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

Handout for Working Group Call
Tuesday 12 December 2017 at 17:00 UTC

Proposed Agenda

1. Roll Call/SOI Updates

2. Complete deliberation on Domain Name Management as a legitimate purpose
   a. Review poll results for Domain Name Management
   b. Finalize definition of this agreed-legitimate purpose
   c. Deliberate on Data Elements needed for Domain Name Management
   Note: Deliberate later on data access and users for that purpose

3. Time permitting, start deliberation on Domain Name Certification as a legitimate purpose

4. Confirm action items and proposed decision points

5. Confirm next WG meeting: Wednesday, 20 December at 06:00 UTC

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

2a) Poll Results for Domain Name Management

- 100% support for Domain Name Management as a legitimate purpose for collecting some registration data

	ANSWER CHOICES	RESPONSES	
a)	Domain Name Management is a legitimate purpose for collecting some registration data, based on the drafting team's definition: 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.	20.83%	5
b)	Domain Name Management is a legitimate purpose for collecting some registration data, based on the extended definition: Information collected to create a new domain name registration, enabling management of the 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.	70.83%	17
c)	Domain Name Management is a legitimate purpose for collecting some registration data, but I wish to propose my own definition of this purpose in the comment box below.	8.33%	2
d)	Domain Name Management is not a legitimate purpose for collecting any registration data.	0.00%	0
	TOTAL		24

#	PLEASE PROVIDE YOUR RATIONALE FOR DISAGREEING WITH THIS PURPOSE OR A PROPOSED ALTERNATIVE DEFINITION	DATE
1	Creating, managing and monitoring a Registrant's own domain name (DN), for the beneficial interest of that registrant, including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information.	12/9/2017 9:05 AM Perrin
2	Purely editorial -- toward the end "unauathorized changes, transfers" should be "unauthorized changes or transfers."	12/8/2017 12:52 PM Shatan
3	The drafting team's definition is fatally flawed -- it does not allow for any changes after the domain is created, and does not allow management of the domain during its lifetime. If you can't manage the domain during its lifetime, you can't update contacts, transfer the domain, add or change nameservers, renew the domain, etc. The drafting team should consider incorporating language from the EWG Report definition.	12/6/2017 9:13 AM Aaron

2b) Finalize definition of Domain Name Management

Let's consider Poll Comment (1)
Creating, managing and monitoring a Registrant's own domain name (DN), for the beneficial interest of that registrant, including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information.

In combination with the preferred Option (b)
Domain Name Management is a legitimate purpose for collecting some registration data, based on the extended definition: Information collected to create a new domain name registration, enabling management of the 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.

Should Option (b) be expanded to reflect the additional concepts and included tasks provided in Comment (1)?

Note: We will deliberate later on data access and users for Domain Name Management

2c) Data needed to support this purpose?

- Review data identified by DT2 as necessary for this purpose
  - Domain Name
  - Registrant Name
  - Registrant Organization
  - Registrant Postal Address (street address, city, state/province, postal code, country)
  - Registrant Phone
  - Registrant Email
  - Registrar Name
  - Registrar Abuse Contact
  - Original Registration Date
  - Creation Date
  - Updated Date
  - Registrar Expiration Date
  - Name Servers
  - Technical Contact (Name / Organization / Email / Phone)
  - Administrative Contact (Name / Organization / Email / Phone)
  - Registry and Registrar domain status
- Identify criteria: What makes data collection legitimate? For example:
  - Why is each data element necessary?
  - What are the consequences of not collecting each data element?
  - Is the use proportional? Does it strike a fair balance between all interests concerned and the data subject's rights and freedoms?
- Test Domain Name Management data needs against criteria
- Reach agreement(s) on data required for Domain Name Management

By considering data for tasks identified by DT2

Tasks:

1. Create registrant id; create domain name; add DNS data for domain name
2. Monitor domain name registration record for changes & correlate with activities
3. Manage set of domain names to keep them under the same administrative control
4. Transfer of domain name registration from one registrar to another or from registrant to new registrant.
5. Check registration database for status/existence of name when DNS does not work
6. Check contact information for ICANN policy compliance

And data needs identified by DT2…

Data:

Data Element	Purpose
Domain Name	Confirm domain name is registered.
Registrant Name	Identify registrant and determine if registrant is an organization or natural person
Registrant Organization	Identify registrant and determine if registrant is an organization or natural person
Registrant Postal Address (street address, city, state/province, postal code, country)	Monitor for any unauthorized changes to this data
Registrant Phone	One means of contacting the registrant for operational issues
Registrant Email	Contact the registrant for operational issues or verification of requests made to registrar to transfer or modify the domain name registration.
Registrar Name	Identify the domain name registrar to contact if registrant is not contactable

And data needs identified by DT2 (continued)

Registrar Abuse Contact	See above.
Original Registration Date	Ensure that the record associated with the domain name is maintained correctly
Creation Date	Ensure that the record associated with the domain name is maintained correctly
Updated Date	Monitor for changes to the registration data
Registrar Expiration Date	Monitor to ensure the domain name is renewed
Name Servers	Monitor to ensure the Nameservers have not been modified without authorization.
Technical Contact Name / Organization / Email / Phone	Contact with any operational issues
Administrative Contact Name / Organization / Email / Phone	Contact with any operational issues. Monitor for possible modifications in domain name management.
Registry and Registrar domain status	Monitor to ensure that the correct statuses are maintained for a domain name registration

Possible WG Agreement:
The following information is to be collected for the purpose of Domain Name Management: <enumerate data agreed upon by WG>

3) Start deliberation on Domain Name Certification

- 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 collecting some registration data and why
  2. Next, identify data elements 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

Domain Name Certification – Intro by DT3

Purpose Name: **Domain Name Certification**

Purpose:
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.

Definition:
The role of a certificate authority (CA) is to bind an identity to a cryptographic key in the form of a cryptographic certificate. In the case of TLS certificate issuance the CA also needs the ability the validate and verify that the identify of the certificate applicant is the same as the entity that owns the domain name (e.g. the Registrant). While the process and rigor of CA validation and verification procedures vary, both by the nature of the certificate desired and the processes of individual CAs, the WHOIS system can be used to validate the certificate applicants ownership of control of the corresponding domain.

Domain Name Certification – Intro by DT3

Tasks:
A Certificate Authority may issue certificates with different validation levels. The three levels of validation in standard use are Domain-validated, Organisation Validation, and Extended Validation. Domain-validated certificates require only demonstration of administrative control over the domain, and so do not require interaction with the RDS, and may be validated only using the DNS (optionally including other mechanisms such as email). They are therefore of limited relevance to this purpose.

Organisation Validated certificates require identification of the organization that requests the certificate, validation methods and levels vary. We have noted Extended Validation certificates as the most explicitly relevant to the purpose, but Organisation Validated certificates are also relevant. Guidelines for the Issuance and Validation of Extended Validation certificates may be found at https://cabforum.org/wp-content/uploads/EV-V1_6_5.pdf

Extended Validation certificates explicitly identify the legal entity that controls a web site as their primary purpose. They apply only to organisations, but for Business Entities (as defined in the EV guidelines 8.5.4) the validation process requires confirming the identity and authority of individuals applying for certificates.

At a high level Certificate Authorities may perform the following tasks.

- Confirm that the enrolling organization (requesting the certificate) is listed as the Registrant in the WHOIS
- Send one of the WHOIS contacts (registrant/admin/technical) an email to confirm domain authorization/control
- Call one of the WHOIS contacts (registrant/admin/technical) to confirm domain authorization/control

Details of how this happens are defined in the CA Browser Forum's (CABForum) Practices Section 3.2.2.4 (https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.2.pdf)

Domain Name Certification – Intro by DT3

Section 3.2.2.4 of the Baseline requirements is explicitly required for Extended Validation certificates by rules 11.7.1 of the Extended Validation Guidelines.

3.2.2.4. Validation of Domain Authorization or Control
3.2.2.4.1 Validating the Applicant as a Domain Contact
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
3.2.2.4.3 Phone Contact with Domain Contact
3.2.2.4.4 Constructed Email to Domain Contact

See DT3: Domain Name Certification PDF for excerpts of the above sections

Note:
DT3 did not find that access to all RDS data was required in all cases, but was required for some CA validation methods.

Users: Describe the parties who often access gTLD registration data in pursuit of this purpose.
Employees of Certificate Authorities and automated systems associated with Certificate Authorities responsible for preforming the validation and verification as described above.

Domain Name Certification – Intro by DT3

Data: List of gTLD registration data often involved in this purpose – for contact data, please identify the data subject (e.g., registrant, tech contact, registrar, etc.) and data element(s) as applicable.

Data Element	Purpose
Domain Name	To match with FQDN placed into the certificate.
Registrant, Tech and Admin Email	A means to contact the owner of the domain name, using manual or automated processes, with the goal of confirming that the identity of the certificate applicant is the same as entity that owns the domain name.
Registrant, Tech and Admin Phone	Used as an alternative method of contact in circumstances where Email is not available or when an additional level of manual or automated verification is needed.
Registrant, Tech and Admin Name	Used when necessary to confirm an individual can or does work for or represent the applying organization.
Registrant, Tech and Admin Postal Address (Street, City, State/Province, Country)	Used to confirm that the organization of the entity that owns the domain name matches the organization of the of the certificate applicant. Also used in authentication/verification scenarios that are postal mail based.

Are there any clarifications necessary to understand this purpose before we can begin deliberating on this purpose?

Is Domain Name Certification a legitimate purpose?

- 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 Domain Name Certification (as drafted by DT3) against criteria
  - *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.*

- Reach agreement(s) on legitimacy of Domain Name Certification as a purpose for collecting some registration data

Confirm action items and decision points

12 December WG Call Meeting Materials:
https://community.icann.org/x/MgByB

Next call: Wednesday, 20 December 2017 at **06:00 UTC**

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.TL
D

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