Introduction to OpenID Connect

April 28, 2020

Michael B. Jones
Identity Standards Architect – Microsoft
Working Together

OpenID Connect

Google
Microsoft
Facebook
Ping Identity
Yahoo!
Symantec
Ebay
NRI
MITRE
AOL
Yahoo Japan
Salesforce
Deutsche Telekom
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/](https://openid.net/connect/)

You’re Probably Already Using OpenID Connect!

• If you have an Android phone or log in at Apple, AOL, Deutsche Telekom, Google, Microsoft, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan, you’re already using OpenID Connect
  – Many other sites and apps large and small also use OpenID Connect
OpenID Connect Range

• Spans use cases, scenarios
  – Internet, Enterprise, Mobile, Cloud
• Spans security & privacy requirements
  – From non-sensitive information to highly secure
• Spans sophistication of claims usage
  – From basic default claims to specific requested claims to collecting claims from multiple sources
• Maximizes simplicity of implementations
  – Uses existing IETF specs: OAuth 2.0, JWT, etc.
  – Lets you build only the pieces you need
Numerous Awards

• OpenID Connect won 2012 European Identity Award for Best Innovation/New Standard

• OAuth 2.0 won in 2013

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

• OpenID Certification program won 2018 Identity Innovation Award

• OpenID Certification program won 2018 European Identity Award
Presentation Overview

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

Keep Simple Things Simple

Make Complex Things Possible
Keep Simple Things Simple

Userinfo endpoint for simple claims about user

Designed to work well on mobile phones
How We Made It Simple

• Built on OAuth 2.0
• Uses JavaScript Object Notation (JSON)
• You can build only the pieces that you need

• Goal: Easy implementation on all modern development platforms
Make Complex Things Possible

- Encrypted Claims
- Aggregated Claims
- Distributed Claims
Key Differences from OpenID 2.0

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

- Artifact Binding working group formed, March 2010
- Major design issues closed at IIW, May 2011
  - Result branded “OpenID Connect”
- 5 rounds of interop testing between 2011 and 2013
  - Specifications refined after each round of interop testing
- Won Best New Standard award at EIC, April 2012
- Final specifications approved, February 2014
- Errata set 1 approved November 2014
- Form Post Response Mode spec approved, April 2015
- OpenID 2.0 to Connect Migration spec approved, April 2015
- OpenID Provider Certification launched, April 2015
- OpenID Federation spec work begun, July 2016
- Relying Party Certification launched, December 2016
- Logout Implementer’s Drafts approved, March 2017
- OpenID Certification program won awards in March 2018 and April 2018
- OpenID Connect for Identity Assurance spec work begun, March 2019
A Look Under the Covers

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

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

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

• Basic requests made using OAuth scopes:
  – openid – Declares request is for OpenID Connect
  – profile – Requests default profile info
  – email – Requests email address & verification status
  – address – Requests postal address
  – phone – Requests phone number & verification status
  – offline_access – Requests Refresh Token issuance

• Requests for individual claims can be made using JSON “claims” request parameter
UserInfo Claims

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

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

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

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

GET /userinfo HTTP/1.1
Host: server.example.com
Authorization: Bearer mF_9.B5f-4.1JqM
Original Overview of Specifications

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
Additional Final Specifications (1 of 2)

• OpenID 2.0 to OpenID Connect Migration
  – Defines how to migrate from OpenID 2.0 to OpenID Connect
    • Has OpenID Connect identity provider also return OpenID 2.0 identifier, enabling account migration
      – https://openid.net/specs/openid-connect-migration-1_0.html
  – Completed April 2015
  – Google shut down OpenID 2.0 support in April 2015
  – AOL, Yahoo, others have replaced OpenID 2.0 with OpenID Connect
Additional Final Specifications (2 of 2)

• OAuth 2.0 Form Post Response Mode
  – Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values auto-submitted by the User Agent using HTTP POST
  – A “form post” binding, like SAML and WS-Federation
    • An alternative to fragment encoding
  – https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html
  – Completed April 2015
  – In production use by Microsoft, Ping Identity
Session Management / Logout (work in progress)

• Three approaches specified by the working group:
  – Session Management
    • https://openid.net/specs/openid-connect-session-1_0.html
    • Uses HTML5 postMessage to communicate state change messages between OP and RP iframes
  – Front-Channel Logout
    • https://openid.net/specs/openid-connect-frontchannel-1_0.html
    • Uses HTTP GET to load image or iframe, triggering logout (similar to SAML, WS-Federation)
  – Back-Channel Logout
    • https://openid.net/specs/openid-connect-backchannel-1_0.html
    • Server-to-communication not using the browser
    • Can be used by native applications, which have no active browser

• Unfortunately, no one approach best for all use cases
• All support multiple logged in sessions from OP at RP
• Recent WG decision to split RP-Initiated Logout into its own spec
  – Is used with all three OP-Initiated Logout mechanisms
• Logout certification tests now in pilot phase
  – WG is testing multiple implementations before making logout specs Final
Federation Specification (work in progress)

- OpenID Connect Federation specification
  - [https://openid.net/specs/openid-connect-federation-1_0.html](https://openid.net/specs/openid-connect-federation-1_0.html)
- Enables establishment and maintenance of multi-party federations using OpenID Connect
- Defines hierarchical JSON-based metadata structures for federation participants
- Second Implementer’s Draft status reached
- Please review and implement!
Identity Assurance Specification (work in progress)

• OpenID Connect for Identity Assurance
  – [https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html)

• JWT representation for verified person data
  – Including information about the identity verification performed
  – Enables legal compliance for some use cases

• Moved to new eKYC and Identity Assurance working group

• In review for second Implementer’s Draft status
  – *Please review!*
Native SSO Specification (work in progress)

- OpenID Connect Native SSO for Mobile Apps specification
  - [https://openid.net/specs/openid-connect-native-sso-1_0.html](https://openid.net/specs/openid-connect-native-sso-1_0.html)
- Enables Single Sign-On across apps by the same vendor
- Assigns a device secret issued by the AS
- New specification written by George Fletcher
  - Please review!
Self-Issued OpenID Provider

• OpenID Connect defines Self-Issued OpenID Provider
  – [https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued](https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued)

• Lets you be your own identity provider
  – Rather than a third party

• Identity represented as asymmetric key pair controlled by you

• Self-Issued OpenID Provider being used to achieve DID auth
Related Working Groups

- **International Government Profile (iGov) WG**
  - OpenID Connect profile for government & high-value commercial applications

- **Enhanced Authentication Profile (EAP) WG**
  - Enables integration with FIDO and other phishing-resistant authentication solutions

- **Mobile Operator Discovery, Registration & authenticaTion (MODRNA) WG**
  - Mobile operator profiles for OpenID Connect

- **Financial-grade API (FAPI) WG**
  - Enables secure API access to high-value services
  - Used for Open Banking APIs in many jurisdictions, including the UK

- **Research and Education (R&E) WG**
  - Profiles OpenID Connect to ease adoption in the Research and Education (R&E) sector

- **eKYC and Identity Assurance WG**
  - JWT format for verified claims with identity assurance information
What is OpenID Certification?

• Enables OpenID Connect and FAPI implementations to be certified as meeting the requirements of defined conformance profiles
  – Goal is to make high-quality, secure, interoperable OpenID Connect implementations the norm

• An OpenID Certification has two components:
  – Technical evidence of conformance resulting from testing
  – Legal statement of conformance

• Certified implementations can use the “OpenID Certified” logo
What value does certification provide?

• Technical:
  – Certification testing gives confidence that things will “just work”
  – No custom code required to integrate with implementation
  – Better for all parties
  – Relying parties explicitly asking identity providers to get certified

• Business:
  – Enhances reputation of organization and implementation
  – Shows that organization is taking interop seriously
  – Customers may choose certified implementations over others
OpenID Connect Certification Profiles

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

• Four logout profiles for OPs and RPs in pilot mode
  – RP-Initiated Logout
  – Session Management Logout
  – Front-Channel Logout
  – Back-Channel Logout
Connect OP Certifications

- OpenID Provider certifications at https://openid.net/certification/#OPs
  - 370 profiles certified for 111 implementations by 91 organizations

- Recent additions:
  - Bitkey, Chinese Academy of Sciences, Ergon Informatik, Ilex International, Samsung Electronics

- Each entry link to zip file with test logs and signed legal statement
  - Test results available for public inspection
Connect RP Certifications

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

• European programmers developed and operate the certification test suites:
  – Roland Hedberg, Sweden
  – Joseph Heenan, UK
  – Serkan Özkan, Turkey
  – Tomas Pazderka, Czech Republic
  – Filip Skokan, Czech Republic
  – Hans Zandbelt, Netherlands

• OpenID Connect leadership also very international:
  – Nat Sakimura, Japan
  – John Bradley, Chile
  – Michael Jones, United States
Use of Self-Certification

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

• Organization decides what profiles it wants to certify to

• Runs conformance tests publicly available at
  https://op.certification.openid.net/ or https://rp.certification.openid.net/
  or https://www.certification.openid.net/

• Once all tests for a profile pass, organization submits certification request to OpenID Foundation containing:
  – Logs from all tests for the profile
  – Signed legal declaration that implementation conforms to the profile

• Organization pays certification fee (for profiles not in pilot mode)
• OpenID Foundation verifies application is complete and grants certification
• OIDF lists certification at https://openid.net/certification/
What does certification cost?

• Not a profit center for the OpenID Foundation
  – Fees there to help cover costs of operating certification program
• Member price
  – $500
• Non-member price
  – $2500
• New profiles in pilot mode are available to members for free
• Costs described at https://openid.net/certification/fees/
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_typecode [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)

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: 2013-04-07T02:25:32Z
Test description: Keys in OP PKI well formed [Config, Dynamic]
Test ID: OP-Discovery-PKIs
Issuer: https://straedge.own.microsoft.com/adfs

Test output

After completing the test flow
Verify base464 url
status: OK
description: Verifies that the base64 encoded parts of a JWE is in fact base464 encoded
[check http response]
status: OK
description: Checks that the HTTP response status is within the 200 or 300 range

Trace output

0.000200 --- DiscoveryRequest ---
0.000299 Provider info from Issuer https://straedge.own.microsoft.com/adfs
0.000305 AD URL: https://straedge.own.microsoft.com/adfs/ssl-well-known/openid-configuration
0.00515 DiscoveryRequest
status: OK
description: Verifies that the base64 encoded parts of a JWE is in fact base464 encoded

0.045557 [JWT]
* "iss": [OIDC]
* "sub": [OIDC]
* "aud": [OIDC]
* "scope": [OIDC]
* "state": [OIDC]
* "exp": [OIDC]
* "nbf": [OIDC]
* "iat": [OIDC]
* "jti": [OIDC]
* "iss": [OIDC]
* "sub": [OIDC]
* "aud": [OIDC]
* "scope": [OIDC]
* "state": [OIDC]
* "exp": [OIDC]
* "nbf": [OIDC]
* "iat": [OIDC]
* "jti": [OIDC]

0.047000 --- END ---

Result
PASS

[Diagram of the OpenID Connect protocol flow]
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**

<table>
<thead>
<tr>
<th>Name of Entity (“Implementer”) Making this Certification</th>
<th>Ping Identity Corporation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software or Service (“Deployment”) Name &amp; Version #</td>
<td>PingFederate Summer 2015 Release</td>
</tr>
<tr>
<td>OpenID Connect Conformance Profile</td>
<td>Basic OpenID Provider</td>
</tr>
<tr>
<td>Conformance Test Suite Software</td>
<td>op.certification.openid.net as of April 10, 2015</td>
</tr>
<tr>
<td>Test Date</td>
<td>April 10, 2015</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Implementer’s Address Information</th>
<th>1001 17th Street, Suite 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>City, State/Province, Postal Code</td>
<td>Denver, CO 80202</td>
</tr>
<tr>
<td>Country</td>
<td>USA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implementer’s Authorized Contact Information</th>
<th>Brian Campbell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Distinguished Engineer</td>
</tr>
<tr>
<td>Phone</td>
<td>720.317.2061</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:bcampbell@pingidentity.com">bcampbell@pingidentity.com</a></td>
</tr>
</tbody>
</table>

**Authorized Signature:**

Name: [Signature]

Title: Chief Technical Officer

Date: April 10, 2015
How does certification relate to interop testing?

• OpenID Connect held 5 rounds of interop testing – see http://osis.idcommons.net/
  – Each round improved implementations and specs
  – By the numbers: 20 implementations, 195 members of interop list, > 1000 messages exchanged

• With interop testing, by design, participants can ignore parts of the specs

• Certification raises the bar:
  – Defines set of conformance profiles that certified implementations meet
  – Assures interop across full feature sets in profiles
Can I use the certification sites for interop testing?

• Yes – please do!
• The OpenID Foundation is committed to keeping the conformance test sites up and available for free to all
• Many projects using conformance testing for regression testing
  – Once everything passes, you’re ready for certification!
• Test software is open source using Apache 2.0 license
  – Some projects have deployed private instances for internal testing
  – Available as a Docker container
Favorite Comments on OpenID Certification

• Eve Maler – VP of Innovation at ForgeRock
  – “You made it as simple as possible so every interaction added value.”

• Jaromír Talíř – CZ.NIC
  – “We used and still are using certification platform mainly as testing tool for our IdP. Thanks to this tool, we have fixed enormous number of bugs in our platform an even some bugs in the underlying library.”

• Brian Campbell – Distinguished Engineer at Ping Identity
  – “The process has allowed us to tighten up our implementation and improve on the already solid interoperability of our offerings in the OpenID Connect ecosystem.”

• William Denniss – Google
  – “We have built the RP tests into the continuous-integration testing pipeline for AppAuth.”
FAPI Certification Status

• Financial-grade API (FAPI) implementations now being certified
• FAPI Part 2 OP certification launched in April 2019
  – 18 implementations certified to date
• Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) launched in September 2019
  – One implementation certified to date
• FAPI Part 2 RP certification tests launched in December 2019
  – One implementation certified to date
What’s next for OpenID Certification?

• Connect Certification code being reimplemented in Java
  – Current implementation in Python
  – Moving to the same code base as FAPI certification
  – Expect migration to Java implementation later this year

• Additional FAPI profiles being developed:
  – FAPI-CIBA RP

• Certification for additional specifications is anticipated:
  – E.g., HEART, MODRNA, iGov, EAP, etc.
OpenID Certification Call to Action

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

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

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

• Slides will be posted at https://self-issued.info/
BACKUP SLIDES
Aggregated Claims

Data Source

Signed Claims

Identity Provider

Claim Values

Relying Party