OpenID Connect Working Group and OpenID Certification

May 21, 2020

Michael B. Jones

Identity Standards Architect – Microsoft
You’re Almost Certainly Using OpenID Connect!

• Android, Apple, AOL, Deutsche Telekom, Google, GSMA Mobile Connect, Microsoft, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, Yahoo! Japan all use OpenID Connect
  – Many other sites and apps large and small use OpenID Connect
Open Letters to Apple

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

• 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
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
    - [https://openid.net/specs/openid-connect-session-1_0.html](https://openid.net/specs/openid-connect-session-1_0.html)
  - Front-Channel Logout
    - Uses HTTP GET to load image or iframe, triggering logout (similar to SAML, WS-Federation)
    - [https://openid.net/specs/openid-connect-frontchannel-1_0.html](https://openid.net/specs/openid-connect-frontchannel-1_0.html)
  - Back-Channel Logout
    - Server-to-communication not using the browser
    - Can be used by native applications, which have no active browser
    - [https://openid.net/specs/openid-connect-backchannel-1_0.html](https://openid.net/specs/openid-connect-backchannel-1_0.html)

- 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
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](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
- 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_0-25.html is current Core errata draft
Use of 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
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 & 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
Federation Specification (work in progress)

• OpenID Connect Federation specification
  – 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 to occur this year

• Please review and implement!
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/
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
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/](https://op.certification.openid.net/) or [https://rp.certification.openid.net/](https://rp.certification.openid.net/) or [https://www.certification.openid.net/](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)
  – See [https://openid.net/certification/fees/](https://openid.net/certification/fees/)
• OpenID Foundation verifies application is complete and grants certification
• OIDF lists certification at [https://openid.net/certification/](https://openid.net/certification/)
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
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
  – 374 profiles certified for 112 implementations by 91 organizations

• Recent additions:
  – Bitkey, Chinese Academy of Sciences, Ergon Informatik, Gluu, 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
FAPI Certification Status

• Financial-grade API (FAPI) implementations 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
  – **News:** Many Java OpenID Connect tests now ready for you to test!

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

• Certification for additional specifications is possible:
  – E.g., eKYC-IDA, HEART, MODRNA, iGov, EAP, R&E, etc.
OpenID Certification Call to Action

• Certify your OpenID Connect and FAPI implementations
• Help us test the Java OpenID Connect tests
  – Joseph Heenan will tell you how