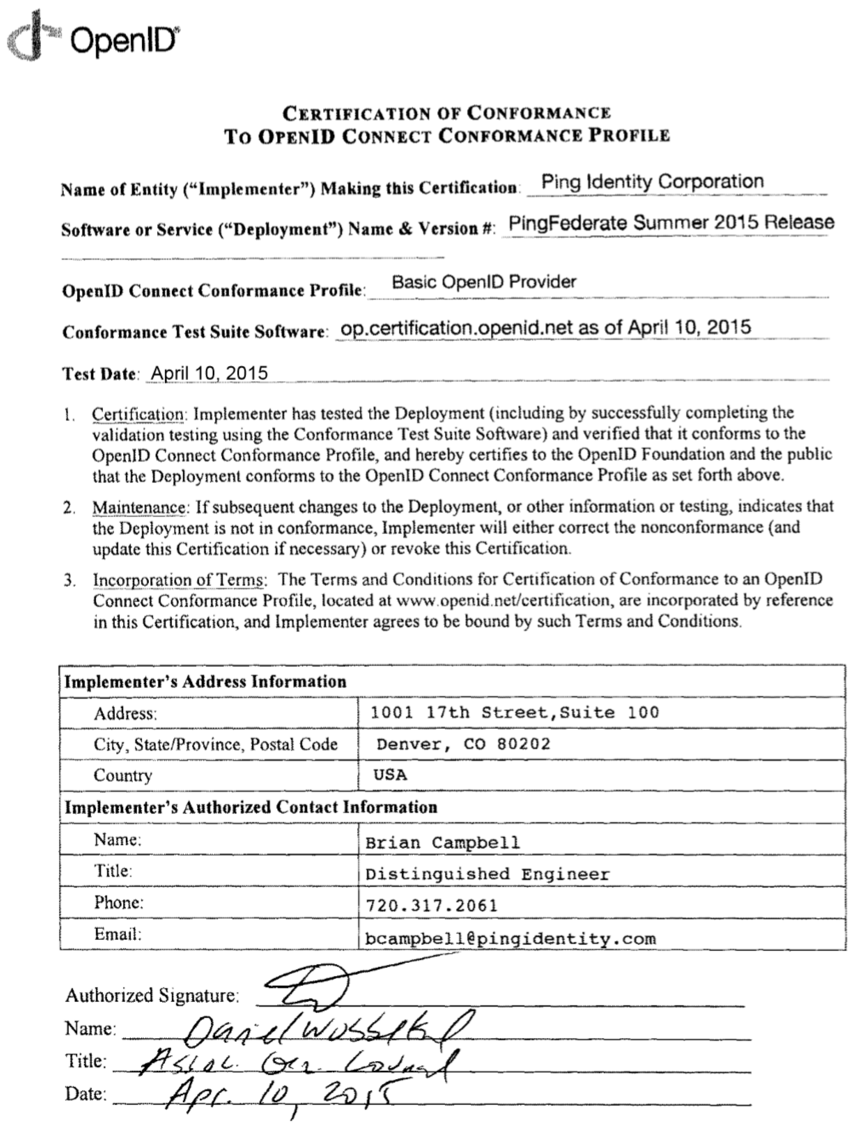
```
  ],
  "issuer": "https://stsadweb.one.microsoft.com/adfs",
  "jwks_uri": "https://stsadweb.one.microsoft.com/adfs/discovery/keys",
  "request_parameter_supported": false,
  "request_uri_parameter_supported": true,
  "require_request_uri_registration": true,
  "response_modes_supported": [
    "query",
    "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_fQ1X0SMt9LRKpH3Xup1lk5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW0lI8FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS_2C
      "use": "sig",
      "x5c": [
        "MIIFrjCCBJagAwIBAgIKEzgGLwABAACESDANBgkqhkiG9w0BAQUFADCBgDETMBEGCgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCW1pY3Jvc29
      ],
      "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: Daniel Wussiel

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.”

What’s next for OpenID Certification?

- Additional profiles being developed:
  - Form Post Response Mode
  - Refresh Token Behaviors
  - Session Management, Front-Channel Logout, Back-Channel Logout
  - OP-Initiated Login
- Additional documentation being produced
  - By Roland Hedberg and Hans Zandbelt
- Certification for additional specifications is anticipated:
  - E.g., HEART, MODRNA, iGov, EAP, FAPI, etc.