Verisign Labs Experiment with Federated Authentication for RDAP

IETF-95 REGEXT Working Group
Scott Hollenbeck
shollenbeck@verisign.com
April 4, 2016

Purpose of the Experiment

- Core RDAP does not support client authentication (needed for differentiated access) in a way that scales
- Can existing RDAP specifications be extended?
  - Produce running code and operational experience to guide development of a proposal for a standard method of using RDAP with *federated authentication*
- Discover interop issues with the RDAP RFCs and federated authentication standards
- Inform policy development

Foundations of the Experiment

- Implement core RDAP for .tv and .cc ccTLDs
  - Both are thin registries
- Add support for federated authentication using OpenID Connect
  - http://openid.net/specs/openid-connect-core-1_0.html
- Implement an Identity Provider to test new identity claims
- Integrate other Identity Providers (IDPs)
- Develop an Internet-Draft proposal for extending RDAP
  - https://datatracker.ietf.org/doc/draft-hollenbeck-weirds-rdap-openid/

Progress of the Experiment

- Launched on 3 February 2016
  - Proposed end on 3 June 2016
- No issues with core RDAP (yet)
- Produced updates to the I-D
- Supports both unauthenticated and authenticated client access
- Support for 4 Identity Providers
  - Gmail, Hotmail, CZ.NIC, Verisign Labs
- Will continue until 3 June 2016 (for now)

Findings Thus Far

- Specifications are remarkably implementable
  - One issue with OpenID Connect browser dependency
- Easy to integrate Relying Parties (RPs) and IDPs
- One issue with OpenID Connect
  - auth_time claim: number; integer or real?
- Easy to add new JSON Web Token (JWT) claims
- Need to add refresh token?
- How to discover supported IDPs?
- Still waiting for cross-area review
- Authorization and access control policies needed!

Next Steps

- More RP/IDP integration
  - Thick registries, where are you?
- Participate in the ICANN PDP
  - Will need to add features as discussions evolve
- Continue to report findings
- Evaluate progress and continue past 3 June as needed