



# **OpenID Connect Working Group**

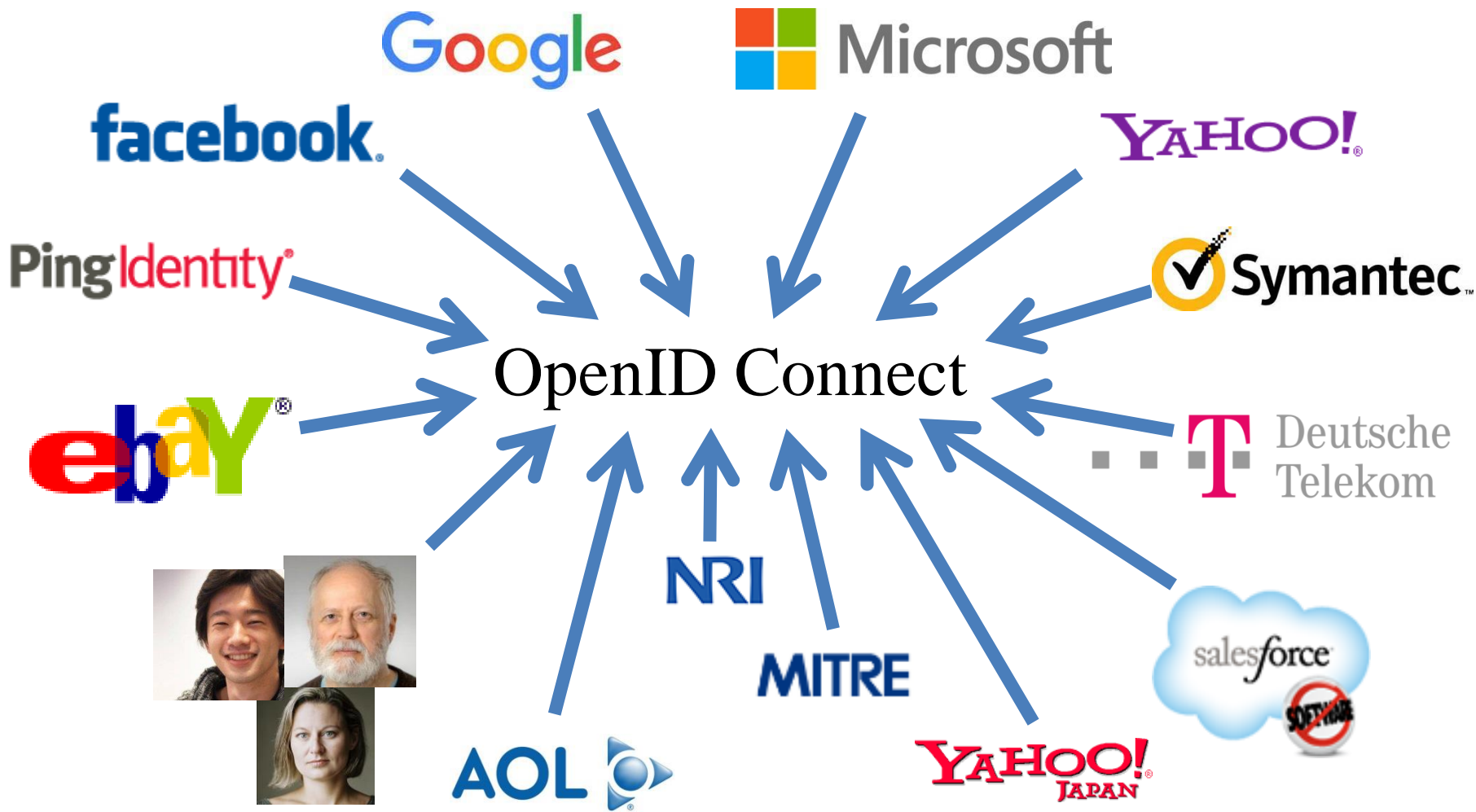
April 2, 2018

**Michael B. Jones**

Identity Standards Architect – Microsoft



# Working Together





# 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



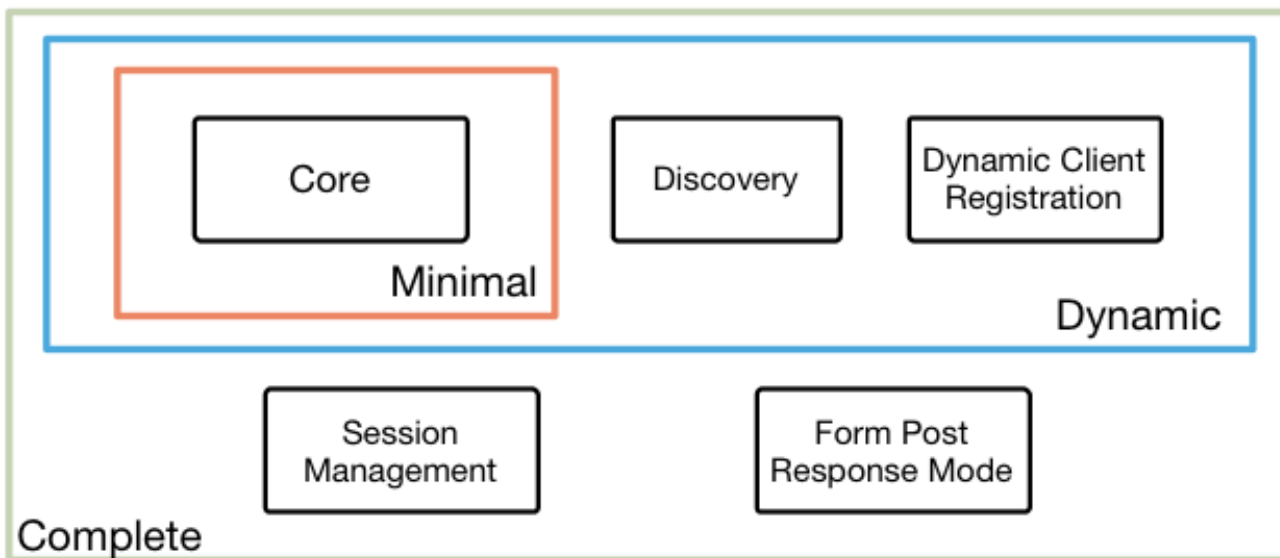
# OpenID

# OpenID Connect

4 Feb 2014

## OpenID Connect Protocol Suite

<http://openid.net/connect>



## Underpinnings





# 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





# 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](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 tested



# Session Management / Logout

- Three approaches being pursued by the working group:
  - Session Management
    - [http://openid.net/specs/openid-connect-session-1\\_0.html](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](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](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
- Is it time to move to Final Specifications?





# 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](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
  - So we can register OpenID Discovery metadata values
  - Spec just progressed to the RFC Editor
- ***I plan to do the remaining edits during IIW***



OpenID

# 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

# 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!





OpenID

# Open Conversation

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