6 March 2023

RE: Questions from the SSAC DS Automation Work Party to ICANN Org

Steve Crocker and Peter Thomassen
SSAC DS Automation Work Party Co-Chairs

Dear Steve Crocker and Peter Thomassen,

This letter is a reply to your questions sent on 8 February 2023 (https://www.icann.org/en/system/files/correspondence/crocker-thomassen-to-sheng-crain-08feb23-en.pdf). We've quoted your questions and provided our responses following each question.

Q1 & Q2.

> 1. Perception regarding direct polling by registry
>
> In about 10 ccTLDs, the registry scan's [*sic*] the registrant's zone to find CDS/CDNSKEY records indicating there's been a change in the registrant's key. The registry then creates a new DS record. This process bypasses the registrar. Some ccTLD registries notify the registrar there's been a change, thereby giving the registrar an opportunity to update its internal database to match the entries in the registry.
>
> In our discussions, we have heard the claim that gTLD registries would be prohibited from doing this because it violates [*sic*] the rule that a registry is not allowed to have direct access to the registrant. We understand the origin of that rule was insistence by the contracted registrars that they own the relationship with the registrants. However, we are not aware of where this restriction is codified.
>
> Q1. Is there a codification of the restriction that gTLD registries may not interact with registrants? Is [*sic*] so, please provide the codification.
>
> Q2. If there is such a codification, would registry scanning for CDS/CDSNKEY records fall within the restriction? The DNS operator is not the same as the registrant, so perhaps the restriction would not apply.

Answers to Q1 & Q2. There is no explicit prohibition for gTLD registries regarding contact with registrants. To offer a service beyond what is enumerated in a registry agreement, gTLD registries may submit a request via the Registry Services Evaluation Policy (RSEP) as described in https://www.icann.org/resources/pages/registries/rsep/policy-en. Using this process, gTLD registries may add a new registry service or modify or remove an existing registry service. It is worth noting that registries are encouraged to seek an informal consultation with ICANN org before submitting an RSEP request.

Q3.

> 2. Clarification of best practice
>
> The Registry Agreement says under "Specification 6 Section 1 (Standards Compliance)": 1.3 DNSSEC: "Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices."
> https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification6.1
>
> Q3. What industry best practices are recognized under this agreement? Are CDS/CDNSKEY scanning included, excluded or uncertain as a best practice? How is this best practice [*sic*] evolved?

Answer to Q3. When the base agreement for gTLD registries was created, the established practice for accepting public-key material by registries was the DNSSEC extension for EPP described in RFC 5910.

CDS and CDNSKEY record scanning is a new and promising technology, however there remain questions with its usage that may need to be addressed by the community, for example:

a) there are ongoing discussions in the IETF regarding the mechanics and consistency of CDS scanning (see https://datatracker.ietf.org/doc/draft-thomassen-dnsop-cds-consistency);
b) no guidance exists with respect to whether registries or registrars are to conduct CDS scanning, and if both registries and registrars are conducting CDS scanning, there exists no guidance on avoiding and resolving conflicts;
c) there is no clarity on whether registrars should be notified by the registry of errors, or the changes made as a result of the scanning, or whether they should be made aware that the scanning is happening;

d) there is no consensus on the precedence of EPP locks over CDS scanning, or vice versa; and
e) if EPP locks take precedence and a registrant publishes CDS records, how the registrant and/or the DNS provider would be informed that the update was prohibited;
f) there is no automated way for a child to learn the parent's preferences on CDS vs CDNSKEY;
g) there has been no consensus on guidelines for practices and procedures concerning initial signing as highlighted in Section 3 of RFC 8078.

Q4.

> 3. Role of DNS operators
>
> The ICANN generic names contractual structure recognizes registries and registrars but does not recognize the existence of separate DNS operators. DNS operators are implicitly treated as if they are providing a higher-level application service, e.g. web hosting or mail service. However, registrant DNS service is more akin to a critical part of the infrastructure and cannot be omitted from a complete picture of the overall DNS environment.
>
> Q4. What guidance do you suggest for bringing DNS operators into the ICANN ecosystem to have a voice in specifying and implementing the critical service of DNSSEC?

Answer to Q4. There are many ways in which those interested in getting actively involved in ICANN activities can do so. ICANN accepts participation through public comments, free and open meetings, and through participation in ICANN Supporting Organizations (SOs) and Advisory Committees (ACs). More information on how a DNS operator may participate in the ICANN ecosystem may be found at https://www.icann.org/resources/pages/how-2012-02-25-en. Further information about how a DNS operator may get involved in policy development at ICANN can be found at https://www.icann.org/en/system/files/files/icann-policy-development-report-16jun21-en.pdf.

ICANN's Generic Names Supporting Organization (GNSO) has a process in place for the recognition of a new Constituency. More information about that process is available on the GNSO website at https://gnso.icann.org/en/group-activities/inactive/2012/improvements/newco-process-en.htm.

We also note that this specific question came up during the recent meeting between SSAC leadership and the GNSO Council during ICANN75 in Kuala Lumpur. Some suggestions that were put forward as part of that conversation were further engagement between DNS Operators and the GNSO's Internet Service Providers & Connectivity Providers (ISPCP) Constituency to discuss if/how DNS Operators may find a home within that Constituency, as well as exploring more regular exchanges with organizations that represent the interests of DNS Operators.

Q5.

> 4. Some registries (at least .de) check that NS are authoritative before they update the delegation (such as by querying SOA and thereby ensuring that the nameserver knows the zone).
>
> Q5. Would gTLD registries be permitted to do the same, or would it be considered a form of a registry interacting directly with the registrant?

Answer to Q5. As stated above, there is no explicit prohibition regarding the interaction between a registry and registrant.

We hope these answers provide the information you are seeking. If you require any follow-up questions or need further information, please do not hesitate to reach out. Like you, ICANN org will be happy to interact informally as needed.

Sincerely,

John Crain
Senior Vice President and Chief Technology Officer
ICANN Org