From: Steve Crocker and Peter Thomassen
Sent: February 8, 2023
To: Steve Sheng and John Crain
Subject: Questions from the SSAC DS Automation Work Party to ICANN Org

During the DS Automation Work Party meeting on 7 Feb 2023, we identified some areas of uncertainty. We seek clarification and/or guidance.

The focus of the work party is automation of the update of the parent's DS record when the child's key is rolled. When the child's key is rolled, the DNSSEC protocol specification requires there to be a corresponding change to the DS record in the parent. The DNSSEC RFCs do not specify the process for making this change.

If the parent is a TLD registry and the child is the registrant's zone, the relevant question is how the registry updates its DS record when the registrant's key is rolled. Often the registrant's DNS service is provided by the registrar. That is, the registrar, in addition to providing registration service, often provides DNS service to the registrant. In such cases, if the registrant's zone is signed with DNSSEC, the registrar can push a changed DS record to the registry via EPP. However, if the registrant's DNS service is <u>not</u> provided by the registrar, there is no specified way for the change to be propagated to the registry. Registrars usually do not provide an automated interface, so the registrant is forced to copy the cryptographic information from the DNS operator and manually type it into the registrar's web interface. This is a process that is time-consuming, error-prone and doesn't scale. The SSAC DS Automation work party is studying this situation. It will prepare a report with findings and recommendations.

During our discussions, we have encountered some questions. We seek guidance and/or answers to the following.

1. Perception regarding direct polling by registry

   In about 10 ccTLDs[1], the registry scan's 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 violate 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.

1 https://github.com/oskar456/cds-updates

Q1. Is there a codification of the restriction that gTLD registries may not interact with registrants? Is 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.

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 evolved?

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?

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?

We appreciate that it may take a little bit of time to consider and respond to these questions. We will be happy to interact informally to clarify these questions or reformulate them if need be.

To facilitate our work, it is not necessary to have responses to all of these questions before answering any of them. Please respond in parts as the answers become available.

Thank you,

Steve Crocker
& Peter Thomassen
DS Automation Work Party Co-Chairs