OpenID Connect Working Group

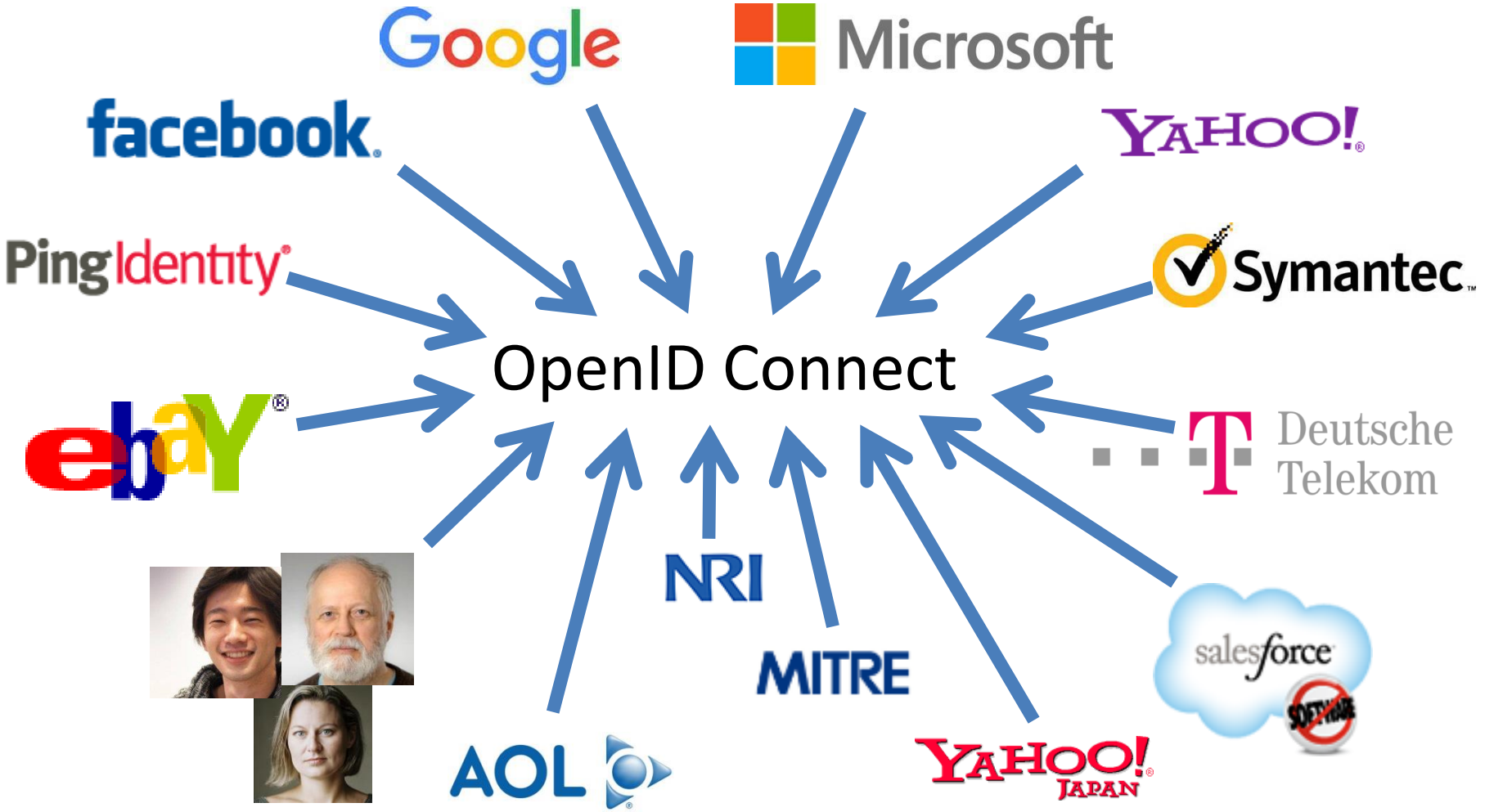
September 13, 2021

Michael B. Jones

Identity Standards Architect – Microsoft

Working Together

OpenID



You're Almost Certainly Using OpenID Connect!

- Android, Apple, AOL, Deutsche Telekom, Google, GSMA Mobile Connect, KDDI, Microsoft, NEC, NTT, Orange, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo! Japan, etc. all use OpenID Connect
  - Many other sites and apps large and small use OpenID Connect
- OpenID Connect is infrastructure
  - Not a consumer brand

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 https://openid.net/connect/

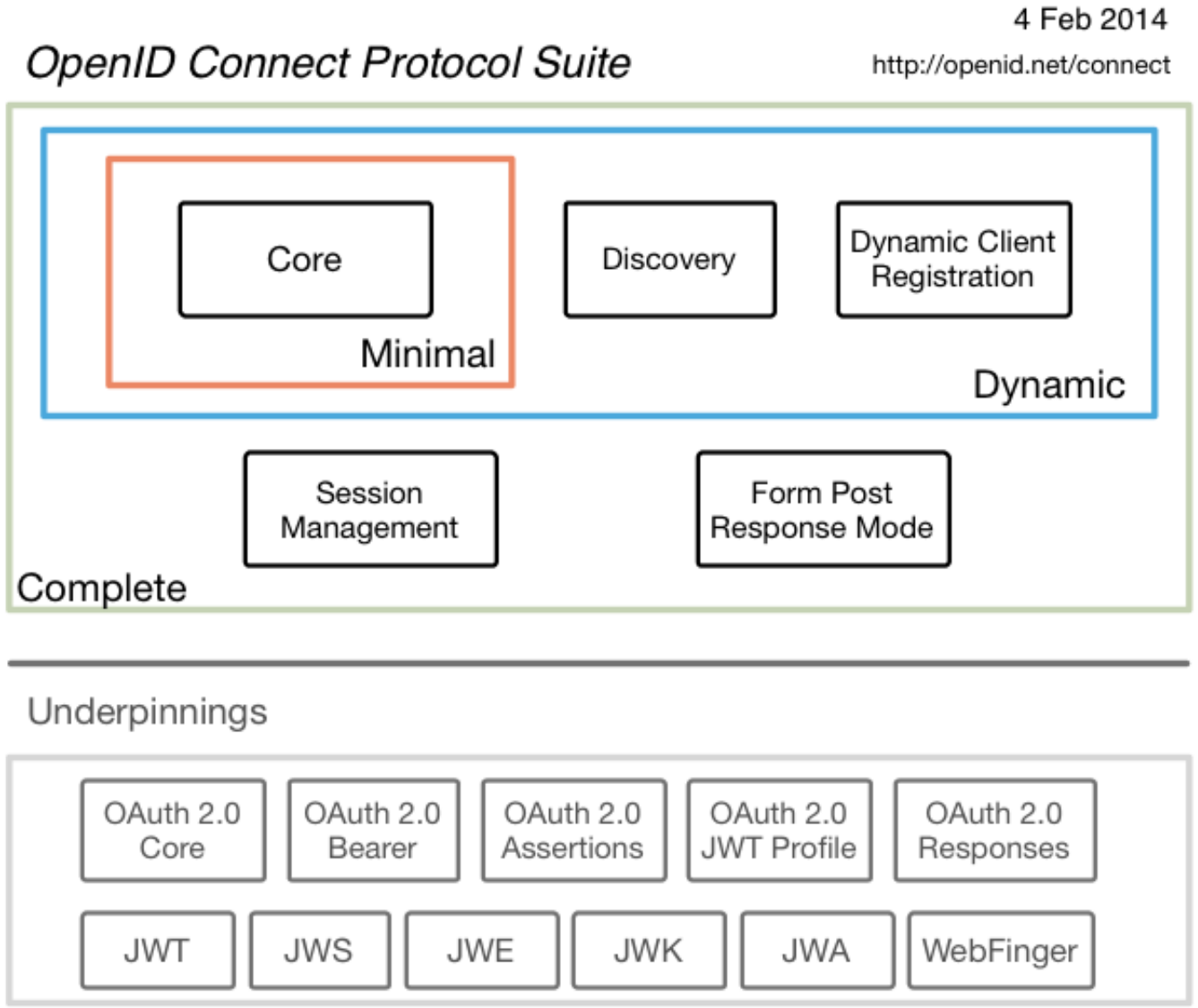
OpenID Connect Range

- Spans use cases, scenarios
  - Internet, Enterprise, Mobile, Cloud, Federated, User-Centric
- 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 in multiple formats 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 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
- JWT/JOSE won in 2014
- OpenID Certification program won 2018 Identity Innovation Award and 2018 European Identity Award

Overview of Original 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…

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
  - Applying lessons learned from large-scale SAML federations
- Defines hierarchical JSON-based metadata structures for federation participants
- Three interop events were held in 2020
  - Specification updated based on implementation feedback
- *New Implementer's Draft, then Final status anticipated*

Self-Issued OpenID Provider V2

- OpenID Connect Core defined Self-Issued OpenID Provider (SIOP)
  - https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued
- Lets you be your own identity provider
  - Rather than a third party
- Being used with ISO Mobile Driver's Licenses (mDL)
  - Enables presentation without "calling home" to the issuer
- Self-Issued OpenID Provider (SIOP) V2 now being defined
  - https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
  - Can be use for DID auth, JWT claims, Verifiable Credentials, etc.
- *Working towards Implementer's Draft status*

OpenID Connect for Verifiable Presentations

- Enables presentation of claims as W3C Verifiable Presentations
  - https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0.html
- Can be used both with third-party and self-issued OPs
- VPs can be returned in ID Token, UserInfo, and new VP Token
- Integration point with DIF Presentation Exchange
- *Please review new draft just published*

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
- Defines full life-cycle of aggregated claims and roles of entities involved
- Supports multiple claims schemas
  - JWT Aggregated and Distributed Claims
  - W3C Verifiable Credentials objects
- *Please review new draft just published*

`prompt=create` Specification

- Initiates user account registration via OpenID Connect
  - https://openid.net/specs/openid-connect-prompt-create-1_0.html
- Requests enabling account creation during authentication
- *Please review new draft just published*

`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
- Has been stable since initial publication
- *Recent WG decision to advance to Final status*

Native SSO Specification

- OpenID Connect Native SSO for Mobile Apps
  - https://openid.net/specs/openid-connect-native-sso-1_0.html
- Enables Single Sign-On (SSO) across apps by the same vendor
- Assigns a device secret issued by the OP
- Deployed by AOL
- *Seeking feedback on applicability to others' use cases*

OP-Initiated Logout

- Enables OP to request that RPs log out end-user's sessions with the OP
- 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 changes 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 (so can be used by native applications)
- All support multiple logged-in sessions from OP at RP
- Session Management & Front-Channel Logout affected by browser privacy changes
- All can be used with RP-Initiated Logout

RP-Initiated Logout

- Enables RP to request that OP log out end-user
  - https://openid.net/specs/openid-connect-rpinitiated-1_0.html
  - Content recently split out of Session Management spec
- Not affected by browser privacy changes
  - (unlike some of the OP-Initiated Logout methods)
- *Updates pending to add* `client_id` *and* `logout_hint` *parameters*

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

Portable Identifiers Under Discussion

- Current subject identifiers are OP-specific
- WG discussing identifiers that you can move between OPs
  - Related to MODRNA Account Porting work
- Potentially both for self-issued OPs and third-party OPs
- W3C DIDs are one such possible identifier type

CIBA Core is Now Final (Related Work)

- OpenID Connect Client-Initiated Backchannel Authentication (CIBA) Core
  - https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html
- Authentication flow with direct Relying Party to OpenID Provider communication without redirects through browser
- *Product of the MODRNA working group*
- *Used by FAPI CIBA Profile*

Related W3C Federated Identity Group

- New W3C Federated Identity Community Group
  - https://www.w3.org/community/fed-id/
- Incubating Web features supporting federated identity and preventing untransparent, uncontrollable tracking on the Web
- For instance, new features may be needed to enable logout when browsers disable support for third-party cookies
- *Informed by discussions in Connect WG Browser Behaviors calls*

Related OpenID Working Groups

- **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 in jurisdictions including UK, Australia, and Brazil
- eKYC and Identity Assurance WG
  - Defines JWT format for verified claims with identity assurance information
- Research and Education (R&E) WG
  - Profiles to ease Connect adoption in Research and Education (R&E) sector

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 and FAPI implementations the norm
- An OpenID Certification has two components:
  - Technical evidence of conformance resulting from testing
  - Legal statement of conformance
- See https://openid.net/certification/
- *Certification requests now very frequent*
  - *The program is now also financially self-sustaining*

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/