RDAP Implementation

Agenda

1. History of Replacing WHOIS protocol
2. RDAP Profile Details
3. Open issues
4. Conclusion and Next Steps

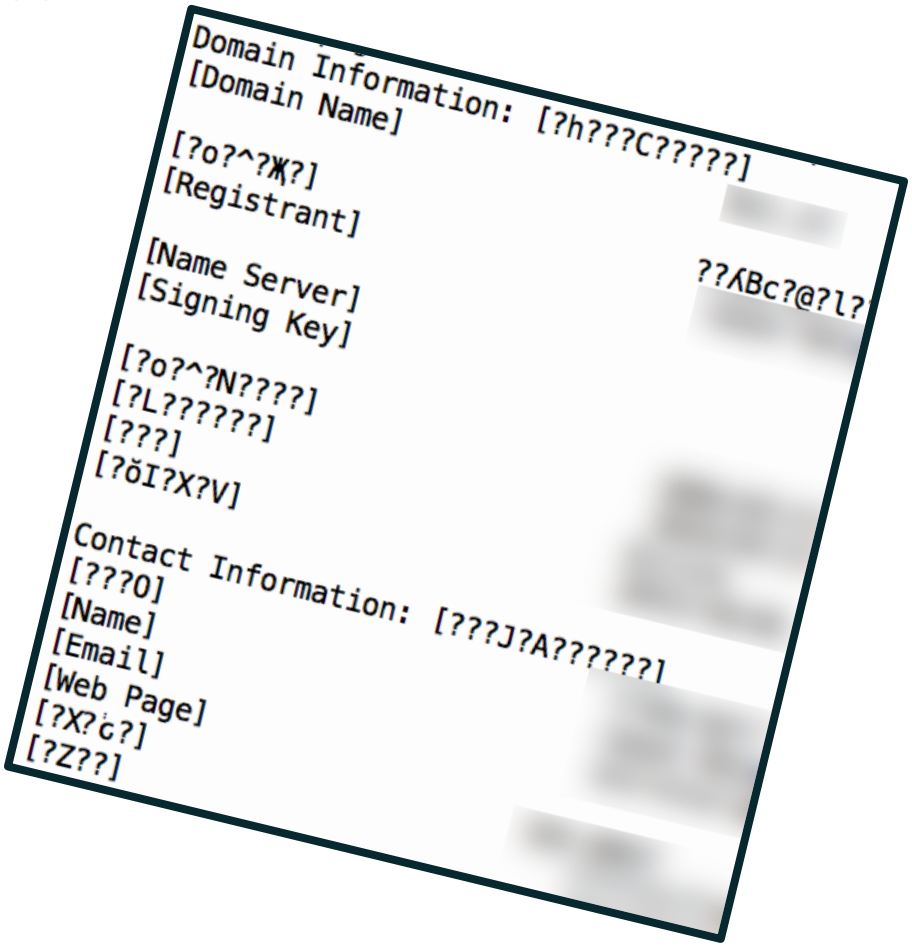
History of Replacing the WHOIS Protocol

Why WHOIS (port-43) should be replaced?

- Non standardized format

Why WHOIS (port-43) should be replaced?

- Not internationalized



Why WHOIS (port-43) should 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

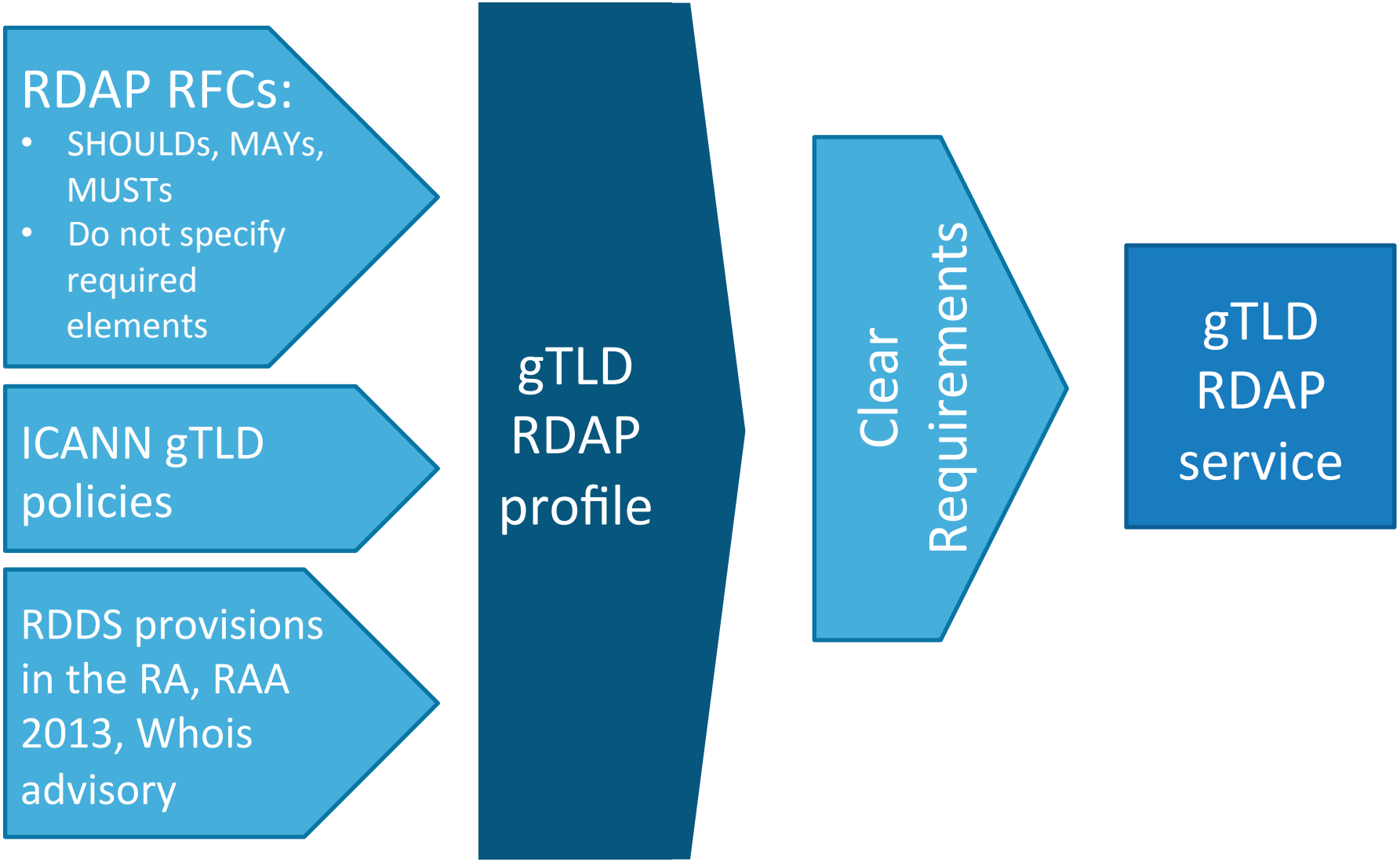
History on Replacing the WHOIS Protocol

- SSAC's SAC 051 Advisory (19 Sep 2011):
  - *The ICANN community should evaluate and adopt a replacement domain name registration data access protocol*
- Board resolution adopting SAC 051 (28 October 2011)
- Roadmap to implement SAC 051 (4 June 2012)
- Registration Data Access Protocol (RDAP) community development within IETF working group started in 2012
- Contractual provisions in: .biz, .com, .info, .name, .org, 2012 Registry Agreement (new gTLDs), and 2013 Registrar Accreditation Agreement

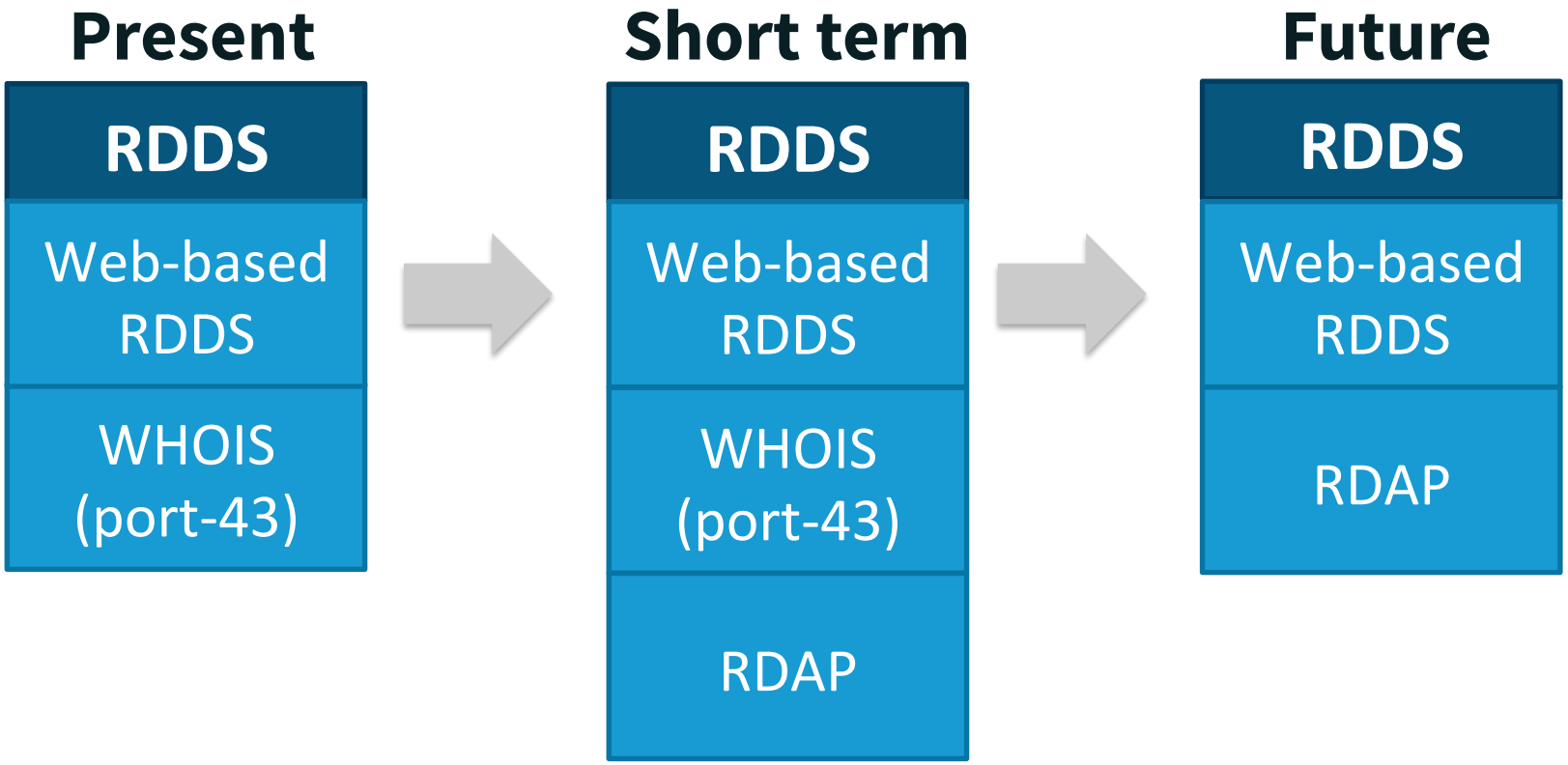
History on Replacing the WHOIS Protocol

- RDAP Request for Comments (RFCs) published in March 2015
- First draft of the gTLD RDAP profile shared for discussion with the community in September 2015.

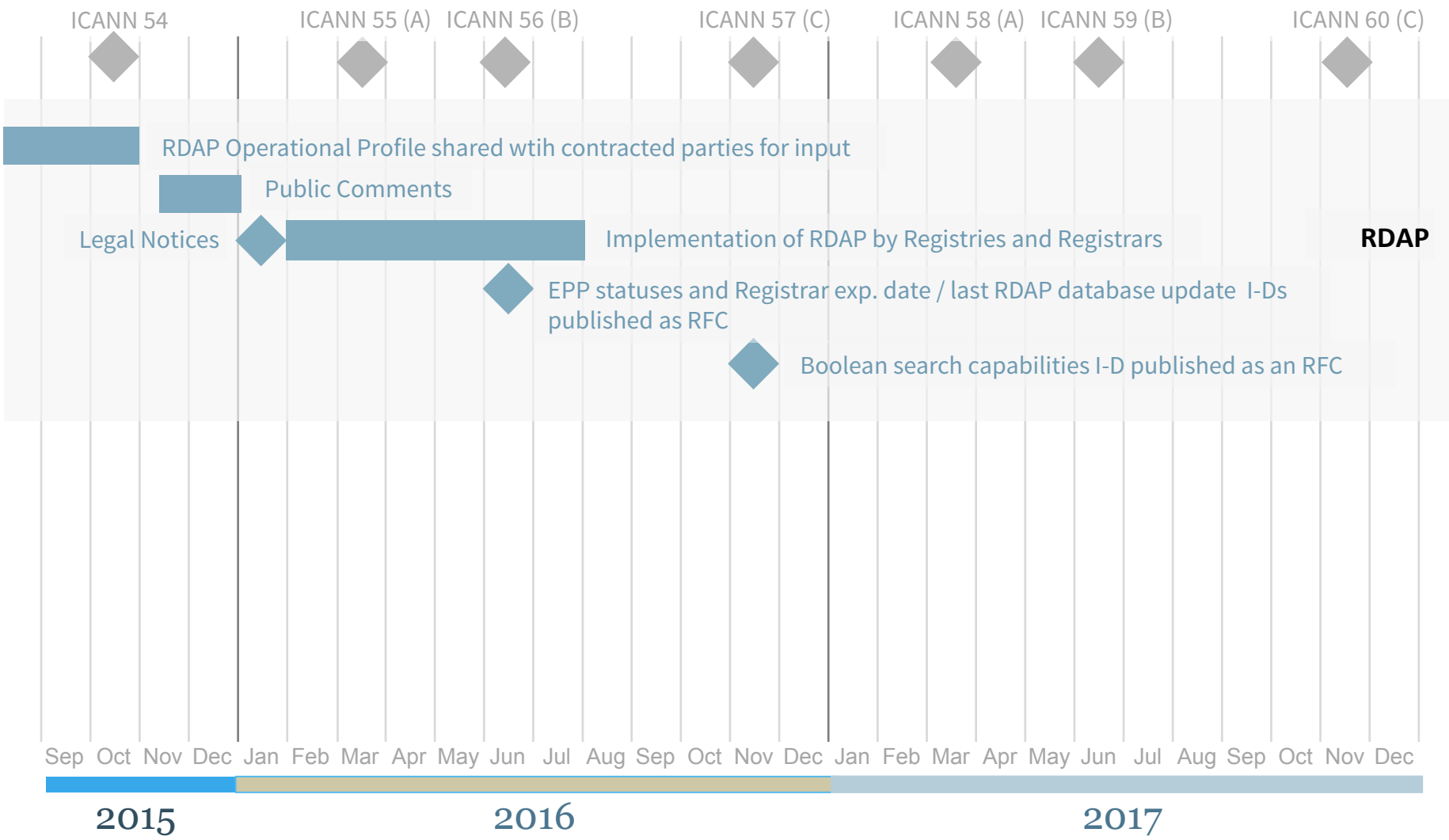
Why do we need an RDAP profile?



How the transition looks like



Implementation Timeline



Transition open questions

- How long after RDAP deployment before turning off (port-43) WHOIS?

- Should the requirement to offer web-based (HTML) RDDS remain after the transition to RDAP?
  - R. Yes

RDAP Profile - details

Transport requirements

- 1.3.2. The RDAP service must be available over HTTPS only. The TLS certificate used for the RDAP service must be issued by a Certificate Authority (CA) trusted by major browsers and mobile OS such as the ones listed in the Mozilla Included CA Certificate List (https://wiki.mozilla.org/CA:IncludedCAs). The CA, the certificate and its usage MUST follow the CAB Forum Baseline Requirements (https://cabforum.org/baseline-requirements-documents). The RDAP service MUST use the best practices for secure use of TLS as described in RFC7525 or its successors.

Transport requirements

- Comments: 1.3.2. I agree that RDAP providers have to offer https, but I don’t see why they can't also offer plain http if they want.

- Reasoning: following the IAB statement on Internet Confidentiality, https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

Transport requirements

- Comments: 1.3.2. The above seem to be guidelines missing specifics. Is the certificate used by the RDAP service domain-validated or organization-validated? What ciphers should be supported?
- Reasoning:
- Discuss how to define best practice requirements regarding x509 certificates.
- RFC7525 should provide enough guidance about the ciphers.

Transport requirements

- 1.3.6. RDAP must be supported over IPv4 and IPv6. The resource records related to the RDAP service MUST be signed with DNSSEC, and the DNSSEC chain of trust from the root trust anchor to the name of the RDAP server MUST be valid at all times. The DNSSEC security algorithm used for zone signing at each level MUST be listed as standardized for Zone Signing in the IANA's Domain Name System Security (DNSSEC) Algorithm Numbers registry.

- 2.8.3. A IANA's Bootstrap registry for Domain Name Space entry MUST be populated after the RDAP service is available over both IPv4 and IPv6 (A and AAAA records are present in the DNS for the domain name used to provide the RDAP service).

Transport requirements

- Comments: 2.8.3 - I don't understand it. Is it supposed to mean don't publish a bootstrap until the server is available on both ipv4 and ipv6? If so that seems redundant with 1.3.6.

- 2.8.3 is about populating the IANA's Bootstrap registry, and 1.3.6 is the requirement for providing service over IPv4 and IPv6.

IDNs

- 1.4.1. Internationalized Domain Name (IDN) RDAP lookup queries of domain names using A-label or U-label format [RFC5890] MUST be supported.

IDNs

- Comments: 1.4.1 it says servers must support A-labels or U-labels, but I expect you mean they have to accept both. Do they have to accept names with a mixture of the two?

- RFC 7482: IDNs SHOULD NOT be represented as a mixture of A-labels and U-labels; that is, internationalized labels in an IDN SHOULD be either all A-labels or all U-labels.
- Should the profile make the SHOULD NOT a MUST NOT?

Response format

- 1.4.4. Leading and trailing space or spaces MUST NOT appear in the RDAP response.
- 1.4.5. RDAP responses MUST NOT contain carriage return and line feed characters. As described in RFC7483 section 4.3, large fields such as notices [RFC7483] and remarks [RFC7483] may be divided in separate strings to improve readability.

Response format

- Comments: 1.4.4 and 1.4.5 - this currently says that all of the JSON has to be returned as one giant line with no line breaks, which doesn't match the examples in RFC 7483 and doesn't make much sense. It it supposed to say there's no leading or trailing spaces or line breaks inside of JSON string values?

- The examples in RFC 7483 are not defining how the actual response should be presented. The JSON response is to be consumed by a computer, and the requirement is to avoid implementers trying to beautify the response.

Caching the IANA’s Bootstrap

- 2.8.2. When the RDAP service base URL needs to be changed, the previous URL and the new one MUST remain in operation until: 1) the IANA's Bootstrap Service registry for Domain Name Space is updated, and 2) the date and time in the Expires HTTP header of a HTTP/GET request performed on the IANA's Bootstrap registry for Domain Name Space (after the new URL has been published) has elapsed.

Caching the IANA's Bootstrap

- Comments: 2.8.2 - says that if a service moves, the old service only needs to stay up until the IANA bootstrap http expiration. That's a week, which seems too short. Once the set of TLDs stabilizes, I expect people will refresh their bootstrap on the order of once a month.

- RFC7484: Clients SHOULD cache the registry, but use underlying protocol signaling, such as the HTTP Expires header field [RFC7234], to identify when it is time to refresh the cached registry.

Registrar’s response

- 3.1.2. Registrar MUST return a 404 response when the Registrar is not the Sponsoring Registrar for the domain name.

Registrar's response

- Comments: 3.1.2 - if you query a registrar for a name, it belongs to someone else, and the registrar happens to know whose it is (an affiliate with a separate RDAP server, perhaps) what's the harm in allowing a 301 to redirect there?

- Reasoning: Allowing the Registrar to redirect could create complex scenarios, for example, response loops.

RDAP Extensions

- 1.3.4. RDAP extensions, if used, MUST be registered in the IANA's RDAP Extensions registry (https://www.iana.org/assignments/rdap-extensions/rdap-extensions.xhtml), as defined in RFC7480. Deployment of RDAP extensions in gTLD Registries operated under agreement with ICANN, are subject to approval by ICANN via the RSEP process.

RDAP Extensions

- Comments: 1.3.4 The above is contrary to the implication from Sec 2.1 of RFC 7483 that "Clients of these JSON responses SHOULD ignore unrecognized JSON members in responses" - this definitely indicates that unregistered or new RDAP extensions may be used without being formally registered as an RDAP extension. We believe it appropriate to change the "MUST" in this section to "SHOULD". One benefit of defining the RDAP protocol is extensibility, and this profile shouldn't be unnecessarily restrictive.

- Reasoning: Interoperability should benefit from the extensions being published in a central registry. The Registry Agreement requires Registries to request ICANN approval for adding fields.

Case preservation

- 1.4.3. The case (i.e. uppercase and lowercase) of the data returned in RDAP responses MUST be preserved.

Case preservation

- Comments: 1.4.3 It is unclear where the original input of the data returned in RDAP response was derived from - are we referring to the EPP data sent by registrars during registration or is the reference specifically for the capitalization mode used in the RDAP request. Why is this a requirement?

- Reasoning: EPP data sent by Registrars during registration. Data should not be automatically lower or upper cased.

Last Update Time

- 1.4.12. RDAP responses MUST contain the last update date and time of the database used to generate the RDAP responses (RDAP database in this document) when an RFC defining this capability has been published. The RDAP database MUST include the registration data in the SRS database.

Last Update Time

- Comments: 1.4.12 We suggest that this be specified with a new field such as "icann_db_timestamp" encoded in the top-level object instead of defining a new event.

- To be discussed.

A-label and U-label

- 1.5.2. The top-level domain object in the RDAP response MUST contain the U-label format of the domain in the unicodeName member [RFC7483], only if the domain name is an IDN.

A-label and U-label

- Comments: 1.5.2 For an IDN domain name, specifying 2 different encodings in the same response seems redundant and leads to wasted bandwidth. Why is the a-label not sufficient?

- Reasoning: For user experience. For example, the client may not know the IDNA version.

Entities

- 1.5.8. The domain object in the RDAP response MUST contain entities with the following roles, exactly one entity per role MUST be present in the response, each of them with a handle (ROID of the contact object, <contact:roid>, as defined in RFC5733) and valid members fn, adr, tel, email (as specified in RFC6350, the vCard Format Specification and its corresponding JSON mapping RFC7095):
  - registrant
  - administrative
  - technical

Entities

- Comments: 1.5.8 This seems to suggest that a prerequisite for implementing RDAP is that the top-level domain (TLD) contain "thick" registry data. That would seem to preclude the deployment of .COM and .NET RDAP services till the registries are fully converted into "thick" registries.

- To be clarified in the next version.

Registrar Registration Expiration Date

- 1.5.14. The domain object in the RDAP response MUST contain the following events:
  - An event with the expiration date of the Registrar, when a RFC defining this capability has been published.

Registrar Registration Expiration Date

- Comments: 1.5.14 Is this meant to apply to registries? Domains at the registry typically auto-renew so they usually do not expire. If it does not apply to registries, this requirement should be moved to Section 3. If it does apply, this implies that a change in the EPP specification is required before the registry can derive this information for the domain..

- The provision applies to the Registry. The thick Whois policy requires the Registries providing the same fields as the Registries, therefore the Registry must get this information from the Registrar.

Allocated Variants

- 1.5.17. If allocated variant domain names exist for the queried domain name or if the domain name is an allocated variant domain name, the domain object in the RDAP response MUST contain a variants member [RFC7483]. The variants relation member MUST contain valid variant relation types as defined in the IANA's RDAP JSON Values registry. If the queried domain name is an allocated variant name, the original name MUST be included in the variants member.

Allocated Variants

- Comments: 1.5.17 The first sentence of this item is unclear. Is the intent that a queried (and allocated) domain having possible variants provide *allocated* variants in the reply? Is the intent that queried names that are variants of an allocated domains produce a domain response with the allocated name as the domain object? The expected behavior should be clarified through examples.

- Only variants that have been allocated. Text will be clarified.

AWIP policy

- 1.5.18. A domain name RDAP response MUST contain a remarks member with a title “EPP Status Codes”, a description containing the string “For more information on domain status codes, please visit https://icann.org/epp” and a links member with the https://icann.org/epp URL.

AWIP policy

- Comments: 1.5.18 Should the status definitions be defined on a top-level object instead of using a "remarks" member? This could be handled much like the suggestion for 1.4.12, with an "icann_" prefix.

- To be discussed.

secureDNS member

- 1.5.19. The domain object in the RDAP response MUST contain a secureDNS member [RFC7483] including at least a delegationSigned element. Other elements (e.g. dsData, maxSigLife) of the secureDNS member MUST be included, if the domain name is signed and the elements are known by the server.

secureDNS member

- Comments: 1.5.19 The above is ambiguous - what exactly is meant by "known to the server"? This phrasing should be changed to "stored by the registry or registrar".

- Text will be clarified.

Searchable Whois

- 2.1. Registries offering searchable Whois service (e.g., per exhibit A of their RA) MUST support RDAP search requests for domains and entities. Entities MUST be searchable by name search pattern as defined in RFC7482 section 3.2.3 in order to allow for searches by contact name or address. Boolean search capabilities (AND, OR) MUST be supported, when a RFC defining this capability has been published.

Searchable Whois

- Comments: 2.1 We believe the purpose of this profile is to define expected behaviors of a complaint RDAP implementation for registries and registrars. It should not mandate compliance with some future, yet-to-be defined RFC and, therefore, the reference to boolean search should be removed.

- To be discussed.

Multiple host objects

- 2.3. If a Registry supports multiple host objects with the same name, the Registry MUST support the capability to respond with a set of host objects in response to a name server lookup, when an RFC defining this capability has been published.

Multiple host objects

- Comments: As with 2.1, the purpose of the profile is to define expectations of conforming registries and registrars, not mandate compliance with undefined requirements.

- To be discussed.

rel:related

- 2.4. The RDAP domain lookup response MUST contain a links object as defined in RFC7483 section 4.2. The links object MUST contain the elements rel:related and href pointing to the Registrar's RDAP URL of the queried domain object.

rel:related

- Comments: 2.4 This requirement is unclear. A domain lookup response will contain a domain object, potentially having links to other objects, including a link back to the domain object itself. The "rel" element is optional in the RFC for good reason; if it's to be required, then the value should be either "self" or "related" depending on whether the link is back to the queried domain object, or to a related object. Regardless, the mandate for such an element is unnecessary and therefore questionable.

- Reasoning: The idea of this requirement is to support an analogous functionality to the the “Whois server” field in the Whois response. To be discussed.

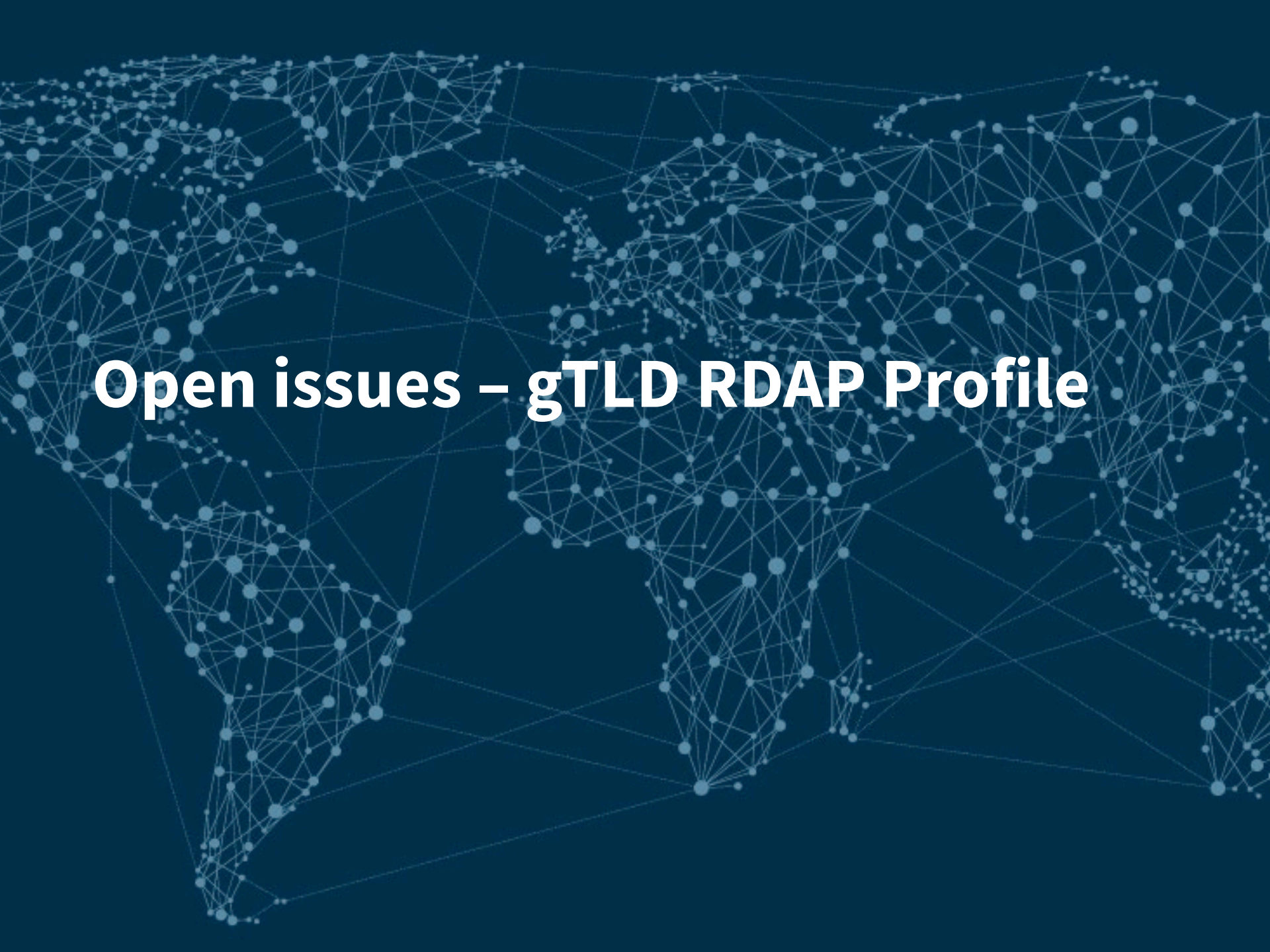
Registrar IANA ID

- 2.9. Entity RDAP queries (registrar queries):
  - 2.9.1. The returned RDAP response MUST be an entity with registrar role, with a handle (IANA Registrar ID) and valid elements fn, adr, tel, email.

Registrar IANA ID

- Comments: 2.9.1 The above implies that Entities are only registrars which conflicts with the RFC definition of Entities as Contacts AND Registrars. It is also not stated that a Registry may only provide information on Registrars that are contracted to resell domains of a specific TLD - this list is not necessarily exhaustive or representative of a list of all registrars - that information is stored with ICANN and IANA.

- Reasoning: Text will be clarified.



Open issues – gTLD RDAP Profile

Open issues – gTLD RDAP Profile

1. Status Codes for Domains
2. Last update of RDAP database
3. Boolean Search Capabilities
4. Multiple host objects for the same name server name
5. Registrar registration expiration date

Status Codes for Domains

- The current Whois provisions require the use the EPP domain statuses codes in responses.
- Not all the EPP domain statuses codes are defined as RDAP values in the base RFCs.

Possible solution:

- There is an Internet Draft that addresses this issue.

Last update of RDAP database

- The base RDAP specification does not define an element to map the "Last update of WHOIS database" RDDS field.

Possible solution:

- There is an Internet Draft that addresses this issue.

Boolean Search Capabilities

- Searchable Whois requires a set of logical operators for search criteria (AND, OR, NOT operators) that are not supported in the base RDAP specifications.

Possible solution:

- The RDAP specifications would need to be extended to support this requirement.

Multiple host objects – one name

- The base RDAP specification does not support the existence of multiple host objects for the same name server name.

Possible solution:

- Use a link member with a rel:collection.

Registrar registration expiration date

- RDAP does not include an event to specify the registrar registration expiration date as described in the RAA 2013.

Possible solution:

- There is an Internet Draft that addresses this issue.

Conclusion and Next Steps

Conclusion and Next Steps

- Reach agreement on to proceed with the 5 open issues around underspecified topics in RFCs.
- Close the open items raised so far in the mailing lists.
- Open public comment period on the updated profile by the second half of November.

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