Federated Authentication for RDAP
Registration Operations Workshop 2015-2

Scott Hollenbeck, Senior Director
shollenbeck@verisign.com

July 19, 2015

VERISIGN®

The Problem

- Clients must be identified and authenticated before a server can make access control and authorization decisions
- Managing individual client credentials will be cumbersome for both client and server
- More than a user name and password is needed
  - Controls are needed to protect personal privacy
- Must be supported by today's web services
- *More in RFC 7481*

The Solution

- Federated authentication!
- Proposal described in an Internet-Draft
  - draft-hollenbeck-weirds-rdap-openid-02
- Uses OpenID Connect
  - http://openid.net/connect/
  - Built on existing OpenID and OAuth standards
  - *“allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner”*

The Approach

- Use existing end-user identity providers
  - http://openid.net/get-an-openid/
  - Can create new providers for specific purposes
- Use existing OpenID Connect software
  - http://openid.net/developers/libraries/
- Use existing RDAP clients and servers
- Deploy and test!

VERISIGN®