OpenID Connect Working Group

Michael B. Jones

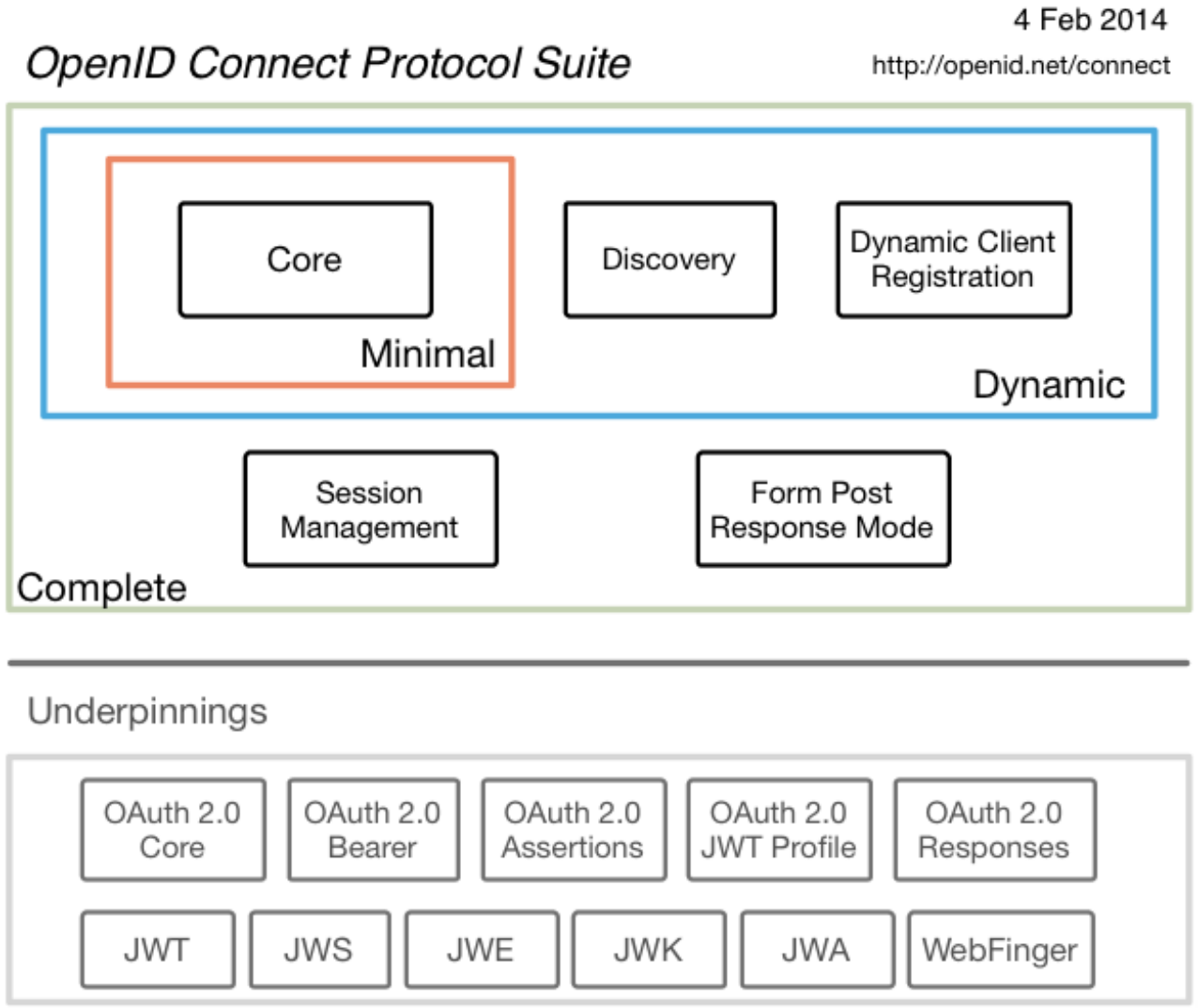
Identity Standards Architect – Microsoft

April 25, 2022

You're Almost Certainly Using OpenID Connect!

- 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



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…

Logout Specifications

- Three approaches to OP-initiated logout specified by the WG:
  - 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
- All support multiple logged in sessions from OP at RP
- All three can be used with RP-Initiated Logout

Logout Specifications (continued)

- Halfway through two-week Working Group Last Call (WGLC)
  - File issues in the Bitbucket OpenID Connect issue tracker
- Following WGLC, we'll start the 60-day Foundation-wide review
  - Followed by vote to approve them as Final Specifications

- Session Management, Front-Channel Logout affected by browser privacy changes
  - Impact described in notes in the specifications

OpenID Connect Federation Specification

- "OpenID Connect Federation 1.0"
- 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
- In production use in Italy
- Actively resolving remaining open issues
  - *In preparation for WGLC and progression to Final status*

`prompt=create` Specification

- "Initiating User Registration via OpenID Connect"
- Requests enabling account creation during authentication
- Became an Implementer's Draft in February 2022

- *Is it time to progress it to Final status?*

Native SSO Specification

- "OpenID Connect Native SSO for Mobile Apps"
- Enables Single Sign-On across apps by the same vendor
- Assigns a device secret issued by the Authorization Server

- *Author George Fletcher requests your feedback*

`unmet_authentication_requirements` Spec

- "OpenID Connect Core Error Code unmet_authentication_requirements"
- Defines new error code `unmet_authentication_requirements`
- Enables OP to signal that it failed to authenticate the End-User per the RP's requirements

- *Author Torsten Lodderstedt requests your feedback*

Claims Aggregation Specification

- "OpenID Connect Claims Aggregation"
- Enables RPs to request and Claims Providers to return aggregated claims through OPs

- *The editors request your feedback*

Self-Issued OpenID Provider V2

- 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"
  - Extends initial SIOP functionality to include DIDs as subjects
  - Usable with verified claims in multiple formats
- SIOP being used with ISO Mobile Driver's Licenses (mDL)
- Recently added support for `response_type=code`
- Implementer's Draft approved February 2022
  - *Actively working towards second Implementer's Draft*

OpenID Connect for Verifiable Presentations Spec

- "OpenID Connect for Verifiable Presentations"
- Defines how to deliver W3C Verifiable Presentation objects with OpenID Connect
- Actually, credential format agnostic
  - For example, could use with ISO Mobile Driver License (mDL)
- Implementer's Draft approved February 2022
  - *Actively working towards second Implementer's Draft*

OpenID Connect for Verifiable Credential Issuance Spec

- "OpenID Connect for Verifiable Credential Issuance"
- Specifies how to issue W3C Verifiable Credentials with OpenID
- Recently added issuer-initiated flow
- Recently changed to be OAuth 2.0-based

- *Actively working towards first Implementer's Draft*

Second Errata Set

- Edits under way for second errata set
- See current editor's drafts at https://openid.bitbucket.io/connect/
  - Updates to Core, Discovery, and Registration published April 18th
- Actively working on completing errata corrections
  - 33 tracked errata issues remain
- Then will hold 45-day Foundation-wide Errata approval vote

- *Publicly Available Specification (PAS) submission to ISO of final OpenID Connect specifications planned*

OpenID Certification

- OpenID Connect and FAPI implementations can be certified as meeting requirements of defined conformance profiles
  - Goal is to make high-quality, secure, interoperable OpenID Connect and FAPI 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
- *1445 certifications of 386 deployments!*

OpenID Certification (continued)

- Certifications listings now come from a database
  - Rather than a hand-edited WordPress page
- Certification program is now financially self-supporting!
  - Open Banking certifications from Brazil and other places got us there
- eKYC-IDA certification tests planned

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 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 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/

Thank you.

Visit: OpenID.net