OpenID

OpenID Connect Working Group

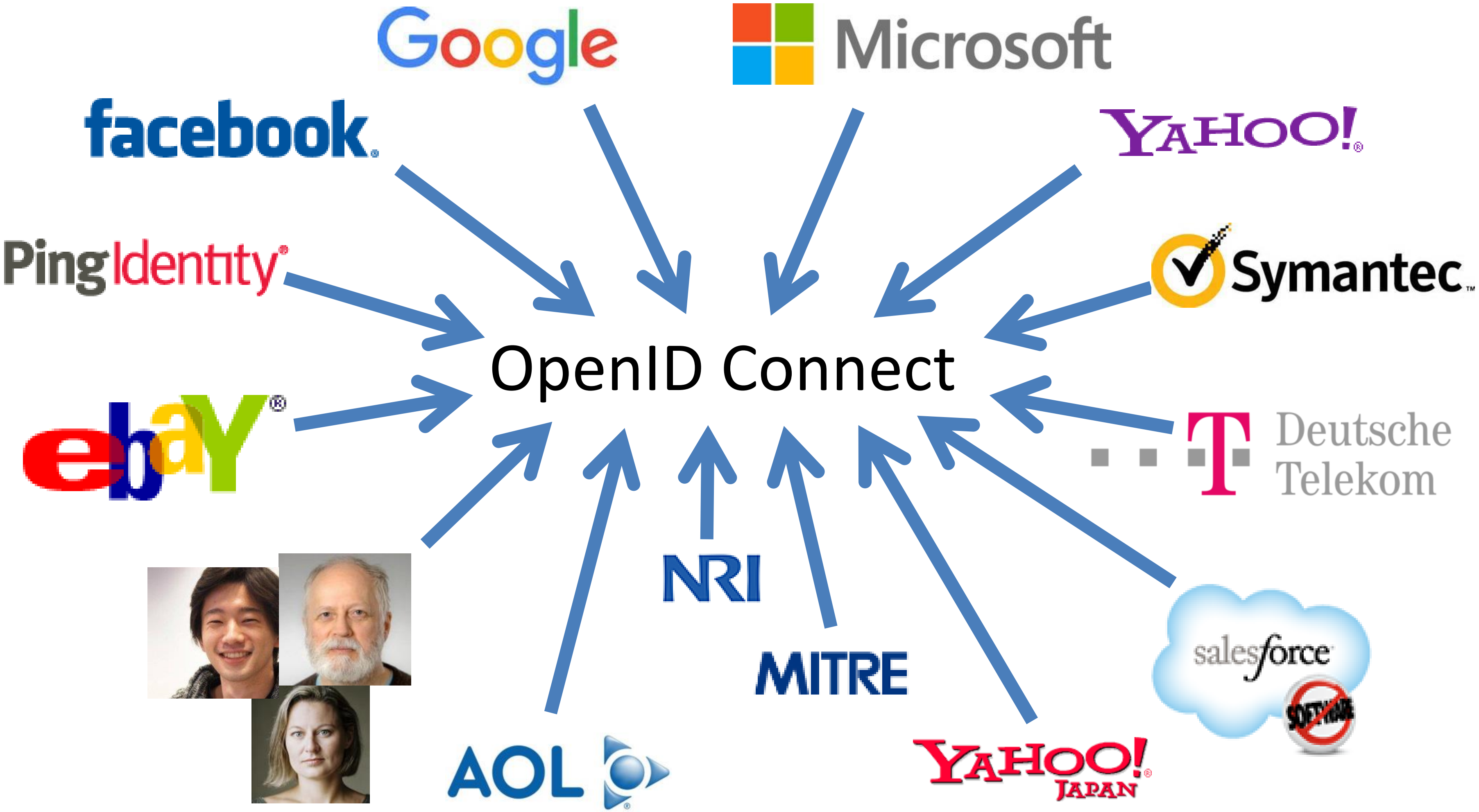
April 29, 2019

Michael B. Jones

Identity Standards Architect – Microsoft

OpenID

Working Together

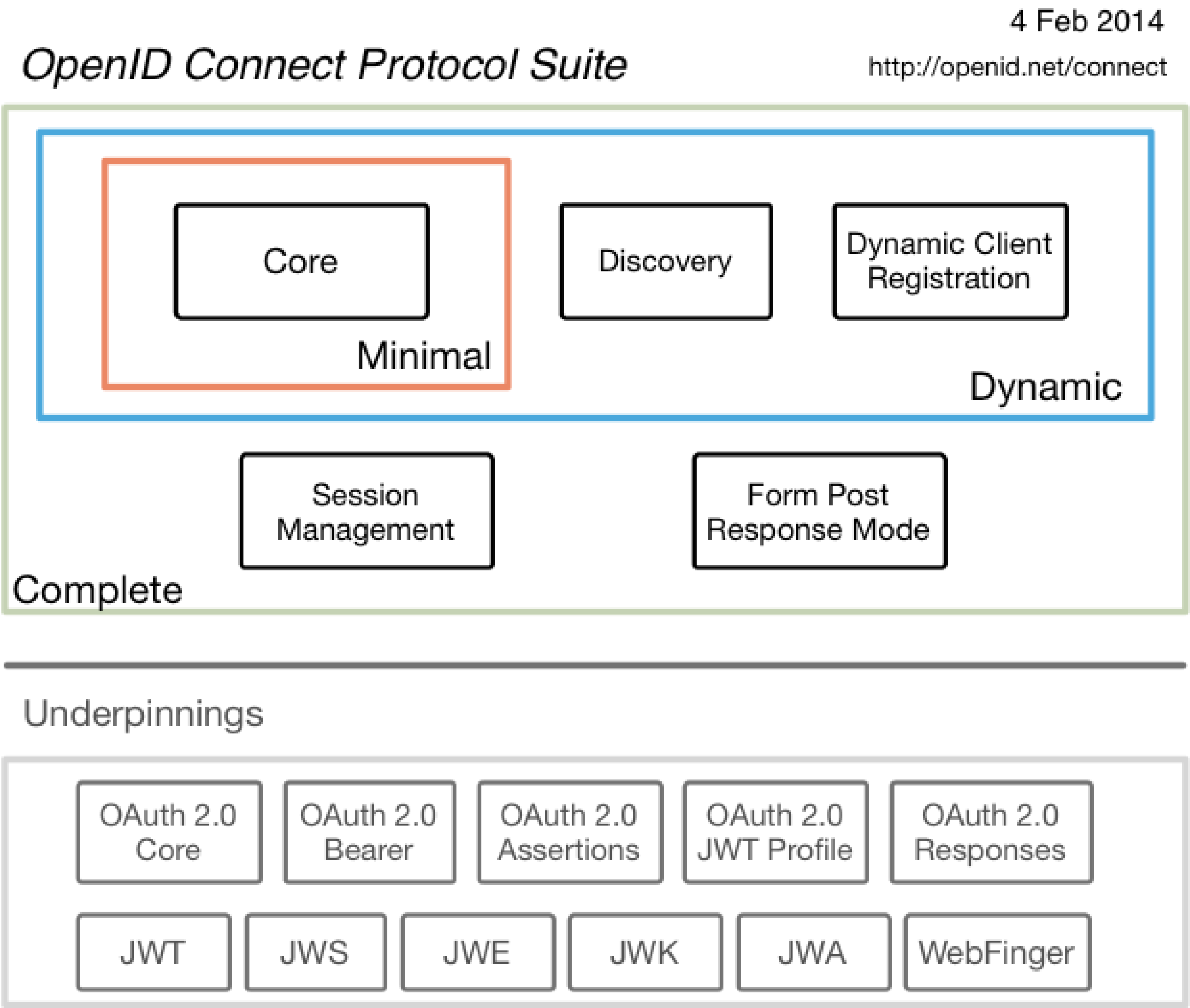


OpenID Connect

You’re Probably Already Using OpenID Connect!

- 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



OpenID Connect Protocol Suite

4 Feb 2014

http://openid.net/connect

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

Session Management / Logout

- 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 options in 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
- All support multiple logged in sessions from OP at RP
- Unfortunately, no one approach best for all use cases
- Certification tests being developed
  - WG plans to test multiple implementations before making specs Final

OpenID Federation Specification

- 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
- Implementer's Draft status reached
- Substantial changes since then
  - ***Please review!***

Identity Assurance

- OpenID Connect for Identity Assurance
  - https://openid.net/specs/openid-connect-4-identity-assurance.html
- Representation for verified person data
  - Enables legal compliance for some use cases
- New specification by Torsten Lodderstedt
  - ***Please review!***

OpenID Native SSO Specification

- Enables SSO across apps by the same vendor
- Assigns a device secret issued by the AS
- New specification being written by George Fletcher
  - ***Watch the mailing list for WG draft soon to come***

Second Errata Set

- 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_0-24.html for current Core errata draft
- ***I plan to work on the errata edits during IIW***

OpenID Current Related Work

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

OpenID Certification

- Enables OpenID Connect and FAPI implementations to be certified as meeting requirements of defined conformance profiles
- Now OP and RP 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
- FAPI OP certification launched April 1, 2019
- 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?