Celebrating Ten Years of OpenID Connect

January 19, 2024

Michael B. Jones

Self-Issued Consulting

Looking Back and Looking Forward

- OpenID Connect became final in February 2014

- Today I’ll briefly share my thoughts on
  - How we created OpenID Connect
  - What we achieved together
  - Lessons learned

In the Beginning

- Artifact Binding for OpenID 2.0 started in 2010
  - Hence the openid-specs-ab@lists.openid.net mailing list name
- But developers were choosing JSON/REST over XML/SOAP
- Pivoted to instead create JSON/REST protocol over OAuth 2.0
- Result branded “OpenID Connect” at IIW in May 2011
- Five rounds of interop testing between 2011 and 2013!
  - Specifications refined after each round of interop testing
- Early developer feedback was priceless
  - Much of the early feedback came from Japan!

Design Philosophy

- Keep simple things simple
- Make complex things possible

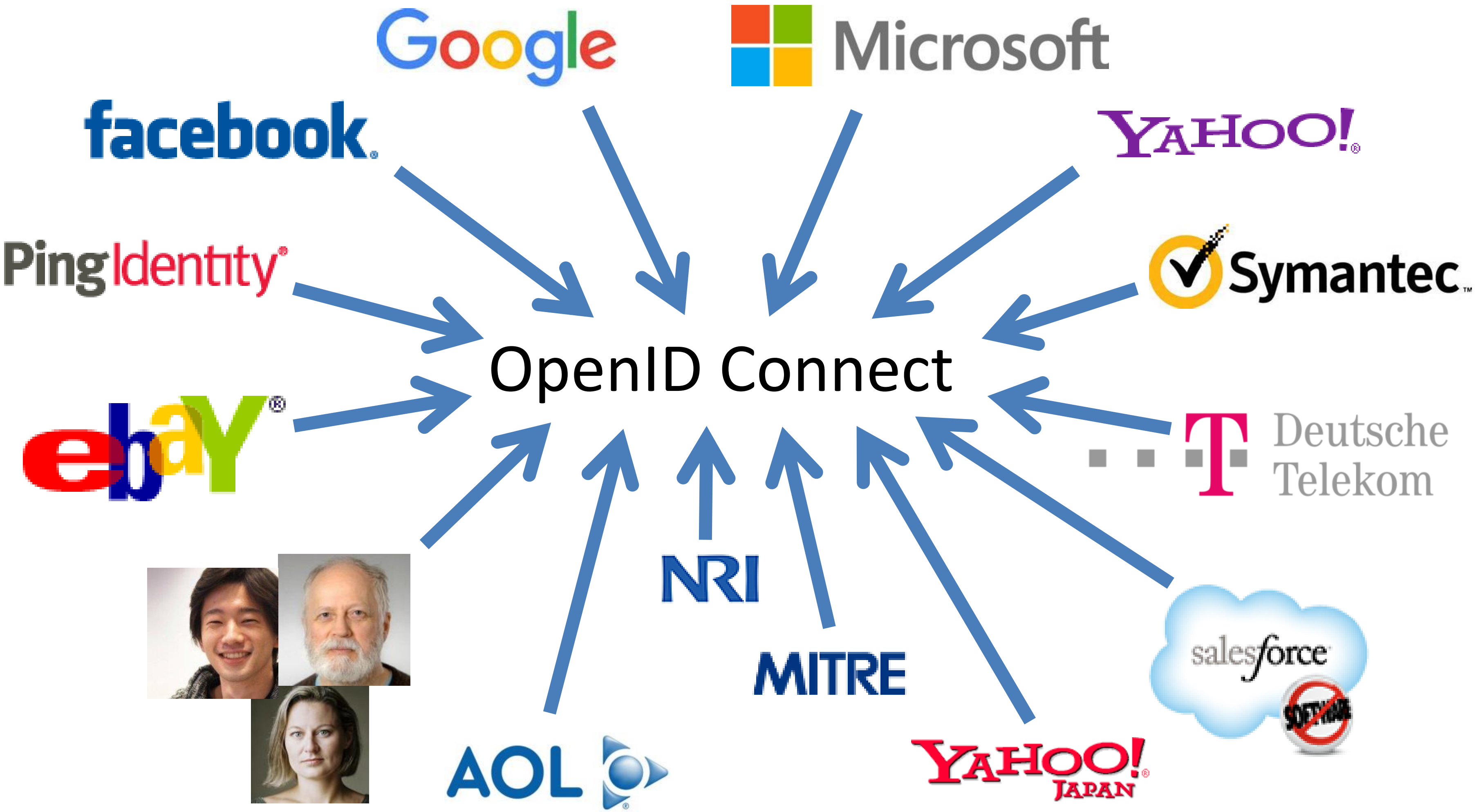
The Nov Matake Test

OpenID

- As we considered new features, we'd ask ourselves:
  - Would Nov want to add it to his implementation?
  - Is it simple enough that he could build it in a few hours?

Broad Participation

OpenID



OpenID Connect

Learning from the Past

OpenID

- Architects had extensive SAML and OpenID 2.0 experience
- Borrowed ideas that already worked well
  - Metadata
  - Authentication Contexts
- Added useful things that were previously hard or missing
  - Support for native applications
  - Encrypted claims
  - Signed requests

Extensible by Design

- Successful systems have to adapt and grow
- Always specified that “additional values may be used”
  - And specified that not-understood values don’t cause errors
  - Enables adding things without breaking existing deployments

- Indeed, many successful Connect (and OAuth) extensions have been created and deployed
  - Including logout and identity assurance

Built using Modular Components

- Created components and features we needed in parallel
  - JSON Web Signature (JWS)
  - JSON Web Encryption (JWE)
  - JSON Web Key (JWK)
  - JSON Web Token (JWT)
  - WebFinger
  - ID Token

What We Achieved

- Most used identity protocol
- Thousands of interoperable implementations
  - In every conceivable language
- Certification Program making interop a reality
- ISO just accepted our submission for republication

Innumerable OpenID Connect Deployments

- Android, AOL, Apple, AT&T, Auth0, Deutsche Telekom, ForgeRock, Google, GrabTaxi, GSMA Mobile Connect, IBM, KDDI, Microsoft, NEC, NRI, NTT, Okta, Oracle, Orange, Ping Identity, Red Hat, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo, Yahoo! Japan, all use OpenID Connect
- And many MANY more!

Lessons Learned

OpenID

- Developers choose things that are simple
  - Developer choice critical to adoption
- Interoperabilty and security require rigorous testing
  - OpenID Certification program was essential to Connect’s success
- Extensibility is critical to long-term success
- Deployments have to be easy to use (or they won’t be used)
  - Most RPs limited IdP choice as a simplification
    - Even though Connect was designed to give users complete choice
- Not everything works out the way you planned