Introduction to OpenID Connect

October 17, 2017

Michael B. Jones
Identity Standards Architect – Microsoft
Working Together
OpenID Connect

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
OpenID

Design Philosophy

Keep Simple Things Simple

Make Complex Things Possible
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
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
OpenID

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
{ "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=af0ifjs1dkj
GET /userinfo HTTP/1.1
Host: server.example.com
Authorization: Bearer mF_9.B5f-4.1JqM
OpenID Connect Specs Overview

OpenID Connect Protocol Suite

Core

Discovery

Dynamic Client Registration

Minimal

Session Management

Form Post Response Mode

Dynamic

Complete

Underpinnings

OAuth 2.0 Core

OAuth 2.0 Bearer

OAuth 2.0 Assertions

OAuth 2.0 JWT Profile

OAuth 2.0 Responses

JWT

JWS

JWE

JWK

JWA

WebFinger

4 Feb 2014

http://openid.net/connect
• 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](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
• 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](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](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
Who has achieved RP Certification?

- RP Certification launched in December 2016
- Relying Party certifications at [http://openid.net/certification/#RPs](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

<table>
<thead>
<tr>
<th>Organization</th>
<th>Implementation</th>
<th>Status RP</th>
<th>Static RP</th>
<th>Hybrid RP</th>
<th>Config RP</th>
<th>Dynamic RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brock Allen</td>
<td>slim-identity.js 1.3</td>
<td>4-Feb-2017</td>
<td>7-Feb-2017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominick Baier</td>
<td>IdentityModel/Client 2.0</td>
<td>27-Jan-2017</td>
<td>6-Feb-2017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Janrain</td>
<td>IDPE 2.0</td>
<td>7-Feb-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roland Hedberg</td>
<td>pyoidc 0.8.4</td>
<td>20-Dec-2016</td>
<td>20-Dec-2016</td>
<td>23-Dec-2016</td>
<td>20-Dec-2016</td>
<td>20-Dec-2016</td>
</tr>
<tr>
<td>Karlsruhe Institut für Technologie, SCC</td>
<td>sitiro 1.0.1</td>
<td>2-Feb-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nov Matake</td>
<td>openID_connect_remote_v1.3.3</td>
<td>20-Jan-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping Identity</td>
<td>PingAnnoe 4.2.2</td>
<td>28-Jan-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping Identity</td>
<td>PingFedora 8.3.1</td>
<td>17-Jan-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filip Skokan</td>
<td>next openID-client 11.3.2.0</td>
<td>10-Dec-2016</td>
<td>15-Dec-2016</td>
<td>15-Dec-2016</td>
<td>15-Dec-2016</td>
<td>15-Dec-2016</td>
</tr>
</tbody>
</table>
How does OpenID Certification work?

• Organization decides what profiles it wants to certify to
• 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/](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
Log from a Conformance Test

Test info
Profile: openid-configuration; config; response-type; code; crypto; sig; registration; static
Timestamp: 2015-04-07T23:58:52Z
Test description: Keys in OP PKCS well formed [Config, Dynamic]
Test ID: OP-Discovey.PKCS
Issue: https://standweb-one.microsoft.com/adfs

Test output
__After completing the test flow__
 [Verify-based44] [Base44]
 status: OK
 description: Verifies that the base44 encoded parts of a JWK is in fact base44 encoded and not just base44 encoded

Trace output
0.000036 DiscoveryRequest --------------
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs' [Verify-based44]
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs:well-known/openid-configuration'
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs/services/trust',
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs/well-known/authorizations/'
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs/well-known/jwks/'
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs/services/trust',
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs/well-known/authorizations/'
0.000036 Provides AD discovery flow 'https://standweb-one.microsoft.com/adfs/well-known/jwks/'

| isa | "iso" |
| vnd | "vnd" |
| utf8 | "utf8" |
| markdown | "markdown" |

| grant_types_supported | [ "authorization_code", "implicit", "client_credentials", "openid" ] |
| id_token_signing_alg_values_supported | [ "RS256" ] |

| issuers | [ "https://standweb-one.microsoft.com/adfs" ] |
| login_hint | [ "https://standweb-one.microsoft.com/adfs/discovery/logins" ] |
| require_auth Audience | [ "https://standweb-one.microsoft.com/adfs/services/trust" ] |

Result
PASS
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

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 non-conformance (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: [Signature]
Title: [Title]
Date: [Date]
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](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](http://openid.net/specs/openid-connect-implicit-1_0.html)
• 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-discovery-1_0.html)
• [http://openid.net/specs/openid-connect-registration-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](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](http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html)