Federated Authentication for RDAP
ICANN-54 Tech Day

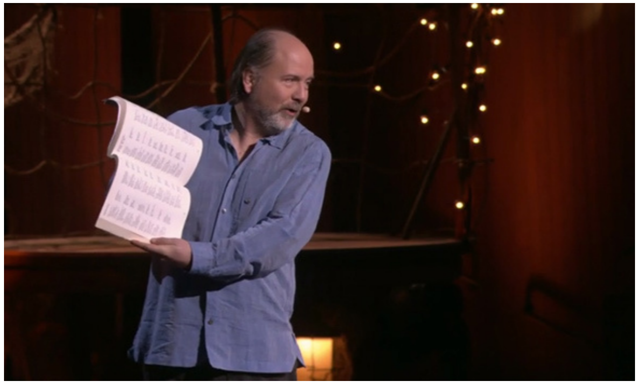
Scott Hollenbeck, Senior Director
shollenbeck@verisign.com

October 19, 2015

VERISIGN

RDAP? What about WHOIS?

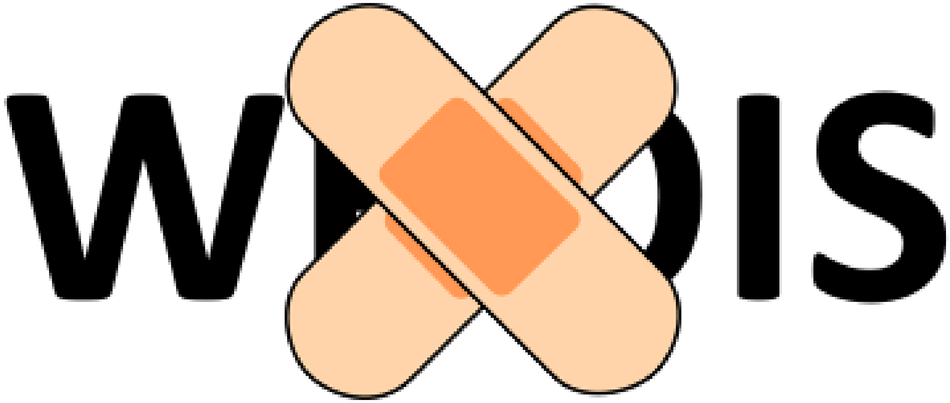
- WHOIS first documented in RFC 812 – *from 1982*!
  - Predates the domain name system (1983 - 1985)
  - Predates the World Wide Web (alt.hypertext publication in 1991)
  - Updated by RFC 954 (1985) and 3912 (2004)
  - Original purpose? From RFC 812:
    - *"it delivers the full name, U.S. mailing address, telephone number, and network mailbox for ARPANET users"*



- Designed for use *within a small community of cooperating users*
- Today: public Internet resource directory
  - Many challenges!
    - …and many contentious attempts to fix via protocol and policy

Image source: http://blog.ted.com/what-the-internet-looked-like-in-1982-a-closer-look-at-danny-hillis-vintage-directory-of-users/

So what about those fixes?



We need to take a different approach!

Expert Working Group on gTLD Directory Services

- Expert Working Group (EWG) formed in February 2013 to:
  - *"Define the purpose of collecting and maintaining gTLD registration data, and consider how to safeguard the data"*[1]
  - *"Provide a proposed model for managing gTLD directory services that addresses related data accuracy and access issues, while taking into account safeguards for protecting data"*[1]
- EWG released final report on 6 June 2014[2]
  - Recommendation
    - *"The EWG recommends that a new approach be taken for registration data access, abandoning entirely anonymous access by everyone to everything in favor of a new paradigm that combines public access to some data with gated access to other data"*
- The big question: *how*?

[1] https://www.icann.org/news/announcement-2-2012-12-14-en

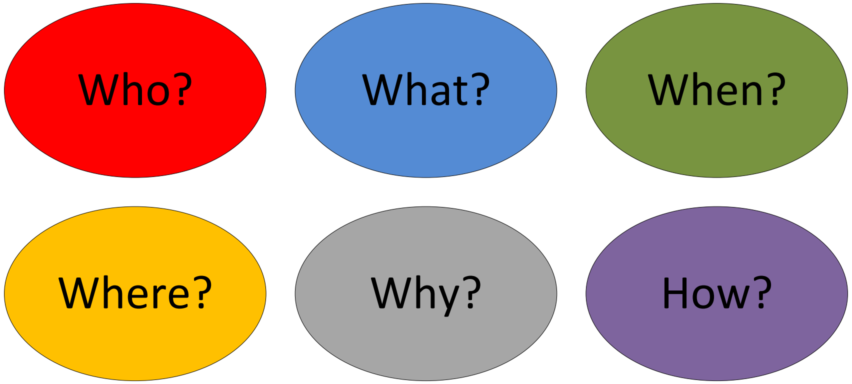
[2] https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

A New Approach Using RDAP

- RDAP: Registration Data Access Protocol
  - *RDAP ≠ WHOIS!*
- Specified in RFCs 7480 – 7484, published March 2015
  - WHOIS inventory and object analysis in RFC 7485
  - Additional specifications still needed for operational use
- Designed to address *technical* issues with WHOIS
  - Lack of standardized command structures
  - Lack of standardized output and error structures
  - Lack of support for internationalization and localization
  - Lack of support for security features including identification, authentication, and access control
  - *Technical solutions can help address policy issues*
- Designed to be easy to implement and operate

Gated Access to Data

- WHOIS: All clients see all data (more or less)
- RDAP: What a client sees can depend on
  - *Who* is asking
  - *What* they're asking for
  - *When* they're asking
  - *Where* they're asking from
  - *Why* they're asking, and
  - *How* they're asking



- RDAP allows a server to make access control decisions based on
  - Client identity
  - Client authorization

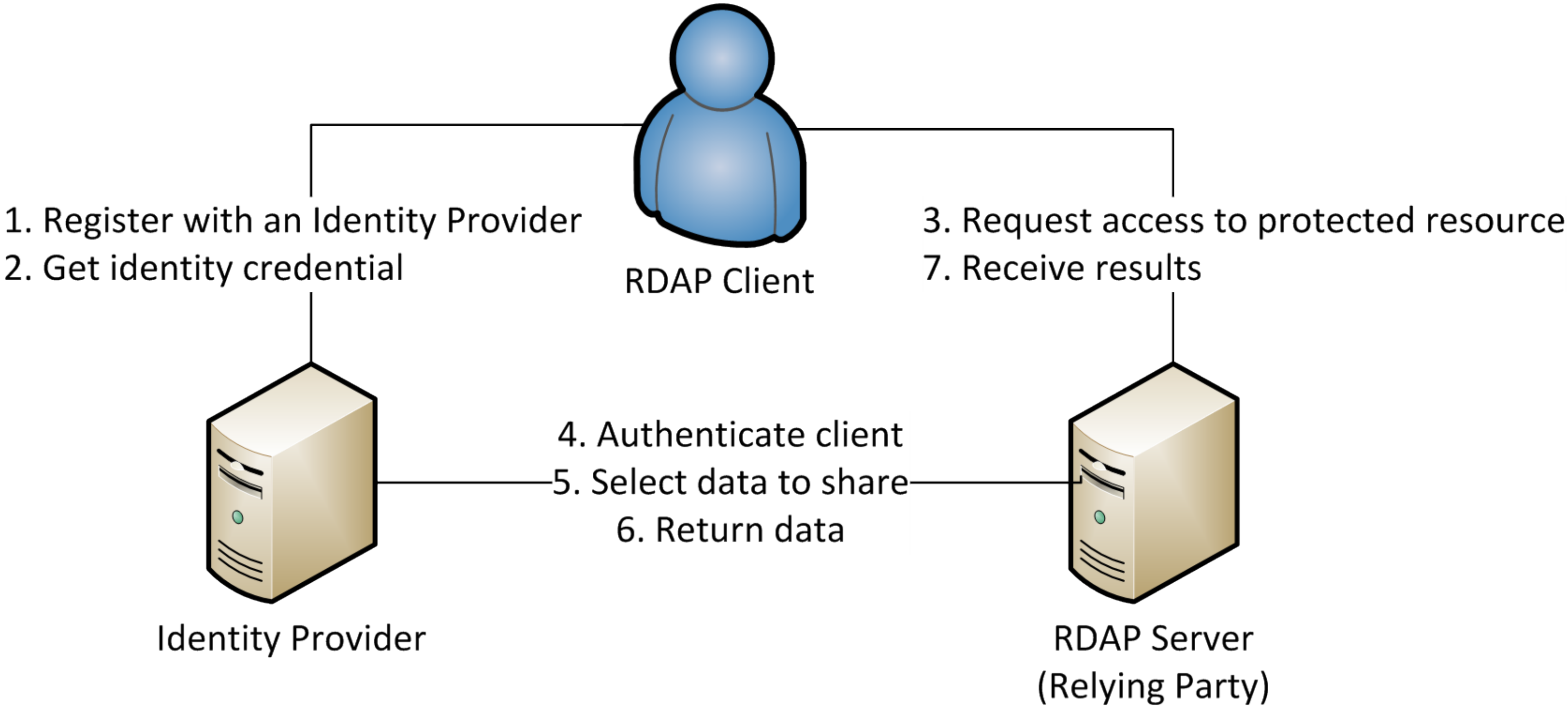
Client Identification and Authorization

- 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 *both* client and data privacy
- Must be supported by today’s web services
- *More in RFC 7481*

One Solution

- Federated authentication!
- Federated authentication?
  - Similar to the “single sign on” concept
  - A means of identifying and authenticating entities based on mutual trust between members of a common community, or federation
  - Credentials are issued to clients by identity providers
  - Credentials are presented by clients to server operators (relying parties)
  - Credentials are sent from server to identity provider for validation
  - Client selects information to be shared with server
  - If all is well – *access granted*!

How does it work?



1. Register with an Identity Provider
2. Get identity credential

RDAP Client

3. Request access to protected resource
7. Receive results

4. Authenticate client
5. Select data to share
6. Return data

Identity Provider

RDAP Server
(Relying Party)

Unauthenticated Query Result

```
{
  "handle": "XXXXXXX-YYYY",
  "objectClassName": "domain",
  "notices": [
    …
  ],
  "rdapConformance": [
    "rdap_level_0"
  ],
  "ldhName": "example.com",
  "secureDNS": {
    …
  },
  "nameservers": [
    …
  ]
}
```

Basic Authenticated Query Result

```
{
  (Unauthenticated results),
  "events": [
    {
      "eventAction": "registration",
      "eventDate": "2001-10-08T13:07:03Z"
     },
     {
      "eventAction": "last changed",
      "eventDate": "2015-08-21T18:01:34Z"
     },
     {
      "eventAction": "expiration",
      "eventDate": "2017-10-08T13:07:03Z"
     }
  ],
  "status": [
   "clientDeleteProhibited -- http://www.icann.org/epp#clientDeleteProhibited",
   "clientRenewProhibited -- http://www.icann.org/epp#clientRenewProhibited",
   "clientTransferProhibited -- http://www.icann.org/epp#clientTransferProhibited",
   "clientUpdateProhibited -- http://www.icann.org/epp#clientUpdateProhibited",
   "serverTransferProhibited -- http://www.icann.org/epp#serverTransferProhibited"
  ]
}
```

Extended Authenticated Query Result

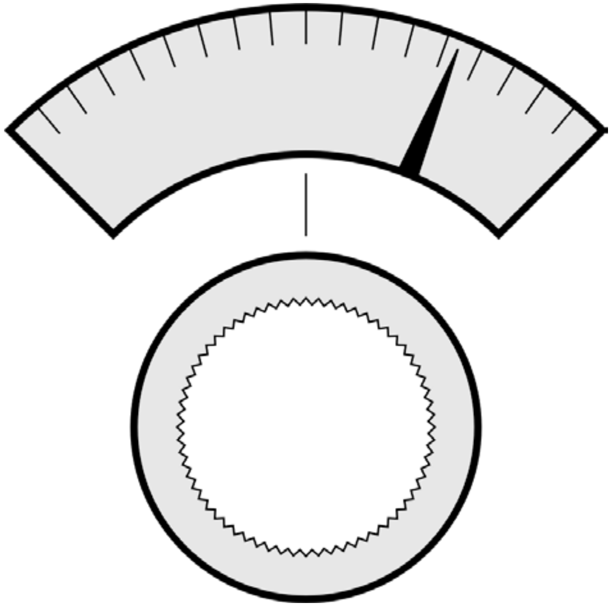
```
{
  (Basic authenticated results),
  "entities": [
    {
      "links": [
        {
          "href": "http://rdap.verisign.com/rdap/entity/XXXXX",
          "rel": "self",
          "type": "application/rdap+json",
          "value": "http://rdap.verisign.com/rdap/entity/XXXXX"
        }
      ],
      "objectClassName": "entity",
        "roles": [
          "technical",
          "billing",
          "administrative",
          "registrant"
        ],
        "vcardArray": [
          …
        ]
    }
  ]
}
```

The Approach

- Proposal described in an Internet-Draft
  - draft-hollenbeck-weirds-rdap-openid-02
- Use 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”*
- Prototype implementation in progress at Verisign Labs

To Do

- Test implementations and share results
  - Open to everyone
  - More server operators needed
- Find appropriate settings for RDAP's "knobs and dials"
- Continue standardization work based on implementation experience
- Inform policy work
  - Among everything else, need policy for identity providers, client authorization, and data access



VERISIGN®