OpenID Connect Working Group

October 28, 2020

Michael B. Jones
Identity Standards Architect – Microsoft
You’re Almost Certainly Using OpenID Connect!

- Android, Apple, AOL, Deutsche Telekom, Google, GSMA Mobile Connect, KDDI, Microsoft, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, Yahoo! Japan all use OpenID Connect
  - Many other sites and apps large and small use OpenID Connect
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
Session Management / Logout
(work in progress)

- Three approaches specified by the working group:
  - Session Management
    - Uses HTML5 postMessage to communicate state change messages between OP and RP iframes
  - Front-Channel Logout
    - Uses HTTP GET to load image or iframe, triggering logout (similar to SAML, WS-Federation)
  - Back-Channel Logout
    - 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
- All three can be used with RP-Initiated Logout
  - Logout certification tests now in production mode
    - WG is gathering data from 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
- Multiple interop events being held this year
- Please review and implement!
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!
unmet_authentication_requirements

Specification (work in progress)

• Defines new error code `unmet_authentication_requirements`
  – https://openid.net/specs/openid-connect-unmet-authentication-requirements-1_0.html

• Enables OP to signal that it failed to authenticate the End-User per the RP’s requirements

• New specification written by Torsten Lodderstedt
  – Please review!
prompt=create Specification (work in progress)

- Initiating User Registration via OpenID Connect specification
  - [https://openid.net/specs/openid-connect-prompt-create-1_0.html](https://openid.net/specs/openid-connect-prompt-create-1_0.html)
- Requests enabling account creation during authentication
- Active discussion of relationships between account creation and use of existing accounts
- New specification written by George Fletcher
  - *Please review!*
Second Errata Set

- Errata process corrects typos, etc. discovered
  - Makes no normative changes
- Edits under way for second errata set
- [https://openid.net/specs/openid-connect-core-1_0-27.html](https://openid.net/specs/openid-connect-core-1_0-27.html) is current Core errata draft
Self-Issued OpenID Provider

• OpenID Connect defines Self-Issued OpenID Provider
  – 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
• WG defining extensions to SIOP using URI as subject
  – Please participate!
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
Open Letters to Apple

• OpenID Foundation wrote open letter to Apple about problems with Sign In with Apple in June 2019

• Apple has since fixed security and interop problems identified!
  – Standard OpenID Connect libraries can now be used in many cases

• Posted a second open letter commending them on the improvements made
Related Working Groups

- **eKYC and Identity Assurance WG**
  - JWT format for verified claims with identity assurance information
- **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 & authenicAtion (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
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
  - http://www.thread-safe.com/