Introduction to OpenID Connect

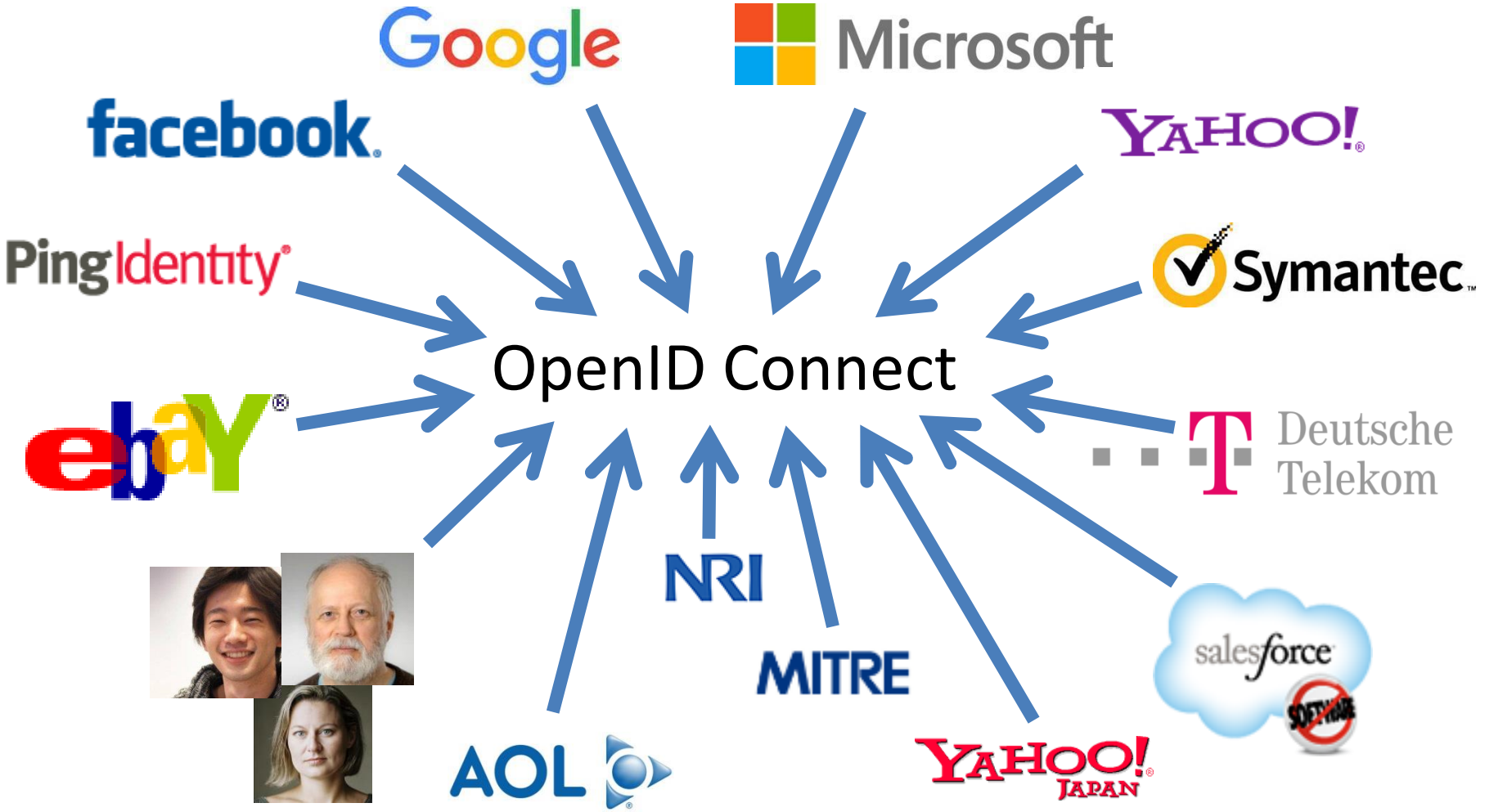
April 28, 2020

Michael B. Jones

Identity Standards Architect – Microsoft

Working Together

OpenID



What is OpenID Connect?

- Simple identity layer on top of OAuth 2.0
- Enables Relying Parties (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!

- If you have an Android phone or log in at Apple, 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
  - https://openid.net/2012/04/18/openid-connect-wins-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 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 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
```

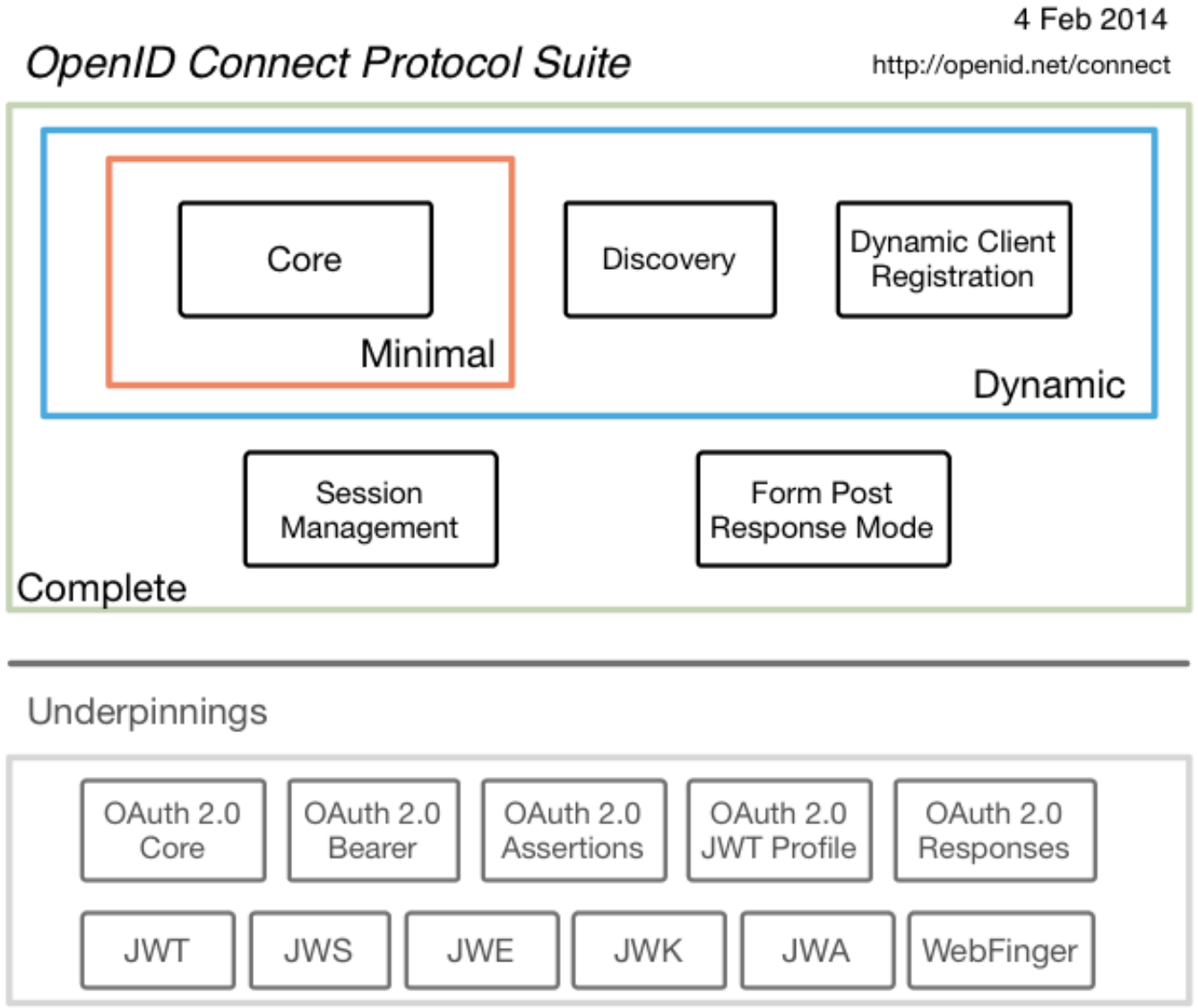
Authorization Response Example


```
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



Additional Final Specifications (1 of 2)

- 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
  - 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

Additional Final Specifications (2 of 2)

- 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
  - https://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 (work 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
- Unfortunately, no one approach best for all use cases
- All support multiple logged in sessions from OP at RP
- Recent WG decision to split RP-Initiated Logout into its own spec
  - Is used with all three OP-Initiated Logout mechanisms
- Logout certification tests now in pilot phase
  - WG is testing multiple implementations before making logout 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
- Second Implementer's Draft status reached
- *Please review and implement!*

Identity Assurance Specification (work in progress)

- 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 new eKYC and Identity Assurance working group
- In review for second Implementer's Draft status
  - *Please review!*

Native SSO Specification (work in progress)

- 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 AS
- New specification written by George Fletcher
  - *Please review!*

Self-Issued OpenID Provider

- OpenID Connect defines Self-Issued OpenID Provider
  - https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued
- Lets you be your own identity provider
  - Rather than a third party
- Identity represented as asymmetric key pair controlled by you

- Self-Issued OpenID Provider being used to achieve DID auth
  - Described at https://self-issued.info/?p=2013

Related Working Groups

- International Government Profile (iGov) WG
  - OpenID Connect profile for government & high-value commercial applications
- Enhanced Authentication Profile (EAP) WG
  - Enables integration with FIDO and other phishing-resistant authentication solutions
- **M**obile **O**perator **D**iscovery, **R**egistration & authe**N**tic**A**tion (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 APIs in many jurisdictions, including the UK
- Research and Education (R&E) WG
  - Profiles OpenID Connect to ease adoption in the Research and Education (R&E) sector
- eKYC and Identity Assurance WG
  - JWT format for verified claims with identity assurance information

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

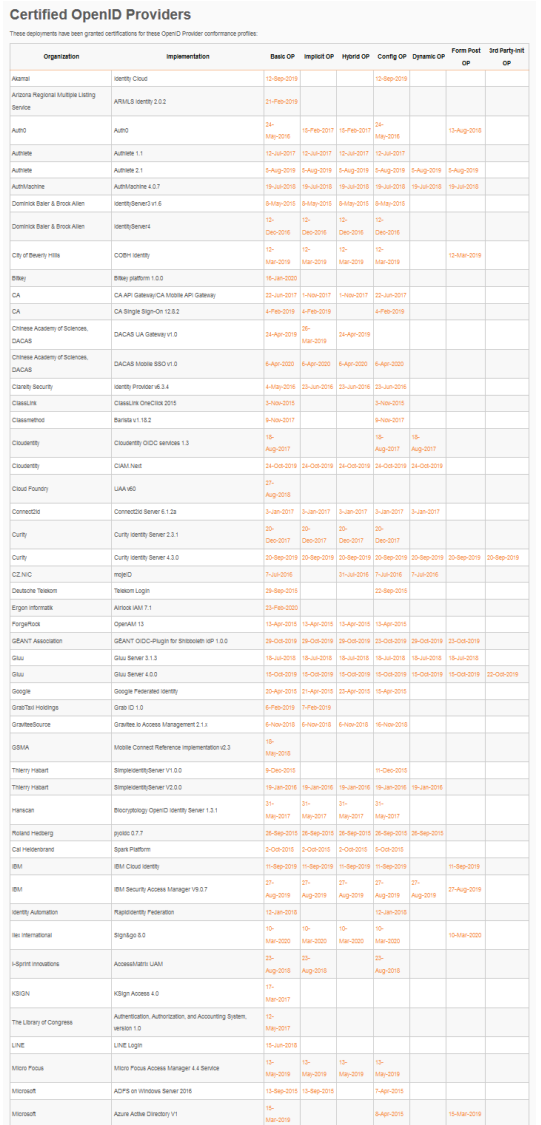
- Now OpenID Connect certification profiles for:
  - Basic OP and Basic RP
  - Implicit OP and Implicit RP
  - Hybrid OP and Hybrid RP
  - OP Publishing and RP Using Configuration Information
  - Dynamic OP and Dynamic RP
  - Form Post Response Mode for OP and RP
  - Third party-initiated login for OP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

New Connect Certification Profiles

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

Connect OP Certifications

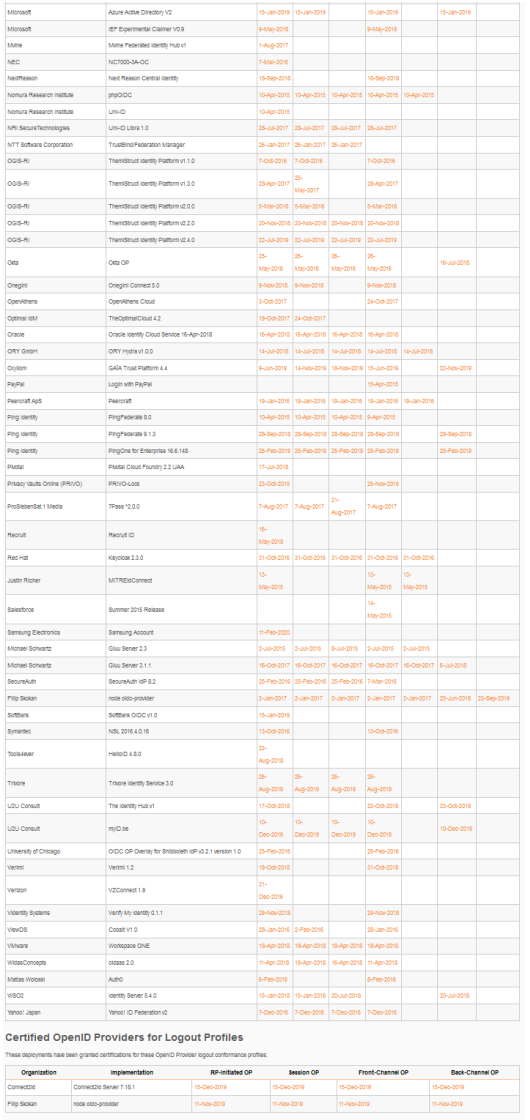
- OpenID Provider certifications at https://openid.net/certification/#OPs
  - 370 profiles certified for 111 implementations by 91 organizations
- Recent additions:
  - Bitkey, Chinese Academy of Sciences, Ergon Informatik, Ilex International, Samsung Electronics
- Each entry link to zip file with test logs and signed legal statement
  - ***Test results available for public inspection***



Certified OpenID Providers

These deployments have been granted certifications for these OpenID Provider conformance profiles:

Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP	Form Post OP	3rd Party-init OP
Akamai	Identity Cloud	12-Sep-2019			12-Sep-2019			
Arizona Regional Multiple Listing Service	ARMLS Identity 2.0.2	21-Feb-2019						
Auth0	Auth0	24-May-2016	15-Feb-2017	15-Feb-2017	24-May-2016		13-Aug-2018	
Authlete	Authlete 1.1	12-Jul-2017	12-Jul-2017	12-Jul-2017	12-Jul-2017			
Authlete	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 Baier & Brock Allen	IdentityServer3 v1.6	9-May-2016	9-May-2016	9-May-2016	9-May-2016			
Dominick Baier & Brock Allen	IdentityServer4	12-Dec-2016	12-Dec-2016	12-Dec-2016	12-Dec-2016			
City of Beverly Hills	COBH Identity	12-Mar-2019	12-Mar-2019	12-Mar-2019	12-Mar-2019		12-Mar-2019	
Bitkey	Bitkey 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 Gateway v1.0	24-Apr-2019	26-Mar-2019	24-Apr-2019				
Chinese Academy of Sciences, DACAS	DACAS Mobile SSO v1.0	6-Apr-2020	6-Apr-2020	6-Apr-2020	6-Apr-2020			
Clarelty Security	Identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016			
ClassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015			
Classmethod	Barista v1.18.2	9-Nov-2017			9-Nov-2017			
Cloudentity	Cloudentity OIDC services 1.3	15-Aug-2017			15-Aug-2017	15-Aug-2017		
Cloudentity	CIAM.Next	24-Oct-2019	24-Oct-2019	24-Oct-2019	24-Oct-2019	24-Oct-2019		
Cloud Foundry	UAA v60	27-Aug-2018						
ConnectID	ConnectID Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017		
Curity	Curity Identity Server 2.3.1	20-Dec-2017	20-Dec-2017	20-Dec-2017	20-Dec-2017			
Curity	Curity Identity Server 4.3.0	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019
CZ NIC	mojeID	7-Jun-2016		31-Jul-2016	7-Jun-2016	7-Jun-2016		
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015			
Ergon Informatik	Airlock IAM 7.1	23-Feb-2020						
ForgeRock	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015			
GÉANT Association	GÉANT OIDC-Plugin for Shibboleth IdP 1.0.0	29-Oct-2019	29-Oct-2019	29-Oct-2019	23-Oct-2019	29-Oct-2019	23-Oct-2019	
Gluu	Gluu Server 3.1.3	18-Jul-2018	18-Jul-2018	18-Jul-2018	18-Jul-2018	18-Jul-2018	18-Jul-2018	
Gluu	Gluu Server 4.0.0	15-Oct-2019	15-Oct-2019	15-Oct-2019	15-Oct-2019	15-Oct-2019	15-Oct-2019	22-Oct-2019
Google	Google Federated Identity	20-Apr-2015	21-Apr-2015	22-Apr-2015	15-Apr-2015			
GrabTaxi Holdings	Grab ID 1.0	6-Feb-2019	7-Feb-2019					
GrantteeSource	Grantee.io Access Management 2.1.x	6-Nov-2016	6-Nov-2016	6-Nov-2016	16-Nov-2016			
GSMA	Mobile Connect Reference Implementation v2.3	15-May-2018						
Thierry Habart	SimpleIdentityServer V1.0.0	9-Dec-2016			11-Dec-2016			
Thierry Habart	SimpleIdentityServer V2.0.0	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016		
Hanscan	Biocryptology OpenID Identity Server 1.3.1	31-May-2017	31-May-2017	31-May-2017	31-May-2017			
Roland Hedberg	pyoidc 0.7.7	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015	26-Sep-2015		
Cal Heldenbrand	Spark Platform	2-Oct-2015	2-Oct-2015	2-Oct-2015	5-Oct-2015			
IBM	IBM Cloud Identity	11-Sep-2019	11-Sep-2019	11-Sep-2019	11-Sep-2019		11-Sep-2019	
IBM	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	
Identity Automation	RapidIdentity Federation	12-Jan-2018			12-Jan-2018			
Ilex International	Sign&go 8.0	10-Mar-2020	10-Mar-2020	10-Mar-2020	10-Mar-2020		10-Mar-2020	
i-Sprint Innovations	AccessMatrix UAM	23-Aug-2018	23-Aug-2018		23-Aug-2018			
KSIGN	KSign Access 4.0	17-Mar-2017						
The Library of Congress	Authentication, Authorization, and Accounting System, version 1.0	12-May-2017						
LINE	LINE Login	15-Jun-2018						
Micro Focus	Micro Focus Access Manager 4.4 Service	13-May-2019	13-May-2019	13-May-2019	13-May-2019			
Microsoft	ADFS on Windows Server 2016	13-Sep-2015	13-Sep-2015		7-Apr-2015			
Microsoft	Azure Active Directory V1	15-Mar-2019			8-Apr-2016		13-Mar-2019	



Microsoft	Azure Active Directory V2	15-Jan-2019	15-Jan-2019		15-Jan-2019		15-Jan-2019	
Microsoft	IDF Experimental Claimer V0.9	9-May-2018			9-May-2018			
Mvine	Mvine Federated Identity Hub v1	1-Aug-2017						
NEC	NC7000-3A-OC	7-Mar-2016						
NextReason	Next Reason Central Identity	19-Sep-2018			19-Sep-2018			
Nomura Research Institute	phpOIDC	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015		
Nomura Research Institute	UmI-ID	10-Apr-2015						
NRI SecureTechnologies	UmI-ID Libra 1.0	28-Jul-2017	28-Jul-2017	28-Jul-2017	28-Jul-2017			
NTT Software Corporation	TrustBindFederation Manager	26-Jan-2017	26-Jan-2017	26-Jan-2017				
OGIS-RI	ThemiStruct Identity Platform v1.1.0	7-Oct-2016	7-Oct-2016		7-Oct-2016			
OGIS-RI	ThemiStruct Identity Platform v1.3.0	29-Apr-2017	29-May-2017		29-Apr-2017			
OGIS-RI	ThemiStruct Identity Platform v2.0.0	5-Mar-2018	5-Mar-2018		5-Mar-2018			
OGIS-RI	ThemiStruct Identity Platform v2.2.0	20-Nov-2018	20-Nov-2018	20-Nov-2018	20-Nov-2018			
OGIS-RI	ThemiStruct Identity Platform v2.4.0	22-Jul-2019	22-Jul-2019	22-Jul-2019	22-Jul-2019			
Okta	Okta OP	25-May-2016	25-May-2016	26-May-2016	26-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-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018			
ORY GmbH	ORY Hydra v1.0.0	14-Jul-2018	14-Jul-2018	14-Jul-2018	14-Jul-2018	14-Jul-2018		
Oxylom	GAIA Trust Platform 4.4	9-Jun-2019	14-Nov-2019	15-Nov-2019	15-Jun-2019		22-Nov-2019	
PayPal	Login with PayPal				15-Apr-2015			
Peercraft ApS	Peercraft	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016		
Ping Identity	PingFederate 8.0	19-Apr-2015	19-Apr-2015	10-Apr-2015	9-Apr-2015			
Ping Identity	PingFederate 9.1.3	28-Sep-2018	28-Sep-2018	28-Sep-2018	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		25-Feb-2019	
Pivotal	Pivotal Cloud Foundry 2.2 UAA	17-Jul-2018						
Privacy Vaults Online (PRIVO)	PRIVO-Lock	23-Oct-2015			29-Nov-2015			
ProSleepenSat.1 Media	TPass *2.0.0	7-Aug-2017	7-Aug-2017	21-Aug-2017	7-Aug-2017			
Recruit	Recruit ID	19-May-2018						
Red Hat	Keycloak 2.3.0	31-Oct-2016	31-Oct-2016	31-Oct-2016	31-Oct-2016	31-Oct-2016		
Justin Richer	MITREidConnect	13-May-2015			13-May-2015	13-May-2015		
Salesforce	Summer 2015 Release				14-May-2015			
Samsung Electronics	Samsung Account	11-Feb-2020						
Michael Schwartz	Gluu Server 2.3	2-Jul-2015	2-Jul-2015	9-Jul-2015	2-Jul-2015	2-Jul-2015		
Michael Schwartz	Gluu Server 3.1.1	16-Oct-2017	16-Oct-2017	16-Oct-2017	16-Oct-2017	16-Oct-2017	5-Jul-2018	
SecureAuth	SecureAuth IdP 8.2	25-Feb-2016	25-Feb-2016	25-Feb-2016	7-Mar-2016			
Filip Skokan	node oidc-provider	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017	2-Jan-2017	25-Jun-2018	23-Sep-2019
Softbank	Softbank OIDC v1.0	15-Jan-2019						
Symantec	NSL 2016.4.0.16	13-Oct-2016			13-Oct-2016			
Tools4ever	HelloID 4.8.0	22-Aug-2018						
Trilsore	Trilsore Identity Service 3.0	25-Aug-2019	25-Aug-2019	26-Aug-2019	26-Aug-2019			
UZU Consult	The Identity Hub v1	17-Oct-2018			23-Oct-2018		23-Oct-2018	
UZU Consult	myID.be	10-Dec-2019	10-Dec-2019	10-Dec-2019	10-Dec-2019		10-Dec-2019	
University of Chicago	OIDC OP Overlay for Shibboleth IdP v3.2.1 version 1.0	25-Feb-2016			25-Feb-2016			
Verimi	Verimi 1.2	19-Oct-2018			31-Oct-2018			
Verizon	VZConnect 1.9	21-Dec-2016						
Vidanity Systems	Verify My Identity 01.1	29-Nov-2018			29-Nov-2018			
ViewDS	Cobalt V1.0	29-Jan-2016	2-Feb-2016		29-Jan-2016			
VMware	Workspace ONE	18-Apr-2018	18-Apr-2018	18-Apr-2018	18-Apr-2018			
WidasConcepts	cidaas 2.0	11-Apr-2018	19-Apr-2018	16-Apr-2018	11-Apr-2018			
Matias Woloski	Auth0	8-Feb-2016			9-Feb-2016			
WSO2	Identity Server 5.4.0	15-Jan-2019	15-Jan-2019	20-Jul-2019			20-Jul-2018	
Yahoo! Japan	Yahoo! ID Federation v2	7-Dec-2016	7-Dec-2016	7-Dec-2016	7-Dec-2016			

Certified OpenID Providers for Logout Profiles

These deployments have been granted certifications for these OpenID Provider logout conformance profiles:

Organization	Implementation	RP-initiated OP	Session OP	Front-Channel OP	Back-Channel OP
ConnectID	ConnectID Server 7.10.1	15-Dec-2019	15-Dec-2019	15-Dec-2019	15-Dec-2019
Filip Skokan	node oidc-provider	11-Nov-2019	11-Nov-2019	11-Nov-2019	11-Nov-2019

Connect RP Certifications

- Relying Party certifications at https://openid.net/certification/#RPs
  - 77 profiles certified for
    30 implementations by
    18 organizations
- Recent additions:
  - Ilex International, Roland Hedberg

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-Init RP
Brock Allen	oidc-client-js 1.3		4-Feb-2017		7-Feb-2017			
Dominick Baier	IdentityModel.OidcClient 2.0	27-Jan-2017			6-Feb-2017			
Damien Bowden	angular-auth-oidc-client 1.0.2		21-Jun-2017		11-Aug-2017			
F5 Networks	BIG-IP 13.1.0 Evergreen	7-Jul-2017						
Thierry Habart	SimpleIdentityServer V1.0.1	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017		
Ilex 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

A Very International Effort

- European programmers developed and operate the certification test suites:
  - Roland Hedberg, Sweden
  - Joseph Heenan, UK
  - Serkan Özkan, Turkey
  - Tomas Pazderka, Czech Republic
  - Filip Skokan, Czech Republic
  - Hans Zandbelt, Netherlands
- OpenID Connect leadership also very international:
  - Nat Sakimura, Japan
  - John Bradley, Chile
  - Michael Jones, United States

Use of Self-Certification

- OpenID Certification uses self-certification
  - Party seeking certification does the testing
  - (rather than paying a 3rd party to do the testing)
- Simpler, quicker, less expensive, more scalable than 3rd party certification
- Results are nonetheless trustworthy because
  - Testing logs are made available for public scrutiny
  - Organization puts its reputation on the line by making a public declaration that its implementation conforms to the profile being certified to

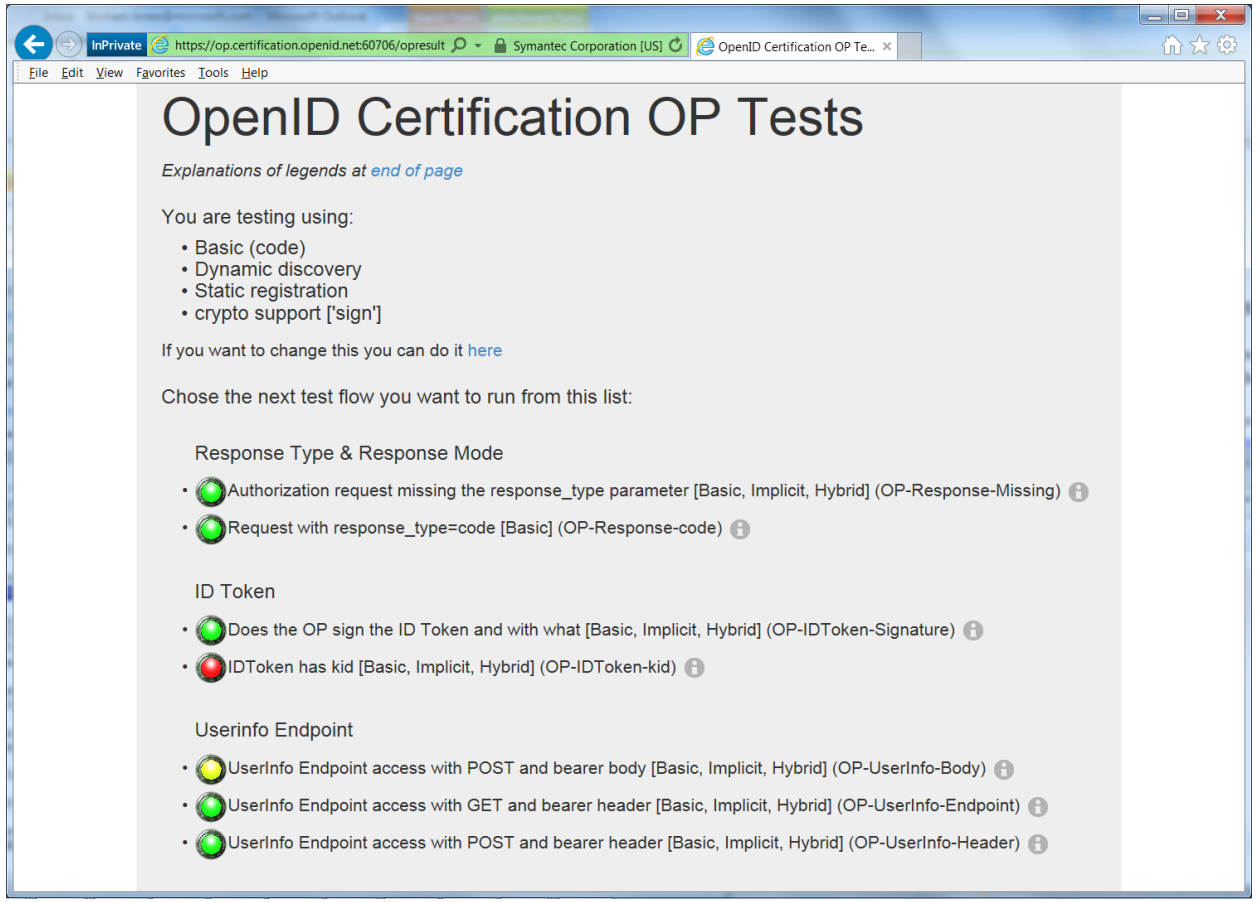
How does OpenID Certification work?

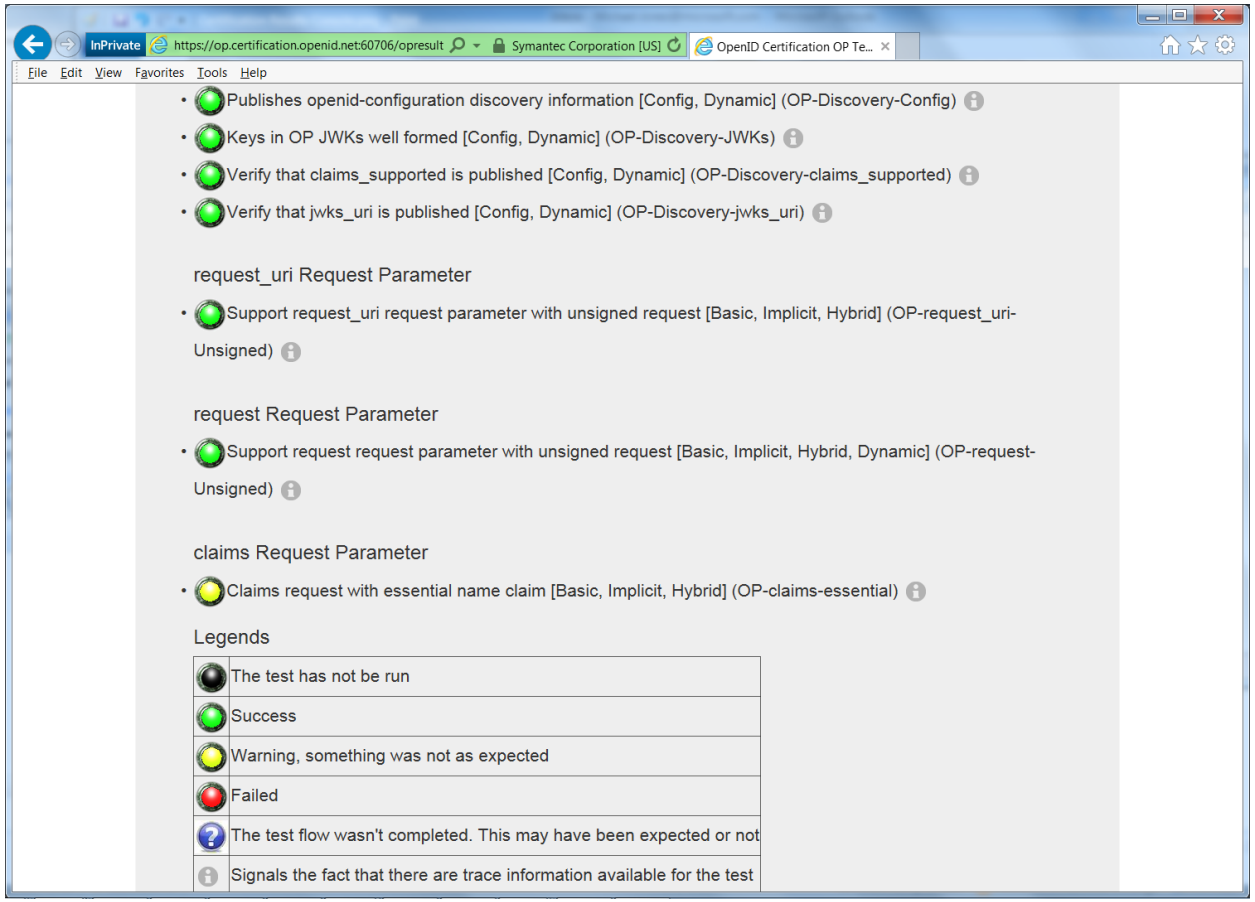
- Organization decides what profiles it wants to certify to
  - For instance, “Basic OP”, “Config OP”, and “Dynamic OP”
- Runs conformance tests publicly available at https://op.certification.openid.net/ or https://rp.certification.openid.net/ or https://www.certification.openid.net/
- Once all tests 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
  - $500
- Non-member price
  - $2500
- 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
__X:==== END ====__
```

Trace output

```
0.000288 ------------ DiscoveryRequest ------------
0.000299 Provider info discover from 'https://stsadweb.one.microsoft.com/adfs'
0.000305 --> URL: https://stsadweb.one.microsoft.com/adfs/.well-known/openid-configuration
0.426715 ProviderConfigurationResponse: {
  "access_token_issuer": "http://stsadweb.one.microsoft.com/adfs/services/trust",
  "authorization_endpoint": "https://stsadweb.one.microsoft.com/adfs/oauth2/authorize/",
  "claims_parameter_supported": false,
  "claims_supported": [
    "aud",
    "iss",
    "iat",
    "exp",
    "auth_time",
    "nonce",
    "at_hash",
    "c_hash",
    "sub",
    "upn",
    "unique_name",
    "pwd_url",
    "pwd_exp",
    "ver"
  ],
  "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": [
    "RS256"
  ],
  "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": [
    "RS256"
  ],
  "version": "3.0",
  "webfinger_endpoint": "https://stsadweb.one.microsoft.com/adfs/.well-known/webfinger"
}
0.846957 JWKS: {
  "keys": [
    {
      "alg": "RS256",
      "e": "AQAB",
      "kid": "f-5GWKyaV6fDdnKB7A3b0llXZ0E",
      "kty": "RSA",
      "n": "ygUNL9XXanKy_fQ1X0SMt9LRKpH3Xup11k5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW0lI8FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS_2C
      "use": "sig",
      "x5c": [
        "MIIFrjCCBJagAwIBAgIKEzgGLwABAACESDANBgkqhkiG9w0BAQUFADCBgDETMBEGCgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCWlpY3Jvc29
      ],
      "x5t": "f-5GWKyaV6fDdnKB7A3b0llXZ0E"
    }
  ]
}
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

OpenID

CERTIFICATION OF CONFORMANCE
TO OPENID CONNECT CONFORMANCE PROFILE

Name of Entity ("Implementer") Making this Certification: Ping Identity Corporation

Software or Service ("Deployment") Name & Version #: PingFederate Summer 2015 Release

OpenID Connect Conformance Profile: Basic OpenID Provider

Conformance Test Suite Software: op.certification.openid.net as of April 10, 2015

Test Date: April 10, 2015

1. Certification: Implementer has tested the Deployment (including by successfully completing the validation testing using the Conformance Test Suite Software) and verified that it conforms to the OpenID Connect Conformance Profile, and hereby certifies to the OpenID Foundation and the public that the Deployment conforms to the OpenID Connect Conformance Profile as set forth above.
2. 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.
3. Incorporation of Terms: The Terms and Conditions for Certification of Conformance to an OpenID Connect Conformance Profile, located at www.openid.net/certification, are incorporated by reference in this Certification, and Implementer agrees to be bound by such Terms and Conditions.

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

Authorized Signature: _____

Name: David Wasserman

Title: Assoc. Gen. Counsel

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 using Apache 2.0 license
  - Some projects have deployed private instances for internal testing
  - Available as a Docker container

Favorite Comments on OpenID Certification

- Eve Maler – VP of Innovation at ForgeRock
  - "You made it as simple as possible so every interaction added value."
- Jaromír Talíř – CZ.NIC
  - "We used and still are using certification platform mainly as testing tool for our IdP. Thanks to this tool, we have fixed enormous number of bugs in our platform an even some bugs in the underlying library."
- Brian Campbell – Distinguished Engineer at Ping Identity
  - "The process has allowed us to tighten up our implementation and improve on the already solid interoperability of our offerings in the OpenID Connect ecosystem."
- William Denniss – Google
  - "We have built the RP tests into the continuous-integration testing pipeline for AppAuth."

FAPI Certification Status

- Financial-grade API (FAPI) implementations now being certified
- FAPI Part 2 OP certification launched in April 2019
  - 18 implementations certified to date
- Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) launched in September 2019
  - One implementation certified to date
- FAPI Part 2 RP certification tests launched in December 2019
  - One implementation certified to date

What's next for OpenID Certification?

- Connect Certification code being reimplemented in Java
  - Current implementation in Python
  - Moving to the same code base as FAPI certification
  - Expect migration to Java implementation later this year
- Additional FAPI profiles being developed:
  - FAPI-CIBA RP
- Certification for additional specifications is anticipated:
  - E.g., HEART, MODRNA, iGov, EAP, etc.

OpenID Certification Call to Action

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

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
  - https://self-issued.info/
- Nat Sakimura's Blog
  - https://nat.sakimura.org/
- John Bradley's Blog
  - https://www.thread-safe.com/

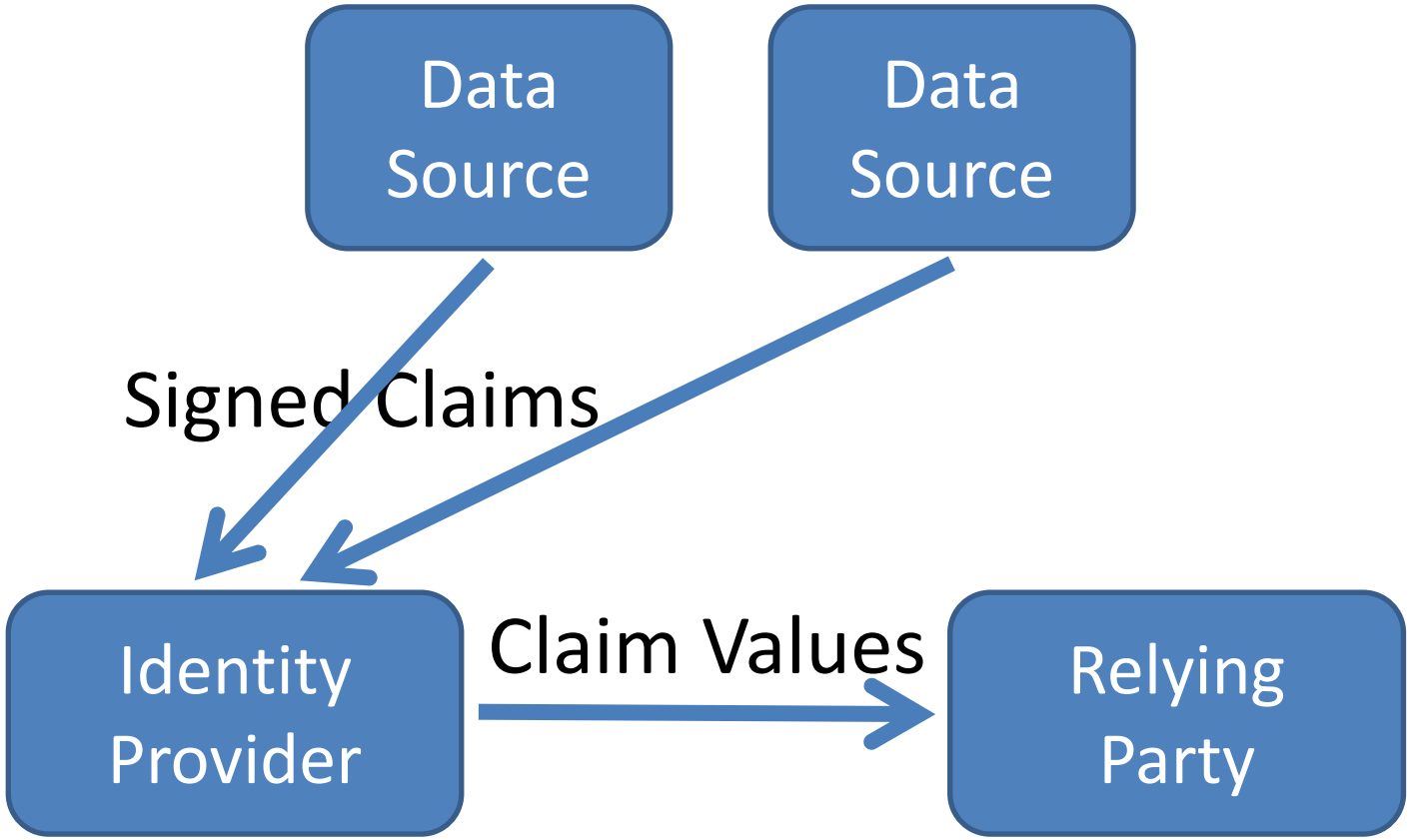
Open Conversation

- 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