OpenID and FIDO

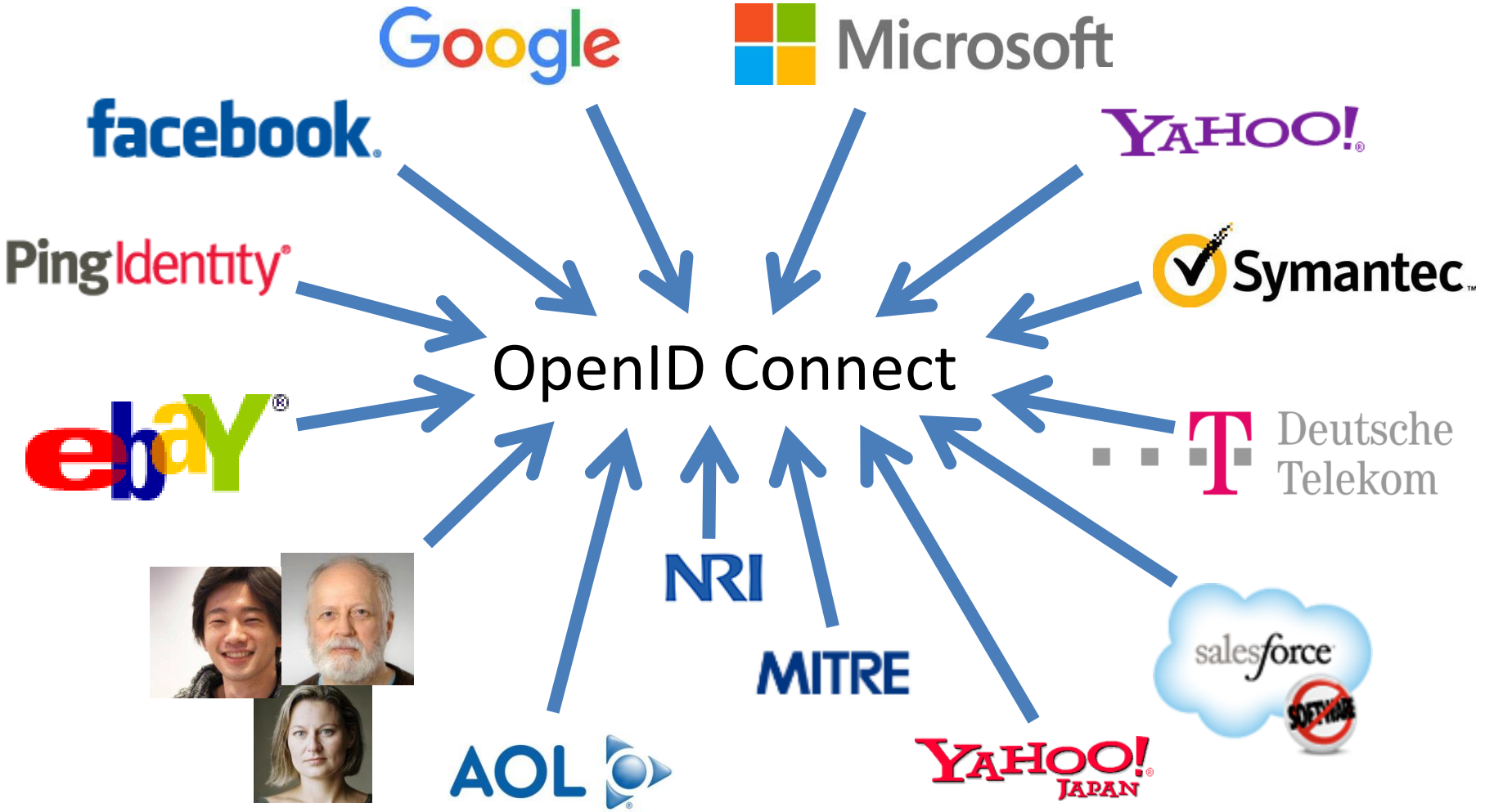
October 21, 2021

Michael B. Jones

Identity Standards Architect – Microsoft

Working Together

OpenID



What is OpenID Connect?

- Simple identity layer on top of OAuth 2.0
- Enables Relying Parties (RPs) to verify identity of end-user
- Enables RPs to obtain basic profile info
- REST/JSON interfaces → low barrier to entry
- Described at https://openid.net/connect/

You're Almost Certainly Using OpenID Connect!

- Android, AOL, Apple, AT&T, Auth0, Deutsche Telekom, ForgeRock, Google, GrabTaxi, GSMA Mobile Connect, IBM, KDDI, Microsoft, NEC, NTT, Okta, Oracle, Orange, Ping Identity, Red Hat, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo, Yahoo! Japan, all use OpenID Connect
  - Many other sites and apps large and small use OpenID Connect
- OpenID Connect is infrastructure
  - Not a consumer brand

OpenID and FIDO are Complementary

- Can use FIDO for phishing-resistant sign-in at OpenID Connect Identity Providers
  - Passwordless login to your Microsoft account
  - Unphishable second factor for your Google account
- Those IdPs then use OpenID Connect to sign you into RPs
  - Hotmail, Skype, Office 365, …
  - Gmail, YouTube, Google Docs, …
- Extends benefits of FIDO to millions of OpenID RPs
  - With no extra work needed by those RPs!

fido™ ALLIANCE

Using FIDO and OpenID Together

Authenticator ⟷ login.microsoftonline.com ⟷ hotmail.com

WebAuthn/FIDO

OpenID Connect

FIDO makes OpenID Phishing-Resistant

- OpenID Connect is intentionally silent on how the person signs in to the IdP
  - Enables IdPs to adopt new authentication methods over time
  - Such as using WebAuthn/FIDO
- FIDO defines phishing-resistant authentication methods
  - Authenticators used for both passwordless login and second factor
- Using them together makes OpenID Connect phishing resistant!

fido™ ALLIANCE

Connective Tissue

- OpenID Connect RPs can request use of phishing-resistant authentication by IdPs
  - WebAuthn/FIDO Authenticators can satisfy these requests
- OpenID Connect Extended Authentication Profile (EAP)
  - https://openid.net/specs/openid-connect-eap-acr-values-1_0.html
  - Defines ACR values for phishing-resistant authentication (`phr`, `phrh`)
  - Defines AMR value for Proof of Possession (`pop`)
- RP can learn whether phishing-resistant authentication was performed by IdP

What is OpenID Certification?

- Enables OpenID Connect (and FAPI) implementations to be certified as meeting the requirements of defined conformance profiles
  - Goal is to make high-quality, secure, interoperable implementations the norm
- An OpenID Certification has two components:
  - Technical evidence of conformance resulting from testing
  - Legal statement of conformance
- Currently 984 certifications of 334 deployments!
- See https://www.certification.openid.net/

Use of Self-Certification

- OpenID Certification uses self-certification
  - Party seeking certification does the testing
  - (rather than paying a 3rd party to do the testing)
- Simpler, quicker, less expensive, more scalable than 3rd party certification
- Results are nonetheless trustworthy because
  - Testing logs are made available for public scrutiny
  - Organization puts its reputation on the line by making a public declaration that its implementation conforms to the profile being certified to

Related Sessions Today

- Global Assured Identity Network (GAIN): Building an Assured Identity Layer for the Internet
  - 10:30-Noon
- Bringing mobile driving licenses (mDL) to the Web and apps
  - 1:30-3:00
- Shared Signals and Events (SSE)
  - 5:00-6:30

fido™ ALLIANCE

Open Conversation

- How are you using FIDO with OpenID Connect?

- *Slides will be posted at https://self-issued.info/*