

OpenID Certification

April 29, 2019

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/
 - Let's go over these tests during IIW

FAPI Certification Status



- FAPI Part 2 OP certification launched April 1, 2019
 - Two certifications completed to date
 - Authlete
 - ForgeRock
- FAPI Part 2 RP certification tests soon to be ready to test
- FAPI CIBA OP and RP certification tests soon to come

Connect OP Certifications

- OpenID Provider certifications at <u>https://openid.net/certification/#OPs</u>
 - 281 profiles certified for91 implementations by74 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



				_		_	_
Ogerleiter	Inglowed day	Relate	heplat 😎	нумен	Cody CP	Opendo De	North Add
trono Regional Multiple Listing Irolan	.006.014+0y202						
40	Auto	2018 26 May 2018		SERVICE SEET	20 May 20 M		DAMP STR
F840	Author 11	0.4307 18.4308	9.620 9.620		0.487 0.487		
rest for Clock Ser	Miniplicant of it	8 May 2018			SW-ZII		
rest Ser Clock Ser	Methylanusi	6 May 2010 10 Chin 2016 10 May 2016 20 Ann 2017 6 Pals 2018	10 Om 2016 10 Om 2016	8 May 2008 10 Own 2018 10 May 2018	DON EN		
ly of Binardy 1986.	CONTRACTO	10 Mar. 2018	13 Mar 2018	10 Mar. 2018	10 miles 2009 2004 2007 4 miles 2019		0 No. 2016
	CLAR Galway Chillian IPT Galway		1864207	144-207			
	CA Rogin Ryn Co 1043		0.040-3018 20.00± 2018 20.0± 20.0± 20.0±				
time hadrop of Barren, NCM	SKOW M Galway v1.0						
looky Streety	Martly Problet 453.0	4 May 2010			21.lan 2310		
lesion.	Genial Crothis 2018 Sension 1, 16.2				1 Sec. 30 S		
inatedly	Geolothy OEC senten 13	314a 2001 814a 2017 20 Aug 2018 2 Jan 2017 20 Dan 2017 7 Aug 2018 20 Aug 20 Aug			1760-3878 1760-3877 1876-9 2877	SIA Nag	
te Cheste	W-40	27 Aug			227		
eren(Dir	GermalDel Street E. Lille	3018 3 Jan 2017	3.2m277	3.3v:2011	3.20-2017	J.av.Eff	
ally	Cody biretty Street 3.3.1	20 Onc.		DO: DIT	200m 2017 1.4620 N 200m 200		
EME	mpili	P.343090		20.3420.00	T-2403078	T.33 30 W	
ndule Stitue	Téleniage	2018 2018			200		
ngellada In	Operated Cl. Observer 3.1.3 Geogle Protectional Markly			18.Ap 20.0 18.Ad 20.0 28.Ap 20.0	15.4-32.0 15.4-32.0		
mph.	Google Production State Sty Code CD 1-0	20 Ayr 2000		28.8pc 20.00	n.p.zu		
and the same	Contract Assess Management 3 La	114-229			10 Spin		
	Mide Grossi Network Ingless Autor d 3	18 May 2018					
	Minde Greeni Retermo Implementation 42.3 Meght kindyllamor 17.22				110w		
-	Bright brightner VIIII Bright brightner VIIII	Wales		Mules 2016 20 May 2017 20 May 2016 2016 2018	2221 2221 15.5m 2201		
tery fished	Brightinelly Breen (D.13) Biorghidage Open Childrelly Breen 1.3.1	20's	19.5m 209 21.6kg 207	2006 W.Mar	234	H-landEW	
article .	Bioghileg-OperChile(ly Street 13.1 spain(177	When you want to be a second or seco	207	XIII	21 May 227 218 218 218 218 218 218 218 218 218		
dard/fedding	opide/STF		20.0mp 2018 200m 2018				
E7Mintered	Spat-Platers	3 (34 300) 10 Jan	2 Car 2018	201300	Side Still Dube		
	Republished y Production Assemblatia USSI	27 A 23 A 42	25 Aug		200 Diday		
per tourists	Assemble to USA	2008 Title	20 Aug 20 M		200		
801	Killige Assets & E	207					
w Library of Congress	Autoritation, Autoritation, and Assaulting System, weeken 1-8	207					
	GRE Logic						
house	ADT or Walson Street 2018				T Apr 2010		
head	Anus Ashe Direkty VI	18 Mar. 2018			1.5p-2018		11 Nav 2016
head	Anue Aube Cleakey Cl				Stain 200		11.00 X 10
treed.	EF Superior of Charac VSS State Probability Market	8 May 2018					
ic.	NCTIONAGE	7 Mar 2016					
all town	Need Resource Control Statestily	1 Aug 2017 7 May 2018 18 Aug 2018			58.8ep 2588		
man Sound Indian	pposs SHD	10 Apr 2000 10 Apr 2000 28 Apr 2007 28 Apr 2017 7 Chr 2000					
Sime Intelligin	GelDides 1.5				20.00		
FT Bellesse Corporation	Traditio Production Manager						
0.4	Terriffical kiroliy Mollows (1.10 Terriffical kiroliy Mollows (2.0	7 (34 200)	Piller 2016 William		TOUGH		
20.4	Terriffical Methy Mallors (13.0 Terriffical Methy Mallors (15.0	38 Apr 3007	207				
20.5	Perolitical biologiful broad 200		20 Nov	20 New			
	OneOf	28 May	2018 2019y	2008 20 May	233 2150y		
mgri	Orașie Connei fili	20 May 2018 20 May 2018 20 May 2018 3 May 2018 3 May 2017 10 May 2017 10 May 2018 10 May 2018	28.46207 28.50 207 7 Ga 230 200p 207 5 Ga 278 208 208 208 208 208 208 208 208 208 20	30 May 2008 20 May 2008	2004 200 0 to 200 20 to 200		
profilers.	Operations Cloud To Operation Cloud						
and the	TerOptimeDate(L2) Orabi Methy Chall Strato 18 Apr 2019 OHT Hydrox LES		20 Car 20 FT 10 Apr 20 FT 10 Apr 20 FT				
erous ero	CHI Hydro LEE			#0.11.E.0		14.543010	
mod lpf	Percel	18 Jan				Maratte	
ng Marily	Pophere 80	30 Apr 2010			14×20		
ng kindly	Proframe 513	18 Jan 2018 18 Ayr 2018 28 Ayr 2018 28 Ayr 2018 17 Ag 2018	10.3m 200 10.4p 200 20.8p 200	10-Jan 2001 10-Apr 2010 20-Bup 2003 20-Pala 2009	10.0p 2010 10.2m 2010 10.4p 2010 2010 2010 2010 2010 2010 10.4p 2017		24,77
ng Marily	PhyDre to Edwards 1983 M						254278
wild	Plote Charlesonly 12 UNI	9.34300					
ney teals (Merc (MEC)	MEGicals	20 Chi 2010					
officiardis / Meda	Theo. (933)	P.Aug/2007 16 May 2016 21 Cts 2006 13 May 2016	TAgES	21.fup 3117	Theory		
and .	Rend D	18 May . 2018					
474	Replical 23.0	31 CM 2016 13 May	T-Co-XN	E-O1 E-S	DOLEN UNA	21 Oct 2018 Chilley	
ele-Malor	MERCHAN	207.0			231	XIII	
Anima	Surrey 2015 Salvano				233		
And Sheets	One Stone 2.3 One Stone 2.1.1		2.36 Z 15 16 Ga Z 17 25 Au 27 B	8.34 2019 10.034 2017 20.04 2016 2.344 2017			1,400
man hali	Branchalt NPE2	28 Polic 2018	20 No. 2016	20 Pale 2006	T No. 2016		
ly Status	male state practile	3.3m2077	3.lim ZITT	3.liv:2017	3.3m3017	Davær	2.iv.29
fflict.	Ballina (RECVI)						
praetos abbaso	ME SHALL W	13 Ou 2016 23 Aug					
N Good	Testedy Navi	2018 17 On 2018			DOLES.		
tenty of Charge	OCCOPOseing for District Of Pall 2 I wonlow 12	18 Ga 2017 28 Pek 2018 23 Jan 2017 18 Jan 2018 20 Ga 2018 27 Ga 2018 28 Pek 2018 20 Ga 2018 20 Ga 2018 21 Ga 2018					
alad .	Think 13	19 (34 200)			E ON E W		
nione	Williams 18						
delly Spires	Trong tilg blandig (CC)	28 Nov 2018 28 Jan 2018 18 Apr 2018			2015an 2021		
m/CR	GMEVES	28.Jan 2018	2746-2018				
han .	Viologous (Mil.	18 Apr 2016	11.4p 21.00				
de Tibeli	Auto 20	11 Apr 2006 6 Poli-2016 18 Jan 2016 7 Chi-2016			ENG 271		
N/S	Martly Borns 5.63			DHES			E-14 E-18
that Japan	Table of Ed Production of	7 On 2016	7 Geo. 2019	70×30%	T Gree 2016		

Connect RP Certifications



- Relying Party certifications at <u>https://openid.net/certification/#RPs</u>
 - 65 profiles certified for26 implementations by18 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 for2 implementations by2 organizations

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		

- Recent additions:
 - Authlete, ForgeRock

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 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 https://op.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/

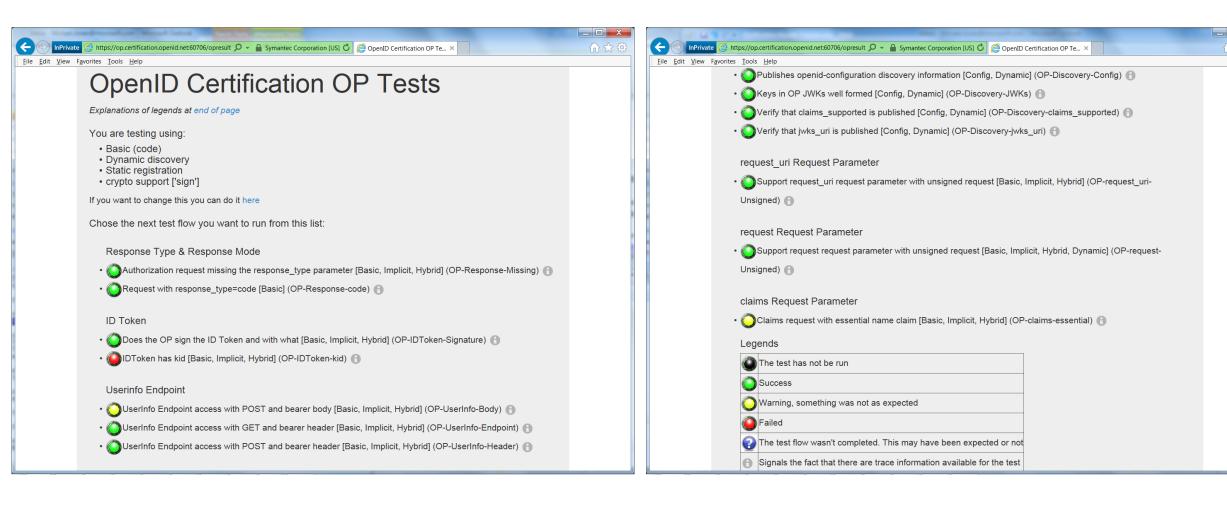
What does certification cost?



- Not a profit center for the OpenID Foundation
 - Fees there to help cover costs of operating certification program
- Member price
 - \$200 for Connect, \$500 for FAPI
 - Connect price will change to \$500 in June 2019
- Non-member price
 - \$999 for 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",
  "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": [
  "issuer": "https://stsadweb.one.microsoft.com/adfs",
  "jwks_uri": "https://stsadweb.one.microsoft.com/adfs/discovery/keys",
  "request narameter 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": [
  "version": "3.0",
  "webfinger endpoint": "https://stsadweb.one.microsoft.com/adfs/.well-known/webfinger"
0.846957 JWKS: {
  "keys": [
      "alg": "RS256",
      "e": "AQAB",
      "kid": "f-5GWKyaV6fDdnKB7A3b011XZ0E",
      "n": "yqUNL9XXanKy fQ1X0SMt9LRKpH3Xup11k5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW0118FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS 20
        "MIIFrjcCBJagAwIBAgIKEzgGLwABAACESDANBgkqhkiG9w0BAQUFADCBgDETMBEGCgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCW1pY3Jvc29
      "x5t": "f-5GWKyaV6fDdnKB7A3b011XZ0E"
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 Releas
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

- <u>Certification</u>: 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.
- 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.
- 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: Danilwussik	
Title: ASIAL Ger Ladas	1
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



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