Next-Generation gTLD Registration Directory Service (RDS) to replace WHOIS PDP WG

Handout for Working Group Call
Tuesday 9 January 2018 at 17:00 UTC

ICANN

Proposed Agenda

1. Roll Call/SOI Updates
2. Complete deliberation on data required for Domain Name Management
   a. Review poll results from 20 December call Question 2
   b. Finalize agreement on data required for Domain Name Management
3. Complete deliberation on Domain Name Certification
   a. Review poll results from 20 December call Question 3
   b. Finalize agreement on Domain Name Certification as a legitimate purpose
4. Start deliberation on “Criminal Activity/ DNS Abuse – Investigation”
5. Confirm action items and proposed decision points
6. Confirm next WG meeting: Tuesday, 16 January at 17:00 UTC

Meeting Materials:
https://community.icann.org/x/QgByB

2) Complete deliberation on data required for Domain Name Management

- See Question 2: https://community.icann.org/download/attachments/74580021/AnnotatedResults-Poll-from-20December.pdf

- 92% supported the possible WG agreement:
  - *The following registration data is needed for the purpose of Domain Name Management: Domain Name, Registrant Name, Registrant Organization, Registrant Email, Registrar Name, Creation Date, Updated Date, Expiration Date, Nameservers, Domain Status, and Administrative Contact.*

- 4 responses gave rationale for adding data not included due to lack of support in calls: Registrant Postal Address & Phone, Technical Contact

- Resolution: Accept rough consensus on above WG agreement and deliberate on additional data after all purposes are discussed

3) Complete deliberation on Domain Name Certification as a purpose

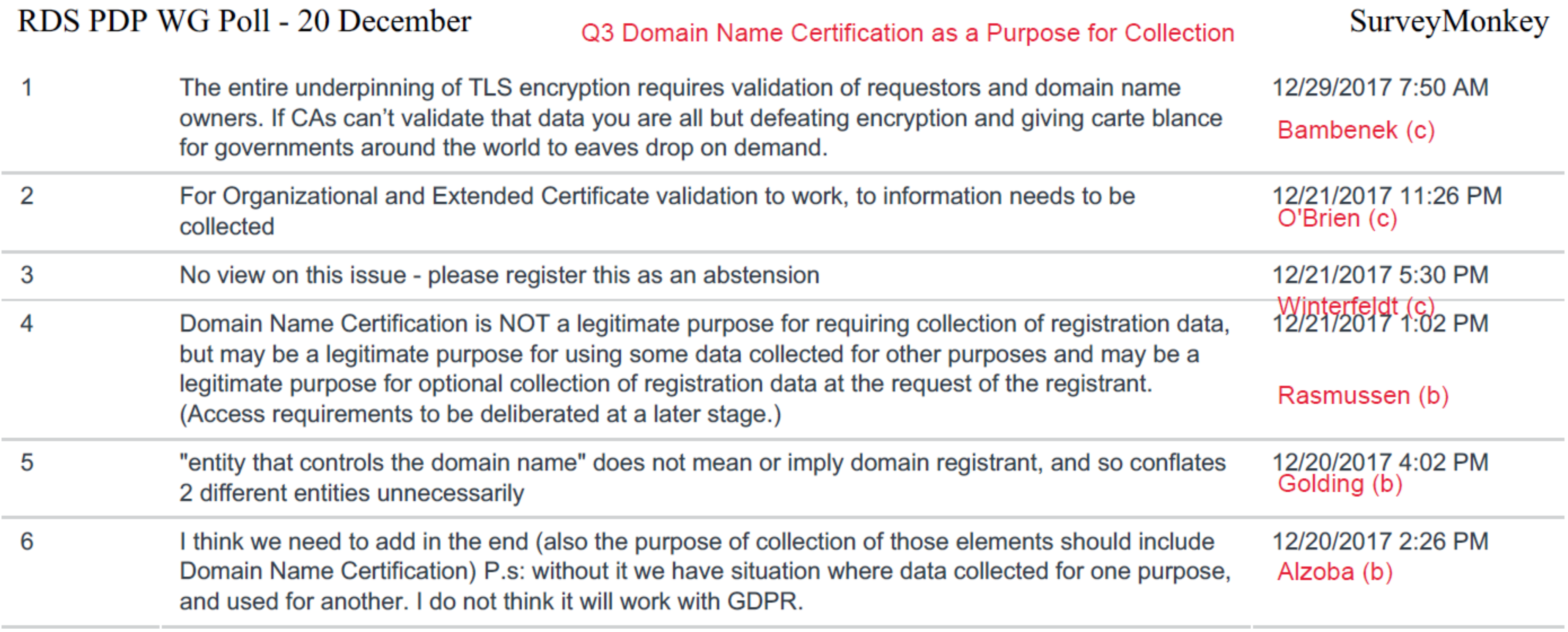
- See Question 3: https://community.icann.org/download/attachments/74580021/AnnotatedResults-Poll-from-20December.pdf

- 84% supported the possible WG agreement:
  - *Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for using some data collected for other purposes. (Access requirements to be deliberated at a later stage.)*

- 3 responses proposed revisions to the above text and 3 gave rationale for treating DN Certification as a legitimate purpose for data collection

- Refer to comments 4, 5, 6 (see next slide)

Q3 Comments



RDS PDP WG Poll - 20 December

Q3 Domain Name Certification as a Purpose for Collection

SurveyMonkey

1	The entire underpinning of TLS encryption requires validation of requestors and domain name owners. If CAs can't validate that data you are all but defeating encryption and giving carte blance for governments around the world to eaves drop on demand.	12/29/2017 7:50 AM Bambenek (c)
2	For Organizational and Extended Certificate validation to work, to information needs to be collected	12/21/2017 11:26 PM O'Brien (c)
3	No view on this issue - please register this as an abstension	12/21/2017 5:30 PM Winterfeldt (c)
4	Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for using some data collected for other purposes and may be a legitimate purpose for optional collection of registration data at the request of the registrant. (Access requirements to be deliberated at a later stage.)	12/21/2017 1:02 PM Rasmussen (b)
5	"entity that controls the domain name" does not mean or imply domain registrant, and so conflates 2 different entities unnecessarily	12/20/2017 4:02 PM Golding (b)
6	I think we need to add in the end (also the purpose of collection of those elements should include Domain Name Certification) P.s: without it we have situation where data collected for one purpose, and used for another. I do not think it will work with GDPR.	12/20/2017 2:26 PM Alzoba (b)

Finalize Possible WG Agreement:

Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for using some data collected for other purposes. (Access requirements to be deliberated at a later stage.)

4) Start deliberation on “Criminal Activity/ DNS Abuse – Investigation” as a legitimate purpose

- Reminder: Our plan for answering “Purpose” charter question

- Take building-block approach, deliberating on each purpose one-by-one
  1. First, agree whether this specific purpose should be considered legitimate for requiring collection of some registration data and why
  2. Next, identify data required to support this specific purpose
     a) Which data may already be collected for another purpose?
     b) Which data may need to be collected for this purpose?
  3. Add any data elements identified to the set of registration data elements potentially made accessible through the RDS
     - For now, defer discussion of collection conditions or access controls which might be applied to each data element

- Note that any agreement on legitimacy of one purpose does not preclude additional purposes being agreed as legitimate for the same or other data

Criminal Activity/ DNS Abuse – Investigation – Intro by DT7

Criminal Investigation or DNS Abuse Mitigation
The broad category of criminal investigation or DNS abuse mitigation covers all use of an RDS to support criminal and other investigations, abuse prevention, security incident response, and other activities to protect people, systems, and networks from detrimental activities. These activities range from criminal activities like extortion, phishing, and provision of child abuse materials to abusive activities including denial-of-service attacks, spam, and harassment.

Three Overall Purposes:

- Criminal Activity/DNS Abuse - **Investigation**
- Criminal Activity/DNS Abuse – Notification
- Criminal Activity/DNS Abuse – Reputation

WE'LL START HERE

https://community.icann.org/download/attachments/74580010/DraftingTeam7-CrimInvAbuseMit-10%20Nov%202017%20clean.pdf

Criminal Activity/ DNS Abuse – Investigation – Intro by DT7

Criminal Activity/DNS Abuse - Investigation

Definition: The following information is to be made available to regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders **for the purpose of enabling identification of the nature of the registration and operation of a domain name linked to abuse and/or criminal activities to facilitate the eventual mitigation and resolution of the abuse identified**:

- Domain metadata (registrar, registration date, nameservers, etc.)
- Registrant contact information
- Registrar contact Information
- DNS contact, etc..

Criminal Activity/ DNS Abuse – Investigation – Intro by DT7

Users: The primary actors in these scenarios include law enforcement, regulatory authorities, cybersecurity professionals, IT administrators, and automated protection systems. Additional actors may include nearly anyone attempting to either track down the source of an online abuse they have experienced or attempting to determine the authenticity of a website or e-mail communication.

Tasks: Using information from the RDS, these actors will, depending upon the circumstances: contact domain owners and/or the entities that provide services for an affected domain to mitigate problems, gather evidence, or notify them of compromises; expand investigations and associations to fully understand the scope of an abuse issue; identify Internet infrastructure involved with detrimental activities, inform protection systems to take protective actions; and, if appropriate and justified, request suspension of domain names. The DT recognizes that the list of users may ultimately need to be narrowly defined to allow for authorized / authenticated access to agreed upon data elements. This applies to all instances in this document where users are mentioned.

Criminal Activity/ DNS Abuse – Investigation – Intro by DT7

Table of purposes and associated use cases
Section 1: **Investigations**

1A-1: Access information held on a domain name to enable security professionals and law enforcement to determine if the domain of a website used for an attack is compromised or registered maliciously.

1A-2: Access information held on a domain name to enable automated security systems to determine if the domain of a website used for an attack is registered maliciously.

1B-1: Access information held on a domain name to enable security professionals and law enforcement to determine domain ownership or involvement with operating a domain name tied to real-world criminal/abuse activities.

1C-1: Access information held on a domain name to enable security professionals and law enforcement to expand knowledge from one known malicious domain to other domains potentially part of the same issue.

1C-2: Access information held on a domain name to enable security professionals and law enforcement to examine all domains sharing one or more key elements tied to abuse to determine if a larger issue exists.

1C-3: Access information held on a domain name to enable security professionals and law enforcement to find potentially compromised domains related to an existing hijacking or domain shadowing incident

1D-1: Access information held on a domain name to enable automated security systems to expand knowledge from one known malicious domain to other domains potentially part of the same issue.

Are there any clarifications necessary to understand this “**Investigation**” purpose before we can begin deliberating on it?

Is Criminal Activity/ DNS Abuse – <u>Investigation</u> a legitimate purpose for collecting data?

- Recall criteria: What makes a purpose legitimate? For example:
  - Does it support ICANN's mission?
  - Is it specific?
  - Is it explained in a way that registrants can understand?
  - Does it explain to registrants what their data will be used for?
  - Is it necessary for the fulfilment of a contract?
  - Other?

- Test **Criminal Activity/ DNS Abuse – <u>Investigation</u>** (as drafted by DT7) against criteria
  - *Information to be made available to regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders for* ***the purpose of enabling identification of the nature of the registration and operation of a domain name linked to abuse and/or criminal activities to facilitate the eventual mitigation and resolution of the abuse identified****: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..*

Is Criminal Activity/ DNS Abuse – Investigation a legitimate purpose for collecting data?

- Reach agreement(s) on legitimacy of **Criminal Activity/ DNS Abuse – Investigation** as a purpose for requiring collection of registration data

Possible WG Agreement for deliberation:

Criminal Activity/ DNS Abuse – Investigation is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for using some data collected for other purposes.

- Note that **Notification** and **Reputation** purposes will be discussed next, separately from any WG agreement(s) on **Investigation**

Confirm action items and decision points

9 January WG Call Meeting Materials:
https://community.icann.org/x/QgByB

Next call: Tuesday 16 January, 2018 at **17:00 UTC**
Agenda will include deliberation on
"Criminal Activity/ DNS Abuse – Notification"
"Criminal Activity/ DNS Abuse – Reputation"

DT definitions for each possible purpose

Name	Single-Sentence Definition
Technical Issue Resolution	Information collected to enable contact of the relevant contacts to facilitate tracing, identification and resolution of incidents related to services associated with the domain name by persons who are affected by such issues, or persons tasked (directly or indirectly) with the resolution of such issues on their behalf.
Academic or Public Interest Research	Information collected to enable use of registration data elements by researchers and other similar persons, as a source for academic or other public interest studies or research, relating either solely or in part to the use of the DNS.
Domain Name Management	Information collected to create a new domain name registration and ensuring that the domain registration records are under the control of the authorized party and that no unauthorized changes, transfers are made in the record.
Individual Internet Use	Collecting the required information of the registrant or relevant contact in the record to allow the internet user to contact or determine reputation of the domain name registration.

DT definitions for each possible purpose

Name	Single-Sentence Definition
Domain Name Certification	Information collected by a certificate authority to enable contact between the registrant, or a technical or administrative representative of the registrant, to assist in verifying that the identity of the certificate applicant is the same as the entity that controls the domain name.
Domain Name Purchase/Sale	Information to enable contact between the registrant and third-party buyer to assist registrant in proving and exercising property interest in the domain name and third-party buyer in confirming the registrant's property interest and related merchantability.
ICANN Contractual Enforcement	Information accessed to enable ICANN Compliance to monitor and enforce contracted parties’ agreements with ICANN.
Regulatory Enforcement	Information accessed by regulatory entities to enable contact with the registrant to ensure compliance with applicable laws.

DT definitions for each possible purpose

Name	Single-Sentence Definition
Legal Actions	Includes assisting certain parties (or their legal representatives, agents or service providers) to investigate and enforce civil and criminal laws, protect recognized legal rights, address online abuse or contractual compliance matters, or to assist parties defending against these kinds of activities, in each case with respect to all stages associated with such activities, including investigative stages; communications with registrants, registration authorities or hosting providers, or administrative or technical personnel relevant to the domain at issue; arbitrations; administrative proceedings; civil litigations (private or public); and criminal prosecutions.
Criminal Activity/ DNS Abuse – Investigation	Information to be made available to regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders for the purpose of enabling identification of the nature of the registration and operation of a domain name linked to abuse and/or criminal activities to facilitate the eventual mitigation and resolution of the abuse identified: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..

DT definitions for each possible purpose

Name	Single-Sentence Definition
Criminal Activity/ DNS Abuse – Notification	Information collected and made available for the purpose of enabling notification by regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders of the appropriate party (registrant, providers of associated services, registrar, etc), of abuse linked to a certain domain name registration to facilitate the mitigation and resolution of the abuse identified: Registrant contact information, Registrar contact Information, DNS contact, etc..
Criminal Activity/ DNS Abuse – Reputation	Information made available to organizations running automated protection systems for the purpose of enabling the establishment of reputation for a domain name to facilitate the provision of services and acceptance of communications from the domain name examined: Domain metadata (registrar, registration date, nameservers, etc.), Registrant contact information, Registrar contact Information, DNS contact, etc..

ICANN's Mission (As amended 1 October 2016)

Section 1.1. MISSION

(a) The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "Mission"). Specifically, ICANN:

(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs"). In this role, ICANN's scope is to coordinate the development and implementation of policies:

- For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2; and

- That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems.

- The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.

(……)

See https://www.icann.org/resources/pages/governance/bylaws-en/#article1 for further details

Annex G-1 of the ICANN Bylaws (As amended 1 October 2016)

ANNEX G-1

The topics, issues, policies, procedures and principles referenced in Section 1.1(a)(i) with respect to gTLD registrars are:

- issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, registrar services, registry services, or the DNS;
- functional and performance specifications for the provision of registrar services;
- registrar policies reasonably necessary to implement Consensus Policies relating to a gTLD registry;
- resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names); or
- restrictions on cross-ownership of registry operators and registrars or resellers and regulations and restrictions with respect to registrar and registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or reseller are affiliated.

Examples of the above include, without limitation:

- principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);
- prohibitions on warehousing of or speculation in domain names by registries or registrars;
- reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);
- maintenance of and access to accurate and up-to-date information concerning registered names and name servers;
- procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility among continuing registrars of the registered names sponsored in a TLD by a registrar losing accreditation; and
- the transfer of registration data upon a change in registrar sponsoring one or more registered names.

Annex G-2 of the ICANN Bylaws (As amended 1 October 2016)

ANNEX G-2

The topics, issues, policies, procedures and principles referenced in Section 1.1(a)(i) with respect to gTLD registries are:

- issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet or DNS;
- functional and performance specifications for the provision of registry services;
- security and stability of the registry database for a TLD;
- registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars;
- resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names); or
- restrictions on cross-ownership of registry operators and registrars or registrar resellers and regulations and restrictions with respect to registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or registrar reseller are affiliated.

Examples of the above include, without limitation:

- principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);
- prohibitions on warehousing of or speculation in domain names by registries or registrars;
- reservation of registered names in the TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);
- maintenance of and access to accurate and up-to-date information concerning domain name registrations; and
- procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility for serving registered domain names in a TLD affected by such a suspension or termination.

Example WHOIS Record From Registry Agreement

```
Domain Name: EXAMPLE.TLD
Domain ID: D1234567-TLD
WHOIS Server: whois.example.tld
Referral URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited

Registrant ID: 5372808-ERL
Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext:
Admin Email: EMAIL@EXAMPLE.TLD

Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD

Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<
```

https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf