

#### **Introduction to OpenID Connect**

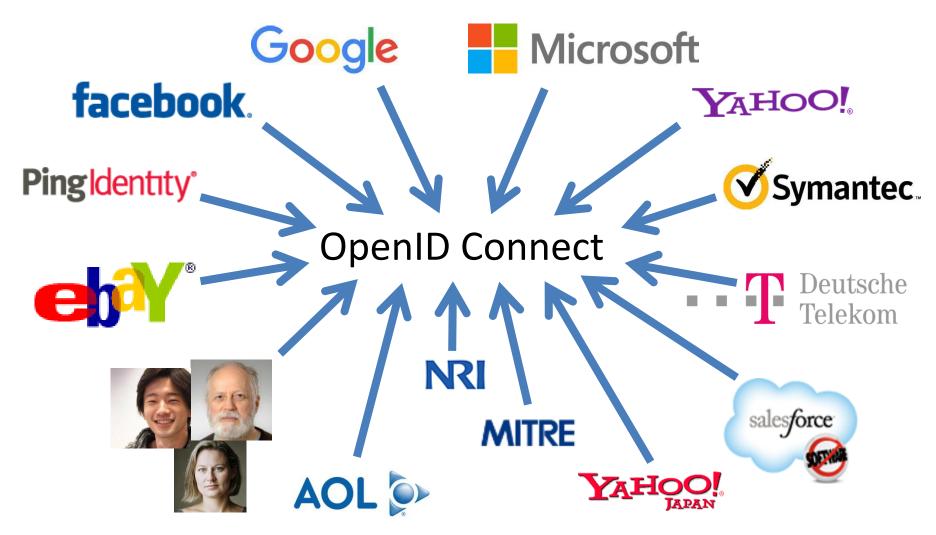
October 10, 2023

Michael B. Jones

**OpenID Foundation** 

#### 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, NRI, 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, JSON Web Token (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)
- Lets you 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 Connect Certification launched, April 2015
- OpenID Federation work begun, July 2016
- OpenID Certification program won awards in March 2018 and April 2018
- Logout specifications became Final, September 2022
- Numerous extension specs under way, including for Verifiable Credentials, 2019-2023
- Errata Set 2 near approval

#### A Look Under the Covers



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

#### **ID** Token



- JSON Web 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
  - addressRequests 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

#### **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
- Can be used with all OP-Initiated Logout methods
- Not affected by browser privacy changes
  - (unlike some of the OP-Initiated Logout methods)
- Final Specification as of September 2022

#### **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
    - <a href="https://openid.net/specs/openid-connect-frontchannel-1">https://openid.net/specs/openid-connect-frontchannel-1</a> 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
- Final Specifications as of September 2022

# unmet\_authentication\_requirements Specification



- OpenID Connect Core Error Code unmet\_authentication\_requirements
  - https://openid.net/specs/openid-connect-unmet-authentication-requirements-1 0.html
- **Defines** unmet\_authentication\_requirements **error code**
- Enables OP to signal that it failed to authenticate the End-User per the RP's requirements

Became Final in November 2022

## prompt=create Specification



- Initiating User Registration via OpenID Connect specification
  - https://openid.net/specs/openid-connect-prompt-create-1 0.html
- Requests enabling account creation during authentication

• Became Final in December 2022

## 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...

#### OpenID Federation Specification



- OpenID Federation specification
  - https://openid.net/specs/openid-federation-1 0.html
- Enables trust establishment and maintenance of multi-party federations
  - Applying lessons learned from large-scale SAML federations
  - Can be used for OpenID Connect, OAuth 2.0 deployments
- Recently renamed from "OpenID Connect Federation" to reflect broader role
  - Can be and is used both with and without OpenID Connect
- Defines hierarchical JSON-based metadata structures for participants
- Three interop events were held in 2020
- In production use in Italian national federations
- Actively resolving remaining open issues
  - Another Implementer's Draft planned soon
  - Then advancement to Final status

## OpenID for Verifiable Credentials



- Family of three specs enabling use of identities that you hold
- Uses the three-party Issuer/Holder/Verifier model
  - An Issuer creates a Verifiable Credential for you to hold
  - You hold it in a Wallet
  - You present it to a Verifier
- Credential format agnostic
  - Can be used w/ W3C VCs, ISO Mobile Driving Licenses (mDL), SD-JWTs, etc.
- Has good privacy properties
  - Issuer doesn't know when/where you're using the credential
- See <a href="https://openid.net/openid4vc/">https://openid.net/openid4vc/</a>

## OpenID for Verifiable Credential Issuance OpenID



- OpenID for Verifiable Credential Issuance specification
  - https://openid.net/specs/openid-4-verifiable-credential-issuance-1 0.html
- Specifies how to issue Verifiable Credentials to Holder/Wallet
- Based on OAuth 2.0
- Credential format agnostic
  - For example, can use with ISO Mobile Driving Licenses (mDL)
- Includes issuer-initiated flow
- Actively working towards first Implementer's Draft

## OpenID for Verifiable Presentations OpenID



- OpenID for Verifiable Presentations specification
  - https://openid.net/specs/openid-4-verifiable-presentations-1 0.html
- Defines how to present Verifiable Presentations to a Verifier
- Based on OAuth 2.0
- Credential format agnostic
  - For example, can use with ISO Mobile Driving Licenses (mDL)
- Second Implementer's Draft approved May 2023
- Actively working towards third Implementer's Draft

### Self-Issued OpenID Provider V2



- OpenID Connect Core defined Self-Issued OpenID Provider (SIOP) functionality
  - Lets you be your own identity provider (rather than a third party)
- Self-Issued OpenID Provider v2 specification
  - https://openid.net/specs/openid-connect-self-issued-v2-1 0.html
  - Extends initial SIOP functionality to include DIDs as subjects
- Credential format agnostic
- SIOP being used with ISO Mobile Driving Licenses (mDL)
- Implementer's Draft approved February 2022
  - Actively working towards second Implementer's Draft

#### Native SSO Specification



- OpenID Connect Native SSO for Mobile Apps specification
  - https://openid.net/specs/openid-connect-native-sso-1 0.html
- Enables Single Sign-On across apps by the same vendor
- Assigns a device secret issued by the Authorization Server
- Deployed by AOL

• Became an Implementer's Draft in December 2022

## Second Errata Set



- Edits were performed to address outstanding errata issues
- See current editors' drafts at <a href="https://openid.bitbucket.io/connect/">https://openid.bitbucket.io/connect/</a>
  - Updates to Core, Discovery, Registration, and Backchannel Logout
- Working Group Last Call for changes ends Monday
- Then will hold 45-day Foundation-wide Errata approval vote
- Publicly Available Specification (PAS) submission to ISO of final OpenID Connect specifications planned

# Related OpenID Working Groups



- Mobile Operator Discovery, Registration, & autheNticAtion (MODRNA)
  - Mobile operator profiles for OpenID Connect
- Financial-grade API (FAPI)
  - FAPI used for Open Finance in jurisdictions including UK, Australia, Brazil, Saudia Arabia, Norway, Germany, Japan, Canada, & more to come...
- eKYC and Identity Assurance
  - Defines JWT format for verified claims with identity assurance information
- Research and Education (R&E)
  - Profiles to ease Connect adoption in Research and Education (R&E) sector
- Digital Credentials Protocols (DCP)
  - Future home of OpenID for Verifiable Credentials (OpenID4VC) specifications

# 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
- Fourth Implementer's Draft approved October 2022

# CIBA Core (Related Work in MODRNA WG)



- OpenID Connect Client-Initiated Backchannel Authentication (CIBA) Core
  - <a href="https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1\_0.html">https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1\_0.html</a>
- Authentication flow with direct Relying Party to OpenID
   Provider communication without redirects through browser
- Used by FAPI CIBA Profile
- Became Final in September 2021

# 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
- 2,772 total certifications to date!



# 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



- Authentication
  - Basic Flow
  - Implicit Flows
  - Hybrid Flows
  - Third Party-Initiated Login Flow
- Discovery (OP Metadata)
- **Dynamic Client Registration**
- Logout
  - RP-Initiated Logout
  - Session Management
  - Front-Channel Logout
  - Back-Channel Logout
- Form Post Response Mode

### **Connect OP Certifications**

- OpenID Provider certifications at https://openid.net/certification/#OPs
  - 595 profiles certified to date for over 150 deployments
- Recent additions:
  - Amwai Tech, Authify, Gluu, LG Uplus,
     Makuake, malachite, Mindgate
     Solutions, MonoCloud, RSA Security,
     Samsung Electronics,
- Each entry link to zip file with test logs and signed legal statement
  - Test results available for public inspection



							Form Bord	Sed Darly Set
Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP	Form Post OP	3rd Party-Ini OP
kamal	identity Cloud	12-Sep-2019			12-Sep-2019			
rizona Regional Multiple Listing en/oe	ARMLS identity 2.0.2	21-Feb-2019						
		24-			24-			
Lutro .	Auth0	May-2016	15-Feb-2017		May-2016		13-Aug-2018	
umere	Authere 1.1		12-Jul-2017	12-Jul-2017	12-Jul-2017			
umete	Authlete 2.1	5-Aug-2019	5-Aug-2019	5-Aug-2019	5-Aug-2019	5-Aug-2019	5-Aug-2019	
AuthVachine	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	identitySenier3 v1.6	8-May-2015 12-	8-May-2015	8-May-2015	8-May-2015			
Cominick Baler & Brook Allen	Identity/Server4	12- Dec-2016	Dec-2016	12- Dec-2016	12- Dec-2016			
City of Beverly Hills	совн ізеняў	12- Mar-2019	12- Mar-2019	12- Mar-2019	12- Mar-2019		12-Mar-2019	
Story	Britisey platform 1.0.0	16-Jan-2020						
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 12.8.2	4-Feb-2019	4-Feb-2019		4-Feb-2019			
Chinese Academy of Sciences, DACAS	DACAS UA Geteway v1.0	24-Apr-2019	26- 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			
SACAS Claretti Security	identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016			
clarety securey	Classi, Int One Click 2015	3-Nov-2015	au-curract6	16	3-Nov-2015			
Classmethod	Barista v1.18.2	9-Nov-2017			9-Nos-2017			
Cloudentity	Cloudentity OIDC services 1.3	18-			18-	18-		
	Cloudentity OIDC services 1.3  CIAM Next	Aug-2017			Aug-2017	Aug-2017		
Cloudentity		24-000-2019	24-Oct-2019	24-06-2019	24-Oct-2019	24-005-2019		
Cloud Foundry	UAA v60	Aug-2018						
Connect2ld	Connect2id Server 6.1.2a	3-Jan-2017 20-	3-Jan-2017 20-	3-Jan-2017 20-	3-Jan-2017	3-Jan-2017		
Durity	Curity identity Server 2.3.1	20- Dec-2017	20- Dec-2017	20- Dec-2017	20- Dec-2017			
Durity	Curity Identity Server 4.3.0	20-Sep-2019	20-Sep-2019	20-Sep-2019			20-Sep-2019	20-Sep-2019
ZNC	mojelD	7-Jul-2016		31-Jul-2016		7-Jul-2016		
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015			
Ergon informatik Forosiffoos	Alricok IAM 7.1 OpenAM 13	23-Feb-2020 13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015			
Porgertook GEANT Association	GBANT OIDC-Plugin for Shibboleth IdP 1.0.0			13-Apr-2016 29-Oct-2019				
Shu	Glu Sener 3.13	18-Jul-2018	18-34-2018	18-34-2018	18-Jul-2018	18-Jul-2018	18-Jul-2018	
Shu Shu	Glu Sener 400	15-0:0-2019	15-Oct-2019	15-04-2019			15-Oct-2019	22-049-2019
Soogle	Google Pederated Identity	20-Apr-2015	21-Apr-2015	23-Apr-2015	15-Apr-2015			
GrabTaxi Holdings	Grab ID 1.0	6-Feb-2019	7-Feb-2019					
GraviteeSource	Gravitee Io Access Management 2.1 x	6-Nov-2018	6-Nov-2018	6-Nov-2018	16-Nov-2018			
SSMA	Mobile Connect Reference implementation v2.3	18- Mai-2016						
Thlerry Habart	SimpleidentityServier 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		
ranacan	Blocryptology OpenID Identity Server 1.3.1	31-	31-	31-				
	pjetec 0.7.7	Maj-2017 26-Sep-2015	May-2017 26-Sep-2015	May-2017 26-549-2015	May-2017			
Notand Hedberg Call Heldenbrand	pjelde 0.7.7 Soark Platform	26-Sep-2015 2-Oct-2015	26-Sep-2015 2-Oct-2015	26-Sep-2015 2-Oct-2015	26-Sep-2015 5-Oct-2015	26-56p-2015		
an Helderdrand BM	IBM Cloud Identity	2-001-2015 11-Sep-2019	11-Sep-2019	11-Sep-2019	11-Sep-2019		11-Sep-2019	
		11-dep-2019 27-	11-sep-2019 27-	11-sep-2019 27-	27-			
BM	IBM Security Access Manager V9.0.7	Aug-2019	Aug-2019	Aug-2019	Aug-2019	Aug-2019	27-Aug-2019	
dentity Automation	Rapidioently Federation	12-Jan-2018 10-	10-	10-	12-Jan-2018			
le: International	51gn&go 8.0	Mar-2020	10- Mar-2020	10- Mar-2000	10- Mar-2020		10-Mar-2020	
Sprint innovations	Accessitratri: UAM	23- Aug-2018	25- Aug-2018		23- Aug-2018			
ISIGN	KSign Access 4.0	17- Mar-2017						
The Library of Congress	Authentication, Authorization, and Accounting System, sension 1.0	12- Maj-2017						
NE	LINE Login	15-Jun-2018						
	Micro Pocus Access Manager 4.4 Senvice	13- Mai-2019	13-	13- Mai(2010	13- May-2019			
filoro Focus								
Micro Pocus Microsoft	ADPS on Windows Server 2016	Maj-2019 13-Sep-2015	13-Sep-2015	may-sorra	7-Apr-2015			

Yenco: Japan Certified Ope	een granted cert	introations for these OpenID Provid Implementation Inver 7.18.1	er logout conformance pri RP-Initiated OP 15-Dec-2019		Session OP	15-Dec-20	ont-Channel		Back-Ch 15-Dec-2019	annel OP
Tehnool Japan  Certified Operation of the company o	een granted cert				Session OP	Pr	ont-Channel	OP .	Back-Ch	annel OP
Yehoo! Japan Certified Ope		tifications for these OpeniO Provid	er logout conformance pri	files:						
Yahoo! Japan	enID Pro									
		viders for Logo	ut Profiles							
		Yahoo! ID Federation v2		7-Dec-2016	/-Dec-2016	/-Dec-2016	r-Dec-2016			
MOULE					7-Dec-2016		7-Dec-2016		20-08-0018	
Mattes Wolceki W902		Auth0 Identity Server 5.4.0		6-Peb-2016	15-Jan-2018	20, 14, 2012	8-Feb-2016		20-Jul-2018	
Aldas Concepts		cidaas 2.0			19-Apr-2018	16-Apr-2018				
VMvare		Workspace ONE			18-Apr-2018		18-Apr-2018			
ViewDS		Cobalt V1.0			2-Feb-2016		28-Jan-2016			
Videntity Systems		Verify My Identity 0.1.1		29-Nov-2018			29-Nov-2018			
				Dec-2016						
Vertzon		VZConnect 1.9		21-						
Verimi		Verimi 1.2		19-Oct-2018			31-Oct-2018			
University of Chicago		OIDC OP Overlay for Shibboleth I	dPv3.2.1 version 1.0	25-Feb-2016			25-Feb-2016			
				Dec-2019	Dec-2019	Dec-2019	Dec-2019		10-040-2019	
U2U Consult		m/D be		10-	10-	10-	10-		10-Dec-2019	
UZU Consult		The identity Hub v1		17-Oct-2018			22-Oct-2018		23-Oct-2018	
Trivore		Trivore identity Service 3.0		Aug-2019	Aug-2019	Aug-2019	Aug-2019			
				26-	26-	26-	26-			
Tools4ever		Helio/D 4.8.0		22- Aug-2018						
				13-Oct-2016 22-						
SoftBank Symanted		SoftBank OIDC V1.0 NSI, 2016.4.0.16		15-Jan-2019 13-Oct-2016			13-001-2016			
Filip Skokan SoftBank		node oldo-provider SoftBank OIDC v1.0		2-Jan-2017 15-Jan-2019	a-281-2017	2-181-2017	2-181-2017	2-UBN-2017	20-207-2018	20-0ep-201
SecureAuth Fillip Skoken		SecureAuth IdP 8.2 node oldo-provider				25-Feb-2016 2-Jan-2017	7-Mar-2016 2-Jan-2017	2-Jan-2017	25-Jun-2018	
Michael Schwartz SecureAuth		Gluu Server 3.1.1 SecureAuth IdP 8.2		16-Oct-2017	16-Oct-2017 25-Feb-2016	16-Oct-2017 25-Feb-2016	16-Oct-2017 7-Mar-2016	16-001-201	t-Jul-2018	
Michael Schwartz Michael Schwartz		Gluu Server 2.3 Gluu Server 3.1.1			2-Jul-2015 16-Oct-2017	8-Jul-2015 16-Oct-2017			6-A4-2018	
Sameung Electronics Michael Schwartz		Sameung Account Glass Senser 2.3		11-Feb-2020 2-Jul-2015		S-310-2015				
							May-2015			
Salesforce		Summer 2015 Release					14-			
Justin Richer		MITREIdConnect		Maj-2015			May-2015	May-2015		
				13-			13-	13-		
Red Hat		Keycloak 2.3.0			31-Oct-2016	31-Oct-2016	31-Oct-2016	31-008-2019		
Recruit		Recruit ID		16- May-2018						
				16-		Aug-2017				
ProSlebenSat 1 Media		7Pass *2.0.0		7-Aug-2017	7-Aug-2017	21- Aug-2017	7-Aug-2017			
Privacy Vaults Online (PF	RMO)	PR/VO-Look		23-Oct-2015			25-Nov-2015			
Pluotal		Photal Cloud Foundry 2.2 LIAA		17-Jul-2018						
Ping identity		PingOne for Enterprise 16.6.148			25-Feb-2019	25-Feb-2019	25-Feb-2019		25-Feb-2019	
Ping identity		PingFederate 9.1.3			28-Sep-2018				28-8ep-2018	
Ping Identity		PingFederate 8.0			10-Apr-2015					
Peercraft ApS		Peercraft			19-Jan-2016		19-Jan-2016	19-Jan-2016		
PayPai		Login with PayPail					15-Apr-2015			
				9-Jun-2019	14-Nov-2019	15-Nov-2019			22-Nov-2019	
ORY GribH Oxidom		ORY Hjers v1.00 GAÎA Trust Platform 4.4			14-Jul-2018 14-Nov-2019	14-Jul-2018 18-Nov-2019	14-Jul-2018 15-Jun-2019		22-Nov-2019	
			qu-2018		16-Apr-2018 14-Jul-2018					
Optimal IdM Oracle		TheOptimalCloud 4.2  Oracle Identity Cloud Service 16-A	im-2018		24-Oct-2017 16-Apr-2018	States over	16-Apr-2018			
OpenAthens Optimal IdM		OpenAthens Cloud TheOstimalCloud 4.2								
Onegini OpenAthens		Onegini Connect 5.0  OpenAthens Cloud		9-Nov-2018 3-Oct-2017	9-Nov-2018		9-Nov-2018 24-Oct-2017			
				May-2016 9-Nov-2018	May-2016	May-2016	May-2016			
Oita		Otta OP		25-	26-	26-	26-		16-Jul-2018	
ogis-Ri		ThemiStruct identity Platform v2.4.	0	22-Jul-2019	22-Jul-2019	22-Jul-2019	22-Jul-2019			
ogis-rti		ThemiStruct identity Platform v2.2.	0	20-Nov-2018	20-Nov-2018	20-Nev-2018	20-Nov-2018			
OGIS-RI		ThemiStruct identity Platform v2.0.	0	5-Mar-2018	5-Mar-2018		5-Mar-2018			
OGIS-RI		ThemiStruct identity Platform v1.3.	0	28-Apr-2017	Maj-2017		28-Apr-2017			
ogis-Ri		Themistruct identity Platform v1.1.	0		7-0d-2016	2. Community	7-0cs-2016			
NTT Software Corporatio		TrustBind Federation Manager			26-Jan-2017					
Nomura Research Institu NRI SecureTechnologies		UNHD Libra 1.0			28-Jul-2017	25, 14, 2017	28-Jul-2017			
Nomura Research Institu Nomura Research Institu		proporac		10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015		
NedReason		Next Reason Central Identity		15-Sep-2018	10-Apr-2015		18-Sep-2018 10-Apr-2015			
NEC		NC7000-3A-OC		7-Mar-2016						
Mothe		Mulne Pederated Identity Hub v1		1-Aug-2017						
Microsoft		EF Experimental Claimer V0.9		9-May-2018			9-May-2018			
ficrosoft		Azure Active Directory V2			15-Jan-2019		15-Jan-2019		15-Jan-2019	

## **Connect RP Certifications**



- Relying Party certifications at <a href="https://openid.net/certification/#RPs">https://openid.net/certification/#RPs</a>
  - 127 profiles certified to date for over 40 deployments
- Recent additions:
  - Erlang Ecosystem Foundation, Filip Skokan, KINTO, SAP, 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/

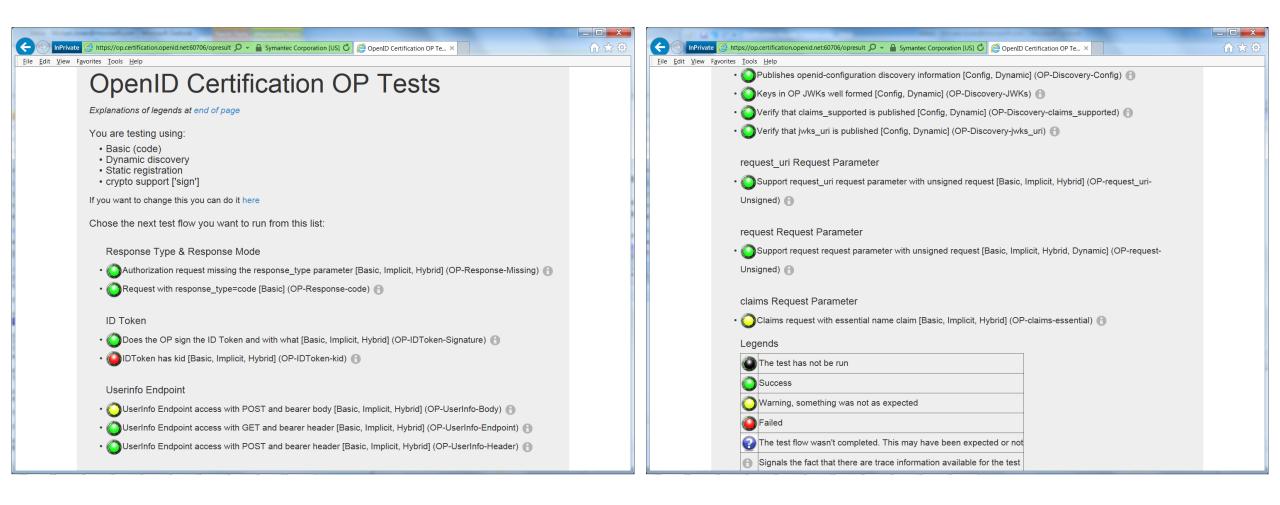
## What does certification cost?



- 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 <a href="https://openid.net/certification/fees/">https://openid.net/certification/fees/</a>

# **Example Testing Screen**





## Log from a Conformance Test



#### Test info

Profile: {'openid-configuration': 'config', 'response type': 'code', 'crypto': 'sign', 'registration': 'static'} Timestamp: 2015-04-07T02:58:53Z Test description: Keys in OP JWKs well formed [Config, Dynamic] Test ID: OP-Discovery-JWKs Issuer: https://stsadweb.one.microsoft.com/adfs

#### Test output

```
After completing the test flow:
[verify-base64url]
       status: OK
       description: Verifies that the base64 encoded parts of a JWK is in fact base64url encoded and not just base64 encoded
[check-http-response]
       status: OK
       description: Checks that the HTTP response status is within the 200 or 300 range
```

#### 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 Release
OpenID Connect Conformance Profile: Basic OpenID Provider
Conformance Test Suite Software: op.certification.openid.net as of April 10, 2015
Test Date: April 10, 2015
1 Certification: Implementer has tested the Deployment (including by successfully completing the

- Certification: Implementer has tested the Deployment (including by successfully completing the
  validation testing using the Conformance Test Suite Software) and verified that it conforms to the
  OpenID Connect Conformance Profile, and hereby certifies to the OpenID Foundation and the public
  that the Deployment conforms to the OpenID Connect Conformance Profile as set forth above.
- Maintenance: If subsequent changes to the Deployment, or other information or testing, indicates that
  the Deployment is not in conformance, Implementer will either correct the nonconformance (and
  update this Certification if necessary) or revoke this Certification.
- Incorporation of Terms: The Terms and Conditions for Certification of Conformance to an OpenID
  Connect Conformance Profile, located at www.openid.net/certification, are incorporated by reference
  in this Certification, and Implementer agrees to be bound by such Terms and Conditions.

Implementer's Address Information	
Address:	1001 17th Street, Suite 100
City, State/Province, Postal Code	Denver, CO 80202
Country	USA
Implementer's Authorized Contact I	nformation
Name:	Brian Campbell
Title:	Distinguished Engineer
Phone:	720.317.2061
Email:	bcampbell@pingidentity.com

Authorized Signature:
Name: Danilwussik
Title: ASIAL Ger Loward
Date: Apr. 10, 25,5

# How does certification relate to interop testing?



- OpenID Connect held 5 rounds of interop testing see <a href="http://osis.idcommons.net/">http://osis.idcommons.net/</a>
  - Starting over a decade ago!
  - Each round improved implementations and specs
  - By the numbers: 20 implementations, 195 members of interop list, > 1000 messages exchanged
- Recently multiple interop testing rounds 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 OpenID 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 new for OpenID Certification? OpenID



- Certification program is now financially self-supporting!
  - Open Banking certifications from Brazil and other places got us there
- OpenID4VC certification tests (for OpenID4VP) started
- eKYC-IDA certification tests planned
- OpenID Federation tests planned

# OpenID Certification Call to Action



- Test your OpenID Connect and FAPI implementations now
  - And once you're ready, certify!
- Join the OpenID Foundation and/or the OpenID Connect working group

## **OpenID Connect Resources**



- OpenID Connect
  - <a href="https://openid.net/connect/">https://openid.net/connect/</a>
- Frequently Asked Questions
  - https://openid.net/connect/faq/
- OpenID Connect Working Group and Specs Status Page
  - https://openid.net/wg/connect/ and https://openid.net/wg/connect/status/
- OpenID for Verifiable Credentials
  - <a href="https://openid.net/openid4vc/">https://openid.net/openid4vc/</a>
- OpenID Certification Program
  - <a href="https://openid.net/certification/">https://openid.net/certification/</a>
- Certified OpenID Connect Implementations Featured for Developers
  - <a href="https://openid.net/developers/certified/">https://openid.net/developers/certified/</a>
- Mike Jones' Blog
  - https://self-issued.info/

# **Open Conversation**



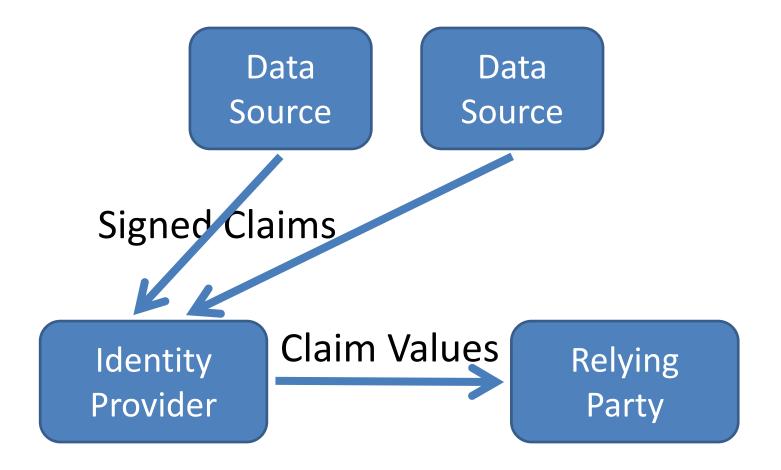
- How are you using OpenID Connect?
- What would you like the working group to know or do?

Slides will be posted at <a href="https://self-issued.info/">https://self-issued.info/</a>

## **BACKUP SLIDES**

# **Aggregated Claims**





## **Distributed Claims**



