



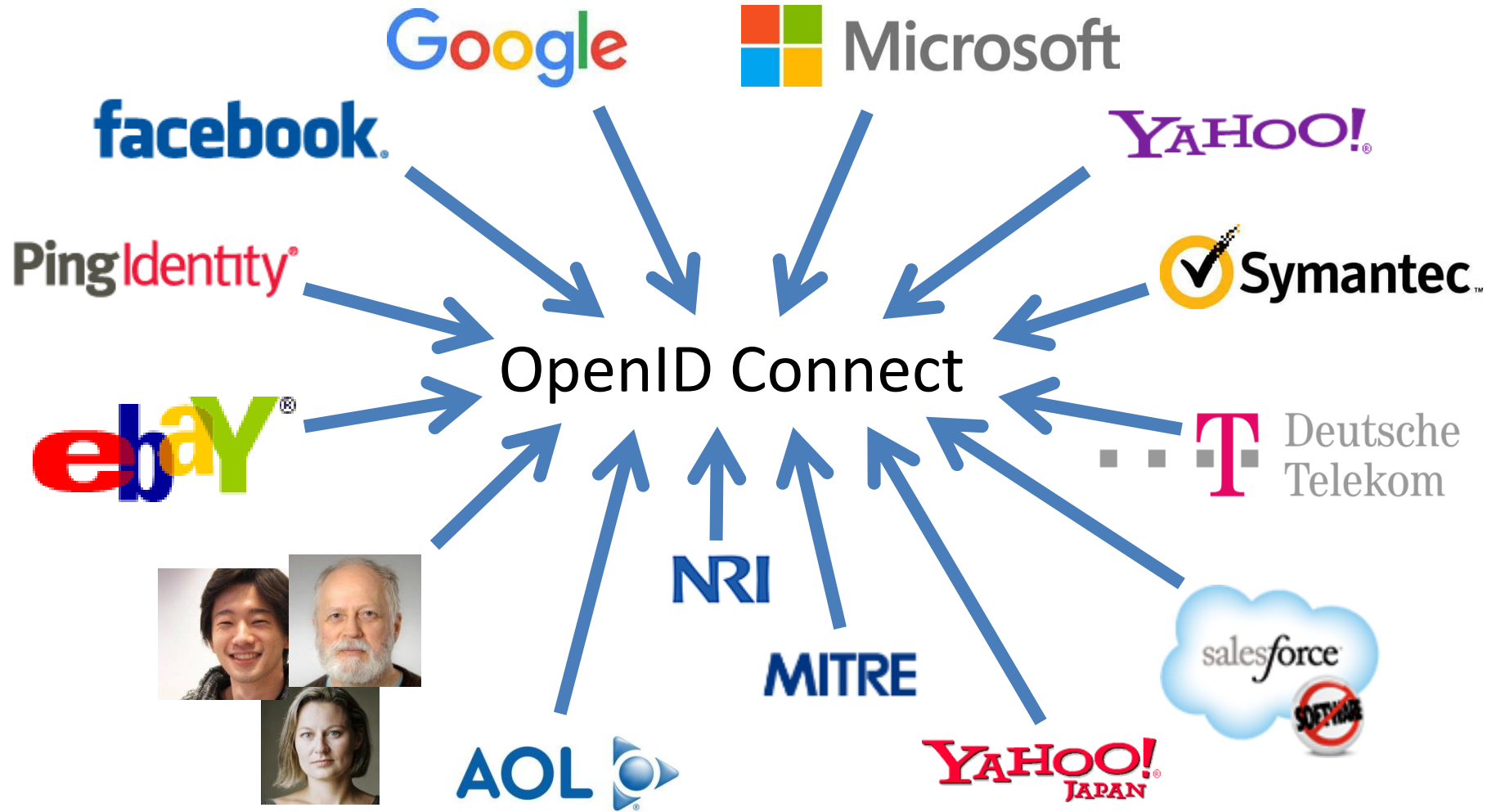
Introduction to OpenID Connect

April 8, 2025

Michael B. Jones

Self-Issued Consulting

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-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)
- 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
- 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-present
- Errata Set 2 approved, December 2023
- **OpenID Connect specs published as ISO PAS specifications, October 2024**
- Errata Set 3 draft published in January 2025 with security fix

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
 - `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=af0ifjldkj
&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=eyJhbGZlNiJ9.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
```

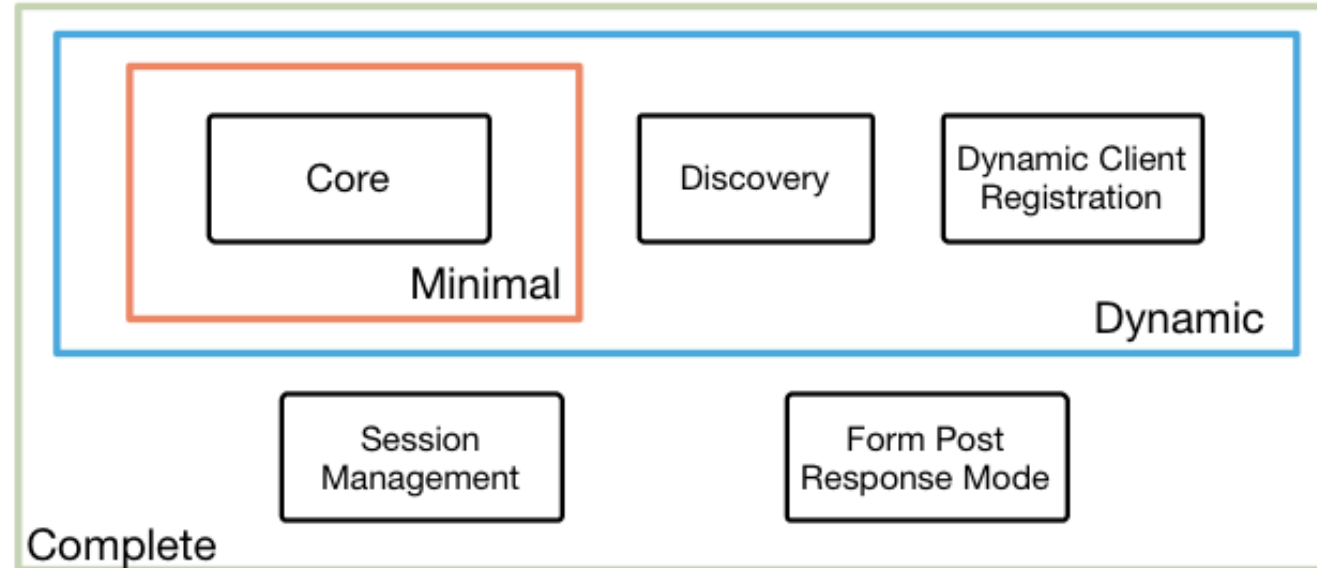
Original Overview of Specifications



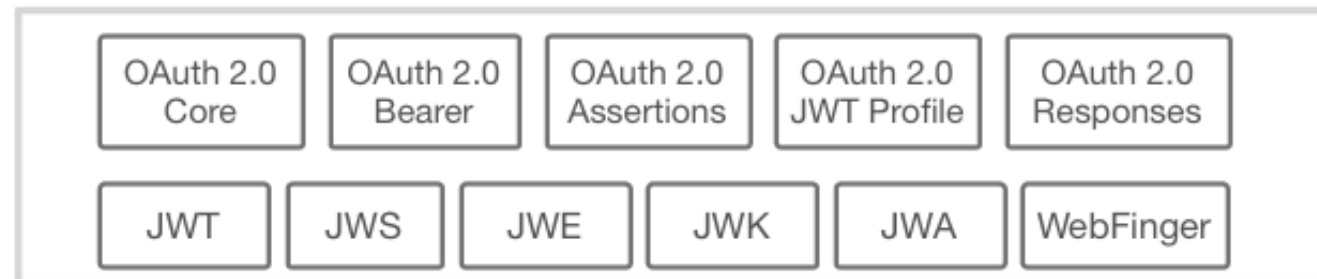
4 Feb 2014

OpenID Connect Protocol Suite

<http://openid.net/connect>



Underpinnings



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
 - 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
- *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*

Celebrating Ten Years of OpenID Connect OpenID

- OpenID Connect specifications were approved in February 2014
- Three celebrations were held
 - January 2024 at Japan OpenID Summit in Tokyo
 - May 2024 at Identiverse in Las Vegas
 - June 2024 at EIC in Berlin
- Presentations from first celebration published at <https://self-issued.info/?p=2481>
- During the celebrations, we shared our perspectives on
 - How we developed OpenID Connect
 - Why it succeeded
 - Lessons we learned along the way
- Lessons learned
 - “Keep simple things simple”
 - Repeated interop testing and incorporating resulting feedback from developers was critical
 - Certification enables an ecosystem of interoperable implementations

OpenID Connect ISO Specifications



- OpenID Connect specifications published as ISO PAS specs, October 2024!
 - Will enable use of OpenID Connect in jurisdictions requiring specs by treaty organizations
- [ISO/IEC 26131:2024 – Information technology – OpenID connect – OpenID connect core 1.0 incorporating errata set 2](#)
 - [ISO/IEC 26132:2024 – Information technology – OpenID connect – OpenID connect discovery 1.0 incorporating errata set 2](#)
 - [ISO/IEC 26133:2024 – Information technology – OpenID connect – OpenID connect dynamic client registration 1.0 incorporating errata set 2](#)
 - [ISO/IEC 26134:2024 – Information technology – OpenID connect – OpenID connect RP-initiated logout 1.0](#)
 - [ISO/IEC 26135:2024 – Information technology – OpenID connect – OpenID connect session management 1.0](#)
 - [ISO/IEC 26136:2024 – Information technology – OpenID connect – OpenID connect front-channel logout 1.0](#)
 - [ISO/IEC 26137:2024 – Information technology – OpenID connect – OpenID connect back-channel logout 1.0 incorporating errata set 1](#)
 - [ISO/IEC 26138:2024 – Information technology – OpenID connect – OAuth 2.0 multiple response type encoding practices](#)
 - [ISO/IEC 26139:2024 – Information technology – OpenID connect – OAuth 2.0 form post response mode](#)

Exciting time for OpenID Connect!



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

OpenID Federation Specification



- https://openid.net/specs/openid-federation-1_0.html
- Enables trust establishment and maintenance of multilateral federations
 - Applying lessons learned from large-scale SAML federations
- Renamed from “OpenID Connect Federation” to reflect broader role
 - Can be used both with and without OpenID Connect
 - For instance, also for trust establishment in Wallet ecosystems
- Three interop events were held in 2020
- In production use in Italy, Australia, Sweden
- Certification tests being written
 - https://openid.net/certification/federation_testing/
- Security analysis by preparing for Final status performed
- In-person interop event being held in Stockholm later this month
- *Plan to take to Final status after applying feedback from interop, certifications*

Vulnerability in JWT Audience for AS (1) OpenID

- Found by University of Stuttgart researchers during OpenID Federation security analysis
- Described in public disclosure
 - <https://openid.net/notice-of-a-security-vulnerability/>
- OpenID Federation fixed
- OpenID Connect Core errata in progress
- FAPI 2.0 fixed
- FAPI 1.0 errata in progress
- CIBA Core errata in progress
- Several OAuth specs being updated by rfc7523bis specification

Vulnerability in JWT Audience for AS (2)

- Fix is requiring that audience value of JWTs sent to the authorization server be ***solely the authorization server issuer identifier***
- Previously, audience values were all over the map, providing ambiguity that attackers could exploit

Due to historical reasons, there is potential ambiguity regarding the appropriate audience value to use when employing JWT client assertion-based authentication (defined in [Section 2.2](#) of [\[RFC7523\]](#) with `private_key_jwt` or `client_secret_jwt` authentication method names per Section 9 of [\[OIDC\]](#)). To address that ambiguity, the issuer identifier URL of the authorization server according to [\[RFC8414\]](#) **SHOULD** be used as the value of the audience. In order to facilitate interoperability, the authorization server **MUST** accept its issuer identifier, token endpoint URL, or pushed authorization request endpoint URL as values that identify it as an intended audience.

OpenID Federation Extended Subordinate Listing



- https://openid.net/specs/openid-federation-extended-listing-1_0.html
- Extends OpenID Federation to provide efficient methods to interact with potentially large number of participating Entities
- Motivated by open finance use cases in Australia, etc.
- ***Implementations and feedback wanted!***

OpenID Federation Wallet Architectures



- https://openid.net/specs/openid-federation-wallet-1_0.html
- Defines entity types for trust establishment for wallet ecosystems with OpenID Federation
 - `openid_wallet_provider`
 - `openid_credential_issuer`
 - `openid_credential_verifier`
- ***Implementations and feedback wanted!***

OpenID Connect Relying Party Metadata Choices



- https://openid.net/specs/openid-connect-rp-metadata-choices-1_0.html
- Lets RPs declare all supported metadata parameters to OPs
 - In existing OpenID Connect Dynamic Client Registration spec, only one value expressed for each choice
- ***Possibly time for an Implementer's Draft***

OpenID for Verifiable Credentials

(Related Work Transferred to DCP WG)



- Family of 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, possibly redacting some claims
- Credential format agnostic
 - Can be used w/ W3C VCs, ISO Mobile Driving Licenses (mDL), SD-JWTs, etc.
- Good privacy properties
 - Issuer doesn't know when/where you're using the credential
- See <https://openid.net/openid4vc/>

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
 - E.g., can use with ISO Mobile Driving Licenses (mDL), SD-JWTs
- Includes issuer-initiated flow

OpenID for Verifiable Presentations



- 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
 - E.g., can use with ISO Mobile Driving Licenses (mDL), SD-JWTs
- *Plan to start reviews to become final at end of this week*

Native Single-Sign-On for Mobile Apps



- 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
- Updates planned to remove use of ID Token
- *Progressing towards Final status*

Related OpenID Working Groups



- **Mobile Operator Discovery, Registration, & authentication (MODRINA)**
 - Mobile operator profiles for OpenID Connect
- **Financial-grade API (FAPI)**
 - FAPI used for Open Finance in jurisdictions including UK, Australia, Brazil, Saudi Arabia, Norway, Germany, Japan, Canada, & more to come...
- **eKYC and Identity Assurance (eKYC-IDA)**
 - Defines JWT format for verified claims with identity assurance information
- **Digital Credentials Protocols (DCP)**
 - Future home of OpenID for Verifiable Credentials (OpenID4VC) specs

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
- *Became Final in October 2024*

CIBA Core

(Related Work in MODRNA WG)



- OpenID Connect Client-Initiated Backchannel Authentication (CIBA) Core
 - https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html
- Authentication flow with direct Relying Party to OpenID Provider communication without redirects through browser
- Used by FAPI CIBA Profile
- Errata 1 draft published with security fix
- *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
- *4,109 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 (RP Metadata)
- Form Post Response Mode
- Logout
 - RP-Initiated Logout
 - Session Management
 - Front-Channel Logout
 - Back-Channel Logout

OpenID Connect OP Certifications



- OpenID Provider certifications at <https://openid.net/certification/#OPs>
 - 695 profiles certified to date for 180 deployments
- Recent certifications
 - Duende Software, Luiky Vasconcelos, malachite, Nevis Security AG
- 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	Confg OP	Dynamic OP	Form Post OP	3rd Party-Int OP
Akamai	Identix Cloud	10-Sep-2018			10-Sep-2018			
Arizona Regional Multiple Listing Service	ARMLS Identix 1.0.2	21-Feb-2019						
Auth0	Auth0	28-Mar-2018	18-Feb-2017	15-Feb-2017	28-Mar-2018		10-Aug-2018	
Authlete	Authlete 1.1	10-Jun-2017	10-Jun-2017	10-Jun-2017	10-Jun-2017			
Authlete	Authlete 2.1	2-Aug-2018	2-Aug-2018	2-Aug-2018	2-Aug-2018	2-Aug-2018	2-Aug-2018	
AuthzOne	AuthzOne 4.0.7	19-Jul-2018	19-Jul-2018	19-Jul-2018	19-Jul-2018			
Control4cast & Brock Allen	IdentixServer v1.6	8-May-2016	8-May-2016	8-May-2016	8-May-2016			
Control4cast & Brock Allen	IdentixServer	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016			
City of Beavert Hills	COB Identity	15-Mar-2019	15-Mar-2019	15-Mar-2019	15-Mar-2019		10-Mar-2019	
Bitly	Bitly platform 1.0.0	16-Jun-2020						
CA	CA API Gateway/CA Mobile API Gateway	20-Jan-2017	1-Nov-2017	1-Nov-2017	20-Jan-2017			
CA	CA Single Sign-On 12.0.2	4-Feb-2019	4-Feb-2019	4-Feb-2019	4-Feb-2019			
Chinese Academy of Sciences, DACAS	DACAS UA Gateway v1.0	24-Apr-2019	24-Apr-2019	24-Apr-2019				
Chinese Academy of Sciences, DACAS	DACAS Mobile BSO v1.0	8-Apr-2020	8-Apr-2020	8-Apr-2020	8-Apr-2020			
Cloudify	Identix Provider v1.3.4	4-May-2018	23-Jul-2018	23-Jul-2018	23-Jul-2018			
Cloudify	Cloudify ODD service 1.3	15-Aug-2017			15-Aug-2017			
Cloudify	CIAM Next	24-Oct-2019	24-Oct-2019	24-Oct-2019	24-Oct-2019			
Cloud Foundry	LAM v60	25-Aug-2018						
Connectix	Connectix Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017			
Curly	Curly Identity Server 2.1.1	20-Dec-2017	20-Dec-2017	20-Dec-2017	20-Dec-2017			
Curly	Curly Identity Server 4.1.0	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019	20-Sep-2019	
CZ.NC	ncp4d	7-Jul-2016		7-Jul-2016	7-Jul-2016			
Deutsche Telekom	Telecom Login	28-Sep-2018			28-Sep-2018			
Ergon Informatics	ERGON IAM 7.1	23-Feb-2020						
ForgeRock	OpenAM 13	15-Apr-2019	15-Apr-2019	15-Apr-2019	15-Apr-2019			
GEANT Association	GEANT ODD-Plugin for Shibboleth v1.0	28-Oct-2019	28-Oct-2019	28-Oct-2019	28-Oct-2019	28-Oct-2019	28-Oct-2019	
Gluu	Gluu Server 3.1.0	16-Jul-2018	16-Jul-2018	16-Jul-2018	16-Jul-2018	16-Jul-2018	16-Jul-2018	
Gluu	Gluu Server 4.0.0	10-Oct-2019	10-Oct-2019	10-Oct-2019	10-Oct-2019	10-Oct-2019	10-Oct-2019	
Google	Google Federated Identity	20-Apr-2019	21-Apr-2019	20-Apr-2019	20-Apr-2019			
GridTee Holdings	Grid ID 1.0	4-Feb-2019	7-Feb-2019					
Grindstone	Grindstone Access Management 2.1.x	4-Nov-2018	4-Nov-2018	4-Nov-2018	4-Nov-2018			
GSMA	Mobile Connect Reference Implementation v2.0	18-May-2018						
Thierry Inpat	SimpleIdP/Server V1.0.0	9-Dec-2018			9-Dec-2018			
Thierry Inpat	SimpleIdP/Server V2.0.0	18-Jan-2018	18-Jan-2018	18-Jan-2018	18-Jan-2018			
hanson	hson/identity OpenID Identity Server 1.3.1	21-May-2017	21-May-2017	21-May-2017	21-May-2017			
Horizon Hedberg	horizon 0.7.7	28-Sep-2018	28-Sep-2018	28-Sep-2018	28-Sep-2018	28-Sep-2018		
Carl Heisterbrand	Spok Platform	2-Oct-2016	2-Oct-2016	2-Oct-2016	2-Oct-2016			
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			
Identity Automation	Identity Automation	12-Jan-2018			12-Jan-2018			
Ne Information	Sign4Sign 0.0	10-Mar-2020	10-Mar-2020	10-Mar-2020	10-Mar-2020		10-Mar-2020	
i-Sprint Innovations	ACORNWATH LAM	23-Aug-2018	23-Aug-2018	23-Aug-2018	23-Aug-2018			
K8Sign	K8Sign Access 4.0	17-Nov-2017						
The Library of Congress	Authentication, Authorization, and Accounting System, version 1.0	17-May-2017						
LINE	LINE Login	15-Jan-2018						
Micro Focus	Micro Focus Access Manager 4.4 Service	15-May-2019	15-May-2019	15-May-2019	15-May-2019			
Microsoft	ADFS on Windows Server 2016	15-Sep-2016	15-Sep-2016	7-Apr-2016				
Microsoft	Azure Active Directory V1	15-Sep-2016			15-Sep-2016		15-Sep-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
Connectix	Connectix Server 1.6.1	10-Dec-2018	10-Dec-2018	10-Dec-2018	10-Dec-2018
Phil Stokan	nose-oid-provider	11-Nov-2019	11-Nov-2019	11-Nov-2019	11-Nov-2019

OpenID Connect RP Certifications



- Relying Party certifications at <https://openid.net/certification/#RPs>
 - 120 profiles certified to date for 44 deployments
- Recent certifications
 - Filip Skokan

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 Mataka	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	OIDCryp v0.6.6	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



OpenID Certification OP Tests

Explanations of legends at [end of page](#)

You are testing using:

- Basic (code)
- Dynamic discovery
- Static registration
- crypto support ['sign']

If you want to change this you can do it [here](#)

Chose the next test flow you want to run from this list:

Response Type & Response Mode

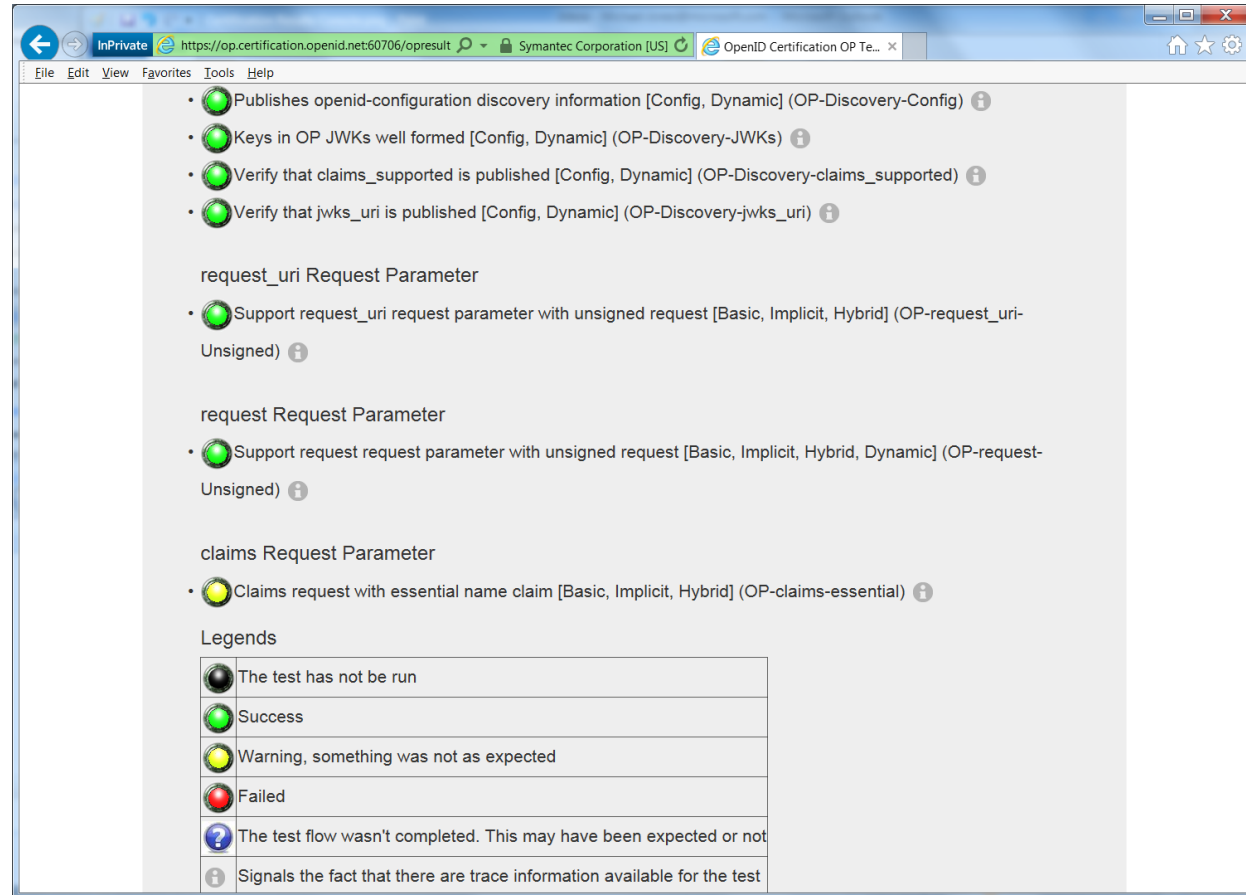
- Authorization request missing the response_type parameter [Basic, Implicit, Hybrid] (OP-Response-Missing) ⓘ
- Request with response_type=code [Basic] (OP-Response-code) ⓘ

ID Token

- Does the OP sign the ID Token and with what [Basic, Implicit, Hybrid] (OP-IDToken-Signature) ⓘ
- IDToken has kid [Basic, Implicit, Hybrid] (OP-IDToken-kid) ⓘ

Userinfo Endpoint

- UserInfo Endpoint access with POST and bearer body [Basic, Implicit, Hybrid] (OP-UserInfo-Body) ⓘ
- UserInfo Endpoint access with GET and bearer header [Basic, Implicit, Hybrid] (OP-UserInfo-Endpoint) ⓘ
- UserInfo Endpoint access with POST and bearer header [Basic, Implicit, Hybrid] (OP-UserInfo-Header) ⓘ



- Publishes openid-configuration discovery information [Config, Dynamic] (OP-Discovery-Config) ⓘ
- Keys in OP JWKS well formed [Config, Dynamic] (OP-Discovery-JWKS) ⓘ
- Verify that claims_supported is published [Config, Dynamic] (OP-Discovery-claims_supported) ⓘ
- Verify that jwks_uri is published [Config, Dynamic] (OP-Discovery-jwks_uri) ⓘ

request_uri Request Parameter

- Support request_uri request parameter with unsigned request [Basic, Implicit, Hybrid] (OP-request_uri-Unsigned) ⓘ

request Request Parameter

- Support request request parameter with unsigned request [Basic, Implicit, Hybrid, Dynamic] (OP-request-Unsigned) ⓘ

claims Request Parameter

- Claims request with essential name claim [Basic, Implicit, Hybrid] (OP-claims-essential) ⓘ

Legends

	The test has not be run
	Success
	Warning, something was not as expected
	Failed
	The test flow wasn't completed. This may have been expected or not
	Signals the fact that there are trace information available for the test

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,
```

```
},
  "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-5GwKyaV6fDdnKB7A3b011XZ0E",
      "kty": "RSA",
      "n": "ygUNL9XXanKy_fQ1X0SMt9LRKpH3Xup11k5mivaw7thYRPrkGARJezV4x-hfk3Rm9qv6ikBgnTW01I8FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS_2C",
      "use": "sig",
      "x5c": [
        "MIIFRjCCBjAgAwIBAgIKEzqGLwABAACESDANBgkqhkiG9w0BAQUFADCBDETMBEgCgmsJomT8ixkARKWA2NvbTEZMBCGCGmsJomT8ixkARKWCW1pY3Jvc25"
      ],
      "x5t": "f-5GwKyaV6fDdnKB7A3b011XZ0E"
    }
  ]
}
0.847706 ===== END =====
```

Result

PASSED

Certification of Conformance



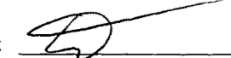
- Legal statement by certifier stating:
 - Who is certifying
 - What software
 - When tested
 - Profile tested
- Commits reputation of certifying organization to validity of results

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 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: Daniel Wossel
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/>
 - Starting over a decade ago!
 - Each round improved implementations and specs
 - By the numbers: 20 implementations, 195 members of interop list, > 1000 messages exchanged
- Multiple interop testing rounds for OpenID Federation
 - Next will be in Stockholm hosted by SUNET at the end of this month
- 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 started
- eKYC-IDA certification tests started
- Shared Signals certification tests started
- OpenID Federation certification tests started

OpenID Certification Call to Action



- Test your OpenID Connect, FAPI, OpenID4VC, OpenID Federation, and Shared Signals implementations now
 - And once you're ready, certify!
- 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/>
- OpenID Connect Working Group and Specifications Pages
 - <https://openid.net/wg/connect/>
 - <https://openid.net/wg/connect/specifications/>
- 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/>

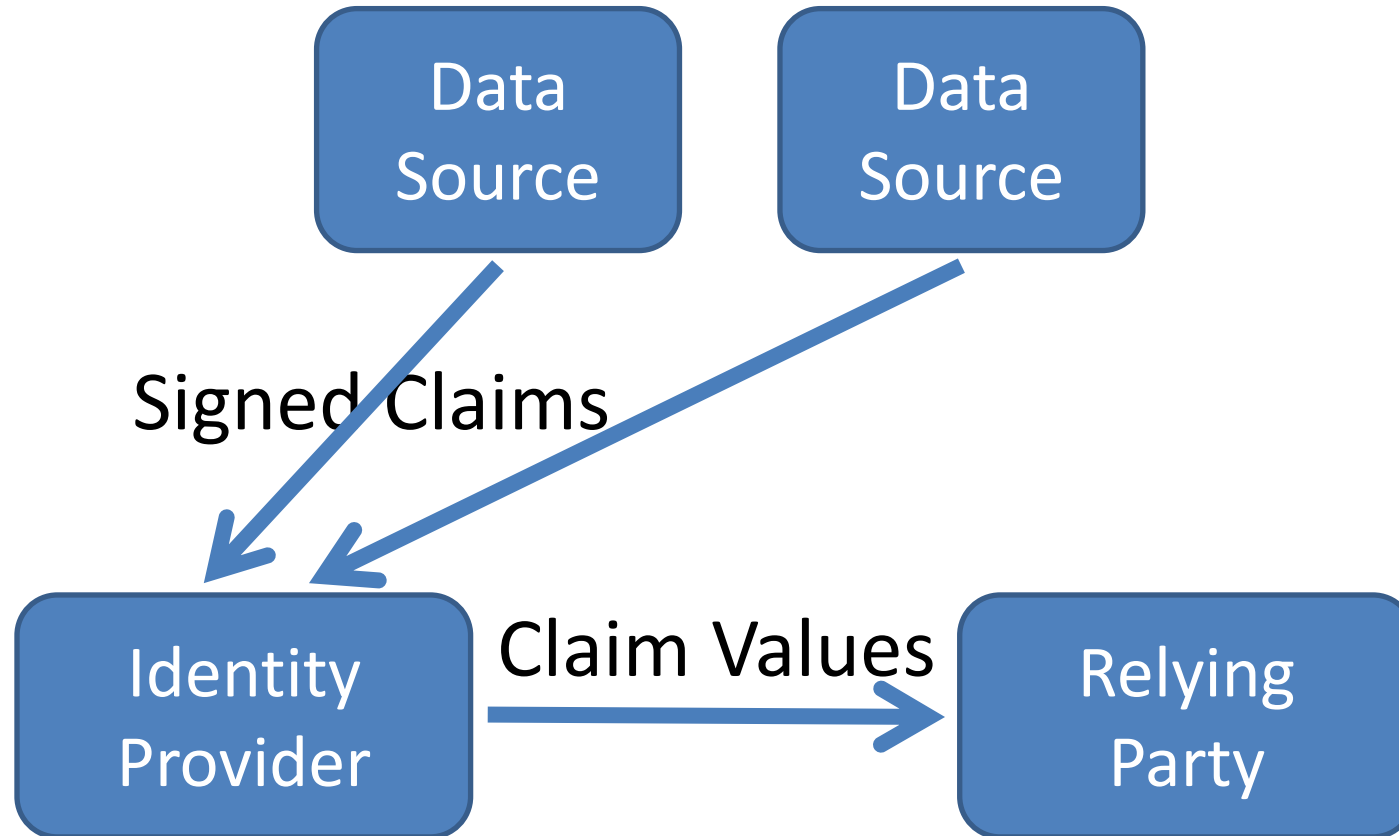
Your Turn!



- 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

