OpenID Connect:
News, Overview, Certification, and Action Items

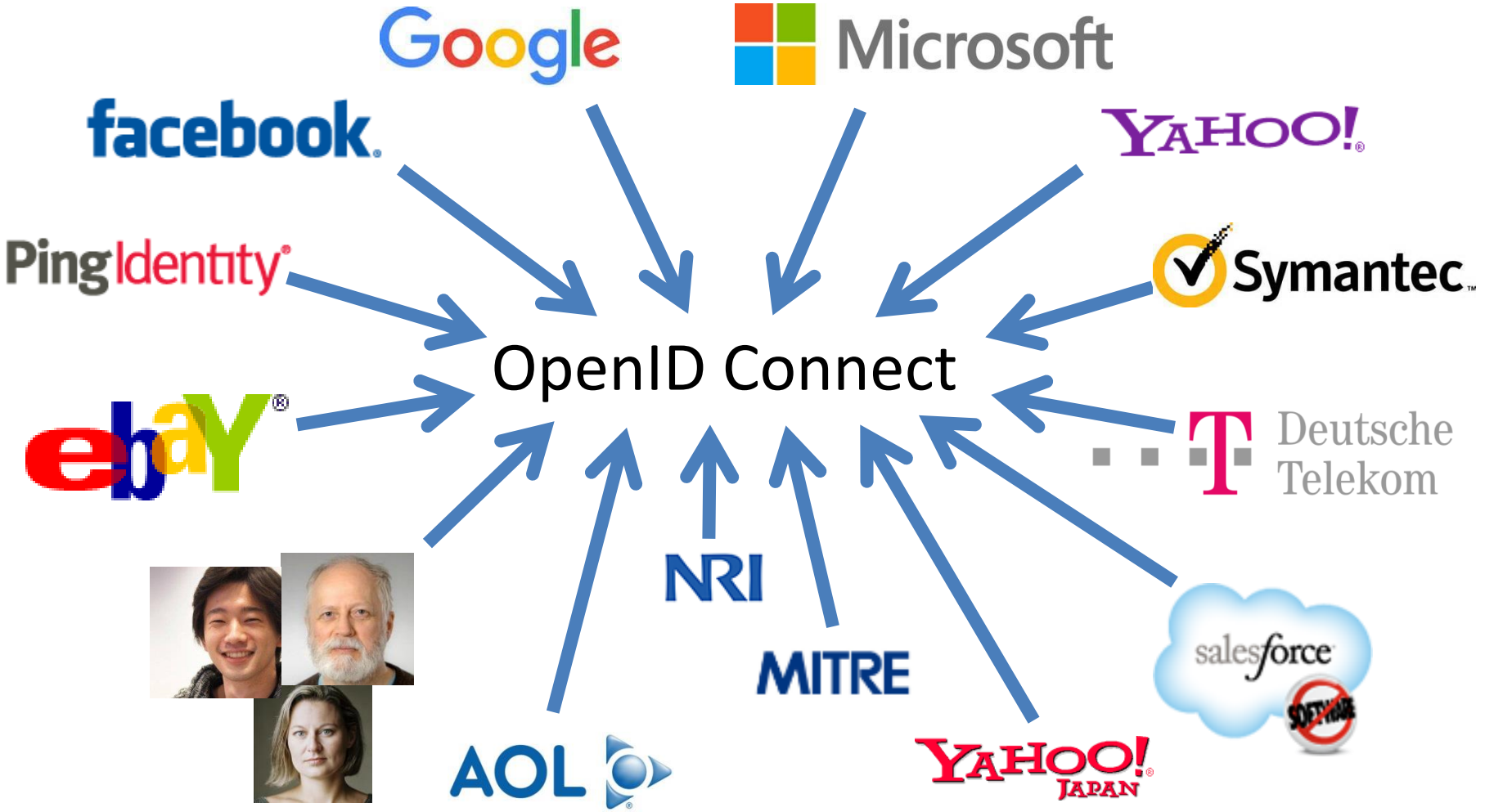
June 24, 2018

Michael B. Jones

Identity Standards Architect – Microsoft

Working Together

OpenID



What is OpenID Connect?

- Simple identity layer on top of OAuth 2.0
- Enables relying parties to verify identity of end-user
- Enables relying parties to obtain basic profile info
- REST/JSON interfaces → low barrier to entry
- See http://openid.net/connect/

You're Probably Already Using OpenID Connect

- If you log in at AOL, Deutsche Telekom, France Connect, Google, Microsoft, mixi, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan or have an Android phone, you're already using OpenID Connect
- Many other sites and apps large and small use OpenID Connect
- OpenID Connect "brand" typically not exposed to end-users

Design Philosophy

OpenID

Keep Simple Things Simple

Make Complex Things Possible

OpenID Connect Range

- Spans use cases, scenarios
  - Internet, Enterprise, Mobile, Cloud
- Spans security & privacy requirements
  - From non-sensitive information to highly secure
- Spans sophistication of claims usage
  - From basic default claims to specific requested claims to collecting claims from multiple sources
- Maximizes simplicity of implementations
  - Uses existing IETF specs: OAuth 2.0, JWT, etc.
  - Lets you build only the pieces you need

Numerous Awards

- OpenID Connect won 2012 European Identity Award for Best Innovation/New Standard
- OAuth 2.0 won in 2013
- JSON Web Token (JWT) & JOSE won in 2014
- OpenID Certification program won 2018 Identity Innovation Award at IDnext
- OpenID Certification program won 2018 European Identity Award for Best Innovation

- *See blog posts at* http://openid.net/

New OpenID Connect Projects

Hot Off the Presses and with Action Items!

JWTConnect RP Libraries

- Google is commissioning creation of high-quality RP libraries
- Intended to be full-functioned and pass OpenID Certification
- Libraries are being donated to OpenID Connect working group
- Initial languages:
  - Python: Finished, certified, and contributed to working group
  - Java: Work in progress
  - JavaScript: Work in progress
- Not the first software projects of the Connect working group
  - The AppAuth libraries are also working group projects

Structure of JWTConnect Libraries

- Each language structures the RP library as four components
  - CryptoJWT
    - JSON Web Token (JWT) implementation and underlying cryptography
  - OidcMsg
    - Serializing, deserializing, and verifying messages + key handling
  - OidcService
    - OpenID Connect request/response pattern, client authentication, binding messages to service endpoints
  - OidcRP
    - OpenID Connect Relying Party (RP) API, bringing all the parts together

Python JWTConnect Implementation

- Python JWTConnect implementation uses 4 GitHub projects
  - https://github.com/openid/JWTConnect-Python-CryptoJWT
  - https://github.com/openid/JWTConnect-Python-OidcMsg
  - https://github.com/openid/JWTConnect-Python-OidcService
  - https://github.com/openid/JWTConnect-Python-OidcRP

Python JWTConnect Instructions

- See the documentation
  - http://oidcrp.readthedocs.io/en/latest/
- See sample RPs
  - https://github.com/openid/JWTConnect-Python-OidcRP/tree/master/chrp
  - Has example configurations for Facebook, GitHub, Google, LinkedIn, Microsoft, Okta, Ping Federate, and Salesforce

- ***Action Item: Give Python JWTConnect a try!***

Form Post Response Mode Certification

- New pair of OpenID Certification profiles being launched at Identiverse
  - OpenID Provider supporting Form Post Response Mode
  - Relying Party supporting Form Post Response Mode
- Tests OP and RP support for
  - OAuth 2.0 Form Post Response Mode
  - http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html

What the Form Post Tests Do

- The conformance tests verify that
  - when `response_mode=form_post` parameter used
  - responses are returned as HTML form parameters using HTTP `POST`
  - Instead of as fragments or query parameters
- Tests cover both success replies and error replies

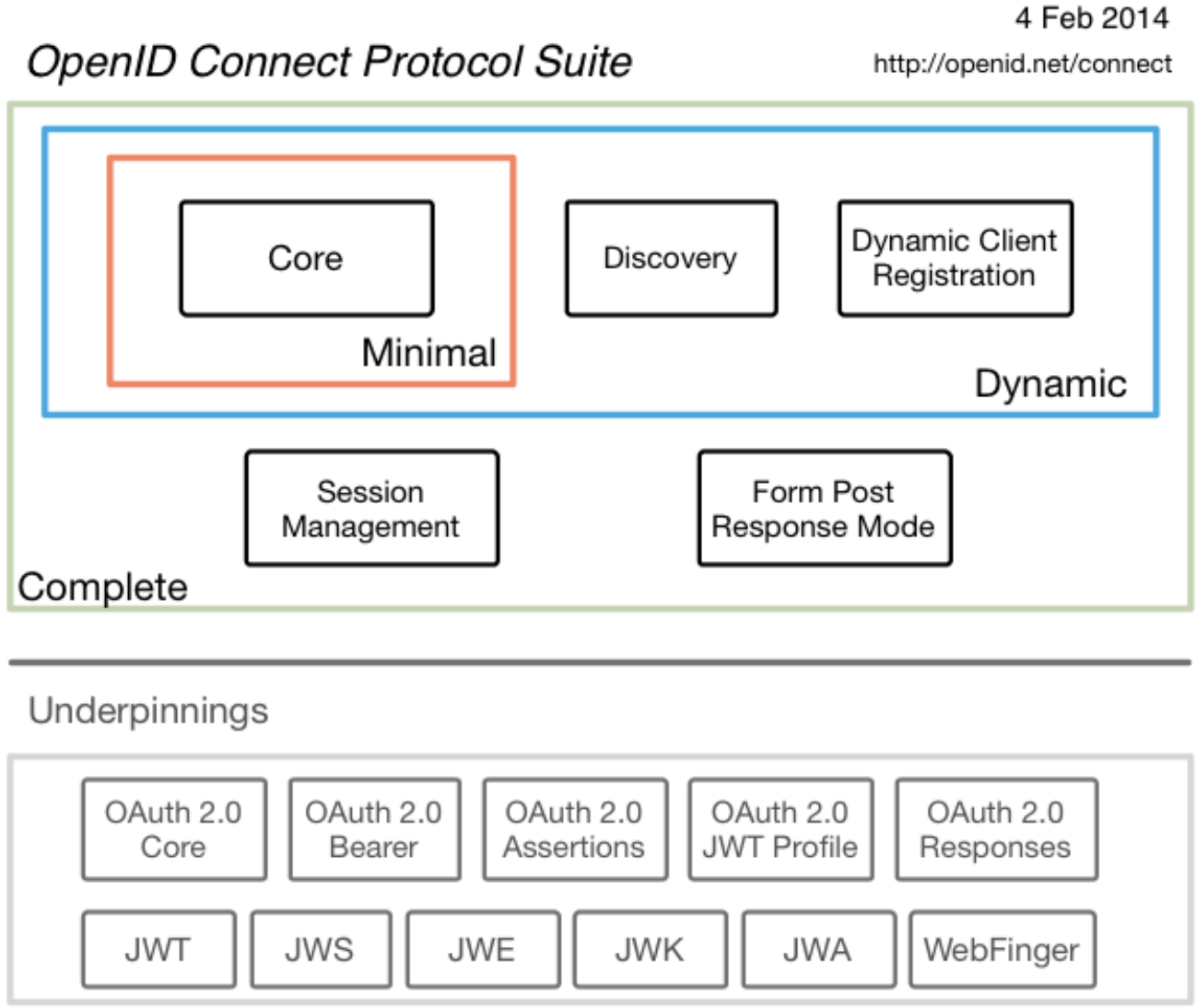
Testing the Tests

- Form Post Response Mode certification tests are ready to test
- These profiles currently in pilot mode
  - OpenID Foundation members can certify against them for free
- There's a checkbox to add these tests to your OP testing config
- See the testing instructions at http://openid.net/certification/

- ***Action Item: Test the tests and certify your implementations!***

OpenID Connect Specifications

Specifications when finalized in 2014



Session Management / Logout (work in progress)

- Three approaches being pursued by the working group:
  - Session Management
    - http://openid.net/specs/openid-connect-session-1_0.html
    - Uses HTML5 postMessage to communicate state change messages between OP and RP iframes
  - Front-Channel Logout
    - http://openid.net/specs/openid-connect-frontchannel-1_0.html
    - Uses HTTP GET to load image or iframe, triggering logout (similar to SAML, WS-Federation)
  - Back-Channel Logout
    - http://openid.net/specs/openid-connect-backchannel-1_0.html
    - Server-to-communication not using the browser
    - Can be used by native applications, which have no active browser
- Unfortunately, no one approach best for all use cases
  - Can be used separately or in combination
- Recent decision made that it's time for them to become Final Specifications
  - ***Action item: Review these specifications now before we vote them to Final status!***

Federation Specification (work in progress)

- OpenID Connect Federation specification
  - http://openid.net/specs/openid-connect-federation-1_0.html
- Enables establishment and maintenance of multi-party federations using OpenID Connect
- Defines hierarchical JSON-based metadata structures for federation participants
- In 45-day review period to become an Implementer's Draft
  - http://openid.net/2018/06/08/public-review-period-for-openid-connect-federation-specification-started/
  - ***Action item: Review the Federation specification!***

Second Errata Set (work in progress)

- Errata process corrects typos, etc. discovered
  - Makes no normative changes
- Edits under way for second errata set
- See http://openid.net/specs/openid-connect-core-1_0-23.html for current Core errata draft
- Waiting for OAuth Authorization Server Metadata spec draft-ietf-oauth-discovery to be final
  - So we can register OpenID Discovery metadata values
  - In Auth48 with the RFC Editor, so should finish any day now
- Expect to see a request for review of errata changes shortly

OpenID Certification

OpenID Certification

- OpenID Certification enables OpenID Connect implementations to be certified as meeting requirements of defined conformance profiles
- Mature OP and RP 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
- Be among the first to test these new Certification profiles!
  - Form Post Response Mode for OP and RP
- See http://openid.net/certification/ and http://openid.net/certification/faq/

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

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

Who has achieved OP Certification?

- OpenID Provider certifications at http://openid.net/certification/#OPs
  - 189 profiles certified for 63 implementations by 53 organizations
- Recent additions:
  - CA, GSMA, Identity Automation, Microsoft, OGIS-RI, Oracle, Recruit, VMware, WidasConcepts, 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 12.6	9-Apr-2016	4-Jan-2018			
Clarelly 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	
Classemethod	Barista v1.18.2	9-Nov-2017			9-Nov-2017	
Cloudentity	Cloudentity OIDC services 1.3	16-Aug-2017			16-Aug-2017	16-Aug-2017
ConnectId	ConnectId 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	22-Apr-2015	15-Apr-2015	
GSMA	Mobile Connect Reference Implementation v2.3	16-May-2016				
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	Bioncryptology 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-2016			12-Jan-2016	
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-2016	13-Sep-2016		7-Apr-2016	
Microsoft	Azure Active Directory				8-Apr-2016	
Microsoft	IEF Experimental Claimer V0.9	9-May-2018			9-May-2018	
Mvine	Mvine Federated Identity Hub v1	1-Aug-2017				
NEC	NC7000-3A-OC	7-Mar-2016				
Nomura Research Institute	pipeOIDC	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015
Nomura Research Institute	UHI-ID	10-Apr-2015				
NRI SecureTechnologies	UHI-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	
OGIS-RI	ThemiStruct Identity Platform v2.0.0	5-Mar-2018	5-Mar-2018		5-Mar-2018	
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			
Oracle	Oracle Identity Cloud Service 16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	
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	8-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	
Recruit	Recruit ID	16-May-2018				
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	
VMware	Workspace ONE	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	
WidasConcepts	oidcsas 2.0	11-Apr-2018	19-Apr-2018	16-Apr-2018	11-Apr-2018	
Mattias Wolloski	Auth0	6-Feb-2016			8-Feb-2016	
WSO2	Identity Server 5.4.0	16-Jan-2018	16-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
  - 54 profiles certified for 20 implementations by 16 organizations
- Recent additions:
  - Roland Hedberg (for Python JWTConnect), KSIGN, Filip Skokan

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
Roland Hedberg	oidcrp 0.4.0	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-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				
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
Filip Skokan	node openid-client ^2.0.0	12-Apr-2018	12-Apr-2018	12-Apr-2018	12-Apr-2018	12-Apr-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

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/

New Work by Related Working Groups

MODRNA Working Group

- **M**obile **O**perator **D**iscovery, **R**egistration & authen**tica**tion (MODRNA)
- http://openid.net/wg/mobile/
- OpenID Connect profile for Mobile Network Operators (MNOs)
- Lets you easily sign in from your phone
- Currently 4 Implementer's Drafts + 2 other drafts
- Specs used by GSMA's Mobile Connect deployments

HEART Working Group

- Health Relationship Trust (HEART)
- http://openid.net/wg/heart/
- Profiles for healthcare data exchange
- Currently 5 Implementer's Drafts

iGov Working Group

- International Government Profile (iGov)
- http://openid.net/wg/igov/
- Profile for government & high-value commercial applications
- Currently two drafts
  - International Government Assurance Profile (iGov) for OpenID Connect 1.0
  - International Government Assurance Profile Use Cases
- Implementer's Draft coming soon

EAP Working Group

- Enhanced Authentication Profile (EAP)
- http://openid.net/wg/eap/
- Two drafts:
  - Token Binding for ID Tokens
  - Integration with phishing-resistant authentication such as FIDO
- Implementers drafts coming soon

FAPI Working Group

- Financial-grade API (FAPI)
- http://openid.net/wg/fapi/
- Enables secure access to financial information
- Currently two Implementer's Drafts
  - read-only access
  - read-write access
- 3 more specs in 5 part series being worked on

RISC Working Group

- Risk and Incident Sharing and Coordination (RISC)
- http://openid.net/wg/risc/
- Voting to approve three Implementer's Drafts under way
  - OpenID RISC Profile of IETF Security Events 1.0
  - OpenID RISC Event Types 1.0
  - OAuth Event Types 1.0

- ***Action Item: Participate in the members vote before Friday at https://openid.net/foundation/members/polls/141***
  - ***Can join OIDF for $25 at https://openid.net/foundation/members/***

Where can I participate & learn more?

- OpenID Blog
  - http://openid.net/
- OpenID Connect Page
  - http://openid.net/connect/
- OpenID Working Groups
  - http://openid.net/wg/
- OpenID Certification
  - http://openid.net/certification/
- OpenID Twitter Feed
  - @openid
- My Blog
  - http://self-issued.info/
- My Twitter Feed
  - @selfissued
- E-mail me
  - mbj@microsoft.com