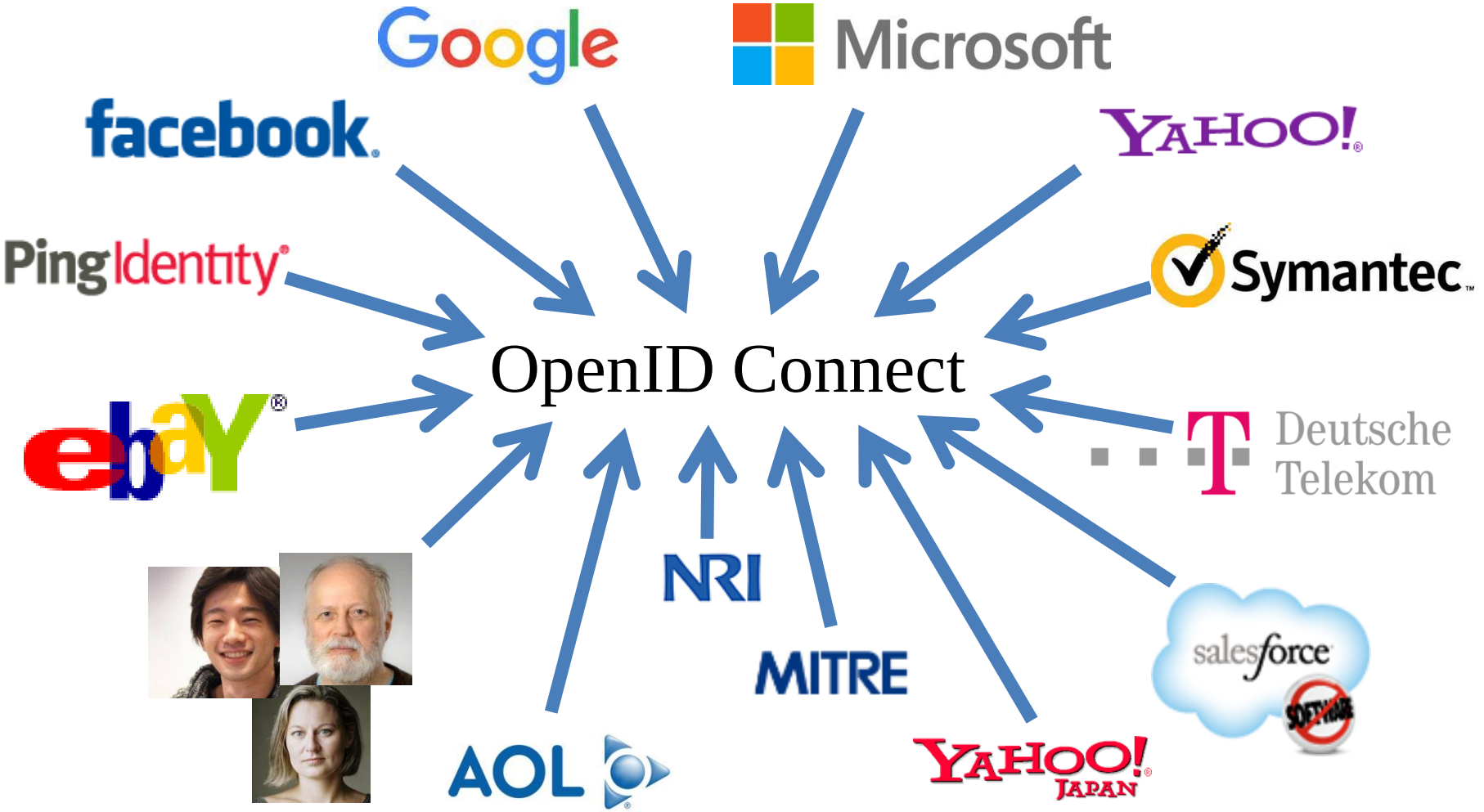
OpenID Connect Working Group

October 16, 2017

Michael B. Jones

Identity Standards Architect – Microsoft

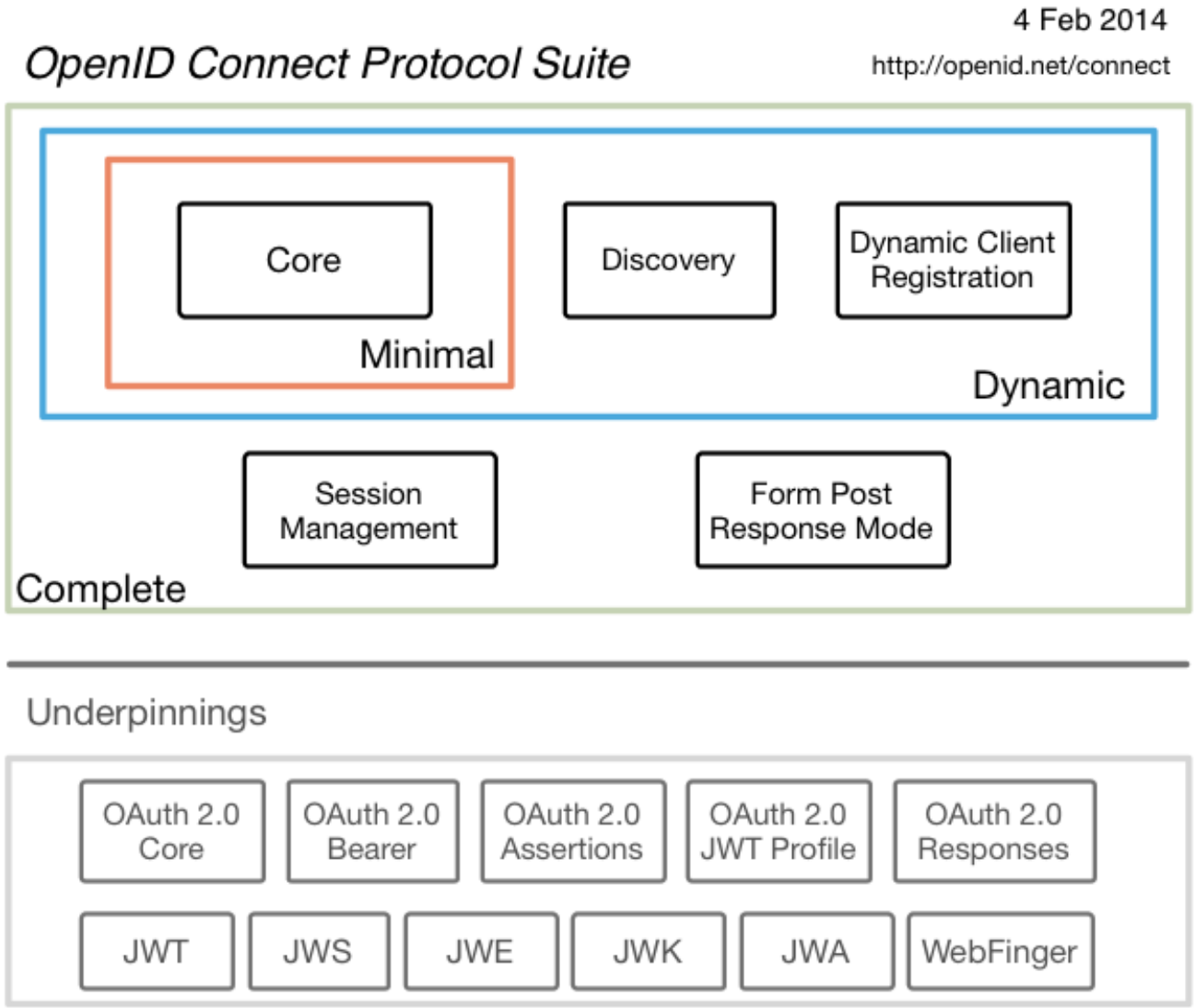
Working Together



You're Probably Already Using OpenID Connect!

- If you log in at AOL, Deutsche Telekom, Google, Microsoft, mixi, NEC, NTT, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan or have an Android phone, you're already using OpenID Connect
  - Many other sites and apps large and small also use OpenID Connect

OpenID Connect



Topics

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

OpenID Federation Specification

- 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

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
- All became Implementer's Drafts in March 2017

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_0-23.html for current Core errata draft
- Waiting for OAuth AS metadata spec draft-ietf-oauth-discovery to finish
  - To register OpenID Discovery metadata values
- Expect a call for review later this year

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 http://openid.net/certification/faq/
  - And accompanying certification presentation!

Open Conversation

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