



OpenID Connect Update

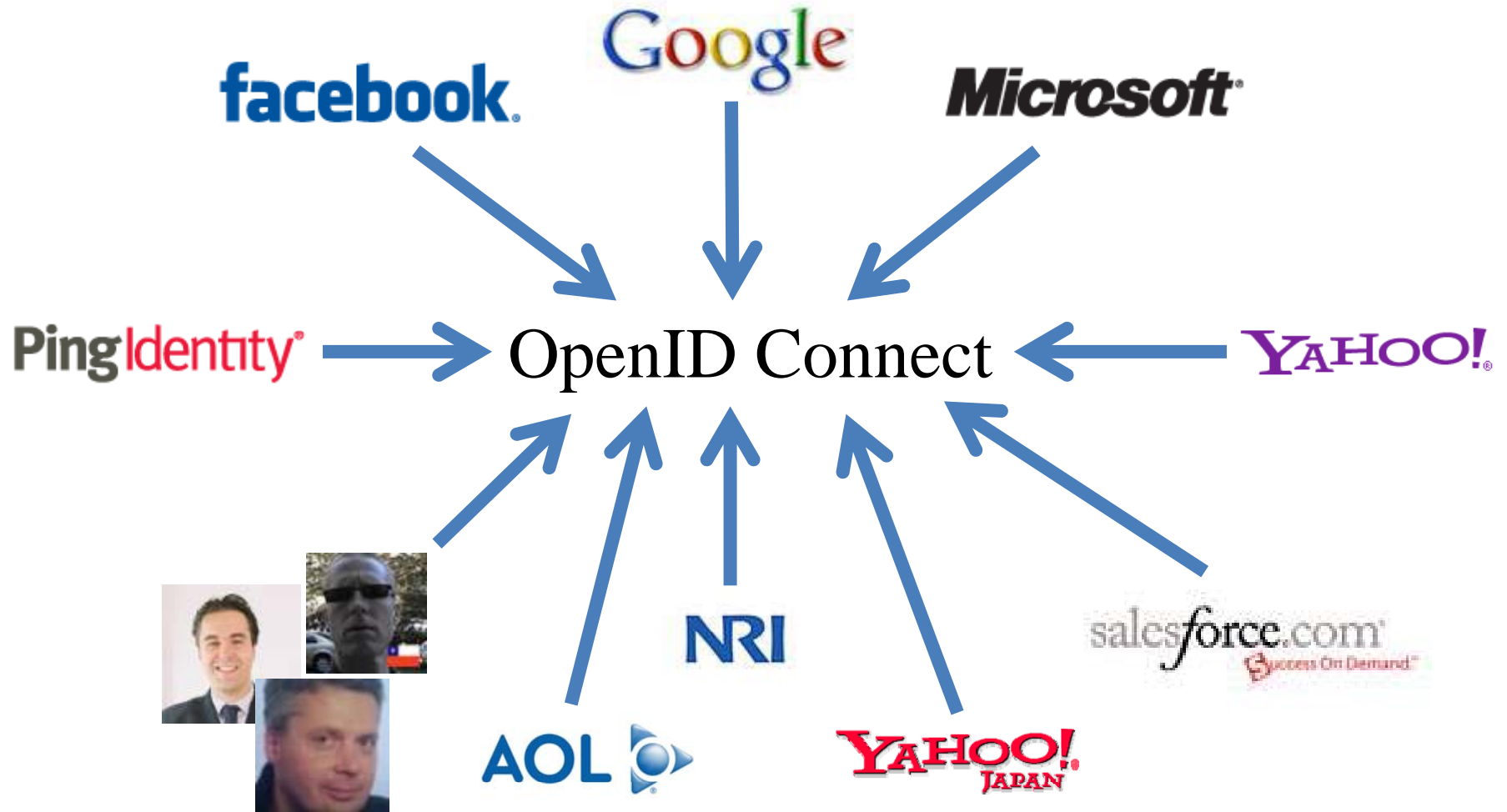
December 1, 2011

Mike Jones

Identity Standards Architect – Microsoft



Working Together





OpenID Presentation Overview

- Recent Timeline
- OpenID Connect Design Criteria
- OpenID Connect Overview
- Developer Feedback Incorporated
- Next Steps
- Resources
- Open Discussion



Recent Timeline

- Weekly spec calls began, Jan 2011
- Open issued closed at IIW, May 2011
- Result branded “OpenID Connect”, May 2011
- Developer feedback, May 2011 to present
- Functionally complete specs, Jul 2011
- Formal issue tracking began, Jul 2011
- Interop testing, Sep & Oct 2011
- Simpler specs published incorporating developer feedback, Sep & Oct 2011
- Decision to move to Implementer’s Drafts, Oct 2011
- Finishing Implementer’s Drafts, Nov 2011



OpenID Key Diffs from OpenID 2.0

- Support for native client applications
- Identifiers using e-mail address format
- Built on OAuth 2.0
- Uses JSON/REST, rather than XML
- Support for higher LOAs



Design Criteria

Easy Things Easy

Harder Things Possible

Modular Design



Easy Things Easy

Standard UserInfo for
Simple “Connect” Ability

Designed to Work Well on
Mobile Phones



OpenID How We Make It Easy

- Build on OAuth 2.0
- Use JavaScript Object Notation (JSON) data structures
- Can only build functionality that you need
- Goal: Easy implementation on all modern web platforms



OpenID Harder Things Possible

Claims Aggregation

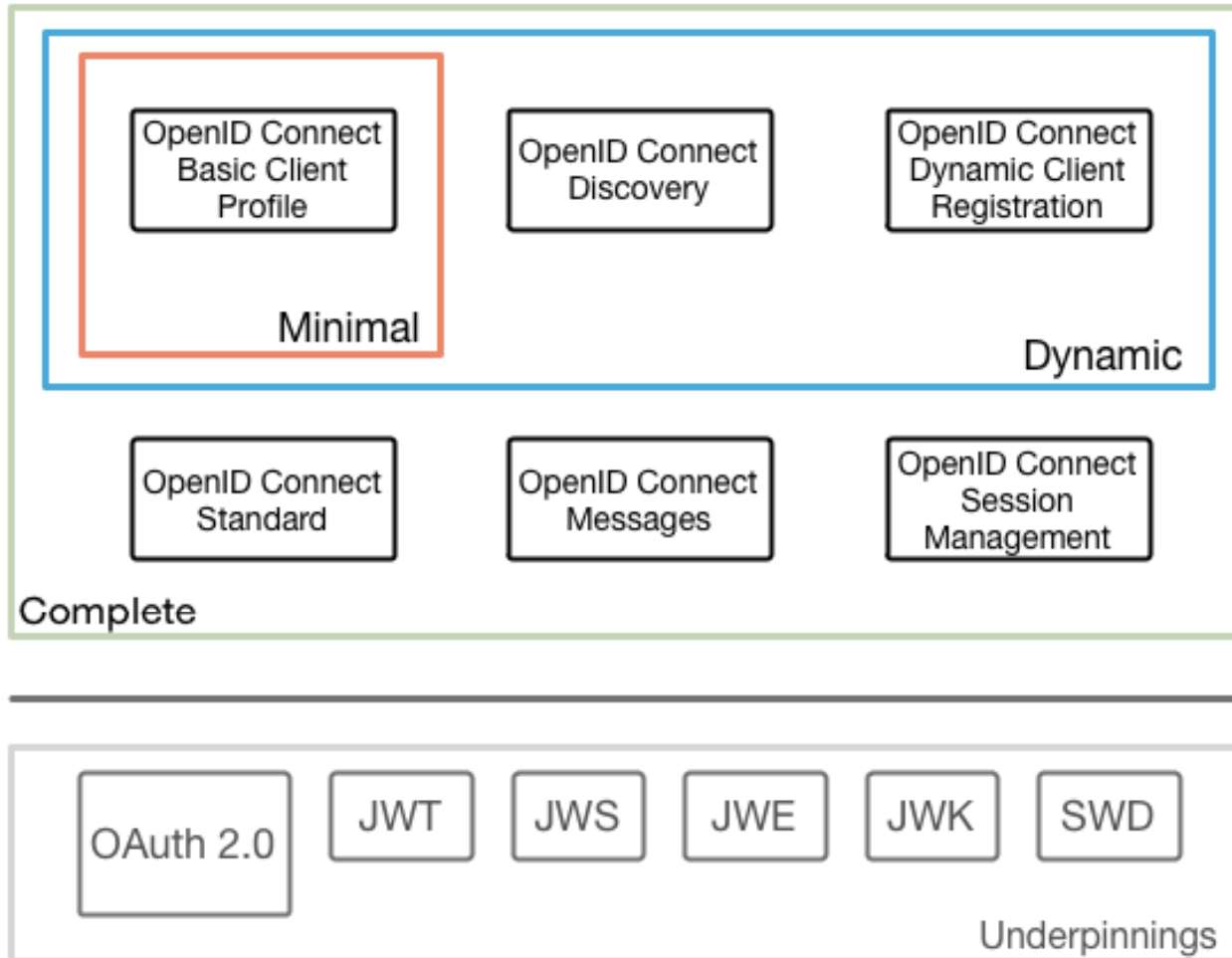
Distributed Claims

Encrypted Claims



OpenID

Connect Overview



OpenID Connect Protocol Suite

6 September 2011

<http://openid.net/connect>



Basic Client Profile

- Single, simple, self-contained client spec
- All you need for web-based RP utilizing pre-configured set of OPs
- http://openid.net/specs/openid-connect-basic-1_0.html



OpenID Discovery & Registration

- Enables dynamic configurations in which sets of OPs and RPs are not pre-configured
 - Necessary for “open” deployments
- Discovery enables RPs to learn about OP endpoints
- Registration enables RPs to use OPs they are not pre-registered with
- http://openid.net/specs/openid-connect-discovery-1_0.html
- http://openid.net/specs/openid-connect-registration-1_0.html



OpenID Messages & Standard

- Messages spec defines data formats exchanged in OpenID Connect messages
- Standard spec is HTTP binding for Messages
- (Basic is profile of Messages and Standard)
- Needed for OPs, native client apps, and RPs needing functionality not in Basic
 - E.g., claims not in default UserInfo set
- http://openid.net/specs/openid-connect-messages-1_0.html
- http://openid.net/specs/openid-connect-standard-1_0.html

 OpenID Session Management

- For OPs and RPs needing session management capabilities
- Example capability: Logout
- http://openid.net/specs/openid-connect-session-1_0.html



Underpinnings

- OAuth 2.0 family of specs
 - OAuth 2.0 core
 - OAuth 2.0 bearer
- JWT family of specs
 - JSON Web Token (JWT)
 - JSON Web Signature (JWS)
 - JSON Web Encryption (JWE)
 - JSON Web Key (JWK)
- Simple Web Discovery (SWD)



Developer Feedback Incorporated

- Asked for simpler, more modular specs
 - Basic Client spec a direct result of this feedback
 - Messages and Standard also a simpler factoring
- Asked for UserInfo schema to be more like Facebook Connect
 - Changed spelling of claim names from camelCase to lowercase_with_underscores
 - Changed from Portable Contacts schema to current one
- Asked for more meaningful JSON identifiers
 - Changed OpenID identifiers to be full words, e.g.:
 - “idt” -> “id_token”
 - “loc” -> “locale”
- Dozens of corrections and clarifications



Connect Next Steps

- Incorporate remaining tracked issue resolutions into the specs
- Membership vote on Implementer's Drafts
- Deployments
- Incorporate feedback arising from deployments
- Membership vote on Final Specifications
- *Other Connect-related work happening in parallel*



Resources

- OpenID Connect Page
 - <http://openid.net/connect/>
- Artifact Binding Working Group Mailing List
 - <http://lists.openid.net/mailman/listinfo/openid-specs-ab>
- OpenID Connect Interop Mailing List
 - <http://groups.google.com/group/openid-connect-interop>
- Mike Jones' Blog
 - <http://self-issued.info/>



Backup Slides



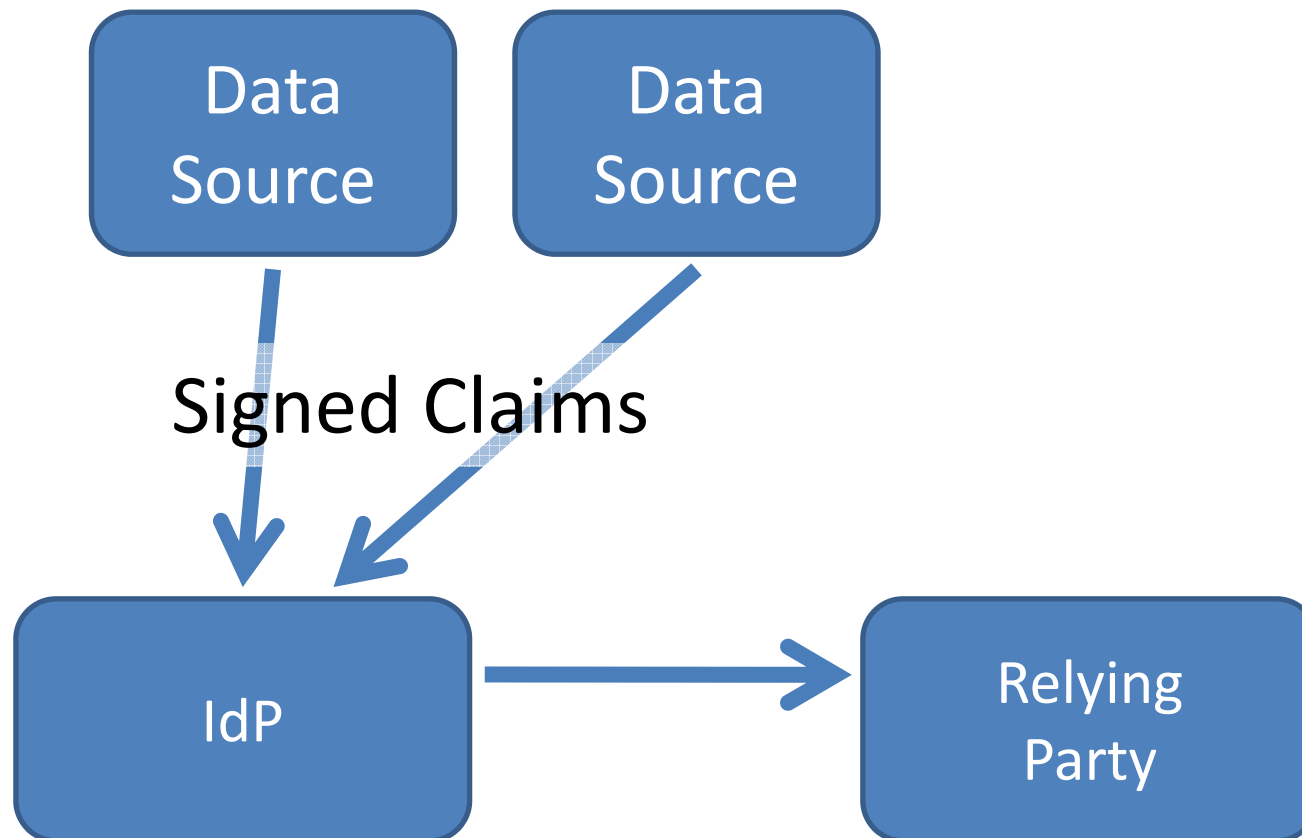
OpenID

Connect Capabilities

- Dynamic Clients
- Mobile Support
- UserInfo Endpoint
- Simple RPs
- Session Management
- OAuth 2 Integration
- Use of JWTs and JSON data structures
- Single Logout
- Aggregated and Distributed Claims
- Encrypted Claims

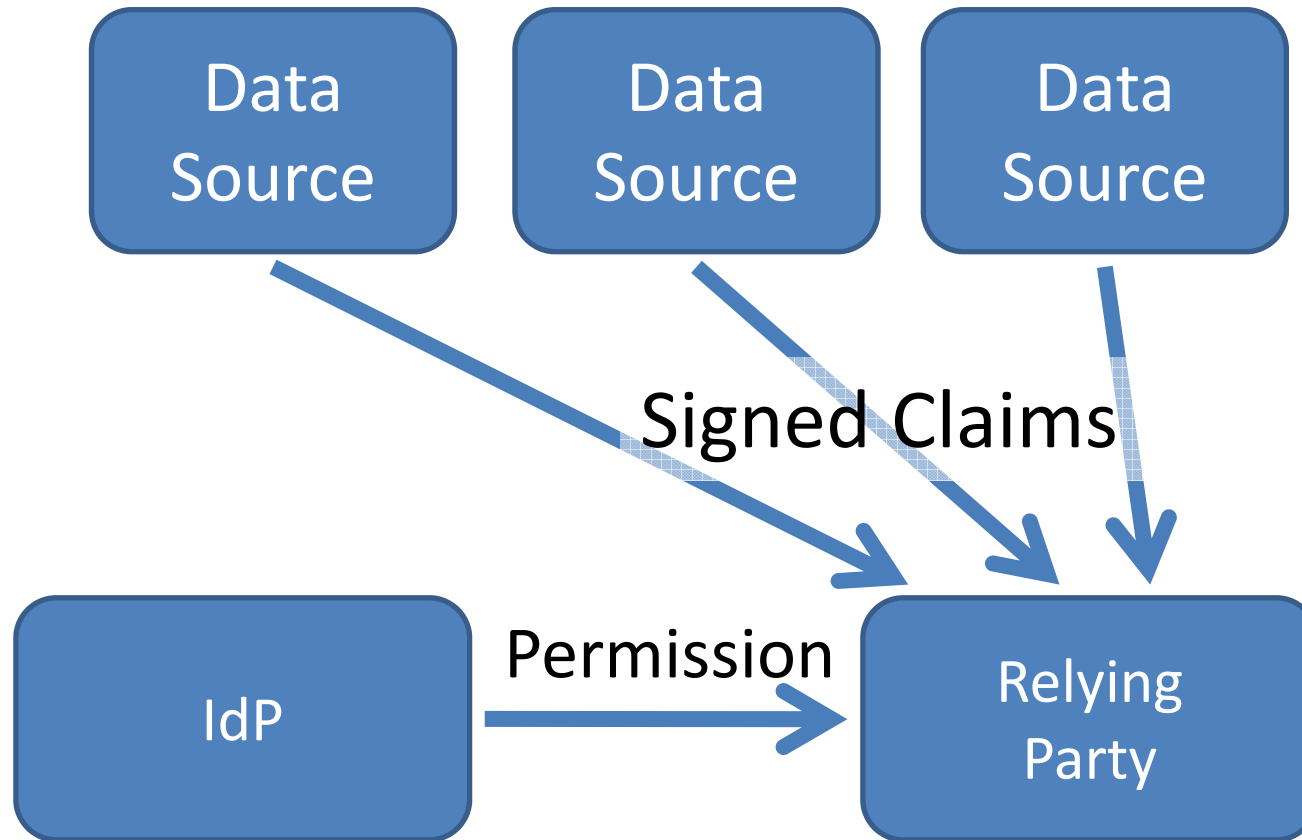


Claims Aggregation





Distributed Claims



Better scalability, etc.



Working Group Participants

- Key working group participants:
 - Nat Sakimura – Nomura Research Institute – Japan
 - John Bradley – Independent – Chile
 - Breno de Medeiros – Google – US
 - Paul Tarjan – Facebook – US
 - Axel Nennker – Deutsche Telekom – Germany
 - Kick Willemse – Independent – Netherlands
 - Chuck Mortimore – Salesforce – US
 - Mike Jones – Microsoft – US
- By no means an exhaustive list!