How It Works: ROW Topics

November 2016

Agenda

1. Introduction
2. History and Background
3. EPP
4. RDAP
5. Q&A


Introduction

What is ROW?

Registration Operations Workshop - an informal industry group & discussion forum for the technical aspects of registration operations in the Domain Name System ecosystem.

One current purpose of the ROW - start preparing for the replacement of WHOIS by its successor, the Registration Data Access Protocol (RDAP), a combined protocol for IP addresses and names registration data.

ROW forums - gathered individuals involved with the operation of domain name registrations systems in discussions around development and deployment of RDAP and Extensible Provisioning Protocol (EPP) extensions.

Timing

July 2016 - ICANN published version 1.0 of the RDAP gTLD Profile.

Today's crucial need - pursue registration operations discussions and solve shared technical problems related to the development and deployment of RDAP and EPP extensions within a broader audience.

RDAP Implementation next steps - will be discussed during the Registration Data Access Protocol Implementation meeting, Monday, November 7, 17:00 - 18:30 IST, Hall 2: https://icann572016.sched.org/event/8dQX/registration-data-access-protocol-implementation

Spring 2017 - next ROW; further details available at: http://regiops.net

Registration Operations Forum

Purpose - raise interest within a broader global audience; open to all interested parties.

Format - tutorials aimed to explore instructional and more advanced information in the fundamentals of Registration Operations, RDAP deployments and EPP extensions.

Content - introduction, history and background of registry operations, evolution Whois, followed by high-level overviews of RDAP deployments and EPP extensions.

Time to further explore - Q&A now and upcoming ROW in spring 2017

How it Works: Registry Operations

Joe Waldron
jwaldron@verisign.com

ICANN-57

VERISIGN®

Key Milestones in the History of Registration Data Services

- 1984: Defense Data Network Network Information Center (DDN-NIC) at Stanford Research Institute (SRI) handled all domain registration services
- 1999: Separation of registry and registrar functions
- 2000 - Present: Introduction of new gTLDs

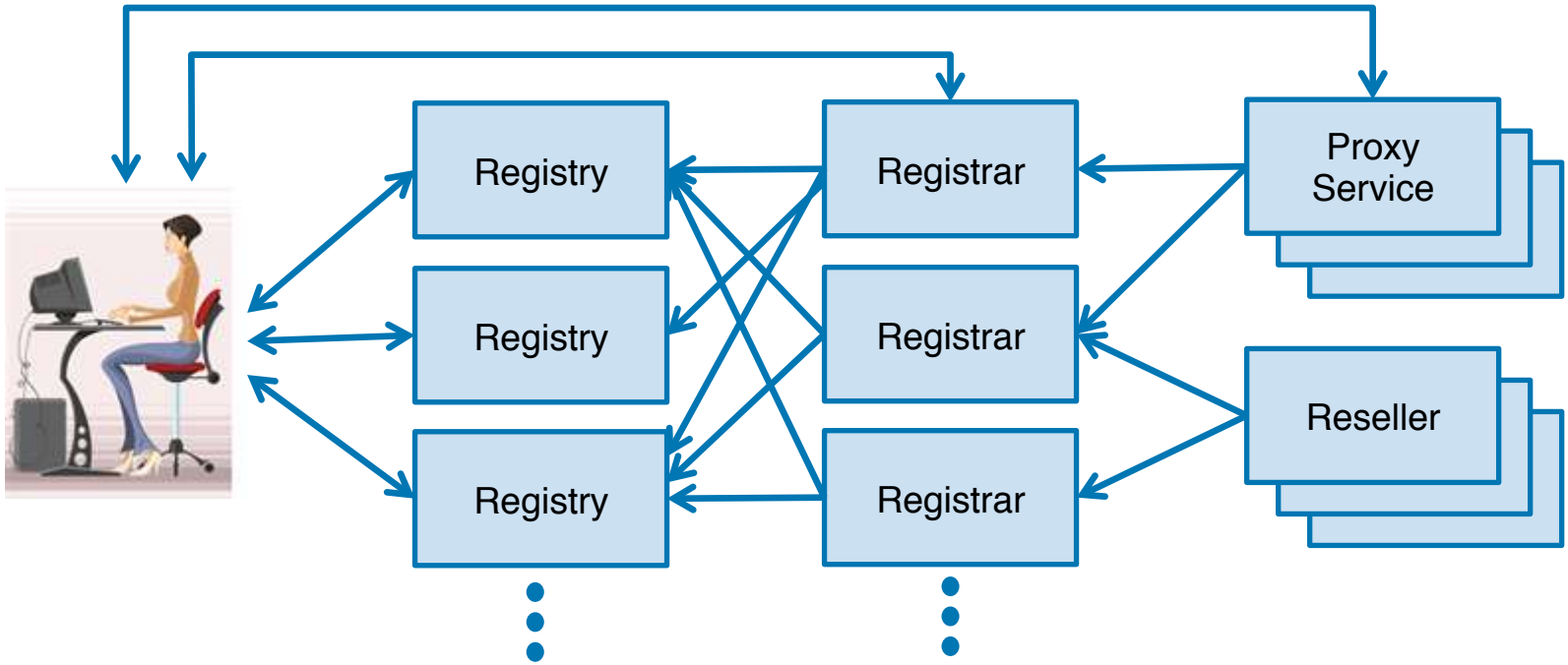
Previous Attempts to replace Whois

- 1995: WHOIS++
- 1997: RWhois
- 2005: IRIS

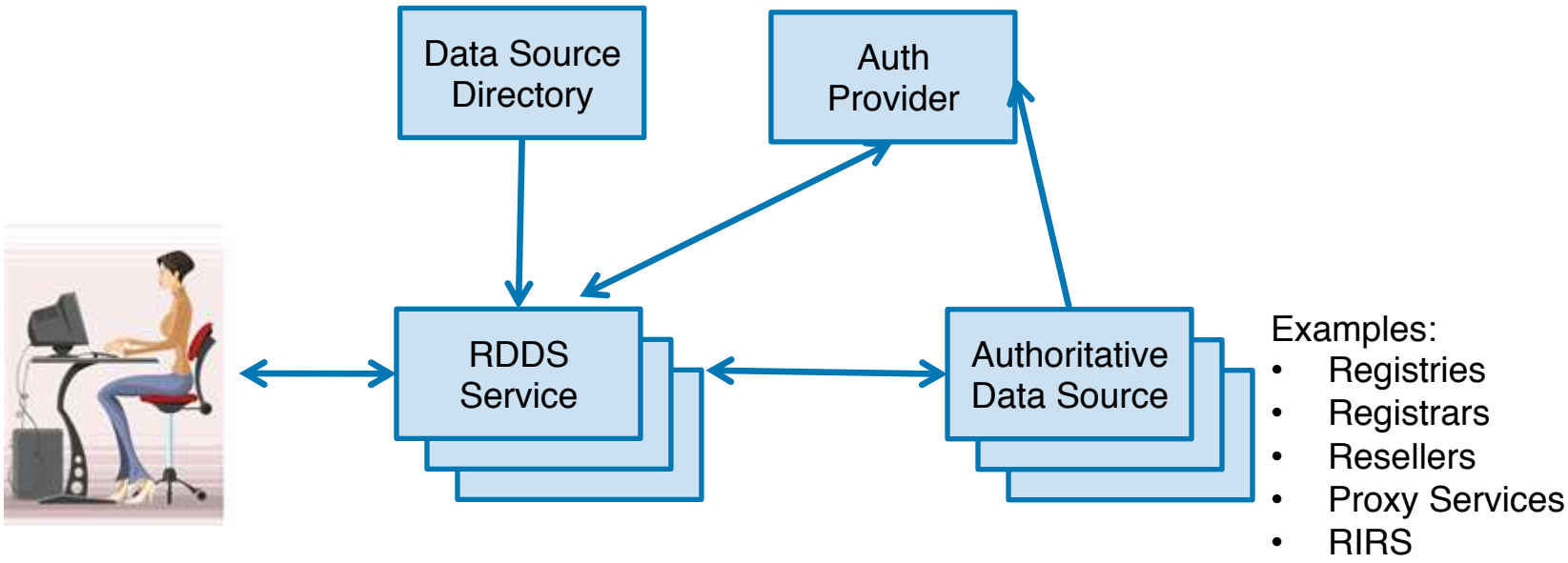
Registration Data Directory Services: What We Need

- Distributed model
- Authoritative data
- Data protection
- Scalability and security
- Standards-based solution

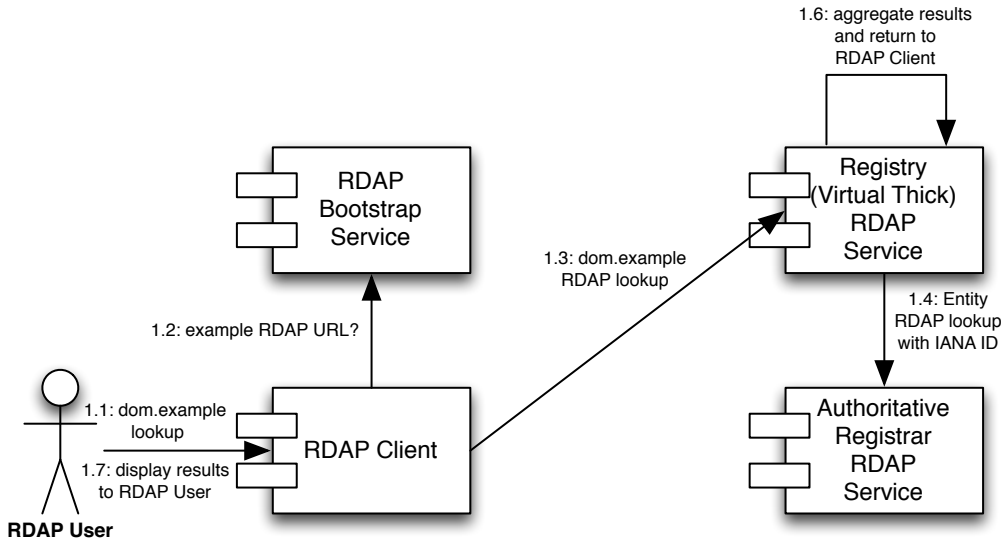
Current Model



Proposed Model

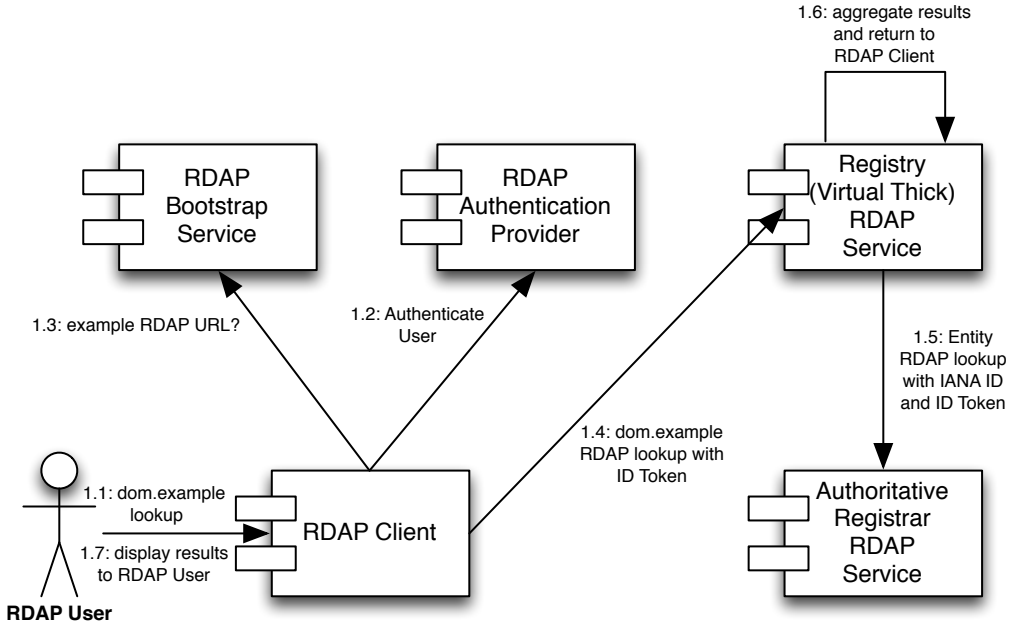


How can RDAP meet these needs?



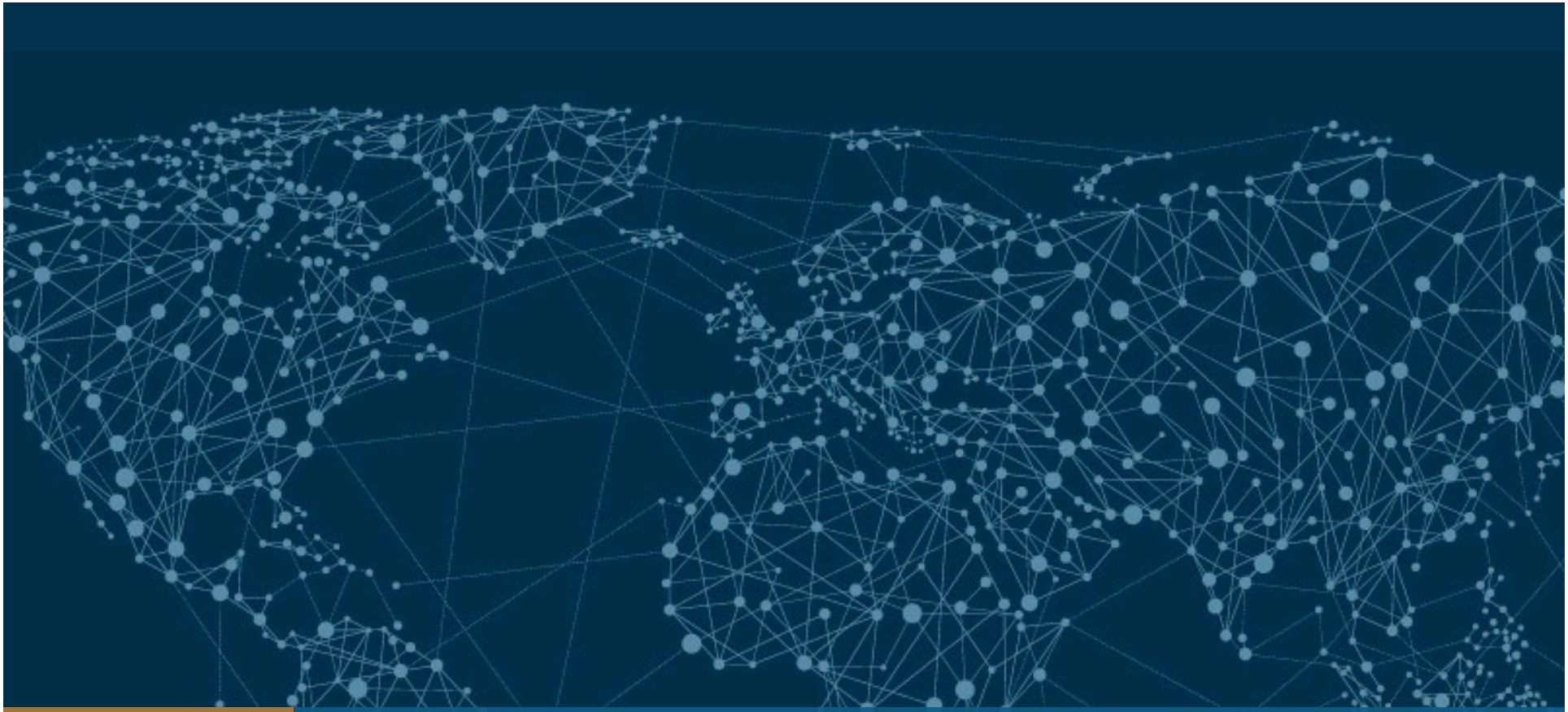
Potential Public (Non-authentication) RDAP Flow

How can RDAP meet these needs?



Potential Authentication and Authorized RDAP Flow

VERISIGN®



How It Works: ROW Topics

3 November 2016

Agenda

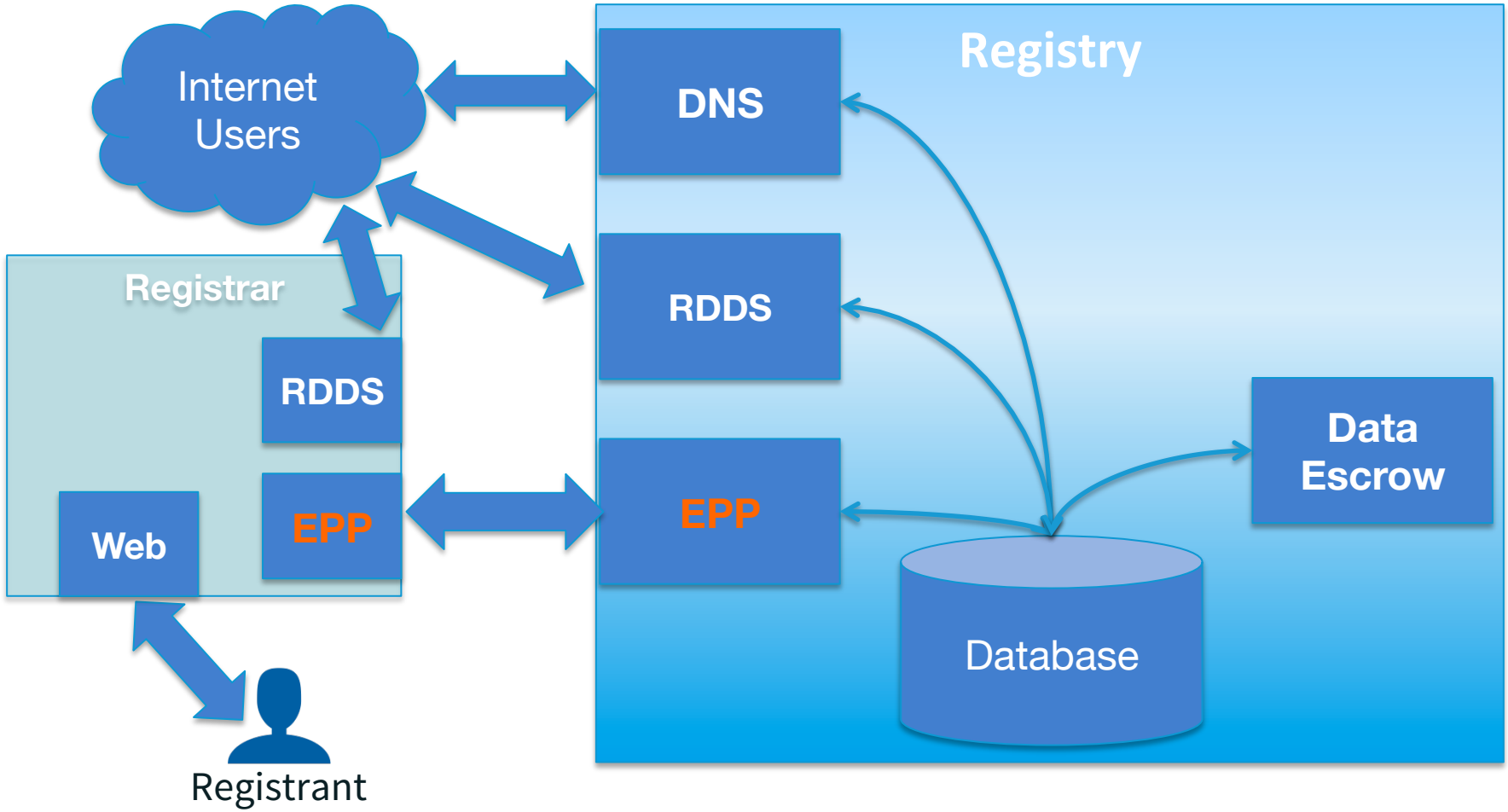
1. Introduction
2. History and Background
3. Extensible Provisioning Protocol
4. Registration Data Access Protocol
5. Q & A


Introduction


History and Background


Extensible Provisioning Protocol

Registry-Registrar Functions



What is Extensible Provisioning Protocol (EPP)?

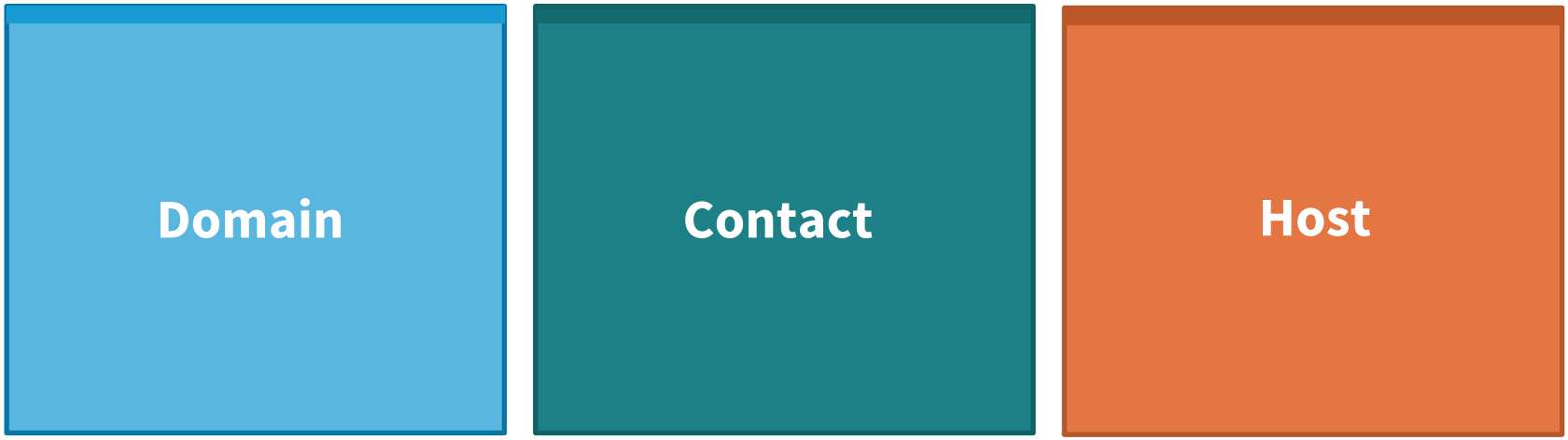
- Designed to manage (create, renew, update, transfer, delete, review) domain names and related objects (e.g. hosts, contacts) in registries.
- Allows registrars to manage domains names with registries.
- Is the standard for communications between domain registries and registrars.

The Protocol

- Uses eXtensible Markup Language (XML), a structured, text-based format used in IT industry.
- Requires use of Transport Layer Security (TLS) protocol in order to provide integrity, confidentiality and mutual, strong client-server authentication.
- March 2004: RFC (3730 - 3734) published.
- May 2007: Updated suite (RFCs 4930 - 4934) published.
- August 2009: Final, current suite (RFCs 5730 - 5734) published.

Type of Objects

EPP supports the following main objects:



EPP Commands

- Session Management Commands
  - Login
  - Logout

- Query Commands
  - Check
  - Info
  - Poll
  - Transfer

- Transform Commands
  - Create
  - Delete
  - Renew
  - Transfer
  - Update

Example

Example <info> command for domain “example.com”:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<epp xmlns="urn:ietf:params:xml:ns:epp-1.0">
  <command>
    <info>
      <domain:info
       xmlns:domain="urn:ietf:params:xml:ns:domain-1.0">
        <domain:name hosts="all">example.com</domain:name>
      </domain:info>
    </info>
    <clTRID>ABC-12345</clTRID>
  </command>
</epp>
```

Extensibility of EPP

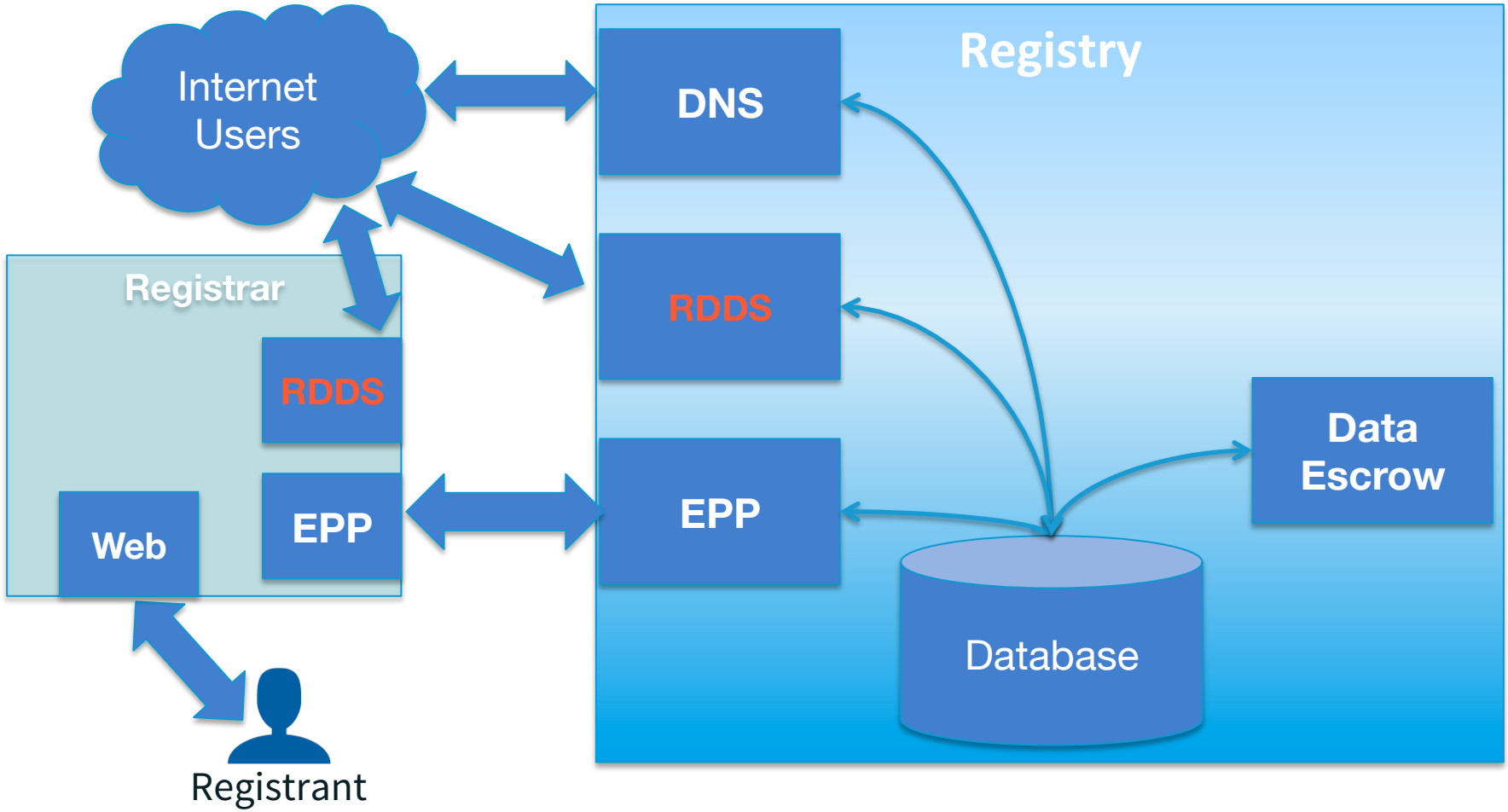
- Extensible protocol, allows Registries to define their own extensions in order to support different business models.
- The REGEXT Working Group in IETF coordinates development of EPP extensions.
- IANA registry of EPP extensions:
  - http://www.iana.org/assignments/epp-extensions/epp-extensions.xhtml

Who Uses EPP?

- All gTLDs
- Several ccTLDs:
  - .ac, .ag, .at, .au, .be, .br, .bz, .ca, .cc, .ch, .cl, .cn, .co, .cr, .cz, .cx, .cz, .dk, .es (over HTTPS), .eu, .fi, .fm, .fr, .gr (over HTTPS), .gs, .hn, .ht, .im, .in, .io, .it (over HTTPS), .ke, .ki, .kz, .la, .lc, .li, .lt, .lu, .lv, .md, .me, .mk, .mn, .ms, .mu, .mx, .na, .nf, .ng, .nl, .no, .nu, .nz, .org, .pe, .pk, .pl (over HTTPS), .ps, .pt, .ru, .ro, .sc, .se, .sh, .si, .su, .tl, .tm, .tv, .tw, .uk, .us, .vc, .ve and .za
- ENUM registries such as those operating the +31, +41, +43, +44 and +48 country codes.
- RIRs:
  - LACNIC


Registration Data Access Protocol

Registry-Registrar Functions



Replacing WHOIS Protocol: Timeline

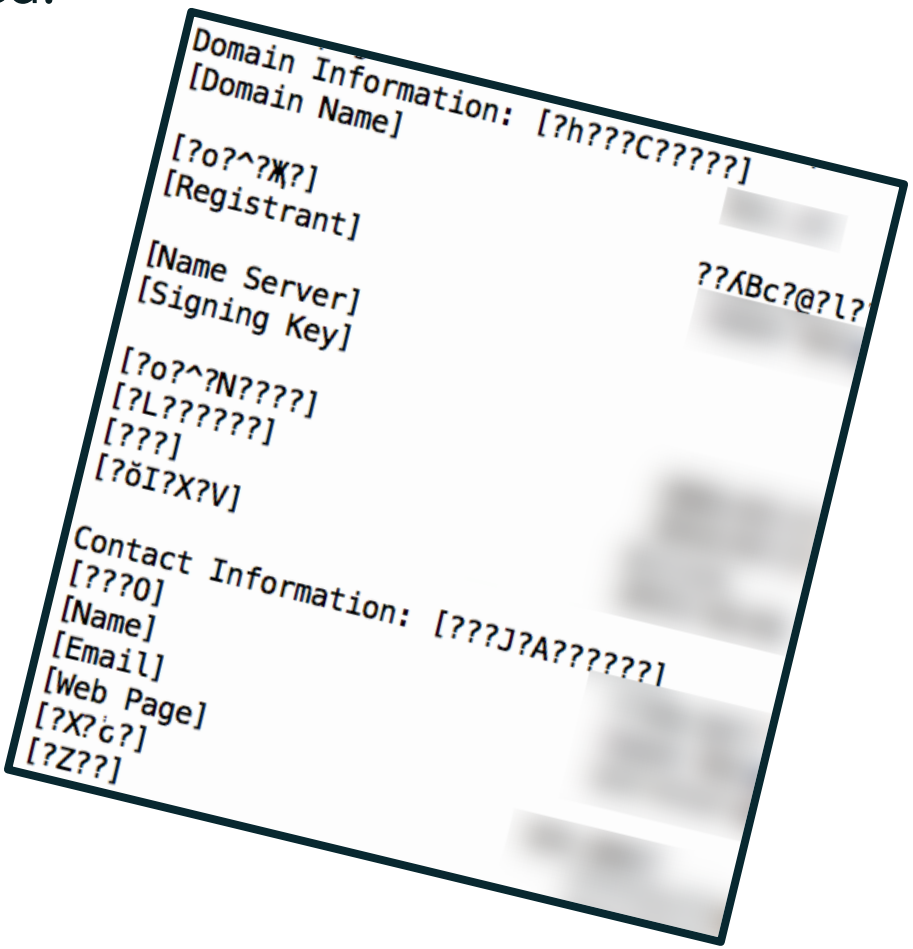
- **19 September 2011:** SSAC's SAC 051: *The ICANN community should evaluate and adopt a replacement domain name registration data access protocol*
- **28 October 2011:** Board resolution adopts SAC 051
- **4 June 2012:** Roadmap to implement SAC 051
- **2012:** RDAP community development within IETF WG begins
- Contractual provisions in: .biz, .cat, .com, .coop, .info, .jobs, .name,
  - .org, .pro, .travel, .xxx, 2012 Registry Agreement (new gTLDs) and 2013 Registrar Accreditation Agreement
- **March 2015:** RDAP IETF RFCs published
- **26 July 2016:** RDAP Profile version 1.0 published

Why Should WHOIS (port-43) Be Replaced?

- Non-standardized format:

Why Should WHOIS (port-43) Be Replaced?

- Not internationalized:



Why Should WHOIS (port-43) Be Replaced?

- Unauthenticated
  - Unable to differentiate between users
- Unable to provide differentiated service
  - The same fields are provided to all users
- Insecure
  - No support for an encrypted response
- No bootstrapping mechanism
  - No standardized way of knowing where to query
- Lack of standardized redirection/reference
  - Different workarounds implemented by TLDs

RDAP Features (1/2)

The Registration Data Access Protocol (RDAP) is a protocol designed to replace the existing WHOIS protocol and provides the following benefits:

- Standardized query, response and error messages
- Secure access to data (i.e., over HTTPS)
- Extensibility (e.g., easy to add output elements)

RDAP Features (2/2)

- Bootstrapping mechanism to easily find the authoritative server for a given query
- Standardized redirection/reference mechanism (e.g., from a registry to a registrar)
- Builds on top of the well-known web protocol, HTTP
- Internationalization support for registration data
- Optionally enables differentiated access (e.g., limited access for anonymous users, full access for authenticated users)

RDAP Examples

- Queries:
  - https://example.com/rdap/domain/blah.example.com
  - https://example.com/rdap/domains?name=example*.com
  - https://example.com/rdap/nameserver/ns1.example.co

- Responses (two pages long for one response):


```
{
  "objectClassName" : "domain",
  "handle" : "XXXX",
  "ldhName" : "xn--fo-5ja.example",
  "unicodeName" : "foo.example",
  "variants" :
  [
    {
      "relation" : [ "registered", "conjoined" ],
      "variantNames" :
      [
        {
          "ldhName" : "xn--fo-cka.example",
          "unicodeName" : "foo.example”
```

Internationalization

- Internationalized domain names supported in both the question and the answer
- Internationalized contact information is supported
- Contact information supports language tags in order to define the language / script of the data
- Replies are JSON formatted, which supports UTF-8
- The transport protocol is HTTP, which supports UTF-8

Bootstrapping

- In the case of new gTLDs, whois.nic.<TLD> is the standard name to find the WHOIS/web-Whois server
- In the case of RDAP, the protocol defines standard bootstrap mechanism that allows a client to find the authoritative server for a particular <TLD>
- RDAP specification explains how to form direct queries and basic search queries
- http://data.iana.org/rdap/dns.json

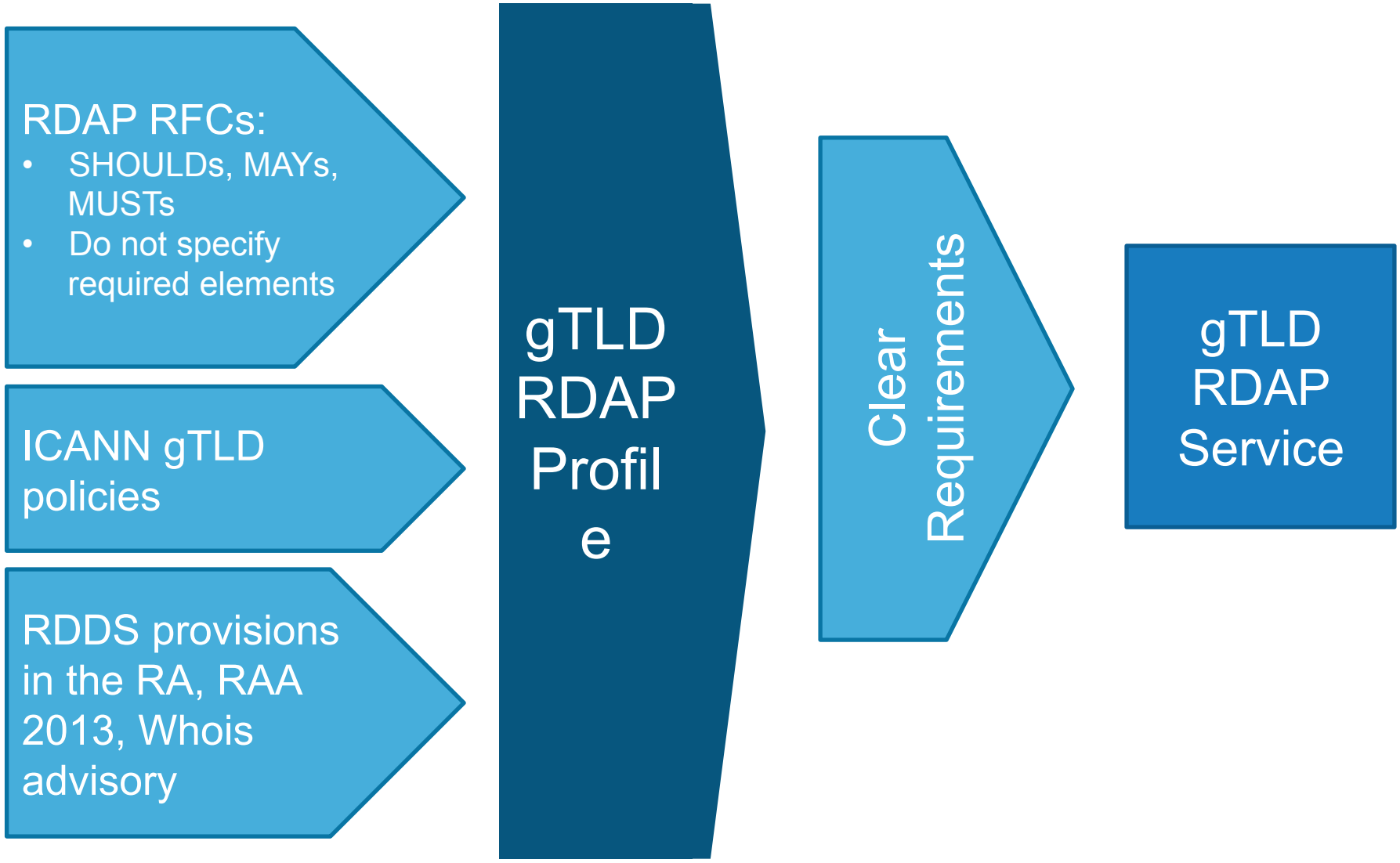
Differentiated Access

- Differentiated access refers to the functionality of showing different subsets of RDDS fields based on who is asking (e.g., limited access for anonymous users, full access for authenticated users)
- As of today, only three gTLDs (.cat, .name, .tel) have a contract provision allowing RDDS with differentiated access
- There is a Policy Development Process (Registration Data Services PDP) in the Generic Names Supporting Organization that has differentiated access in scope

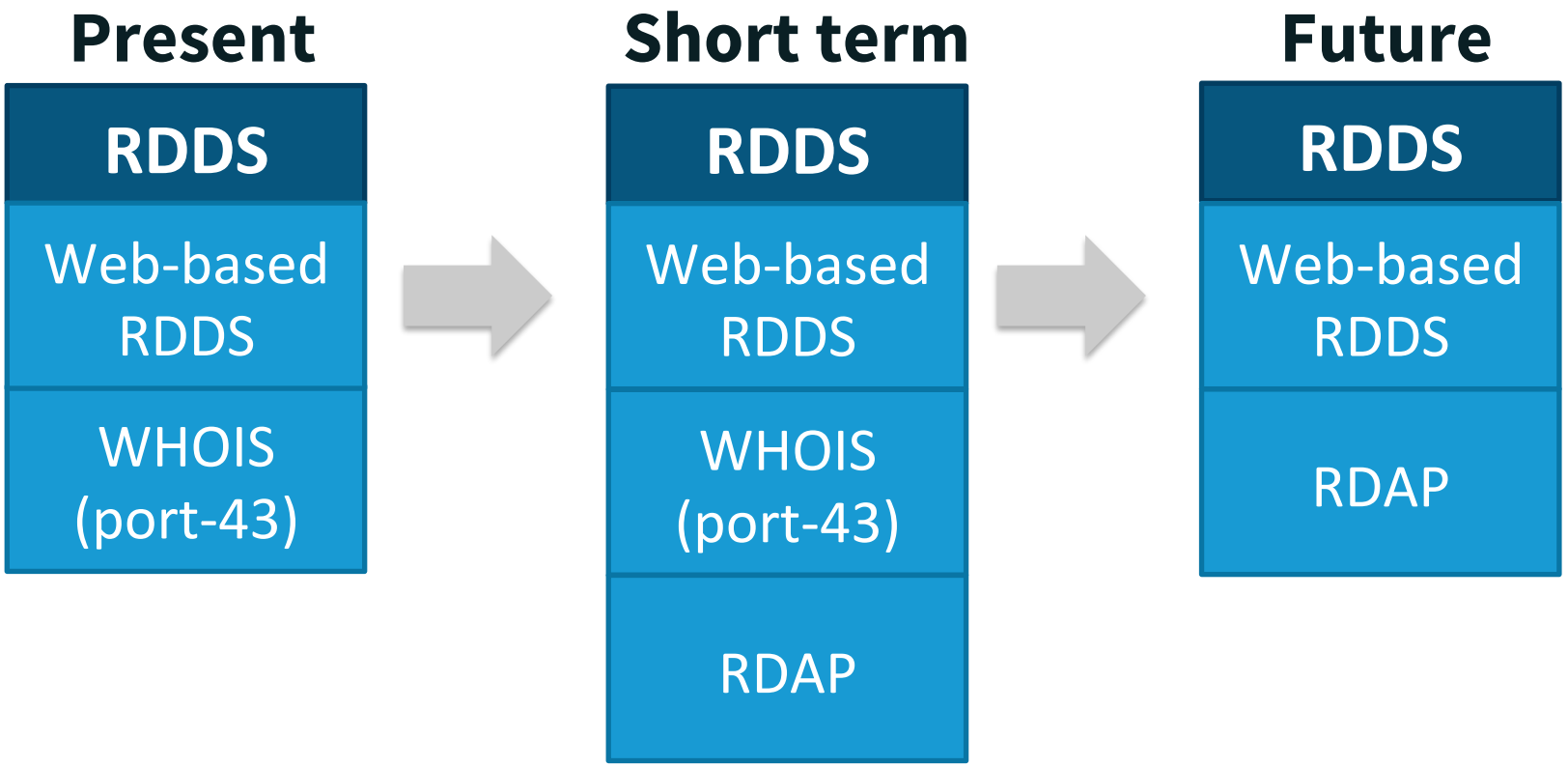
Thin Data in RDAP

- In a thin domain registry the domain contact information is held by the registrar. The registry RDDS only holds a referral to the registrar, the registration, expiry, creation, update date, name servers and domain status.
- A thick domain registry holds all of the contact information needed for the domain names.
- With RDAP, a Registry can point the end-user to the Registrar's RDAP in order to obtain authoritative information maintained by the Registrar.

RDAP in gTLDs



Transition


Present
RDDS
Web-based RDDS
WHOIS (port-43)
Short term
RDDS
Web-based RDDS
WHOIS (port-43)
RDAP
Future
RDDS
Web-based RDDS
RDAP

Engage with ICANN

Thank You and Questions

Reach us at: globalsupport@icann.org
Website: icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations

Q&A

More information about the ROW on:
http://regiops.net

Thank you to ROW series sponsors:

ICANN