OpenID

OpenID Connect Working Group

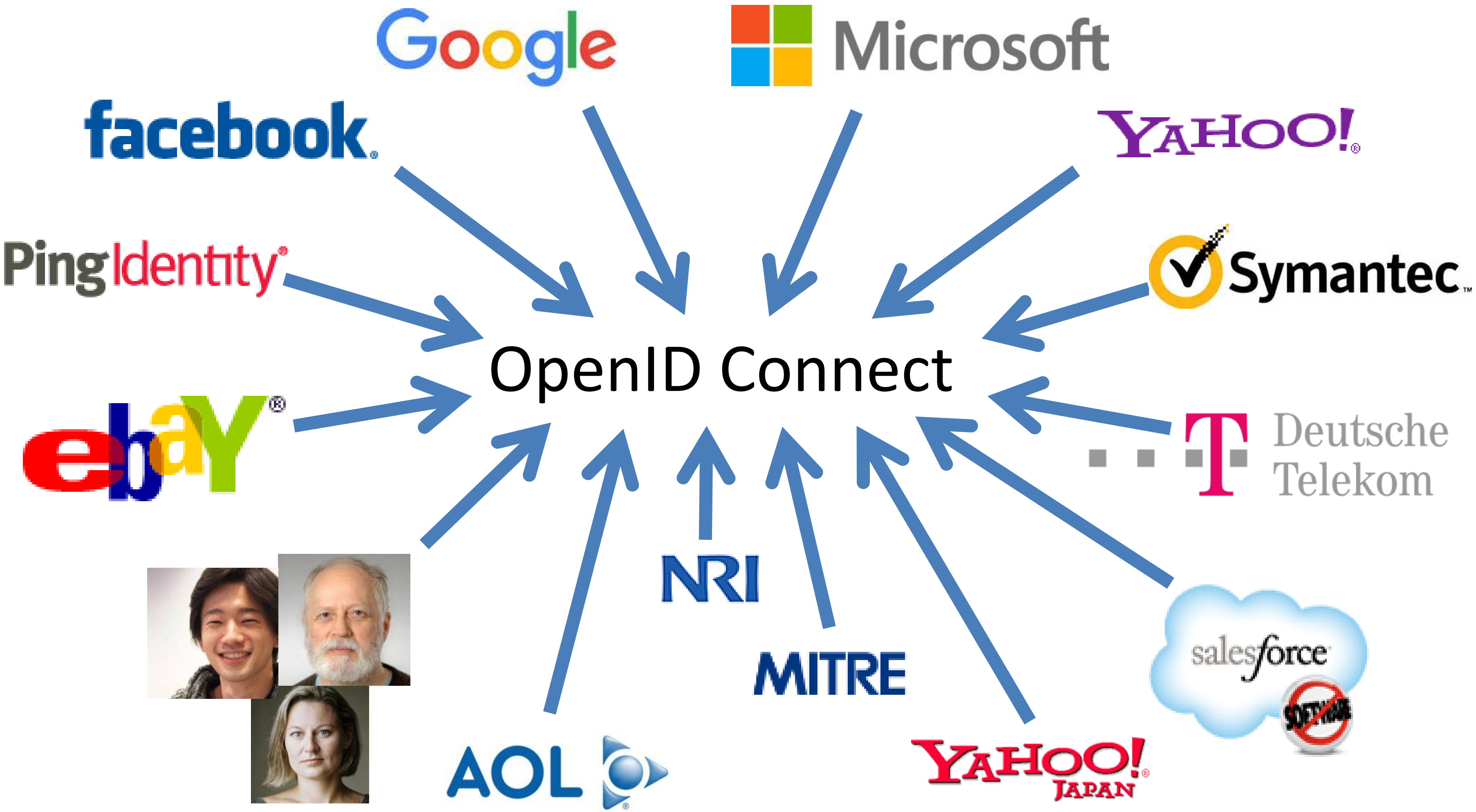
May 15, 2018

Dr. Michael B. Jones

Identity Standards Architect – Microsoft

Working Together

OpenID



OpenID Connect

What is OpenID Connect?

- Simple identity layer on top of OAuth 2.0
- Enables RPs to verify identity of end-user
- Enables RPs to obtain basic profile info
- REST/JSON interfaces → low barrier to entry
- Described at http://openid.net/connect/

You’re Probably Already Using OpenID Connect!

OpenID

- If you have an Android phone or log in at 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

OpenID

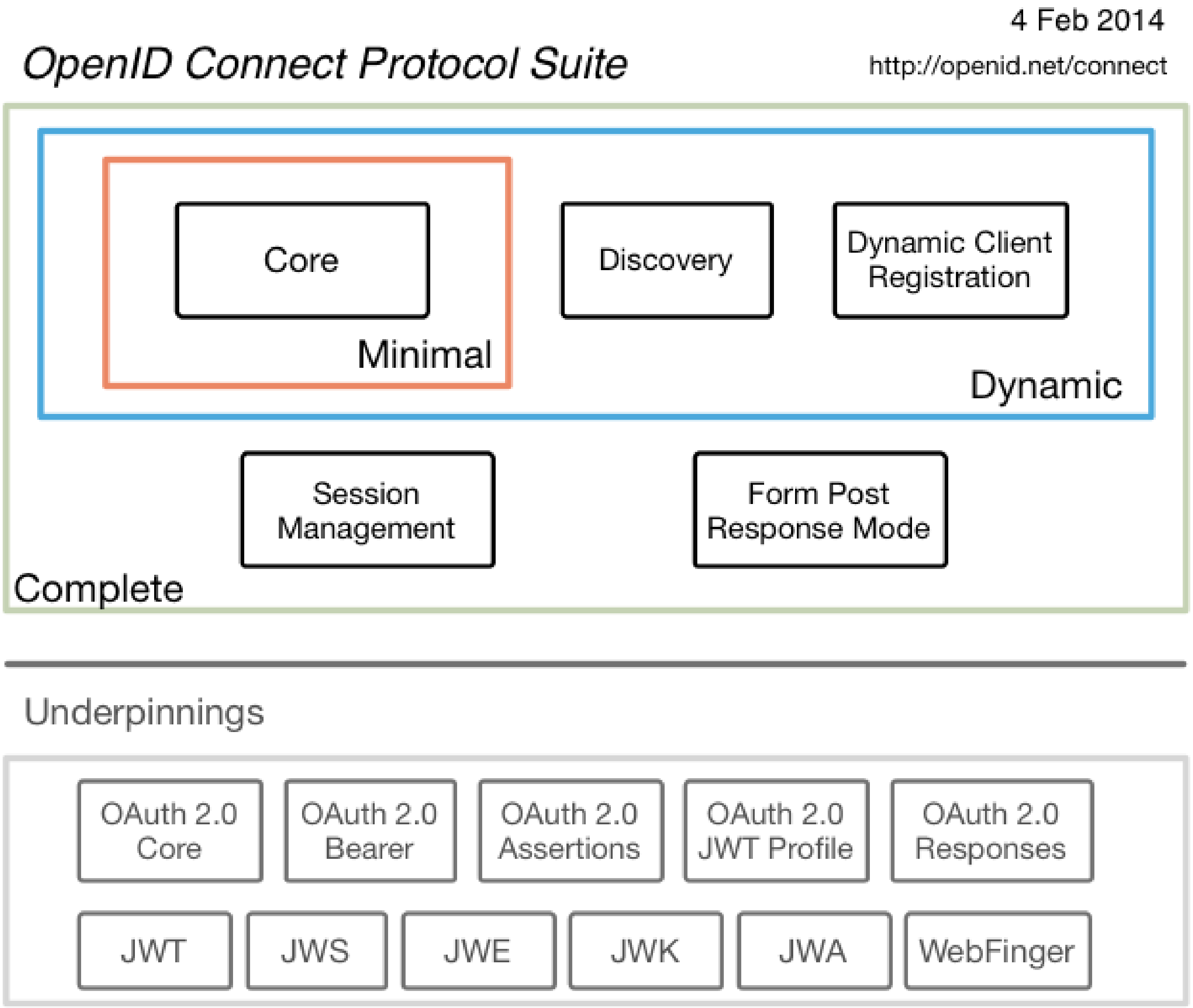
- Spans use cases, scenarios
  - Internet, Enterprise, Mobile, Cloud
- Spans security & privacy requirements
  - From non-sensitive information to highly secure
- Spans sophistication of claims usage
  - From basic default claims to specific requested claims to collecting claims from multiple sources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

Numerous Awards

OpenID

- OpenID Connect won 2012 European Identity Award for Best Innovation/New Standard
  - http://openid.net/2012/04/18/openid-connect-wins-2012-european-identity-and-cloud-award/
- OAuth 2.0 won in 2013
- JSON Web Token (JWT) & JOSE won in 2014
- OpenID Certification program won 2018 Identity Innovation Award
  - http://openid.net/2018/03/29/openid-certification-program-wins-2018-identity-innovation-award/

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

OAuth 2.0 Form Post Response Mode (additional Final Specification)

OpenID

- 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
- http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html
- Completed April 2015
- In production use by Microsoft, Ping Identity

OpenID 2.0 to OpenID Connect Migration (additional Final Specification)

OpenID

- 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
- http://openid.net/specs/openid-connect-migration-1_0.html
- Completed April 2015
- Google shut down OpenID 2.0 support in April 2015
- Yahoo, AOL, others also plan to replace OpenID 2.0 with OpenID Connect

Current Work

- Federation Specification
- Session Management / Logout
- Second Errata Set
- Current Related Work
- OpenID Connect Certification

Session Management / Logout (work in progress)

- Three approaches being pursued by the working group:
  - Session Management
    - http://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
    - http://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
    - http://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
  - Can be used separately or in combination
- Became Implementer's Drafts in March 2017
  - Recent decision made that it's time for them to become Final Specifications

Federation Specification (work in progress)

- Roland Hedberg created OpenID Connect Federation specification
  - http://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
- Prototype implementations being interop tested w/ each other
- Recent decision to progress it to an Implementer's Draft

Second Errata Set
(work in progress)

- Errata process corrects typos, etc. discovered
  - Makes no normative changes
- Edits under way for second errata set
- See http://openid.net/specs/openid-connect-core-1_0-23.html for current Core errata draft
- Waiting for OAuth AS metadata spec draft-ietf-oauth-discovery to be final
  - So we can register OpenID Discovery metadata values
  - Now in the hands of the RFC Editor
- Expect to see request for review of errata changes shortly

Current Related Work

- International Government Profile (iGov) Working Group
  - Developing OpenID Connect profile for government & high-value commercial applications
- Enhanced Authentication Profile (EAP) Working Group
  - Enables Token Bound ID Tokens
  - Enables integration with FIDO and other phishing-resistant authentication solutions

OpenID Certification

- OpenID Certification enables OpenID Connect implementations to be certified as meeting requirements of defined conformance profiles
- Now OP and RP 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
- See http://openid.net/certification/
  - And accompanying certification presentation!

Open Conversation

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

OpenID Connect Resources

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