Introduction to OpenID Connect

October 23, 2018
Michael B. Jones
Identity Standards Architect – Microsoft
Working Together

OpenID Connect

Google
Microsoft
Facebook
Ping Identity
eBay
NRI
MITRE
AOL
Yahoo!
Symantec
Deutsche Telekom
Salesforce
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 have an Android phone or log in at 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

• OAuth 2.0 won in 2013

• JSON Web Token (JWT) & JOSE won in 2014

• OpenID Certification program won 2018 Identity Innovation 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, 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
- OpenID Certification program won Best Identity Innovation award, March 2018
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"
}

OpenID
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=af0ifjs1dkj
&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
UserInfo Request Example

GET /userinfo HTTP/1.1
Host: server.example.com
Authorization: Bearer mF_9.B5f-4.1JqM
OpenID Connect Spec Overview

OpenID Connect Protocol Suite

Core
Discovery
Dynamic Client Registration

Minimal

Session Management
Form Post Response Mode

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
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](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 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
Session Management / Logout (works 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 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

- Unfortunately, no one approach best for all use cases
- Became Implementer’s Drafts in March 2017
  - Working group decided this year to advance them to Final Specification status
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
- Still under active development
  - *Please review!*
- Prototype implementations being interop tested w/ each other
What is OpenID Certification?

• Enables OpenID Connect 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
What can be certified now?

• Six conformance profiles of OpenID Providers:
  – Basic OpenID Provider
  – Implicit OpenID Provider
  – Hybrid OpenID Provider
  – OpenID Provider Publishing Configuration Information
  – Dynamic OpenID Provider
  – Form Post OpenID Provider (in pilot mode)

• Six corresponding conformance profiles of OpenID Relying Parties:
  – Basic Relying Party
  – Implicit Relying Party
  – Hybrid Relying Party
  – Relying Party Publishing Configuration Information
  – Dynamic Relying Party
  – Form Post Relying Party (in pilot mode)
Who has achieved OP Certification?

• OpenID Provider certifications at http://openid.net/certification/#OPs
  – 174 profiles certified for 57 implementations by 49 organizations

• Recent additions:
  – Auth0, CA, Classmethod, Cloudentity, Connect2id, Curity, Hanscan, Identity Automation, KSIGN, Library of Congress, Mvine, NRI, NTT, OGIS-RI, OpenAthens, Optimal Idm, ProSiebenSat.1, Michael Schwartz, Filip Skokan, WSO2

• Each entry link to zip file with test logs and signed legal statement
  – Test results available for public inspection
Who has achieved RP Certification?

- Relying Party certifications at [http://openid.net/certification/#RPs](http://openid.net/certification/#RPs)
  - 44 profiles certified for 18 implementations by 16 organizations

- Recent additions:
  - Brock Allen, Damien Bowden, F5 Networks, Janrain, Karlsruher Institut für Technologie, Tom Jones, KSIGN, Manfred Steyer, NRI, ZmartZone IAM
A Very International Effort

- European programmers developed and operate the certification test suite:
  - Roland Hedberg, Sweden
  - Hans Zandbelt, Netherlands
  - Filip Skokan, Czech Republic

- 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

• 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/
Example Testing Screen
Log from a Conformance Test
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
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 Python 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.”
What’s next for OpenID Certification?

• Advance Form Post Response Mode profiles to production status
• Additional profiles being developed:
  – Session Management, Front-Channel Logout, Back-Channel Logout
  – Refresh Token Behaviors
  – 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 now
• Help us test the new OP tests
• Join the OpenID Foundation and/or the OpenID Connect working group
OpenID Connect Resources

- OpenID Connect
  - [http://openid.net/connect/](http://openid.net/connect/)
- Frequently Asked Questions
  - [http://openid.net/connect/faq/](http://openid.net/connect/faq/)
- Working Group Mailing List
  - [http://lists.openid.net/mailman/listinfo/openid-specs-ab](http://lists.openid.net/mailman/listinfo/openid-specs-ab)
- OpenID Certification Program
  - [http://openid.net/certification/](http://openid.net/certification/)
- Certified OpenID Connect Implementations Featured for Developers
  - [http://openid.net/developers/certified/](http://openid.net/developers/certified/)
- Mike Jones’ Blog
- Nat Sakimura’s Blog
- John Bradley’s Blog
Open Conversation

• How are you using OpenID Connect?
• What would you like the working group to know or do?
BACKUP SLIDES
Aggregated Claims

- Data Source
- Data Source
- Signed Claims
- Identity Provider
- Claim Values
- Relying Party
Distributed Claims

- Data Source
- Identity Provider
- Claim Refs
- Signed Claims
- Relying Party

OpenID
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)
Core Specification

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

• http://openid.net/specs/openid-connect-core-1_0.html
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
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](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
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)