

# **OpenID Certification**

September 30, 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**



- Now OpenID Connect certification profiles for:
  - Basic OP and Basic RP
  - Implicit OP and Implicit RP
  - Hybrid OP and Hybrid RP
  - OP Publishing and RP Using Configuration Information
  - Dynamic OP and Dynamic RP
  - Form Post Response Mode for OP and RP
  - New: Third party-initiated login for OP and RP
  - New: Logout OP tests in pilot mode

## New Connect Certification Profiles



- Third Party Initiated Login for OPs and RPs
  - Be one of the first to certify for these profiles!
- 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**



- Financial-grade API (FAPI) implementations now being certified
- FAPI Part 2 OP certification launched in April 2019
  - Nine implementations certified to date
- New: Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) launched in September 2019
  - One implementation certified to date
- FAPI Part 2 RP certification tests soon to be ready to test

# **Connect OP Certifications**

- OpenID Provider certifications at <a href="https://openid.net/certification/#OPs">https://openid.net/certification/#OPs</a>
  - 323 profiles certified for
     100 implementations by
     80 organizations
- Recent additions:
  - Akamai, Authlete, Chinese Academy of Sciences, Curity, Grab Taxi, IBM, Micro Focus, OGIS-RI, Oxyliom, Filip Skokan, Trivore
- Each entry link to zip file with test logs and signed legal statement
  - Test results available for public inspection



The Color of the Color of State 1 (1985)The Color of State 1 (1985)T								
Mathematical patternsMathematical pattern	Ogododke	Inglowed the	Autor	inglish (**	HANGE	Cody CP	Openin Dr	Non-Pail OF
Mathematical patternsMathematical pattern	Access Riginal Malphristing Similar	.098.814+0y.252						
MANDMA	ARE	AMI	36 May 2016		SEPAGE SEFF	21 May 27 M		DAy 27 K
Mathematical patterns of the p	Artes	Addison 11						
Material School of Material	Design Size & Book Wes	Mediphered of di	1 May 2018	19w-201				
Material School of Material	Detect Stir S Souk Mon	taintlyforund				13 Own 2786		
Material School of Material	Opel Book His	CORTANIA	10 Mar 2018	13 Mar. 2018	10 Mar. 2008	1316br 2316		0 na. 274
Material School of Material	ca.	CIAN Géray Chillian IN Géraly		186×207	184200			
Management of the control of	EA.	Chillegh Rips Co. SEC						
Management of the control of	Criesus hashing of Barrein, DACHE	SKOW UK Galendy v1.3						
100	Cherily Streety	Sandy Provider of Cl. C	4 May 2016			25.bm 25%		
Machine Sample of Machine	Genica.	Genia Ordin 201						
Machine Sample of Machine	Challelly	Genderily OEC seniors 13	MAg			18.hap	18.Aug	
Machine Sample of Machine	Grad Plantily	W-60	PAp					
Machine Sample of Machine	GreenShil	GermaDel Street E.1.2b	3018 3.34+307	3.imZfT	3.3m2077	3.im207	Liver	
Machine Sample of Machine	Dely	Cody bleetly Brear 23.1	20 Onc.	20 Own 20 T	20 Dec	200m 207		
Machine Sample of Machine	GOME	repili)	7.3430W		2-71 X 0	T. AND TO 100	T.33 30 W	
Machine Sample of Machine	Destroite Stateum	Tildhon Lagin	27.5					
Machine Sample of Machine	Progettion (See	Operated Cl.						
Machine Sample of Machine	Gogle	Google Production libridgy	28 Apr 2010		20. Apr 20.00	the Rt		
Management of the control of	Dadediuse	Graden in Asserts Management 2.14				Ni San		
Name         Path         Name         Name <th< td=""><td>-</td><td>National Report Street Co.</td><td></td><td></td><td></td><td>200</td><td></td><td></td></th<>	-	National Report Street Co.				200		
			2018			11.0m		
Management of the control of		manuscriptor VIII	W.Jan			200 Major		
Management of the control of	Triang Value	Strakeline (SSS)	2016 2016	275	201	230	Maratte	
1968	Herman	Bargistay OperChitetly Steve 13.1	207	207	XIII	207		
1968	Palaral Vandering	opide/STF	28 Ny. 2018	21 Sep 21 S	20 By 2018		20.8sp 20.00	
1968	Gil Hilliantermi	Spat-Mallern						
1968	same Advanta	represent Politician		DAg		233 25.hap		
1968	April broadists	Assessable to Line	2018	2018		201		
1968	NORTH THE REAL PROPERTY.	Olgo hum 43	207					
1968	The Library of Company	Autoritation, Autoritation, and Assessing System, sension 1-3	2017					
1968	LREE	UNE Login	18.3an 2018					
1968	Monad	APE or Welson Street 2018	13 Avy. 2018	13.5mp 2018		TAp-2018		
1968	Manual	Anne Autor Clerolog VT	18 Mar.			t tyrill li		11 tale 2010
1968	Monad	Anne Aube Omaloy 10						Sie XS
	Manual	SP System of China VSS	8 May 2018					
	Mile							
Marcha   M	Nethone	Strail Strature Cardial Streetly	18 Steps			16.hop		
	Norman Tenansi I trabab	ACK						
	Neman Research Institute NPE Street Technologies	GeED GeeD LE						
	NET Subsect Coperation	TwiffedPelester Mesger						
1	COSTA ME	Terriffical bitrilly Mallorev I.1.0						
1	COSTANIA COSTANIA	Terriffical Striffy Mallores (3.0	28 Ayr 2011	207		20,027		
1	COMPANIE OF THE PARIE OF THE PA	Terriford Santy Malors (EE)						
	COLLAR	Terrifical birdly Mallor d 2.0	2018	2018	2008 2008	233		
	One One	One OF	2016		2006	200		
	Operatitions.	Openitions Clean						
	Cydrodistic	TeOphedDesic2	18 Out 2017	2000-207				
March   Marc	Official					10.14 3010	14.543010	
March   Marc	Prophil Prophilips	Coprodit PlayNot Proceed	18 Jan	18.im	Man			
March   Marc	Play blody	Paghasa-10	2016 10 Ayr 2016	2016 10.4p-2016	2016 10 Apr 2010	234 1.4-3/8		
March   Marc	Meghanity	Pophainan \$13	28 Aug. 2018	28 May 2018	28 Aug. 2008	28.8cp 2338		20,077
March   Marc	Play Sandy	PhyDie to Dateptor WATM						20027
Marcha   M	Posts	Please Class Proceedy 3.2 UNA	17.34 30M					
March   Marc	Program Date (MIC)	MBClink				20 San 2013		
March   Marc	Professorita? Meda	79m 933	*Again	1AqXII	21.hap 3017	The SET		
March   Marc	Read	Rend D	18 May .					
March   Marc	Notice	Replieb 230	21 CM 2000	T ON EN	E OI ES	POUR	2104201	
March   Marc	Antin Plates	MPRisCorred	13 May- 2018			23.50g- 23.55	0.00y 3044	
Made   Marke   Marke	Bilenbese	Survey 2015 National				11.10gr 2333		
Made   Marke   Marke	Mited Silverin	On Serve 23 On Serve 23						
Made   Marke   Marke	Broamhair	Smooth SPE2	28 Pole		20 Pale	Time 2016		
Made   Marke   Marke	Hydister	main stale praction	2.3m2077	Jan 277	2.3m2077	3 Jan 2017	2.iv.EC	21.iv 29
Made   Marke   Marke	Refflicts.	Bellink (KK:v10	18.Jan 2018					
Made   Marke   Marke	Syrantes	NE WHALM	13 Ou 2010			DOLEN		
Made   Marke   Marke	Tables Market	MARCHES .	27.8					
Maring (Agricum	Litterally of Change	OKCOPORING to Militable to Publish to 12 1 person 12	20 Park					
Maring (Agricum	Make	Team 1.3	2016 19 Okt 2016			ZN ZOLZE		
Maring (Agricum	Melone	Wilmed 18						
March	Valently Systems	tony top tomory CE11				2016-		
Marco   Marc	VestEll	GMP/13	28.Jen					
MacContant   March	When	Windragener CPAS	3014 38 Apr 2008	N. b. XX	58. Apr 2010	2700 UA hpr 2018		
	WhiteComple Male White	nites 20						
2004   2004	1003							
	Valued Japan	Talant & Probation &	3018 7 Ge (2016	2018 7 Geo-2018	7 Great W	T Dec 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, Filip Skokan

Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic RP	Form Post RP	3rd Party-Init 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	
Filip Skokan	node openid-client ^3.0.0	11-May-2019	11-May-2019	11-May-2019	11-May-2019	11-May-2019	11-May-2019	
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
  - 13 profiles certified for9 implementations by9 organizations
- Recent additions:
  - Actual banks!

Organization	Implementation	FAPI R/W OP w/ MTLS	FAPI R/W OP w/ Private Key
Authlete	Authlete 2.1	1-Apr-2019 [view]	1-Apr-2019 [view]
Cater Allen	CA Open Banking v1.3.0		4-Sep-2019 [view]
Coutts & company	F23		27-Sep-2019 [view]
Curity	Curity Identity Server 4.3.0	20-Sep-2019 [view]	20-Sep-2019 [view]
Filip Skokan	node oidc-provider ^6.5.0	20-Aug-2019 [view]	20-Aug-2019 [view]
ForgeRock	ForgeRock Financial 3.1.0-credence		1-Apr-2019 [view]
Ozone	Ozone Sandbox v3.1	6-Jun-2019 [view]	6-Jun-2019 [view]
Ping Identity	PingFederate 9.2.3	29-May-2019 [view]	
Sainsbury's Bank PLC	Sainsbury's Bank Digital IAM Platform (version 19.8.8)		9-Aug-2019 [view]

#### FAPI-CIBA OP Certifications



- FAPI-CIBA OP Certifications at https://openid.net/certification/#FAPI-CIBA OPs
  - 3 profiles certified for
    - 1 implementation by
    - 1 organization
- Recent additions:
  - Authlete first to certify

Organization	Implementation	FAPI-CIBA OP poll w/ MTLS	FAPI-CIBA OP poll w/ Private Key	FAPI-CIBA OP Ping w/ MTLS	FAPI-CIBA OP Ping w/ Private Key
Authlete	Authlete 2.1	16-Sep-2019 [view]	16-Sep-2019 [view]	16-Sep-2019 [view]	16-Sep-2019 [view]

# 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 <a href="https://op.certification.openid.net/">https://op.certification.openid.net/</a> or <a href="https://www.certification.openid.net/">https://www.certification.openid.net/</a>
- 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 <a href="https://openid.net/certification/">https://openid.net/certification/</a>

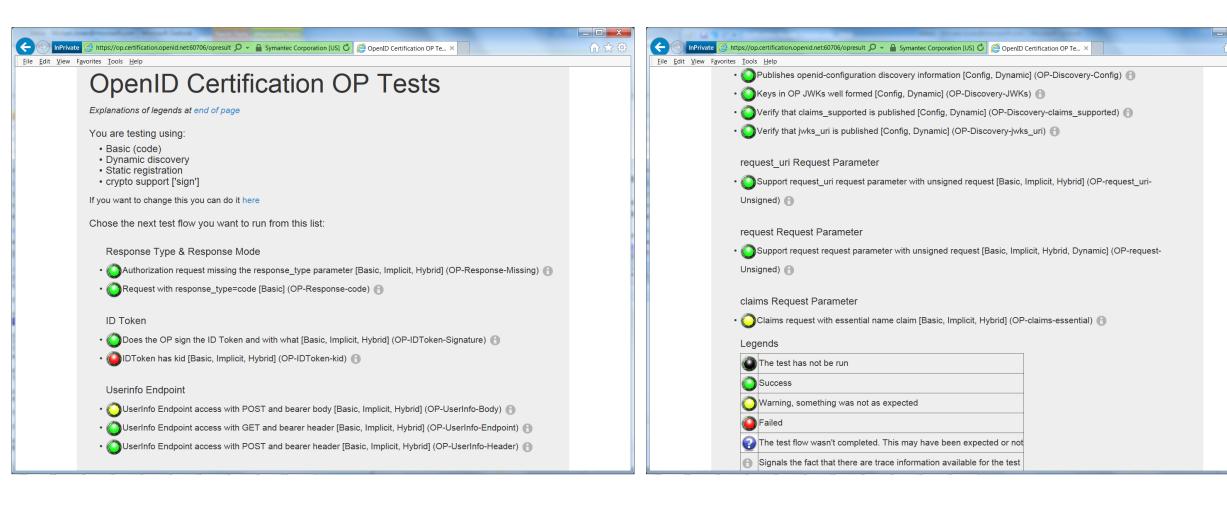
# What does certification cost?



- Not a profit center for the OpenID Foundation
  - Fees there to help cover costs of operating certification program
- Member price
  - **-** \$500
- Non-member price
  - **-** \$2500
- New profiles in pilot mode are available to members for free
- Costs described at <a href="https://openid.net/certification/fees/">https://openid.net/certification/fees/</a>

# **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 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.
- 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 Gez Ladas	1
Date: Apr. 10 2015	

# How does certification relate to interop testing?



- OpenID Connect held 5 rounds of interop testing see <a href="http://osis.idcommons.net/">http://osis.idcommons.net/</a>
  - 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 to exit pilot mode
  - RP-Initiated Logout, Session Management, Front-Channel Logout, Back-Channel Logout
  - Refresh Token Behaviors
- Additional FAPI profiles being developed:
  - FAPI-CIBA OP just launched
  - FAPI RP
  - 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