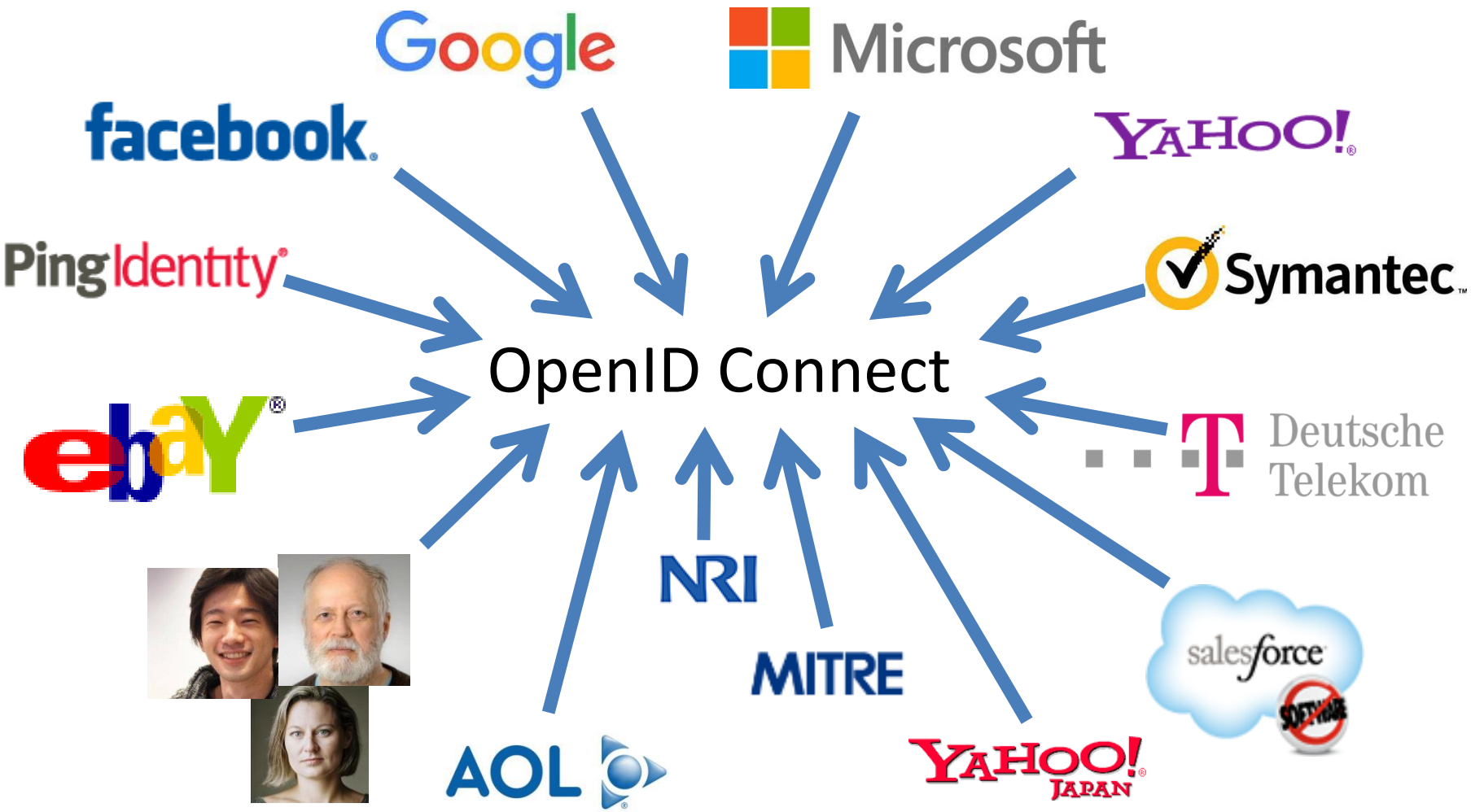
Introduction to OpenID Connect

October 17, 2017

Michael B. Jones

Identity Standards Architect – Microsoft

OpenID Working Together



What is OpenID Connect?

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

You're Probably Already Using OpenID Connect!

- If you log in at AOL, Deutsche Telekom, Google, Microsoft, mixi, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan or have an Android phone, 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

Presentation Overview

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

Design Philosophy

Keep Simple Things Simple

Make Complex Things Possible

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*

OpenID

Complex Things Possible

- Encrypted Claims
- Aggregated Claims
- Distributed Claims

Key Diffs from OpenID 2.0

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

OpenID Connect Timeline

- Artifact Binding working group formed, Mar 2010
- Major design issues closed at IIW, May 2011
  - Result branded “OpenID Connect”
- Functionally complete specs, Jul 2011
- 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
- Relying Party Certification launched December 2016
- Logout Implementer’s Drafts approved March 2017

A Look Under the Covers

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

ID Token

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

ID Token Claims Example


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

Claims Requests

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

UserInfo Claims

- sub
- name
- given_name
- family_name
- middle_name
- nickname
- preferred_username
- profile
- picture
- website
- gender
- birthdate
- locale
- zoneinfo
- updated_at
- email
- email_verified
- phone_number
- phone_number_verified
- address

UserInfo Claims Example


```
{
 "sub": "248289761001",
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "email": "janedoe@example.com",
 "email_verified": true,
 "picture": "http://example.com/janedoe/me.jpg"
}
```

Authorization Request Example

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

Authorization Response Example

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

UserInfo Request Example

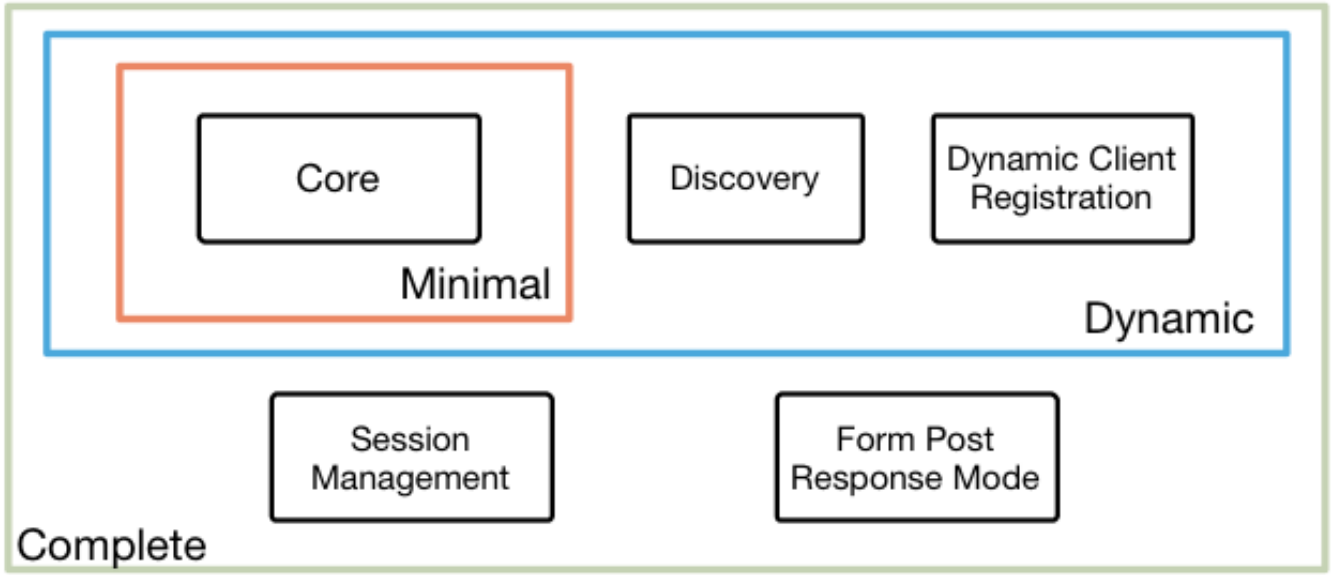
```
GET /userinfo HTTP/1.1
Host: server.example.com
Authorization: Bearer mF_9.B5f-4.1JqM
```

OpenID Connect Specs Overview

4 Feb 2014

OpenID Connect Protocol Suite

http://openid.net/connect



Underpinnings

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
  - http://openid.net/specs/openid-connect-migration-1_0.html
  - Completed April 2015
  - Google shut down OpenID 2.0 support in April 2015
  - Yahoo, others also plan to replace OpenID 2.0 with OpenID Connect

Additional Final Specifications (2 of 2)

- 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 that are auto-submitted by the User Agent using HTTP POST
  - A “form post” binding, like SAML and WS-Federation
    - An alternative to fragment encoding
  - http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html
  - Completed April 2015
  - In production use by Microsoft, Ping Identity

Federation Specification (work in progress)

- Roland Hedberg created OpenID Connect Federation specification
  - http://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

Session Management / Logout (work in progress)

- Three approaches being pursued by the working group:
  - Session Management
    - http://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
    - http://openid.net/specs/openid-connect-frontchannel-1_0.html
    - Uses HTTP GET to load image or iframe, triggering logout
    - Similar to options in SAML, WS-Federation
  - Back-Channel Logout
    - http://openid.net/specs/openid-connect-backchannel-1_0.html
    - Server-to-communication not using the browser
    - Can be used by native applications, which have no active browser
- All support multiple logged in sessions from OP at RP
- Unfortunately, no one approach best for all use cases
- All became Implementer's Drafts in March 2017

What is OpenID Certification?

- OpenID Certification enables OpenID Connect implementations to be certified as meeting the requirements of defined conformance profiles
- 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

Conformance Profiles

- Five conformance profiles of OpenID Providers:
  - Basic OpenID Provider
  - Implicit OpenID Provider
  - Hybrid OpenID Provider
  - OpenID Provider Publishing Configuration Information
  - Dynamic OpenID Provider
- Five corresponding conformance profiles of OpenID Relying Parties:
  - Basic Relying Party
  - Implicit Relying Party
  - Hybrid Relying Party
  - Relying Party Publishing Configuration Information
  - Dynamic Relying Party

Who has achieved OP Certification?

- OpenID Provider certifications at http://openid.net/certification/#OPs
- 124 profiles certified for
  39 implementations by
  36 organizations
- Recent additions:
  - Dominick Baier & Brock Allen, Connect2ID, KSIGN, NTT Software, OGIS-RI, Red Hat, Filip Skokan, Symantec, Verizon, Yahoo! Japan
- Each entry in table a link to zip file containing test logs and signed legal statement of conformance
  - Test results available for public inspection

Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP
Auth0	Auth0	24-May-2016	15-Feb-2017	15-Feb-2017	24-May-2016	
Dominick Baier & Brock Allen	IdentityServer3 v1.8	8-May-2015	8-May-2015	8-May-2015	8-May-2015	
Dominick Baier & Brock Allen	IdentityServer4	12-Dec-2016	12-Dec-2016	12-Dec-2016	12-Dec-2016	
Clareity 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	
Connect2id	Connect2id Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017
CZ.NIC	mojeID	7-Jul-2016		31-Jul-2016	7-Jul-2016	7-Jul-2016
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015	
ForgeRock	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015	
Google	Google Federated Identity	20-Apr-2015	21-Apr-2015	23-Apr-2015	15-Apr-2015	
Thierry Habart	SimpleIdentityServer V1.0.0	9-Dec-2015			11-Dec-2015	
Thierry Habart	SimpleIdentityServer V2.0.0	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016
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	
KSIGN	KSign Access 4.0	17-Mar-2017				
Microsoft	ADFS on Windows Server 2016	13-Sep-2015	13-Sep-2015		7-Apr-2015	
Microsoft	Azure Active Directory				8-Apr-2015	
NEC	NC7000-3A-OC	7-Mar-2016				
Nomura Research Institute	phpOIDC	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015	10-Apr-2015
Nomura Research Institute	Uni-ID	10-Apr-2015				
NTT Software Corporation	TrustBind/Federation Manager	26-Jan-2017	26-Jan-2017	26-Jan-2017		
PayPal	Login with PayPal				15-Apr-2015	
OGIS-RI	ThemiStruct Identity Platform v1.1.0	7-Oct-2016	7-Oct-2016		7-Oct-2016	
Okta	Okta OP	26-May-2016	26-May-2016	26-May-2016	26-May-2016	
Peercraft ApS	Peercraft	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016
Ping Identity	PingFederate	10-Apr-2015	10-Apr-2015	10-Apr-2015	9-Apr-2015	
Privacy Vaults Online (PRIVO)	PRIVO-Lock	23-Oct-2015			25-Nov-2015	
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	
Michael Schwartz	Gluu Server 2.3	2-Jul-2015	2-Jul-2015	8-Jul-2015	2-Jul-2015	2-Jul-2015
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
Symantec	NSL 2016.4.0.16	13-Oct-2016			13-Oct-2016	
University of Chicago	OIDC OP Overlay for Shibboleth IdP v3.2.1 version 1.0	25-Feb-2016			25-Feb-2016	
Verizon	VZConnect 1.9	21-Dec-2016				
ViewDS	Cobalt V1.0	28-Jan-2016	2-Feb-2016		28-Jan-2016	
Matias Woloski	Auth0	8-Feb-2016			8-Feb-2016	
Yahoo! Japan	Yahoo! ID Federation v2	7-Dec-2016	7-Dec-2016	7-Dec-2016	7-Dec-2016	

Who has achieved RP Certification?

- RP Certification launched in December 2016
- Relying Party certifications at http://openid.net/certification/#RPs
- 34 profiles certified for 12 implementations by 11 organizations
- To date:
  - Brock Allen, Dominick Baier, Thierry Habart, Janrain, Roland Hedberg, KIT SCC, NRI, Nov Matake, Ping Identity, Filip Skokan, Hans Zandbelt

Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic 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	
Thierry Habart	SimpleIdentityServer V1.0.1	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017
Janrain	IDPD 2.6.0	7-Feb-2017				
Roland Hedberg	pyoidc 0.9.4	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016
Karlsruher Institut für Technologie, SCC	oidcc 1.0.1	2-Feb-2017			2-Feb-2017	
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	
Filip Skokan	node openid-client ^1.3.0	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016
Hans Zandbelt	mod_auth_openidc 2.1.2	13-Dec-2016			13-Dec-2016	13-Dec-2016

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 http://op.certification.openid.net/ or http://rp.certification.openid.net/
- Once all tests for a profile pass, organization submits certification request to OpenID Foundation containing:
  - Logs from all tests for the profile
  - Signed legal declaration that implementation conforms to the profile
- Organization pays certification fee (for profiles not in pilot mode)
- OpenID Foundation verifies application is complete and grants certification
- OIDF lists certification at http://openid.net/certification/ and registers it in OIXnet at http://oixnet.org/openid-certifications/

What does certification cost?

- Not a profit center for the OpenID Foundation
  - Fees there to help cover costs of operating certification program
- Member price
  - $200 per new deployment
- Non-member price
  - $999 per new deployment
  - $499 per new deployment of an already-certified implementation
- Covers as many profiles as you submit within calendar year
- New profiles in pilot mode are available to members for free
- Costs described at http://openid.net/certification/fees/

What's next for OpenID Certification?

- Additional profiles being developed:
  - Form Post Response Mode
  - Refresh Token Behaviors
  - Session Management, Front-Channel Logout, Back-Channel Logout
  - OP-Initiated Login
- Additional documentation being produced
  - By Roland Hedberg and Hans Zandbelt
- Certification for additional specifications is anticipated:
  - E.g., HEART, MODRNA, iGov, EAP, FAPI, etc.

OpenID Certification Call to Action

- Certify your OpenID Connect implementations
- Help us test the soon-to-come new profiles
- Join the OpenID Foundation and/or the OpenID Connect working group

OpenID Connect Resources

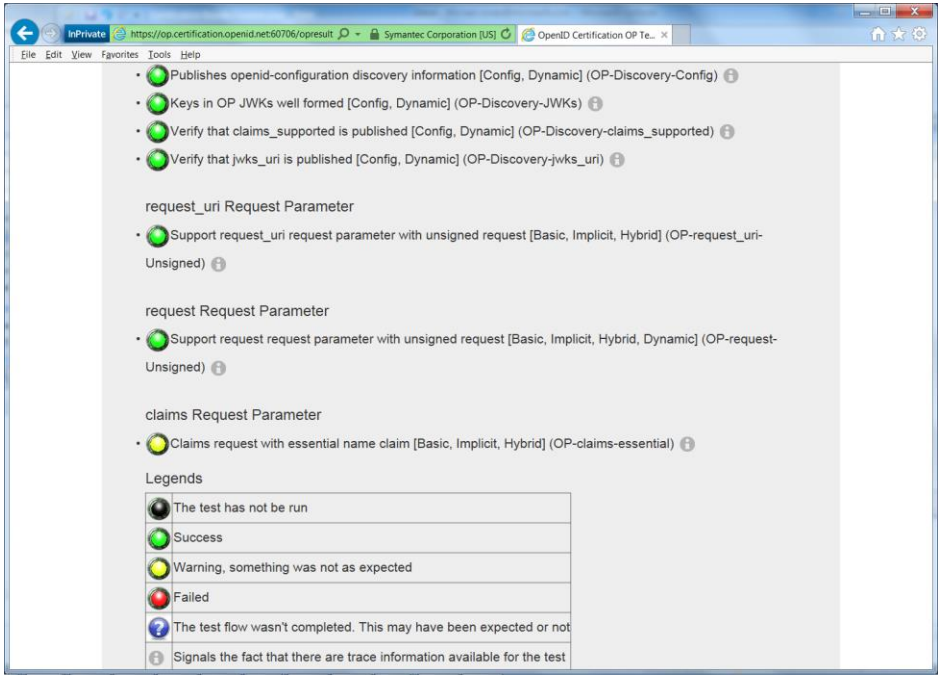
- OpenID Connect
  - http://openid.net/connect/
- Frequently Asked Questions
  - http://openid.net/connect/faq/
- Working Group Mailing List
  - http://lists.openid.net/mailman/listinfo/openid-specs-ab
- OpenID Certification Program
  - http://openid.net/certification/
- Certified OpenID Connect Implementations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

Open Conversation

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

BACKUP SLIDES

OpenID 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,
```

```
  ],
  "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": "yg0NL9XXanKy_fQlX0SMt9LRKpH3Xupllk5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW0lI8FqotLcXmvIBqtbIDfSh59utslr0QLRUVKS_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

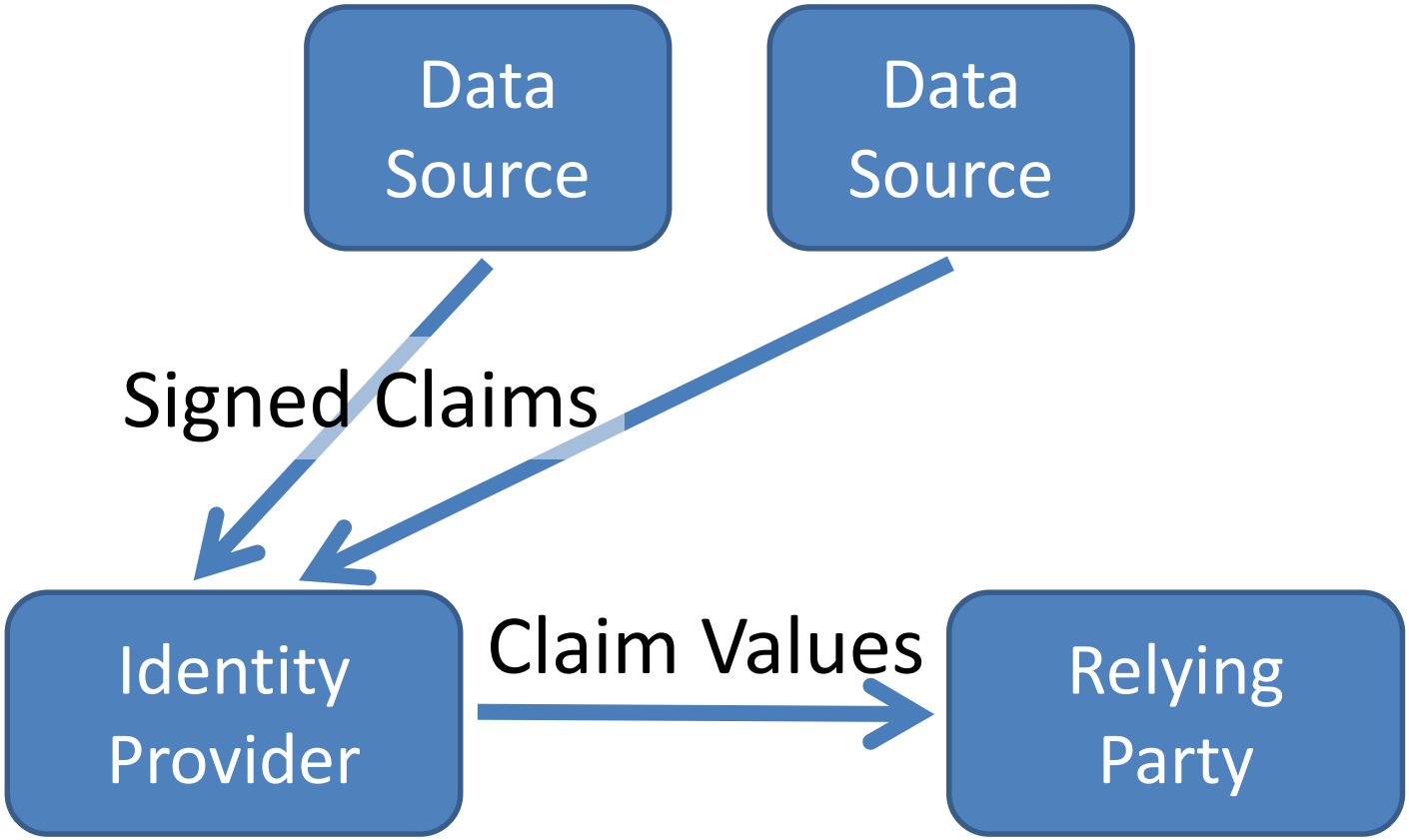
Test Date: April 10, 2015

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.

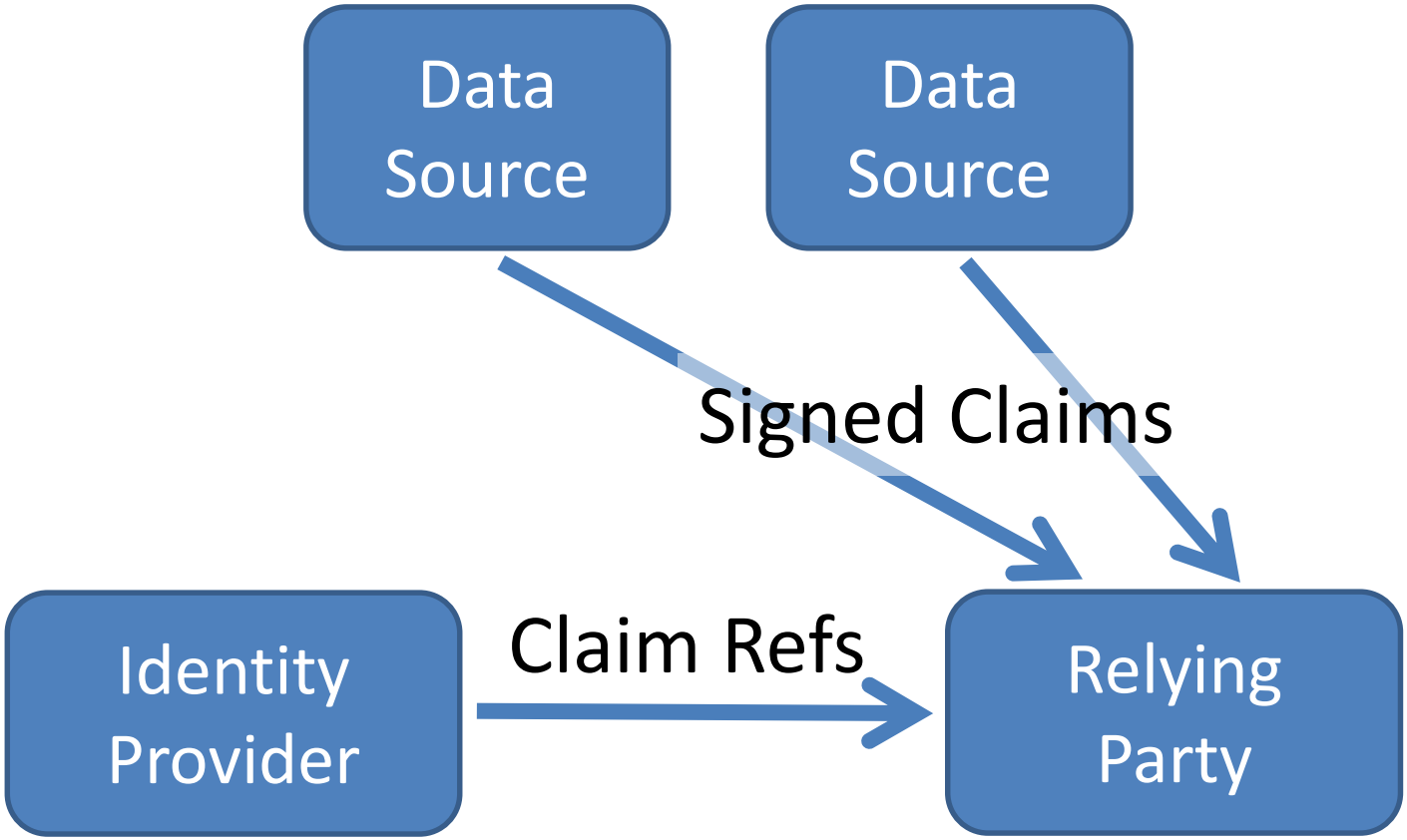
Implementer's Address Information	
Address:	1001 17th Street,Suite 100
City, State/Province, Postal Code	Denver, CO 80202
Country	USA
Implementer's Authorized Contact Information	
Name:	Brian Campbell
Title:	Distinguished Engineer
Phone:	720.317.2061
Email:	bcampbell@pingidentity.com

Authorized Signature:
Name: Daniel Wobbleton
Title: Asst. Gen. Counsel
Date: Apr. 10, 2015

Aggregated Claims



Distributed Claims



Basic Client Implementer's Guide

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

- http://openid.net/specs/openid-connect-basic-1_0.html

Implicit Client Implementer's Guide

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

- http://openid.net/specs/openid-connect-implicit-1_0.html

OpenID Discovery & Registration

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

- http://openid.net/specs/openid-connect-discovery-1_0.html
- http://openid.net/specs/openid-connect-registration-1_0.html

Core Specification

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

- http://openid.net/specs/openid-connect-core-1_0.html

Session Management

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

- http://openid.net/specs/openid-connect-session-1_0.html

OAuth Response Types

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

- http://openid.net/specs/oauth-v2-multiple-response-types-1_0.html

OpenID Form Post Response Mode

- Defines how to return OAuth 2.0 Authorization Response parameters using HTML form values auto-submitted by User Agent using HTTP POST
- http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html