

Introduction to OpenID Connect

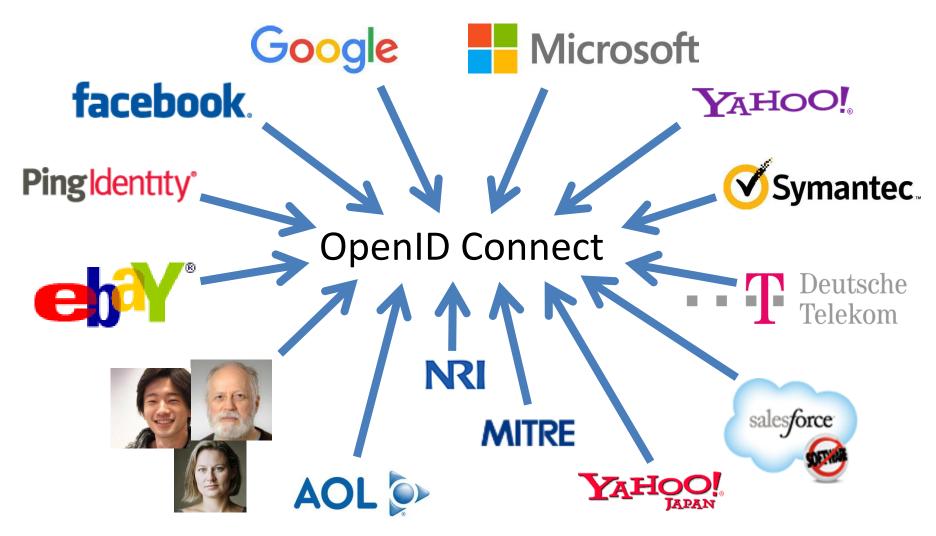
October 12, 2021

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 Almost Certainly Using OpenID Connect! OpenID



- Android, AOL, Apple, AT&T, Auth0, Deutsche Telekom, ForgeRock, Google, GrabTaxi, GSMA Mobile Connect, IBM, KDDI, Microsoft, NEC, NTT, Okta, Oracle, Orange, Ping Identity, Red Hat, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo, Yahoo! Japan, all use OpenID Connect
 - Many other sites and apps large and small use OpenID Connect
- OpenID Connect is infrastructure
 - Not a consumer brand

OpenID Connect Range



- Spans use cases, scenarios
 - Internet, Enterprise, Mobile, Cloud, Federated, User-Centric
- 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 in multiple formats 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
 - https://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, March 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 Connect Certification launched, April 2015
- OpenID Federation work begun, July 2016
- Logout Implementer's Drafts approved, March 2017
- OpenID Certification program won awards in March 2018 and April 2018
- Numerous extension specifications under way, including for user-centric identity, 2019-2021

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 Response Example



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

Original Overview of Specifications



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

OpenID 2.0 to OpenID Connect Migration (Additional Final Specification)



- 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
- https://openid.net/specs/openid-connect-migration-1 0.html
- Completed April 2015
- Google shut down OpenID 2.0 support in April 2015
- AOL, Yahoo, others have replaced OpenID 2.0 with OpenID Connect

OAuth 2.0 Form Post Response Mode (Additional Final Specification)



- 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
- https://openid.net/specs/oauth-v2-form-post-response-mode-1 0.html
- Completed April 2015
- In production use by Microsoft, Ping Identity

Exciting time for OpenID Connect! OpenID



- More happening than at any time since original specs created
- I'll give you a taste of the exciting work happening...

OP-Initiated Logout



- Enables OP to request that RPs log out end-user's sessions with the OP
- 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 changes 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 (so can be used by native applications)
- All support multiple logged-in sessions from OP at RP
- Session Management & Front-Channel Logout affected by browser privacy changes
- All can be used with RP-Initiated Logout

RP-Initiated Logout



- Enables RP to request that OP log out end-user
 - https://openid.net/specs/openid-connect-rpinitiated-1 0.html
 - Content recently split out of Session Management spec
- Not affected by browser privacy changes
 - (unlike some of the OP-Initiated Logout methods)
- Updates pending to add client_id and logout_hint parameters

Federation Specification



- 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
 - Applying lessons learned from large-scale SAML federations
- Defines hierarchical JSON-based metadata structures for federation participants
- Three interop events were held in 2020
 - Specification updated based on implementation feedback
- Third Implementer's Draft review, then Final status anticipated

Self-Issued OpenID Provider V2



- OpenID Connect Core defined Self-Issued OpenID Provider (SIOP)
 - https://openid.net/specs/openid-connect-core-1 0.html#SelfIssued
- Lets you be your own identity provider
 - Rather than a third party
- Being used with ISO Mobile Driver's Licenses (mDL)
 - Enables presentation without "calling home" to the issuer
- Self-Issued OpenID Provider (SIOP) V2 now being defined
 - https://openid.net/specs/openid-connect-self-issued-v2-1 0.html
 - Can be use for DID auth, JWT claims, Verifiable Credentials, etc.
- Working towards Implementer's Draft status

OpenID Connect for Verifiable Presentations



- Enables presentation of claims as W3C Verifiable Presentations
 - https://openid.net/specs/openid-connect-4-verifiable-presentations-1 0.html
- Can be used both with third-party and self-issued OPs
- VPs can be returned in ID Token, UserInfo, and new VP Token
- Integration point with DIF Presentation Exchange
- Please review new draft just published

Claims Aggregation Specification



- Enables RPs to request and Claims Providers to return aggregated claims through OPs
 - https://openid.net/specs/openid-connect-claims-aggregation-1 0.html
- Defines full life-cycle of aggregated claims and roles of entities involved
- Supports multiple claims schemas
 - JWT Aggregated and Distributed Claims
 - W3C Verifiable Credentials objects
- Please review new draft just published

prompt=create Specification



- Initiates user account registration via OpenID Connect
 - https://openid.net/specs/openid-connect-prompt-create-1 0.html
- Requests enabling account creation during authentication
- Please review new draft just published



- Defines new error code unmet authentication requirements
 - https://openid.net/specs/openid-connect-unmet-authenticationrequirements-1 0.html
- Enables OP to signal that it failed to authenticate the End-User per the RP's requirements
- Has been stable since initial publication
- Recent WG decision to advance to Final status

Native SSO Specification



- OpenID Connect Native SSO for Mobile Apps
 - https://openid.net/specs/openid-connect-native-sso-1 0.html
- Enables Single Sign-On (SSO) across apps by the same vendor
- Assigns a device secret issued by the OP
- Deployed by AOL
- Seeking feedback on applicability to others' use cases

Portable Identifiers Under Discussion OpenID



- Current subject identifiers are OP-specific
- WG discussing identifiers that you can move between OPs
 - Related to MODRNA Account Porting work
- Potentially both for self-issued OPs and third-party OPs
- W3C DIDs are one such possible identifier type

Second Errata Set



- Errata process corrects typos, etc. discovered
 - Makes no normative changes
- Edits under way for second errata set
- https://openid.net/specs/openid-connect-core-1 0-27.html is current Core errata draft

Identity Assurance Specification (Related Work in eKYC-IDA WG)



- OpenID Connect for Identity Assurance
 - https://openid.net/specs/openid-connect-4-identity-assurance-1 0.html
- JWT representation for verified person data
 - Including information about the identity verification performed
 - Enables legal compliance for some use cases
- Moved to eKYC and Identity Assurance working group in 2019
- Now at second Implementer's Draft status
 - Please review!

CIBA Core is Now Final (Related Work in MODRNA WG)



- OpenID Connect Client-Initiated Backchannel Authentication (CIBA) Core
 - https://openid.net/specs/openid-client-initiated-backchannelauthentication-core-1 0.html
- Authentication flow with direct Relying Party to OpenID
 Provider communication without redirects through browser
- Product of the MODRNA working group
- Used by FAPI CIBA Profile

Related W3C Federated Identity Group



- New W3C Federated Identity Community Group
 - https://www.w3.org/community/fed-id/
- Incubating Web features supporting federated identity and preventing untransparent, uncontrollable tracking on the Web
- For instance, new features may be needed to enable logout when browsers disable support for third-party cookies
- Informed by discussions in Connect WG Browser Behaviors calls

Related OpenID Working Groups



- Mobile Operator Discovery, Registration & autheNticAtion (MODRNA) WG
 - Mobile operator profiles for OpenID Connect
- Financial-grade API (FAPI) WG
 - Enables secure API access to high-value services
 - Used for Open Banking in jurisdictions including UK, Australia, and Brazil
- eKYC and Identity Assurance WG
 - Defines JWT format for verified claims with identity assurance information
- Research and Education (R&E) WG
 - Profiles to ease Connect adoption in Research and Education (R&E) sector

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 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



- There are 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
 - Third Party-Initiated Login for OP and RP
 - Logout for OP and RP

Newest Connect Certification Profiles OpenID



- Four logout profiles for OPs and RPs in production mode
 - RP-Initiated Logout
 - Session Management Logout
 - Front-Channel Logout
 - Back-Channel Logout

Connect OP Certifications

- OpenID Provider certifications at <u>https://openid.net/certification/#OPs</u>
 - 445 profiles certified for
 135 implementations by
 100 organizations
- Recent additions:
 - Authlete, Curity, Duende Software,
 Ekinoks, Gluu, Steffen Klössel,
 LoginRadius, NAT.Consulting, Nomidio,
 OGIS-RI, Oracle, Filip Skokan
- 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	Form Post OP	3rd Party-init
iamal	Identity Cloud	12-Sep-2019			12-Sep-2019			
rizona Regional Multiple Listing	ARMLS Identity 2.0.2	21-Feb-2019						
lenice		24-						
Auth0	Auth0	24- May-2016	15-Feb-2017	15-Feb-2017	24- May-2016		13-Aug-2018	
Notice .	Authore 1.1	12-Jul-2017	12-30-2017	12-34-2017	12-Jul-2017			
Notice .	Authlete 2.1	5-Aug-2019	5-Aug-2019	5-Aug-2019	5-Aug-2019	5-Aug-2019	5-Aug-2019	
AuthMachine	AuthMachine 4.0.7	19-Jul-2018	19-Jul-2018	19-Jul-2018	19-Jul-2018	19-Jul-2018	19-Jul-2018	
Dominick Baler & Brook Allen	identityServer3 v1.6	8-May-2015	8-May-2015	8-May-2015	8-May-2015			
Dominick Baler & Brook Allen	identity/Senver4	12-	12-	12-	12-			
John Sec. & Cross-rec.	No. report to 1	Dec-2016	Dec-2016	Dec-2016	Dec-2016			
Dity of Beverly Hills	COSH Identity	12- Mar-2019	12- Mar-2019	12- Mar-2019	12- Mar-2019		12-Mar-2019	
Story	Bitter platform 1.0.0	16-Jan-2020	N-10-18	10.00-20.00	1121-2019			
DA .	CA API Gateway/CA Mobile API Gateway	22-Jun-2017	1-Nov-2017	1-Nov-2017	22-Jun-2017			
DA .	CA Single Sign-On 12.82	4-Feb-2019	4-Feb-2019		4-Feb-2019			
Chinese Academy of Sciences.			26-					
DACAS	DACAS UA Gateway v1.0	24-Apr-2019	Mar-2019	24-Apr-2019				
Chinese Academy of Sciences.	DACAS Mobile SSO v1.0	6-Apr-2020	6-Apr-2020	6-Apr-2020	6-Apr-2020			
DACAS								
Clareity Security	identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016			
DiassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015			
Classmethod	Barista v1.18.2	9-Nov-2017			9-Nov-2017			
Cloudentity	Cloudentity CIDC services 1.3	18- Aug-2017			18- Aug-2017	18- Aug-2017		
Dioudentity	CIAM Net			24-Oct-2019		24-Oct-2019		
Cloud Foundry	UAA160	Aug-2018						
Connect2ld	Connect2id Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017		
Dunity	Curity Identity Server 2.3.1	20-	20-	20-	20-			
		Dec-2017	Dec-2017	Dec-2017	Dec-2017			
Dunity	Curity identity Server 4.3.0	20-Sep-2019	20-Sep-2019	20-Sep-2019			20-Sep-2019	20-Sep-2019
CZNIC	mojelD	7-Jul-2016		31-Jul-2016		7-Jul-2016		
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015			
Ergon informatik	Alricok IAM 7.1	23-Feb-2020						
ForgeRook	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015			
GEANT Association	GEANT OLDC-Plugin for Shibboleth IdP 1.0.0 Glau Senier 3.1.3			29-Oct-2019 18-Jul-2018	23-0ct-2019 18-Jul-2018	29-0ds-2019 18-Jul-2018		
Shu	Glus Sener 3.1.3	18-Jul-2018 15-Oct-2019	18-Jul-2018 15-Oct-2019	18-Jul-2018 15-Ods-2019			18-Jul-2018 15-Oct-2019	22-049-2019
Soogle	Google Federated identity	20-Apr-2015	21-Apr-2015	23-Apr-2015	15-Apr-2015			22-00-2019
Joogle GrabTasi Holdings	Google received identity	20-Apr-2015 6-Ext-2019	7-Feb-2019	23-Apr-2010	10-Apr-2010			
GraviteeSource	Gravitee to Access Management 2.1.x	6-Nov-2018	6-Nov-2018	6-Nov-2018	16-Nov-2018			
		18-						
SSMA	Mobile Connect Reference implementation v2.3	May-2018						
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		
Hanecan	Bloorystology OpenID Identity Server 1.3.1	31+						
		May-2017	May-2017	May-2017	May-2017			
Notand Hedberg	pyoloc 0.7.7	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015		
Call Heldenbrand	Spark Platform	2-Oct-2015	2-Oct-2015	2-Oct-2015	5-Oct-2015			
ВМ	IBM Cloud identity	11-Sep-2019 27-	11-Sep-2019 27-	11-Sep-2019 27-	11-Sep-2019		11-Sep-2019	
вм	IBM Security Access Manager V9.0.7	27+ Aug-2019	27+ Aug-2019	27- Aug-2019	27- Aug-2019	27- Aug-2019	27-Aug-2019	
dentity Automation	Rapidicentity Federation	12-Jan-2018			12-Jan-2016			
tes International	Sign&go 8.0	10-	10-	10-	10-		10-Mar-2020	
ret imernational	argnago o 0	Mar-2020	Mar-2000	Mar-2000	Mar-2020		10-1/8/-2020	
-Sprint innovations	AccessMatrix UAM	23-	23-		23-			
		Aug-2018	Aug-2018		Aug-2018			
ISIGN	KSign Access 4.0	17- Mar-2017						
	Authentication, Authorization, and Accounting System,	12-						
The Library of Congress	version 1.0	May-2017						
INE	LINE Login	15-Jun-2018						
Viicro Focus	Micro Pocus Access Manager 4.4 Sen/ce	13-	13-	13-	13-			
		May-2019	May-2019	May-2019	May-2019			
Norosoft	ADPS on Windows Server 2016	13-Sep-2015	13-Sep-2015		7-Apr-2015			
		15-			8-Apr-2015		15-Mar-2019	

Microsoft		Azure Active Directory V2			15-Jan-2019		15-Jan-2019		15-Jan-2019	
Microsoft		IEF Experimental Claimer VO.9		9-May-2018			9-May-2018			
MMne		Mine Pederated Identity Hub v1		1-Aug-2017						
NEC		NC7000-3A-OC		7-Mar-2016						
NedReason		Next Reason Central Identity		15-Sep-2010			15-Sep-2018			
Nomura Research Institute		priportic		10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015		
Nomura Research Institute		UNHD		10-Apr-2015						
NRI SecureTechnologies		UNHD 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		7-008-2016			
OGIS-RI		ThemiStruct identity Platform v1.3.	0	28-Apr-2017	May-2017		28-Apr-2017			
ogis-Ri		ThemiStruct identity Platform v2.0.	0	5-Mar-2016	5-Mar-2016		5-Mar-2018			
ogis-ru		ThemiStruct identity Platform v2.2.	0	20-Nov-2018	20-Nov-2018	20-Nov-2018	20-Nev-2018			
ogis-Ri		ThemiStruct Identity Platform v2.4.	0		22-Jul-2019	22-Jul-2019	22-346-2019			
				25-	26-	26-	26-			
Otta		Olta OP		May-2016	May-2016	May-2016	May-2016		16-Jul-2018	
Onegini		Onegini Connect 5.0		9-Nov-2018	9-Nov-2018		9-Nov-2018			
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-A	kar-0018		16-Apr-2018	16-Apr-2018	16-Apr-2018			
ORY GribH		ORY Hydra v1.0.0			14-201-2018		14-Jul-2018	14-34-2015		
Ontrom Onton		GAIA Trust Platform 4.4		9-Jun-2019	14-30H2018	18-Noi-2019	15-Jun-2019		22-Nov-2019	
PajPal		GAIA Trust Platform 4.4 Login with PayPail		9-20n-2019			15-Jun-2019 15-Apr-2015		22-1000-2019	
Peercraft ApS		Peercraft			19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016		
Ping identity		PingFederate 5.0			10-Apr-2015	10-Apr-2015				
Ping identity		PingFederate 9.1.3			28-Sep-2018				28-Sep-2018	
Ping identity		PingOne for Enterprise 16.6.148			25-Feb-2019	25-Feb-2019	25-Feb-2019		25-Feb-2019	
Plvotal		Photal Cloud Foundry 2.2 UAA		17-Jul-2018						
Privacy Vaults Online (PRI	MO)	PR/VO-Look		23-Oct-2015			25-Nov-2015			
ProSlebenSat 1 Media		7Pass *2.0.0		7-Aug-2017	7-Aug-2017	21-	7-Aug-2017			
						Aug-2017				
Recruit		Recruit ID		16- May-2018						
Red Hat		Keyoloak 2:3:0			31-Oct-2016	31-Oct-2016	31-Oct-2016			
Justin Richer		MITREldConnect		13- Maj-2015			13- May-2015	13- May-2015		
				Maj-2015			14-	May-2015		
Salesforce		Summer 2015 Release					May-2015			
Sameung Electronics		Sameung Account		11-Feb-2020						
Michael Schwartz		Glau Sener 2 3				S-310-0015				
Michael Schwartz		Glus Server 3.1.1			16-Oct-2017	16-Oct-2017		16-Oct-2017	6-34-2018	
SecureAuth		SecureAuth IdP 8.2		25-Feb-2016		25-Feb-2016	7-Mar-2016		6-20-2016	
Filip Skokan		node oldo-provider		2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017	25-Jun-2018	23-Sep-2019
SoftBank		SoftBank OIDC v1.0		15-Jan-2019						
Symantec		NSL 2016.4.0.16		13-Oct-2016			13-001-2016			
Tools4ever		HelioiD 4.80		22-						
				Aug-2018						
Trivore		Trixore identity Service 3.0		26- Aug-2019	26- Aug-2019	26- Aug-2019	26- Aug-2019			
				17-Oct-2018	- agravis	- agravis	22-Oct-2018			
U2U Consult		The identity Hub v1		17-Oct-2018		10-	22-Oct-2018 10-		23-Oct-2018	
U2U Consult		my/D.be		10- Dec-2019	10- Dec-2019	10- Dec-2019	10- Dec-2019		10-Dec-2019	
University of Chicago		OIDC OP Overlay for Shibboleth I	(Dut 2 transles 1 C	25-Pet-2016			25-Feb-2016			
		Verimi 1.2	DF 10.2 VE1800 1.0	19-Oct-2018			31-Oct-2018			
Verimi		veini (2					a-00-2018			
Vertzon		VZConnect 1.9		21- Dec-2016						
Videntity Systems		Verify My Identity 0.1.1		29-Nov-2018			29-Nov-2018			
ViewDR		Const V1 0			2-Fep-2016		29-Nov-2018 28-Jan-2016			
ViewDS Vithware		Cobalt V1.0 Workspace ONE								
				18-Apr-2018	18-Apr-2018	18-Apr-2018				
WidasConcepts		cidaas 2.0			19-Apr-2018	16-Apr-2018	11-Apr-2018			
Matias Wolceki		Auth0		6-Feb-2016			8-Feb-2016			
					15-Jan-2018				20-Jul-2018	
W902				7-Dec-2016	7-Dec-2016	7-Dec-2016	7-Dec-2016			
		Yahoo! ID Federation v2								
wsoz Yahoo! Japan Certified Ope		oviders for Logo								
wsoz Yahoo! Japan Certified Ope				fies:						
wsoz Yahoo! Japan Certified Ope		oviders for Logo			Session OP	Pr	ont-Channel	OP .	Back-Ch	annel OP
WSO2 Yahoo! Japan Certified Ope These deployments have bei		OVIDERS FOR LOGO OVIDERS FOR LOGO Implementation	er logout conformance pro			15-Dec-20			Beck-Ch 5-Dec-2019	annel OP

Connect RP Certifications



- Relying Party certifications at https://openid.net/certification/#RPs
 - 98 profiles certified for34 implementations by21 organizations
- Recent additions:
 - Gluu, Filip Skokan, Ulrik Strid,
 ZmartZone

Certified Relying Parties

These deployments have been granted certifications for these Relying Party conformance profiles

Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic RP	Form Post RP 3rd Party-I	nit 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		
llex International	Sign&go 8.0	10-Mar-2020						
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					
KSIGN	KSign Trust Thing 1.2				10-Oct-2019			
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		

Certified OpenID Relying Parties for Logout Profiles

These deployments have been granted certifications for these OpenID Relying Party logout conformance profiles

Organization	Implementation	RP-Initiated RP	Session RP	Front-Channel RP	Back-Channel RP
Roland Hedberg	OIDCrp v.0.6.6	20-Mar-2020	20-Mar-2020	20-Mar-2020	20-Mar-2020

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://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/

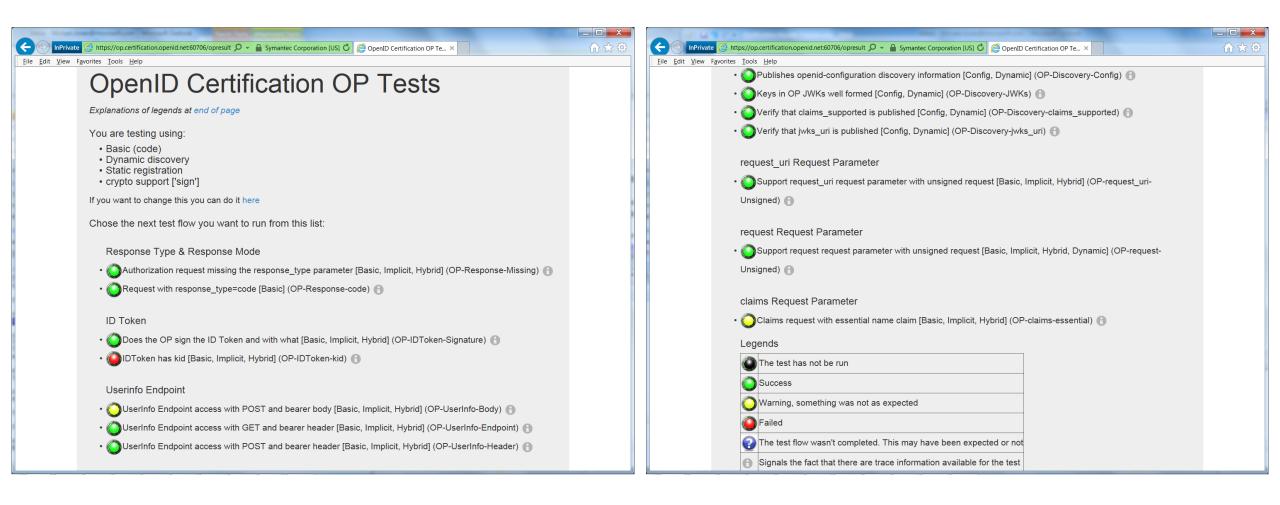
What does certification cost?



- Not a profit center for the OpenID Foundation
 - Fees there to help cover costs of operating certification program
- Member price
 - **-** \$700
- Non-member price
 - **-** \$3500
- 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	ase
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
- Interop testing now happening for OpenID Connect Federation
- 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 site 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 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



- Connect Certification code was reimplemented in Java
 - Now in the same code base as FAPI certification
 - Migration to new implementation occurred at end of August 2020
- Additional FAPI profiles being developed:
 - FAPI-CIBA RP
- Certification for additional specifications is anticipated:
 - E.g., eKYC-IDA, HEART, MODRNA, iGov, EAP, R&E, etc.

OpenID Certification Call to Action



- Certify your OpenID Connect and FAPI implementations now
- Help us test the new tests
 - Especially, test your Logout implementations and provide feedback
- Join the OpenID Foundation and/or the OpenID Connect working group

OpenID Connect Resources



- OpenID Connect Description
 - https://openid.net/connect/
- Frequently Asked Questions
 - https://openid.net/connect/faq/
- OpenID Connect Working Group
 - https://openid.net/wg/connect/
- OpenID Certification Program
 - https://openid.net/certification/
- Certified OpenID Connect Implementations Featured for Developers
 - https://openid.net/developers/certified/
- Mike Jones' Blog
 - https://self-issued.info/

Open Conversation



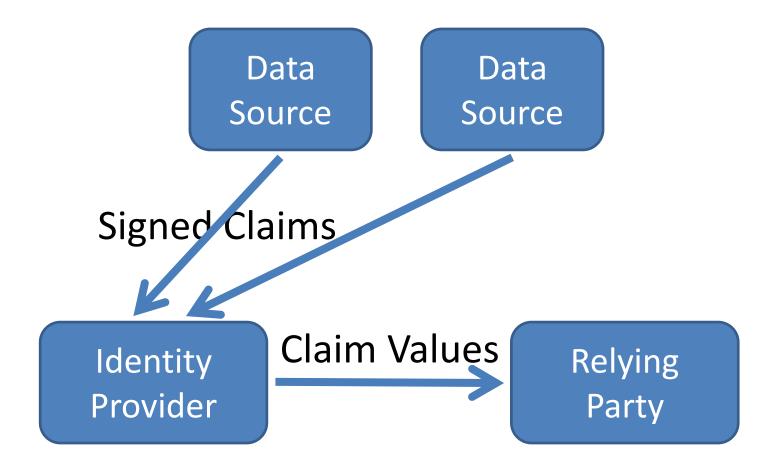
- How are you using OpenID Connect?
- What would you like the working group to know or do?

Slides will be posted at https://self-issued.info/

BACKUP SLIDES

Aggregated Claims





Distributed Claims



