

Introduction to OpenID Connect

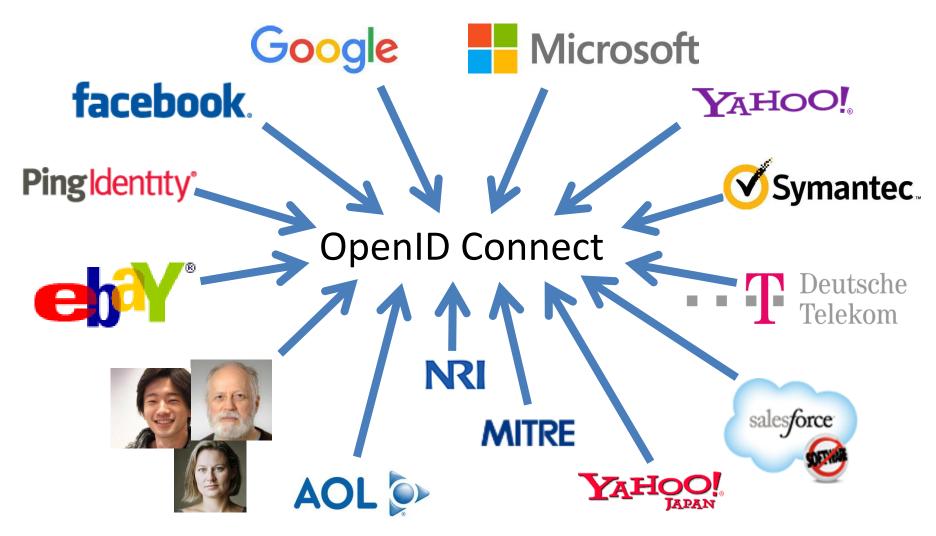
April 30, 2019

Michael B. Jones

Identity Standards Architect – Microsoft

Working Together





What is OpenID Connect?



- Simple identity layer on top of OAuth 2.0
- Enables Relying Parties (RPs) to verify identity of end-user
- Enables RPs to obtain basic profile info
- REST/JSON interfaces → low barrier to entry
- Described at https://openid.net/connect/

You're Probably Already Using OpenID Connect! OpenID



- If you have an Android phone or log in at AOL, Deutsche Telekom, Google, Microsoft, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan, you're already using OpenID Connect
 - Many other sites and apps large and small also use OpenID Connect

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
 - http://openid.net/2012/04/18/openid-connectwins-2012-european-identity-and-cloud-award/
- OAuth 2.0 won in 2013
- JSON Web Token (JWT) & JOSE won in 2014
- OpenID Certification program won 2018 Identity Innovation Award
- OpenID Certification program won 2018 European Identity Award



Presentation Overview



- Introduction
- Design Philosophy
- Timeline
- A Look Under the Covers
- Overview of OpenID Connect Specs
- More OpenID Connect Specs
- OpenID Certification
- Resources

Design Philosophy



Keep Simple Things Simple

Make Complex Things Possible

Keep Simple Things Simple



UserInfo endpoint for simple claims about user

Designed to work well on mobile phones

How We Made It Simple



- Built on OAuth 2.0
- Uses JavaScript Object Notation (JSON)
- You can build only the pieces that you need

• Goal: Easy implementation on all modern development platforms

Make Complex Things Possible



Encrypted Claims

Aggregated Claims

Distributed Claims

Key Differences from OpenID 2.0



- Support for native client applications
- Identifiers using e-mail address format
- UserInfo endpoint for simple claims about user
- Designed to work well on mobile phones
- Uses JSON/REST, rather than XML
- Support for encryption and higher LOAs
- Support for distributed and aggregated claims
- Support for session management, including logout
- Support for self-issued identity providers

OpenID Connect Timeline



- Artifact Binding working group formed, Mar 2010
- Major design issues closed at IIW, May 2011
 - Result branded "OpenID Connect"
- 5 rounds of interop testing between 2011 and 2013
 - Specifications refined after each round of interop testing
- Won Best New Standard award at EIC, April 2012
- Final specifications approved, February 2014
- Errata set 1 approved November 2014
- Form Post Response Mode spec approved, April 2015
- OpenID 2.0 to Connect Migration spec approved, April 2015
- OpenID Provider Certification launched, April 2015
- OpenID Federation spec work begun, July 2016
- Relying Party Certification launched, December 2016
- Logout Implementer's Drafts approved, March 2017
- OpenID Certification program won awards in March 2018 and April 2018
- OpenID Connect for Identity Assurance spec work begun, March 2019

A Look Under the Covers



- ID Token
- Claims Requests
- UserInfo Claims
- Example Protocol Messages

ID Token



- JWT representing logged-in session
- Claims:
 - iss Issuer
 - sub Identifier for subject (user)
 - aud Audience for ID Token
 - iat Time token was issued
 - − exp − Expiration time
 - nonce Mitigates replay attacks

ID Token Claims Example



```
"iss": "https://server.example.com",
"sub": "248289761001",
"aud": "0acf77d4-b486-4c99-bd76-074ed6a64ddf",
"iat": 1311280970,
"exp": 1311281970,
"nonce": "n-0S6_WzA2Mj"
```

Claims Requests



- Basic requests made using OAuth scopes:
 - openid Declares request is for OpenID Connect
 - profile Requests default profile info
 - email Requests email address & verification status
 - address Requests postal address
 - phone Requests phone number & verification status
 - offline access Requests Refresh Token issuance
- Requests for individual claims can be made using JSON "claims" request parameter

UserInfo Claims



- sub
- name
- given name
- family_name
- middle name
- nickname
- preferred username
- profile
- picture
- website

- gender
- birthdate
- locale
- zoneinfo
- updated at
- email
- email verified
- phone number
- phone number verified
- address

UserInfo Claims Example



```
"sub": "248289761001",
"name": "Jane Doe",
"given name": "Jane",
"family name": "Doe",
"email": "janedoe@example.com",
"email verified": true,
"picture": "http://example.com/janedoe/me.jpg"
```

Authorization Request Example



```
https://server.example.com/authorize
?response_type=id_token%20token
&client_id=0acf77d4-b486-4c99-bd76-074ed6a64ddf
&redirect_uri=https%3A%2F%2Fclient.example.com%2Fcb
&scope=openid%20profile
&state=af0ifjsldkj
&nonce=n-0S6_WzA2Mj
```

Authorization Response Example



```
HTTP/1.1 302 Found
Location: https://client.example.com/cb
#access_token=mF_9.B5f-4.1JqM
&token_type=bearer
&id_token=eyJhbGzI1NiJ9.eyJz9Glnw9J.F9-V4IvQ0Z
&expires_in=3600
&state=af0ifjsldkj
```

UserInfo Request Example



GET /userinfo HTTP/1.1

Host: server.example.com

Authorization: Bearer mF_9.B5f-4.1JqM

OpenID Connect Specs Overview

JWT

JWS

JWE



4 Feb 2014 OpenID Connect Protocol Suite http://openid.net/connect Dynamic Client Core Discovery Registration Minimal Dynamic Form Post Session Response Mode Management Complete Underpinnings OAuth 2.0 OAuth 2.0 OAuth 2.0 OAuth 2.0 OAuth 2.0 JWT Profile Core Bearer Assertions Responses

JWK

JWA

WebFinger

Additional Final Specifications (1 of 2) OpenID

- OpenID 2.0 to OpenID Connect Migration
 - Defines how to migrate from OpenID 2.0 to OpenID Connect
 - Has OpenID Connect identity provider also return OpenID 2.0 identifier, enabling account migration
 - http://openid.net/specs/openid-connect-migration-1 0.html
 - Completed April 2015
 - Google shut down OpenID 2.0 support in April 2015
 - Yahoo, others also plan to replace OpenID 2.0 with OpenID Connect

Additional Final Specifications (2 of 2) OpenID

- OAuth 2.0 Form Post Response Mode
 - Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values auto-submitted by the User Agent using HTTP POST
 - A "form post" binding, like SAML and WS-Federation
 - An alternative to fragment encoding
 - http://openid.net/specs/oauth-v2-form-post-response-mode-1 0.html
 - Completed April 2015
 - In production use by Microsoft, Ping Identity

Session Management / Logout (works in progress)



- Three approaches specified by the working group:
 - Session Management
 - https://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
 - https://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
 - https://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
- All support multiple logged in sessions from OP at RP
- Unfortunately, no one approach best for all use cases
- Certification tests being developed
 - WG plans to test multiple implementations before making specs Final

Federation Specification (work in progress)



- OpenID Connect Federation specification
 - https://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
- Implementer's Draft status reached
- Substantial changes since then
 - Please review!

Identity Assurance Specification (work in progress)



- OpenID Connect for Identity Assurance
 - https://openid.net/specs/openid-connect-4-identity-assurance.html
- Representation for verified person data
 - Enables legal compliance for some use cases
- New specification by Torsten Lodderstedt
 - Please review!

What is OpenID Certification?



- Enables OpenID Connect and FAPI implementations to be certified as meeting the requirements of defined conformance profiles
 - Goal is to make high-quality, secure, interoperable OpenID Connect implementations the norm
- 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 OpenID



- 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

OpenID Connect OP Certifications



- OpenID Provider certifications at https://openid.net/certification/#OPs
 - 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

Access Regional Multiple Listing	hatenida.	Select		*****			Para Paul
State	hylometallar	Asiete	heplad Of	House	Cudyor	Opening	*
	MRX 14+4/252	2018					
ARC	Add	20 May 2018					DAy 201
Addition	Author 11 Author 657	10.14.001					
Control See S See S See	Methodoxical class	10.14 2000 0.14 2000					
Denna See & Seak Sho	Methdored	8 May 2018 10 Chin 2018 10 Mai 2018 20 Jan 2017	10000	6 May 2003 10 One 2016 10 May 2016	130m		
		2018 13 Mar	201	2008 10 Mar	230		
Opril Brook Hills	CBOLLey	2018	2018	2010	016a 228 23.km 227		
DA .	CLM Gavey Clistic IM Gavey	20.len 2017	186-27	156×2017			
EA	0.8yh8y0:083						
Cheese hashing of Barrens, SNCM	DIDWA George (1)		20 Mar 20 M 20 Ann 20 M				
Clarify Streety	Strilly Provider of Cl.d.				25.5an 2251 3.5au 2018		
Gastira.	Clantick CorClab 2018 Serbins 1, 163	314+308					
Generalisal	Setting 1 M3	Side SET Side SET Side SET Side SET SIDE SET FAMILIES SER SES SES SES SES SES SES SES SES S			61ko 3017 55.kap 2217		
Goaletty	Gradelly OEC senior, 13	207			35.hap 237	18.Aug 2017	
Declarate	W-60	27 Aug					
Germille	Germaliki Rever 6 Lila	2.4m207					
Date	Cuty birtly Serve 23.1	20 Dec	Sides 200m 2017		200m		
COMC	mp40				200m 2017 1 A43018 2018 2018		
GCMC	Tables Legis						
Destroire Soldone Progettina	Question Copin	3018 13 Ayr 2003			210 U-p-270		
	Questili D. Cha Street 3.1.3						
Graph Graph	Classificate 3.1.3 Classific Probability Classific 1.0	18.34 2011 28.4y 2011 6.7y 2011					
OnlineThilitys							
Controlliner	Ginder in Assess Management 2.1.a	0.00×2000	1 No. 27	6 No. 27 W	30 Since 2238		
comm	Note Green Schools Ingless below 43	18 May-					
They blind		30'8 1 On 200					
Trimy Value	Single Street VIII						
They laked	Strakklandy-Berner 10.0.0	19 Jan 2016 21 May 2017 20 July 2018 2 Cha 2018 10 July 2018		10.3m 2011 10.May 2017 20.May 2010 2010 2010 2010 2010	200 9.30 200 207 207 209 200 200	May dow	
	Resident Confession Street 111	21 May	10.2m 210 210 217 213 210 210 210	St.May.	21 May		
	and the same of th	2017	2017	2017	207		
Nation/Yeslang	ppiik-0.77					20.0kg 20.0kg	
GPMIntend	Spati Mellers	3 (34 300)	2-0w/2518	3-014 3010	8-0w 30 H		
Medig Subrestien	Republically Protestion	10.les 2018					
) Spirit benedities.	Assertation USE	25 Ap 278 17 Ma 287 15 May 287 15	20 Aug		25 hap		
		2018	2018		230		
NOMEN .	10kgo Assens 4.0	207					
To Chap of Corpora	Authorization, Authorization, and Assauling System, sension 1.0	13 May .					
LPRE	What						
		2018 23 Barr	-				
Monadi	APE or Western Bross 2018	2018			TApZII		
Monet	Anan Adve Clinical VII	18 Mar			tip 20		11 Nov 277
Money	Anus Autus Chrokey VIII						
Money							
Moter	Mine Probability Sales 1						
MIC	NOTED IN CIC	7 May 30 W 18 Rep. 2018					
NewPerson	Sinsi Namur Carbol Strolly	18 Alejo					
Norman Research Smillsder	9000	10 Apr 2010					
Norman Research Shellhale	pycoc SHD SHEUlas U	18 Ay 2011					
ME Brown Statesdages	GHELIMA LE	28 Au 2017 28 Au 2017 7 Ou 2016	28.3an 28.3an 2017 1 On 2016	36.34.3017 36.344 3017			
MT Balleon Corporation	Trailin/Pointire Marager	207					
COST PE	Terriforal Methy Mallerey (1.10		TOWER		TOURS		
COSTA ME	Terriford Melly Mallers 13.0	28 Apr 2011	25 Way 2017		36.5p. 30.0		
CORNE	Tendinal Melly Males 450	25 Nov. 2018 25 Nov. 2018 26 May 2018 5 Nov. 2018	200-200 200- 200 200 200 200 200		200-200 200- 200 200- 200 200-		
COST. FE	Tendinal Melly Malare 020	20 Nov.		20 New 2018 20 May 2016			
no.	00.00	28 May	20 May	20 May .	20 May		
	OLD P						
OpenStitutes.	Oregin Greeni ED OpenNers Clauf						
Dybrud Mil	TwOptro#Soul 62		20-5a-201				
Deale DRY-Deale	Onde Metally Grad Strate Wildyr 2018 ONE Hydray LLD						
Popular Popular	Off Hydrov LES Engine ProPisi				11421		
	Personal Property Communication Communicatio		18 Jan	95.Jan			
Property and the second state of the second st			19.3an 2010			H-lav-DER	
			18.3m 2018 13.4p 27.0 28.3mp	Main EM Valyr EW Staley		Malan (ES)	
			10.3m 2010 10.4p 2010 20.8p 2010	19.3an 2016 13.4pc 2010 26.8ep 2018		Mark III	24-71
Pleased light Play bloodly Play bloodly Play bloodly	Proposition ST Programme ST To ST		19.3m 2018 10.4p-2019 2038 2038 2038 2038	10 Jan 2006 10 Apr 2010 20 Apr 2008 20 Apr 2008	218-y 228 228 234 235 235	H.iardEB	24-27 24-27
	Proceedii Proglindonici 830 Proglindonici 933 Proglindonici 933 Proglindonici 933 Prodd Charles Educator 938 188 Prodd Charles Procedy 22 1886	19 Jan 2010 10 Apr 2020 20 Apr 2018 20 Apr 2018 20 Apr	10.5m 200 10.4p 200 203 203 204 200	10.5m 200 10.4p 2010 20.8p 2010 2010 2010	218-y 228 228 234 235 235	H.iar-SER	2.6-y 271
Pleased light Play bloodly Play bloodly Play bloodly	Proposition ST Programme ST To ST		11.3m 200 11.4p 200 20.3p 200 200 200	10.3m 200 10.4p 2010 20.8p 2010 2010 2010		H.lav.EU	Ray III
Pleased light Play bloodly Play bloodly Play bloodly	Proced Profinded SI Profinded SI Profinded SI Profinded SI Profit Gardynamy SI Profit	18 Jan 2016 10 Apr 2016 20 Jap 2018 20 Pub 2018 17 Jan 2018 23 Chi 2018	11.5m 200 10.4p-200 20.8p- 200 200 200 7.6p-200	W. Jan 2006 V. Apr 2000 2006 2006 2000 P. Aug	1.4p 210 28.8p 231 254 255 255	H.lar XVIII	21.5-y 211
Personal Apil Prog Sanday Prog Sanday Prog Sanday Prostal Prosent Visido Codine (PRECO) Productorida I Sanda	Present Population III Population Populat	18 Jan 2018 18 Ay 2018 26 By 2018 28 Pels 2018 27 Au 2018 25 Cor 2018	19.5m 2018 10.5p-2019 2018 2018 2018 10.5m 10.5m	M.Jan 2006 Vi.Apr.2010 2006 2006 2006 D.Aug 2007	1.1p-2110 28.3by 2001 2001 2001 2010 2010	Mardin	Blay St
Pleased light Play bloodly Play bloodly Play bloodly	Mercald MagNation ESI MagNation ESI MagNation ESI Master M	18 Jan 2018 18 Ay 2018 26 By 2018 28 Pels 2018 27 Au 2018 25 Cor 2018	10.5m 2010 10.4p 2010 20.3m 2010 2010 7.4m 2010	Mulan 2006 Vulge 2008 2008 2008 2008 2009 2009 2009 2009	1.1p-2110 28.3by 2001 2001 2001 2010 2010	19.5ar-3019	28-y 271
Personal Apil Prog Sanday Prog Sanday Prog Sanday Prostal Prosent Visido Codine (PRECO) Productorida I Sanda	Personal Programme 10.3 Prog	18 Jan 2018 18 Ay 2018 26 By 2018 28 Pels 2018 27 Au 2018 25 Cor 2018	10.5m 200 10.5p 200 20.5p 200 200 7.5p 200	10.3m 200 200 200 200 200 200 200 200 200 20	1.0 p. 270 270 270 270 270 270 270 7.0 p. 277	Harden 31 October	2.5 ₉ .27
Proceedings Prog Sending Prog Sending Prog Sending Prog Sending Proceeding Pr	Proceed To Programme To To Programme To To Programme To To Programme To	18 Jan 2018 18 Ay 2018 26 By 2018 28 Pels 2018 27 Au 2018 25 Cor 2018	10.00 100 10.4p 200 20.8p 201 201 201 201 201 201 201 201 201 201	Mulan Edit Vulgo 2008 2008 2008 2008 2008 2008 2008 2008	10 (p. 270) 20 (p. 200) 20 (p.	H-landER	Bay St
Personal Apil Prog Sanday Prog Sanday Prog Sanday Prostal Prosent Visido Codine (PRECO) Productorida I Sanda	Personal Programme 10.3 Prog	18 Jan 2016 10 Apr 2016 20 Jap 2018 20 Pub 2018 17 Jan 2018 23 Chi 2018	State St	M. Jan 2006 V. Apr 2006 St. Bep 2006 2016 2016 2016 2016 2017	1.0 p. 270 270 270 270 270 270 270 7.0 p. 277	31 Ox 2010 Charge 2010	BAG ST
Proceedings Prog Sending Prog Sending Prog Sending Prog Sending Proceeding Pr	Amend Tophysion In Co. Polyhysion In Co. Polyhysion In Co. Polyhysion In Co. Polyhysion In Co. Polyholida In Co. Polyhol	19. Jun 200 20 Jun 200 20 Jun 200 20 Jun 200 20 Car 20 20 Car 20 2	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	SI OUSTIN	2.5 ₉ 21
Proceedings Prog Sending Prog Sending Prog Sending Prog Sending Proceeding Pr	Proceed To Programme To To Programme To To Programme To To Programme To	19. Jun 200 19. Ju	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	21 Co 2010 Chap 2010 S. A. 2010 N. Co 2017	21.0-y 271
Proceedings Prog Sending Prog Sending Prog Sending Prog Sending Proceeding Pr	Total Conference Confe	19. Jun 200 19. Ju	9.5s 200 10a/233 25a/233 27a 27a 27a 27a 27a 27a 27a 27a 27a 27a	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	JI Col JUN (186y 200 3 Ad JUN (100s JUN	2.6 ₉ .21
Proceedings Prog Sending Prog Sending Prog Sending Prog Sending Proceeding Pr	Named Polymere 10.1 Polymere 1	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	10.5m (200 Chys 200 C	10 (p. 270) 20 (p. 200) 20 (p.	JI OADEN UMBy 200 2 ALEN MOADEN	SACTION STATES
Peace of Apil Pe	Total Conference Confe	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	31 Ox 30 W 10 Ox 30 W 20 X 20 X	Shy Si
Peace of Apil Pe	America Angliname (1) Anglinam	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	J. Col. 2019 J. Co	Shy Si
Page 10 (1) Page 1	Anada Anada	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	33 GASEN Usesy 200 2-AASEN 3-AASEN 3-AASEN	ZA-ZI
Amount ly II Proposition of Proposit	American Company Compa	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	J.J. Col. 2019 United States J. Add 2019 J. Add 2019 J. Add 2019 J. Add 2019 J. Add 2019	20-21 20-21 5422 24-20
Page 10 (1) Page 1	Marie Manganani	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	JJ CAZEN Using 200 JAJ 200 Using 200 JAJ 200 Using 200 JAJ 200	24-21 24-21 24-21
Amend Apl Proposition Proposit	Name **Speciments** **Specim	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	3.1 Gal 2010 Unitary 2.00 2.00 2.00 2.00 2.00 2.00 2.00 2.0	20-21 20-21 20-21
Amount ly II Proposition of Proposit	Facility	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	J. GALETY J. J. GALETY J. J. J. GALETY J. J. J. GALETY	SAUST
Amend Apl Proposition Proposit	Name **Speciments** **Speciments** **Addressive of the Control	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	10 (p. 270) 20 (p. 200) 20 (p.	Mulecille Michaelle Juliani Julia Julia Julia Julia Julia Julia Julia Julia Ju	RADE RADE RADE RADE RADE RADE RADE RADE
Amend Apl Proposition Proposit	Name **Speciments** **Speciments** **Addressive of the Control	19. Jun 2009 10. J	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	14y 200 204y 204 205 205 205 205 206 206 206 206 206 206 206 206 206 206	31 Ga 37 ti Gray 27 ti S.M. 27 ti Mickel 27 Ti	Shy Si
Personal (III) Pergelating Per	Seal	19. Au 19	Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	14-20 20 20 20 20 20 20 20 20 20 20 20 20 2	J.J. GAZEN Uses 200 J.A.J. STO J.A.J. STO J.	SALES
Proposition of Propos	New York Control of the Control of t	9.44 (19.4 (Nap 201 Nap 201 Tagilif	27 Aug 2017 27 Ool 2019	14y 200 204y 204 205 205 205 205 206 206 206 206 206 206 206 206 206 206	Modelin Modeli	SALES
Personal (III) Pergelating Per	New York Control of the Control of t	9.44 (19.4 (May 200 May 200 FAqSH	27 Aug 2017 27 Ool 2019	14-20 20 20 20 20 20 20 20 20 20 20 20 20 2	J.I. Cal 2018 Ching 2018 S.A.I 2019 Windows P.	Say Si
Neward Mill. Preparating Prepa	New York Control of the Control of t	Man (Man (Man (Man (Man (Man (Man (Man (May 200 May 200 FAqSH	27 Aug 2017 27 Ool 2019	14-20 20 20 20 20 20 20 20 20 20 20 20 20 2	J.J. Cal 2010 Ching 2000 D.J. and 2010 S.J. and 2010 S.J. and 2010 S.J. and 2010	Say Si
Proposition of Propos	Seal	9.44 (19.4 (May 200 May 200 FAqSH	27 Aug 2017 27 Ool 2019	14p.200 20by 20by 20by 20by 20by 20by 20by 2	J.J. GAZEN Uses J.J. ST. S.	2.0-20 2.0-20 2.0-20 2.0-20

OpenID 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	

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? OpenID



- 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://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 https://openid.net/certification/ and registers it in OIXnet at http://oixnet.org/openid-certifications/

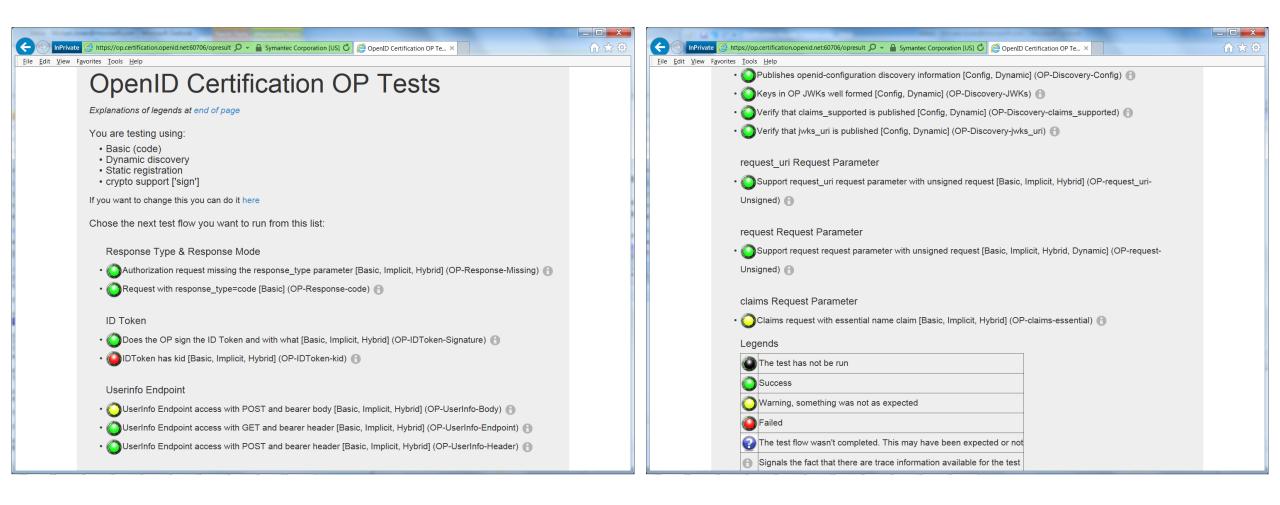
What does certification cost?



- 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
```

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 2C
        "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 Rele			
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
- 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:	4
Name: Dans	1WUSS160
Title: ASLOC. (12. Codas
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 (OpenID



- 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? OpenID



- 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.

OpenID Certification Call to Action OpenID



- 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

OpenID Connect Resources



- OpenID Connect
 - https://openid.net/connect/
- Frequently Asked Questions
 - https://openid.net/connect/faq/
- Working Group Mailing List
 - https://lists.openid.net/mailman/listinfo/openid-specs-ab
- OpenID Certification Program
 - https://openid.net/certification/
- Certified OpenID Connect Implementations Featured for Developers
 - https://openid.net/developers/certified/
- Mike Jones' Blog
 - http://self-issued.info/
- Nat Sakimura's Blog
 - http://nat.sakimura.org/
- John Bradley's Blog
 - http://www.thread-safe.com/

Open Conversation

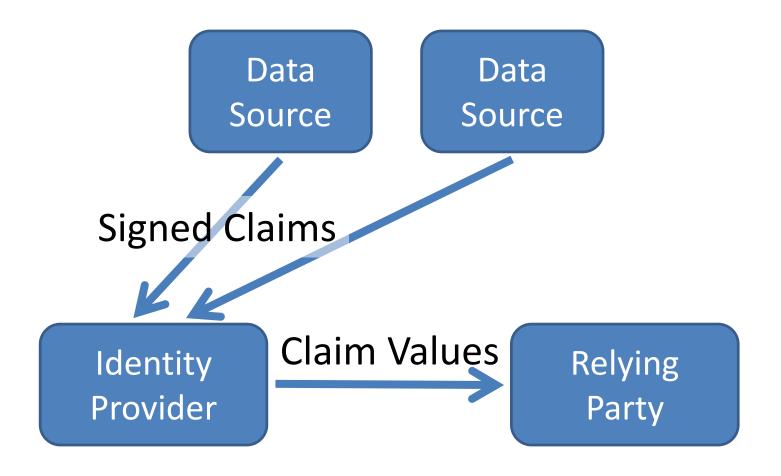


- How are you using OpenID Connect?
- What would you like the working group to know or do?

BACKUP SLIDES

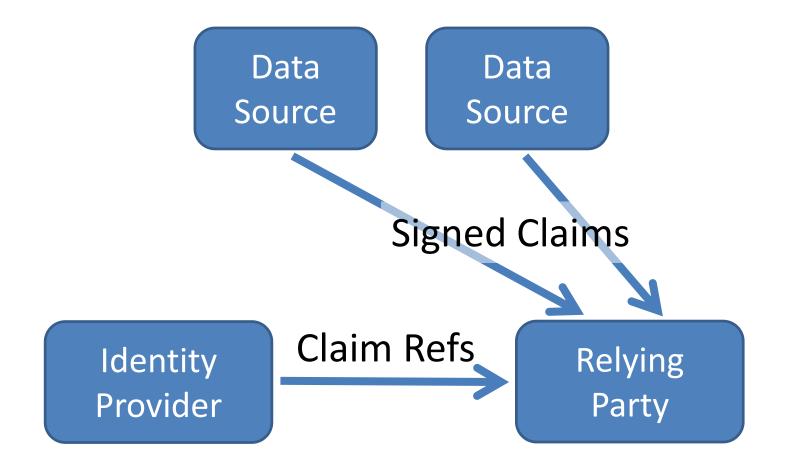
Aggregated Claims





Distributed Claims





Basic Client Implementer's Guide



- Single, simple, self-contained Web client spec
 - For clients using OAuth "code" flow
- All you need for Web server-based RP
 - Using pre-configured set of OPs

http://openid.net/specs/openid-connect-basic-1 0.html

Implicit Client Implementer's Guide OpenID



- Single, simple, self-contained Web client spec
 - For clients using OAuth "implicit" flow
- All you need for user agent-based RPs
 - Using pre-configured set of OPs

http://openid.net/specs/openid-connect-implicit-1 0.html

Core Specification



 Defines data formats and messages used for OpenID Connect authentication and claims

http://openid.net/specs/openid-connect-core-1 0.html

Discovery & Registration



- Enables dynamic configurations in which sets of OPs and RPs are not pre-configured
 - Necessary for open deployments
- Discovery enables RPs to learn about OP endpoints
- Dynamic registration enables RPs to use OPs they don't have pre-existing relationships with

- http://openid.net/specs/openid-connect-discovery-1 0.html
- http://openid.net/specs/openid-connect-registration-1 0.html

Session Management



- For OPs and RPs needing session management capabilities
 - Enables logout functionality
 - Enables account switching

http://openid.net/specs/openid-connect-session-1 0.html

OAuth Response Types



- Defines and registers additional OAuth response types:
 - -id token
 - none
- And also defines and registers combinations of code, token, and id token response types

http://openid.net/specs/oauth-v2-multiple-response-types 1 0.html

Form Post Response Mode



 Defines how to return OAuth 2.0 Authorization Response parameters using HTML form values auto-submitted by User Agent using HTTP POST

 http://openid.net/specs/oauth-v2-form-post-response-mode-1 0.html