



# OpenID Certification

October 16, 2017

**Michael B. Jones**

Identity Standards Architect – Microsoft

# What is OpenID Certification?



- OpenID Certification 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

# 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

# What can be certified now?



- 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

# Who has achieved OP Certification?



- OpenID Provider certifications listed at <http://openid.net/certification/#OPs>
- 124 profiles certified for 39 implementations by 36 organizations
- Recent additions:
  - Dominick Baier & Brock Allen, Connect2ID, KSIGN, NTT Software, OGIS-RI, Red Hat, Filip Skokan, Symantec, Verizon, Yahoo! Japan
- Each entry in table a link to zip file containing test logs and signed legal statement of conformance
  - 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 |             |
| 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 |             |
| Clarity 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  |             |
| Connect2id                    | Connect2id Server 6.1.2a                              | 3-Jan-2017  | 3-Jan-2017  | 3-Jan-2017  | 3-Jan-2017  | 3-Jan-2017  |
| CZ.NIC                        | mojelD  | 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 |
| Roland Hedberg                | pyoido 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  |             |
| KSIGN                         | KSign Access 4.0                                      | 17-Mar-2017 |             |             |             |             |
| Microsoft                     | ADFS on Windows Server 2016                           | 13-Sep-2015 | 13-Sep-2015 |             | 7-Apr-2015  |             |
| Microsoft                     | Azure Active Directory                                |             |             |             | 8-Apr-2015  |             |
| 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 |             |             |             |             |
| NTT Software Corporation      | TrustBind/Federation Manager                          | 28-Jan-2017 | 28-Jan-2017 | 28-Jan-2017 |             |             |
| PayPal                        | Login with PayPal                                     |             |             |             | 15-Apr-2015 |             |
| OGIS-RI                       | ThemiStruct Identity Platform v1.1.0                  | 7-Oct-2016  | 7-Oct-2016  |             | 7-Oct-2016  |             |
| Okta                          | Okta OP   | 25-May-2016 | 25-May-2016 | 25-May-2016 | 25-May-2016 |             |
| 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 |             |
| 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              | Glue Server 2.3                                       | 2-Jul-2015  | 2-Jul-2015  | 8-Jul-2015  | 2-Jul-2015  | 2-Jul-2015  |
| 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  |             |
| Yahoo! Japan                  | Yahoo! ID Federation v2                               | 7-Dec-2016  | 7-Dec-2016  | 7-Dec-2016  | 7-Dec-2016  |             |

# Who has achieved RP Certification?



- RP Certification launched in December 2016
- Relying Party certifications listed at <http://openid.net/certification/#RPs>
- 34 profiles certified for 12 implementations by 11 organizations
- To date:
  - Brock Allen, Dominick Baier, Thierry Habart, Janrain, Roland Hedberg, KIT SCC, NRI, Nov Matake, Ping Identity, Filip Skokan, Hans Zandbelt

| Organization                             | Implementation                | Basic RP    | RP Implicit | Hybrid RP   | Config RP   | Dynamic RP  |
|--|-------------------------------|-------------|-------------|-------------|-------------|-------------|
| Brook Allen                              | oidc-client-js 1.3            |             | 4-Feb-2017  |             | 7-Feb-2017  |             |
| Dominick Baier                           | IdentityModel.OidcClient 2.0  | 27-Jan-2017 |             |             | 6-Feb-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 |
| Karlsruher Institut für Technologie, SCC | oidcc 1.0.1                   | 2-Feb-2017  |             |             | 2-Feb-2017  |             |
| 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 |
| Hans Zandbelt                            | mod_auth_openidc 2.1.2        | 13-Dec-2016 |             |             | 13-Dec-2016 | 13-Dec-2016 |

# Use of Self-Certification



- OpenID Certification uses self-certification
  - Party seeking certification does the 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 <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 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) ⓘ

request\_uri Request Parameter

- 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 Request Parameter

- Support request\_uri request parameter with unsigned request [Basic, Implicit, Hybrid] (OP-request\_uri-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-5GWKyav6fDdnKB7A3b01lXZ0E",
      "kty": "RSA",
      "n": "ygUNL9XXanKy_fQlX0Smt9LRKpH3Xup1lk5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW01I8FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS_2C",
      "use": "sig",
      "x5c": [
        "MIIFRjCCBjAgIwIBAgIKeZgGLwABAACESDANBgkqhkiG9w0BAQUFADCBgDETMBEgGmSjOmT8ixkARKWA2NvbTEZMBCGCGmSjOmT8ixkARKWCW1pY3Jvc2U="
      ],
      "x5t": "f-5GWKyav6fDdnKB7A3b01lXZ0E"
    }
  ]
}
0.847706 ===== END =====
```

## Result

PASSED

# Certification of Conformance



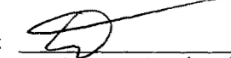
- Legal statement by certifier stating:
  - Who is certifying
  - What software
  - When tested
  - Profile tested
- Commits reputation of certifying organization to validity of results

## 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](http://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 Wussick  
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.



# Call to Action



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

# Where can I learn more?



- 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](mailto:mbj@microsoft.com)