OpenID

OpenID Connect Working Group

December 9, 2021

Michael B. Jones

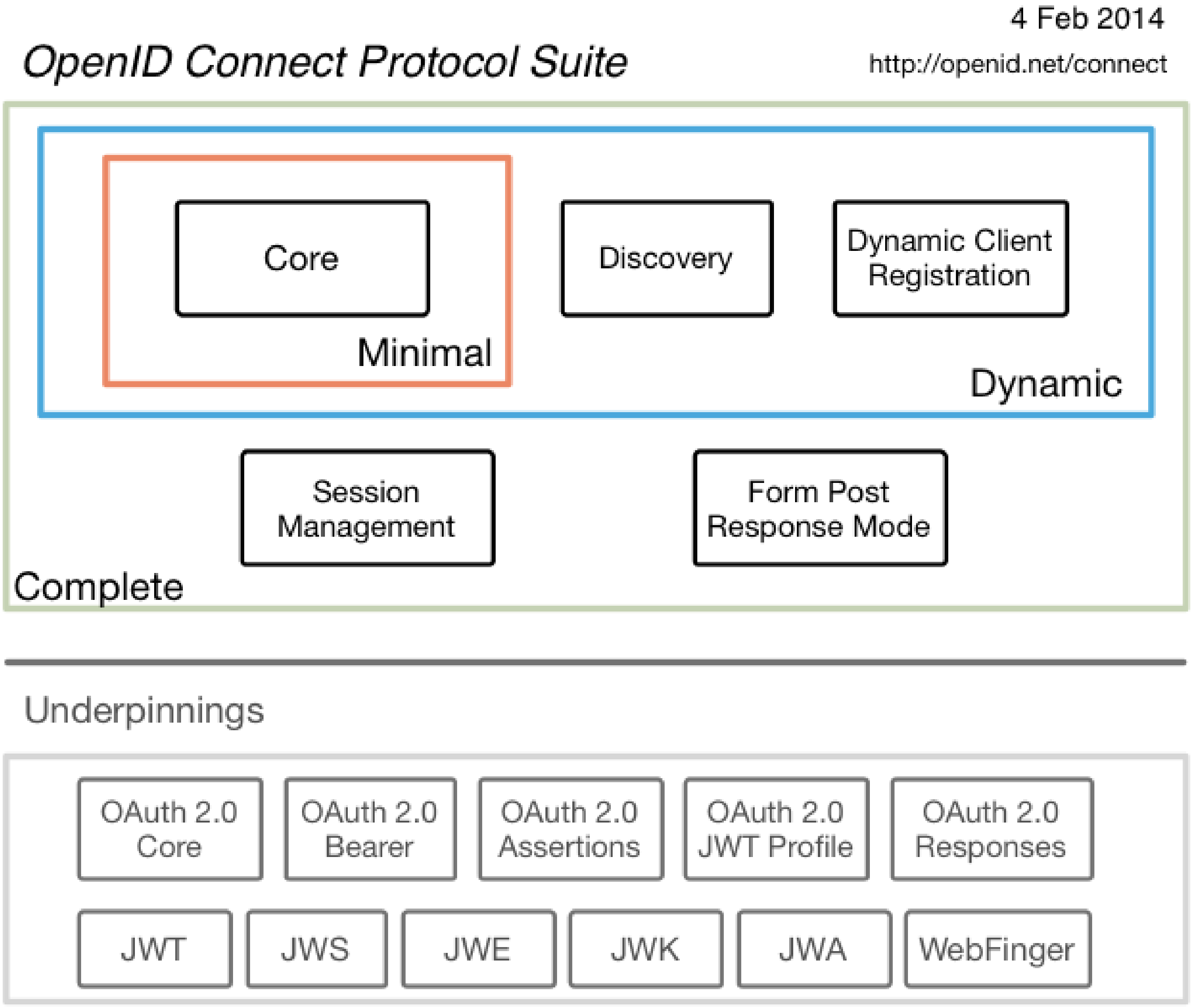
Identity Standards Architect – Microsoft

You’re Almost Certainly Using OpenID Connect!

OpenID

- Android, AOL, Apple, AT&T, Auth0, Deutsche Telekom, ForgeRock, Google, GrabTaxi, GSMA Mobile Connect, IBM, KDDI, Microsoft, NEC, NTT, Okta, Oracle, Orange, Ping Identity, Red Hat, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo, Yahoo! Japan, all use OpenID Connect
  - Many other sites and apps large and small use OpenID Connect
- OpenID Connect is infrastructure
  - Not a consumer brand

Original Overview of Specifications



4 Feb 2014

OpenID Connect Protocol Suite

http://openid.net/connect

Core

Minimal

Discovery

Dynamic Client Registration

Dynamic

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

Exciting Time for OpenID Connect!

- More happening than at any time since original specs created
- I’ll give you a taste of the exciting work happening…

Session Management / Logout

- 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
- All support multiple logged in sessions from OP at RP
- All three can be used with RP-Initiated Logout
  - https://openid.net/specs/openid-connect-rpinitiated-1_0.html
- Updates pending to RP-Initiated Logout for `client_id` parameter, etc.
- Session Management, Front-Channel Logout affected by browser privacy changes

Federation Specification

- 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
- Three interop events were held in 2020
  - Specification updated based on implementation feedback
- Third Implementer's Draft just published

`prompt=create` Specification

OpenID

- 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
- Initial Implementer’s Draft review starts this week

Native SSO Specification

- OpenID Connect Native SSO for Mobile Apps specification
  - 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
- Author George Fletcher requests your feedback

unmet_authentication_requirements Specification

- 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
- Author Torsten Lodderstedt requests your review

Claims Aggregation Specification

- Enables RPs to request and Claims Providers to return aggregated claims through OPs
  - https://openid.net/specs/openid-connect-claims-aggregation-1_0.html
- Specification initiated by Nat Sakimura and Edmund Jay

Self-Issued OpenID Provider V2

- OpenID Connect Core defined Self-Issued OpenID Provider (SIOP)
  - Lets you be your own identity provider
    - Rather than a third party
- Self-Issued OpenID Provider v2 Spec
  - https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
  - Extends initial SIOP functional to include DIDs as subjects
  - Usable with verified claims in multiple formats
- SIOP being used with ISO Mobile Driver’s Licenses (mDL)
  - Enables use without “calling home” to the issuer when used
- Initial Implementer’s Draft review to begin within days

OpenID Connect for Verifiable Presentations

- Specifies using W3C Verifiable Presentation objects with OpenID Connect
  - https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html
  - An alternate representation of verified claims
  - Parallel to OpenID Connect for Identity Assurance
  - Defines how deliver Verifiable Presentations with OpenID Connect
  - Initial Implementer's Draft review to begin within days

OpenID Connect for Verifiable Credential Issuance

OpenID

- Specifies how to issue Verifiable Credentials with OpenID Connect
  - https://bitbucket.org/openid/connect/src/master/individual/draft-lodderstedt-openid-connect-4-credential-issuance-1_0.md
  - Work begun by Torsten Lodderstedt and Kristina Yasuda
  - Was just adopted by the working group

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 is current Core errata draft

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
- Now over a thousand certifications!

Related Working Groups

- eKYC and Identity Assurance WG
  - JWT format for verified claims with identity assurance information
- **M**obile **O**perator **D**iscovery, **R**egistration & authe**N**tic**A**tion (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 and Brazil
- Research and Education (R&E) WG
  - Profiles OpenID Connect to ease adoption in the Research and Education (R&E) sector
- 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

OpenID Connect Resources

OpenID

- OpenID Connect Description
  - https://openid.net/connect/
- Frequently Asked Questions
  - https://openid.net/connect/faq/
- OpenID Connect Working Group
  - https://openid.net/wg/connect/
- 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/