OpenID Meeting at IETF 90

Mike Jones

July 20, 2014

Possible Topics

- OpenID Connect
- Related IETF Specifications
- Account Chooser
- Native Applications

OpenID Connect

- Most specifications finished in February 2014
- Remaining to do:
  - Finish Session Management/Logout
  - Finish form post binding
  - Errata
  - OpenID 2.0 transition specification
  - Application/Sector Profiles

OpenID 2.0 Transition Spec

- Defines how to correlate OpenID 2.0 identifiers with OpenID Connect identifiers
- Allows migration forward
- Google, Yahoo, others will turn off OpenID 2.0
- Leif suggested a deployment best practices guide, including things about migration issues

Planned OpenID Connect Profiles

- Mobile Profile
  - With GSMA
  - Chaired by Torsten Lodderstedt of DT
  - Possibly use data from mobile network to discover IdP
  - Possibly create a registration profile
  - Possibly create level of assurance profile
  - Aspects of trust framework membership
- Healthcare Information Exchange Profile
  - With US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC)
  - And MIT Kerberos Consortium

Related IETF Specifications

- Finished
  - OAuth 2.0 – RFC 6749, RFC 6750
  - WebFinger – RFC 7033
- Nearly Finished
  - JWT and JOSE
  - OAuth Assertions and JWT Assertion Profile
  - OAuth Dynamic Registration
- Just Getting Started
  - Authorization Code PoP draft-sakimura-oauth-tcse
  - JWK Thumbprint draft-jones-jose-jwk-thumbprint-00
  - OAuth Authentication draft-hunt-oauth-v2-user-a4c

Account Chooser

- Nat Sakimura moving specification forward
- New functionality
  - Pre-loading account identifiers by trusted IdPs
  - Intended to help solve the bootstrapping problem

Native Applications

- Single-sign-on for native apps on phones
- Sign into IdP once – use sign-in from many apps

OpenID Connect at Deutsche Telekom

- Torsten gave a presentation on OpenID Connect at Deutsche Telekom

News from Japan

- Kaoru Maeda reported that the OpenID Connect implementation by mixi and Yahoo Japan uses an additional “server_state” parameter
- He said that Ryo Ito plans to submit a draft describing it to the OAuth working group