RDAP for gTLD Registries and Registrars

11 April 2019

Agenda

- Introduction
- What both registries and registrars need to know
- What registries need to know
- What registrars need to know

Introduction

Issues with WHOIS (Port-43)

- No standardized format
- Lack of Support for Internationalization
- Unable to authenticate and thus provide different outputs depending on the user
- Lookup only; no search support
- Lack of standardized redirection/reference
- No standardized way of knowing what server to query
- Insecure
  - Cannot authenticate the server
  - Cannot encrypt data between server and client

RDAP Features [1/2]

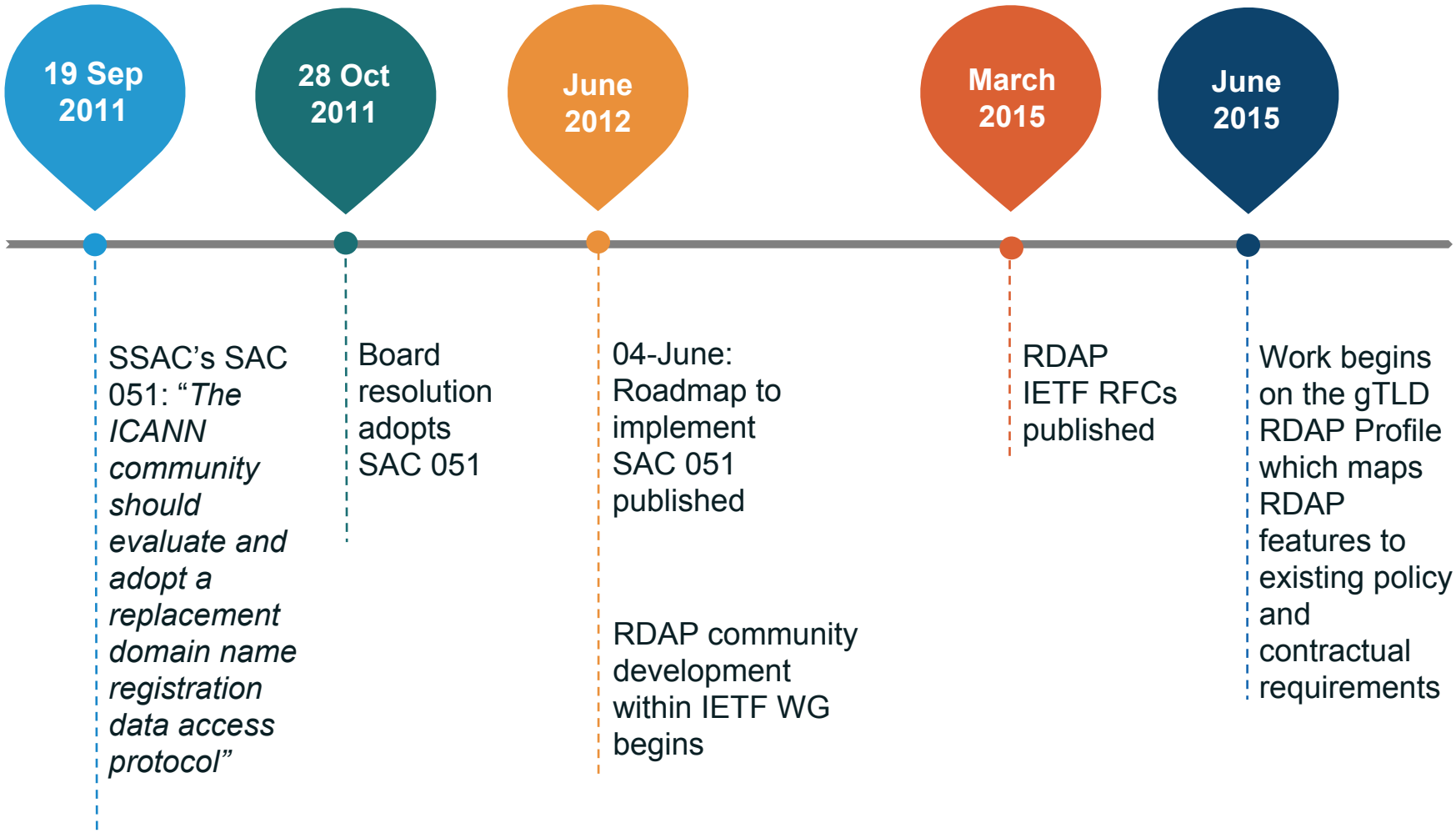
RDAP is a protocol designed in the IETF (RFCs 7480 - 7484) to replace the existing WHOIS protocol and provides the following benefits:

- Standardized query, response and error messages
- Secure access to data
  - Over HTTPS
- Extensibility
  - Easy to add output elements
- Enables differentiated access
  - Limited access for anonymous users
  - Full access for authenticated users

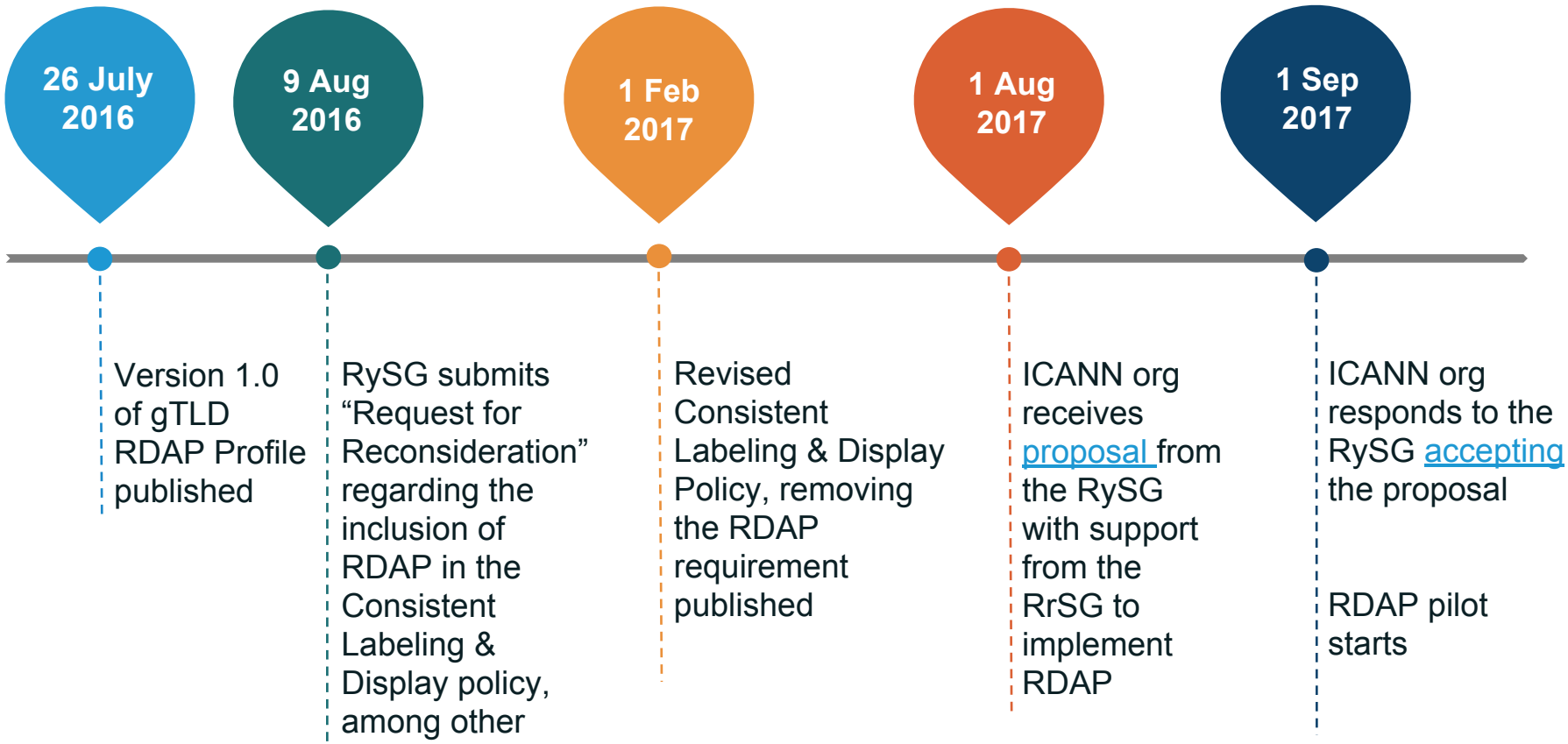
RDAP Features [2/2]

- Bootstrapping mechanism to easily find the authoritative server for a given query
- Standardized redirection/reference mechanism
  - From a registry to a registrar
- Builds on top of HTTP, the well-known web protocol
- Internationalization support for registration data
- Enables searches for objects
  - Domain Names

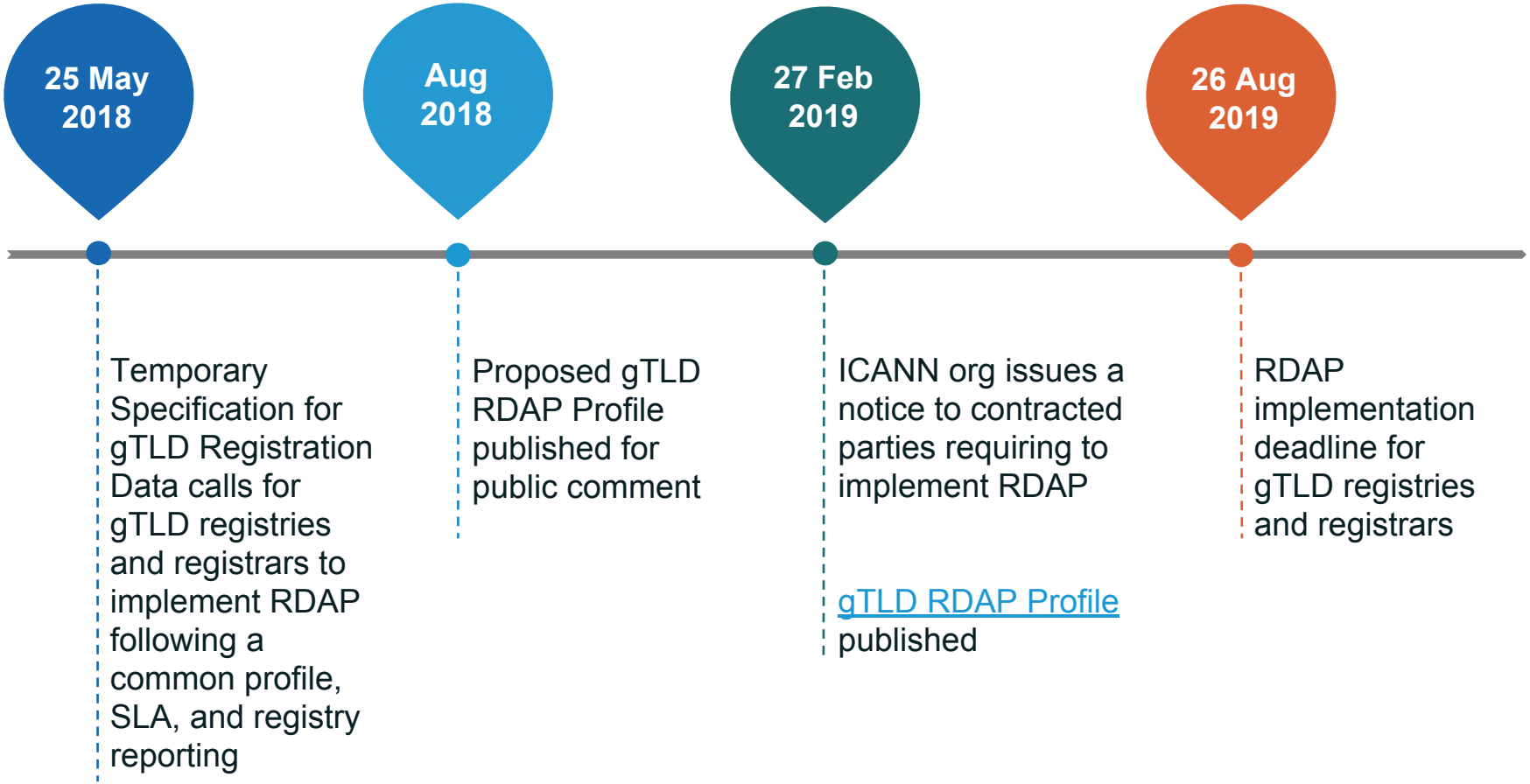
Chronology of RDAP Implementation [1/3]



Chronology of RDAP Implementation [2/3]



Chronology of RDAP Implementation [3/3]

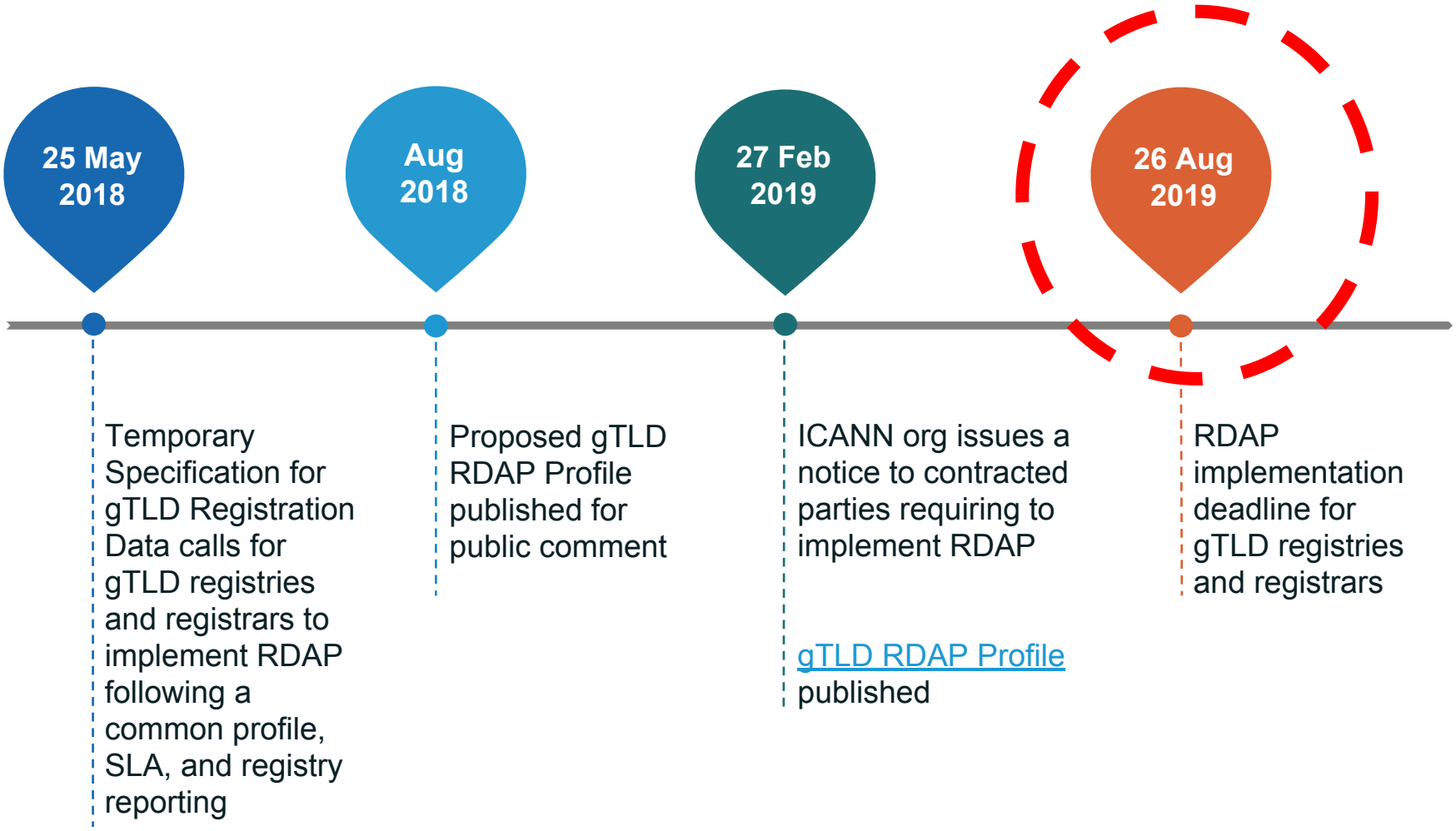


Implementation Status

- Temporary Specification for gTLD Registration Data calls for gTLD registries and registrars to implement RDAP:
  - Following a common gTLD RDAP profile
  - SLA, and
  - Registry reporting requirements
- ICANN org and the contracted parties continue to work on finalizing the SLA, and registry reporting requirements
- 26 August 2019 is set as the deadline for gTLD registries and registrars to implement an RDAP service

What both registries and registrars need to know

Deadline to Implement RDAP



gTLD RDAP Profile

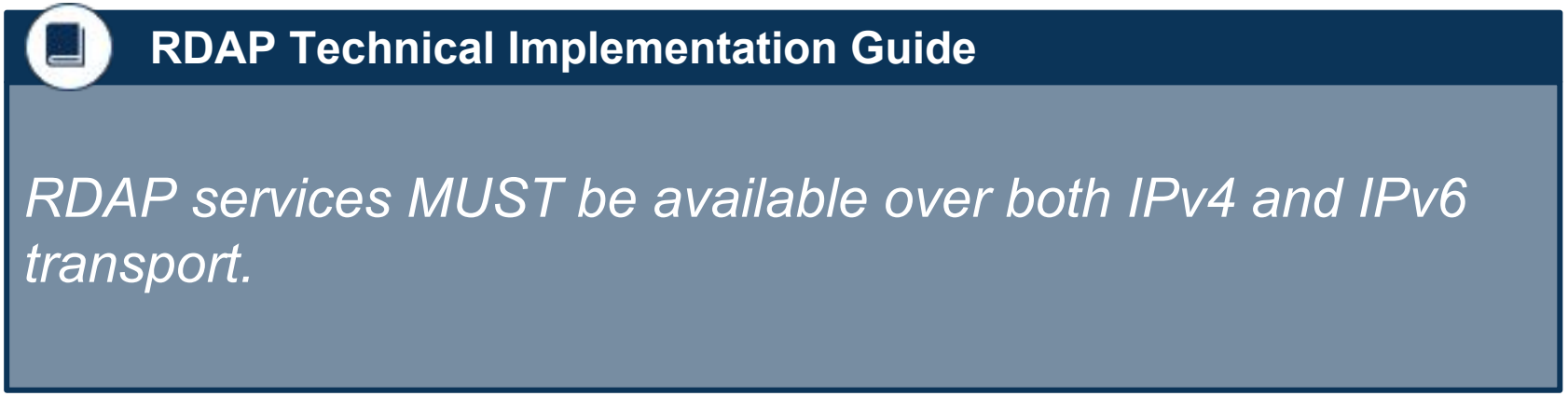
https://www.icann.org/gtld-rdap-profile

- Created jointly with a group of gTLD registries and registrars
- Consists of 2 documents:
  - RDAP Technical Implementation Guide
  - RDAP Response Profile
- ICANN org recommends gTLD registries and registrars to implement their RDAP service based on the RDAP profile published on February 2019

IPv6 and IPv4 Transport

- The Technical Implementation Guide states:

  RDAP services MUST be available over both IPv4 and IPv6 transport.



TLS Server Certificate Anchoring

- HTTPS-only service following RFC 7525 best practices
- It's recommended that the TLS certificate used in the RDAP server is anchored to a well-known CA and/or using DANE

RDAP Technical Implementation Guide

An RDAP client SHOULD be able to successfully validate the TLS certificate used for the RDAP service with a TLSA record from the DNS (RFC 6698 and RFC 7671) published by the RDAP service provider. The certificate(s) for the RDAP service associated by DNS-Based Authentication of Named Entities (DANE) SHOULD satisfy the requirements of section 1.5.

DNSSEC

- Having DNSSEC signatures enables secure DNS resolution of services, therefore is advised that the DNS records used for RDAP are DNSSEC-signed and chained up to the root zone key

RDAP Technical Implementation Guide

The resource records for the RDAP service SHOULD be signed with DNSSEC, and if DNSSEC is in place, the DNSSEC chain of trust from the root trust anchor to the name of the RDAP server MUST be valid.

DNSSEC Fields in Output

- The current WHOIS requirements regarding DNSSEC is to add a field that specifies if the delegation is signed or not (i.e., DNSSEC: signedDelegation / unsigned)

- RDAP allows the Registry to specify the complete set of DNSSEC parameters (e.g., keyTag, digest, etc)

RDAP Response Profile

DNSSEC - The domain object in the RDAP response MUST contain a secureDNS member [RFC7483] including at least a delegationSigned element. Other elements (e.g. dsData) of the secureDNS member MUST be included, if the domain name is signed and the elements are stored in the Registry or Registrar database, as the case may be.

Country Codes Instead of Names in Responses

- The vCard standard defines that an address contains the full country name instead of ISO-3166-1-alpha-2 country code as it has been the norm in WHOIS
- A new parameter is in the process of being registered to support ISO-3166-1-alpha-2 country codes

ISO-3166-1-alpha-2 parameter available?	Country name component of the 'adr' structure
No	MAY be populated with country code
Yes	MUST be empty (and country code parameter MUST be used)

IDN Query Support

- One of the main features of RDAP is the support for internationalization

RDAP Technical Implementation Guide

The RDAP server MUST support Internationalized Domain Name (IDN) RDAP lookup queries using A-label and U-label format [RFC5890] for domain names.

Cross-Origin Resource Sharing

- RDAP supports web clients querying data from different RDAP servers

RDAP Technical Implementation Guide

When responding to RDAP valid requests, an RDAP server MUST include the Access-Control-Allow-Origin response header, as specified by [W3C.REC-cors-20140116]. Unless otherwise specified, a value of "" MUST be used.*

Redaction Requirements

- The redaction requirements from the Temporary Specification for gTLD Registration Data (https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#temp-spec) apply to RDAP
- The Response Profile document describes how redaction is expected to happen in RDAP

What registries need to know

Registry's RDAP Base URL

- Registries should register the RDAP base URL for their respective TLDs with IANA

RDAP Technical Implementation Guide

The base URL of Registry RDAP services MUST be registered in the IANA's Bootstrap Service registry for Domain Name Space (https://www.iana.org/assignments/rdap-dns/rdap-dns.xhtml), as described in RFC 7484 , through the IANA Root Zone Management system. A separate entry is required for each TLD.

- The process is the same as for any other update to the delegation information. It's recommended to use the Root Zone Management System, but other methods are available

- More information can be found at: https://www.iana.org/domains/root/manage

Reference to Sponsoring Registrar's RDAP Service

RDAP Technical Implementation Guide

A registry server RDAP response to a domain query MUST contain a links object as defined in [RFC7483] section 4.2., in the topmost JSON object of the response. The links object MUST contain the elements rel:related and href containing the Registrar's RDAP URL of the queried domain object if the Registrar's RDAP URL has been defined.

- ICANN was asked to setup a (temporary) central repository of gTLD registrar's RDAP base URLs

Where to Find a Registrar's RDAP Base URL

- The central repository will facilitate registries to find the RDAP base URL of a registrar's RDAP server

- The registrar RDAP bootstrap file is going to be available in May 2019 at:

  https://www.iana.org/assignments/registrar-ids

What registrars need to know

RDAP Base URL

- A central repository will facilitate registries to find the RDAP base URL of a registrar's RDAP server
- The registrar RDAP base URL will be captured in a self-service field in RADAR
- Once the functionality is available (expected in April 2019) registrars will be notified via email

Contact Handles in Thin Registries

- The gTLD RDAP Profile defines that entity handles should contain the Repository Object Identifier (ROID) of the contact object.
- Thin registrations do not have contact objects in the Registry. In this case, the Registrar will use a unique identifier within the Registrar as the entity handle.

RDAP Response Profile

The entity handle in the RDAP response MUST contain the Repository Object Identifier (ROID of the contact object, <contact:roid>, as defined in RFC 5733) for the Contact object. For example, a Registrar could obtain the ROID from the Registry via EPP and cache the information locally. The RAA 2013 defines that this information MUST be shown if available from the Registry. If this information is not available from the Registry (e.g., a "thin" Registry), the handle MUST contain the unique identifier within the Registrar.

HTTP 404 Responding to Names Not Sponsored

- In order to avoid potential corner cases (e.g. query loops), Registrars must respond with an HTTP 404 status code for domain name queries for which the Registrar is not the sponsor.

RDAP Response Profile

A Registrar MUST return an HTTP 404 response to a domain name request when the Registrar is not the Sponsoring Registrar for the domain name.

Resources

Server and Client Implementations Available

- RDAP server open-source projects:
  - DNSBelgium
  - Red Dog
- RDAP client projects:
  - ICANN's prototype RDAP web client
  - CentralNIC's code and web client
  - DNSBelgium
  - NicInfo
  - OpenRDAP

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: globalsupport@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg