Security and Stability of the DNS Topics

The following are a set of general topic areas to underpin the study of this question. The question is predicated by scoping this topic to matters that fall with ICANN's remit. The broader consideration of the security and stability of the DNS ecosystem, its architecture, technologies, applicable standards, vendors, operating practices and actors is a topic that intersect with ICANN's mission in a number of areas, but the general topics are substantially larger matters and will not be considered as part of this review.

The focal point here is those activities that are directed or coordinated by ICANN or the PTI, or where ICANN has a substantive presence by virtue of hosting the community-driven policy process or through existing activities.

1. Root Zone Management Practices

ICANN coordinates the contents of the root zone of the public DNS system, so consideration of the security aspects of the way in which this responsibility is fulfilled is relevant to this topic. Sub-topics include:

TLD Label management (what labels go in the root zone)

- What guidelines and constraints govern the labels that are placed into the root zone of the DNS?

  For example, are single character domains, either in Ascii or in their Unicode equivalent permitted? Are two letter codes other than those defined through ISO3166 permitted?

  This report should either enumerate these constraints, or preferably reference such a document that the community use as a reference document as to the permissible labels in the DNS. If such a document does not exist then perhaps it shiould and we might recommend as such.

  The constraints on labels for delegated names in the root zone of the DNS are policy-based constraints, using policies as developed by the GNSO and the CCNSO and approved by the Board. Single character ascii names are not permitted as delegated labels in the root zone, nor are the punycode representations of single unicode characters. Two character ascii names are permitted, but only as specified by the ISO3166 maintenance authority, with delegation to entities corresponding to the entities specified by ISO 3166.

  The original DNS label constraint set was specified in RFC1035, RFC1123 and RFC2181. This specifically refers to ascii labels. Permissible Unicode names are specified by RFC5891 (IDNA2008). Where the prevailing policies and the IETF specifications differ, ICANN permits labels under the prevailing policies.

  There are no clear policies relating to the DNS names used in non-delegation labels, such as to be found in the root zone's name server records and associated glue records.

Comment [1]: How is it done today? Do we have a specific limit/challenge to the current practice? Do we have a new approach to recommend? To what extent will the proposed approach be successful?

- How are these constraints managed by ICANN, and how are the constraints communicated to the community?

  For example, are the procedures used by ISO3166 in the management of two letter country codes binding on the DNS? What procedures are in place to ensure that retirement of a two letter code from the ISO 3166 registry is coordinated with the retirement of the corresponding two letter code in the DNS. If these procedures are not synchronised what measures have been taken by ICANN to ensure that the two name spaces do not diverge?

Formatted: Font:8 pt, Font color: Auto

  We may wish to pass this as a query to ICANN staff, and record our response to their answers to this question.

Formatted: Font:(Default) Arial, 11 pt, Font color: Black

Formatted: Indent: Left: 1", Add space between paragraphs of the same style, No bullets or numbering

- How is change control exercised over these constraints?

  Presumably, one could envisage a scenario where some group is wanting to change these constraints. What process would ICANN follow to examine such a request for a change in these constraints?

  For example, is ICANN bound to exclusively follow the specifications as described in current RFCs? Under what circumstances, if any, might ICANN reach a conclusion to deviate from the RFCs? If if were to do so how would ICANN codify its adopted specifications?

- What extent impacts and behavior relate to labels that will be, or are, in the Root zone, how can this be longitudinally considered?

This issue is exemplified by the name collisions work [Verisign TR, S&P publication, US-CERT TA]

The domain name space is a space of all possible labels that could be described by the syntax roles of a "valid" domain name. This space forms a far larger set than the set of delegated names. As names are added to the root zone of the DNS, such names are being drawn from a notional 'unused' domain name pool. At the time time there are other parties also drawing names from the same name pool for their own use. Such actions include the registration of labels in the IETF's Special Use Names registry, the use of names in contexts that are not the DNS (such as multicast DNS, or DNS resolution based on the ToR network, and similar), or the use of names in private network realms?

[We should perhaps reference some recent SDSAC studies on this topic]

- If a proposed TLD contains non-ascii unicode characters (IDN) what procedures are followed to ensure that the label meets these criteria?

Historically, the contents of the TLDs listed in the Root Zone have been constrained by technical specifications developed by the IETF and published as RFCs. RFC1034 described the "LDH" rule, of ascii characters that are permissible in labels in the root zone, and the equivalence of upper and lower case. Punycode is an encoding of any unicode character into a LDH-constrained label. The implication is that using a very strict literal interpretation of this LDH rule could allow any Unicode character to be permitted into a DNS label, including dashes and characters that display as period characters, as well as punctuation characters and diacritics.

What approach is used to ensure that the Unicode characters encoded in DNS labels also conform to some unicode equivalent of the LDH rule? Or is the LDH tule only relevant for the ascii character set?

What studies and reference material is ICANN using to provide appropriate guidance to the community on the use of unicode characters in the DNS?

This question refers to the matters raised in SSAC 084 and the EPSRP?

NS and DS record management in the Root Zone

When a name is delegated in the root zone, the delegation is reflected by the presence of NS records in the root zone, and the DNSSEC security binding is reflected by the presence of DS records in the root zone.

- Are appropriate security practices used to ensure that changes are duly authorised by the correct party prior to inclusion onto the root zone?

ICANN (or perhaps PTI) staff should be in a position to provide an answer to this question which this review can then comment

- Are the NS and DS records validated by ICANN (or PTI) prior to inclusion in the root zone? What steps are taken if validation fails?

If PTI is not in a position to validate a registered DNSSEC crypto algorithm, and hence unable to validate a DS record signed with the algorithm, should it accept this DS record without validation or not?

- Are these records, and the associated glue records, regularly audited to ensure their continuing accuracy?

Respective roles of RSSAC and ICANN

The Root Server operators serve an authoritative copy of the current root zone contents from their secondary servers. While the content of the root zone is the same across all root servers, these server operators have considerable latitude as to how the root zone is served in terms of finer level of granularity of the technical aspects of the service.

Formatted: Font:(Default) Arial, 11 pt, Font color: Auto

Formatted: Indent: Left: 1", Add space between paragraphs of the same style, No bullets or numbering

Formatted: Indent: Left: 0.75", Add space between paragraphs of the same style, No bullets or numbering

Formatted: Font:8 pt, Font color: Auto

Formatted: Font color: Auto

Formatted: Indent: Left: 1", Add space between paragraphs of the same style, No bullets or numbering

Formatted: Font:(Default) Arial, 11 pt, Font color: Black

Formatted: Font color: Auto

Comment [2]: Do these better fit the ICANN SSR subteam?

Deleted: So all NS and DS records be validated by PTI all of the time? What procedures are used to audit the root zone and what steps are taken if any of the entries fail this audit?

Formatted: Font:(Default) Arial, 11 pt, Font color: Black

- How consistent are the contents across all Root servers (letters and instances)?
- How much lag is there in attaining consistency after a change?
- Are there any instances of sustained inconsistency or variation, and how would this be detected?
- Is it appropriate that such variation exists across the Root Servers?

  The finer level of detail of how each root server responds to queries are largely undocumented, and it is unclear if this diversity enhances or compromises the security and resilience of the root service.

  It is also unclear how this question fits into the SSR2 study. Is this a RSSAC Review question? A topic for SSAC study? Is this a detail of a more generic question for SSR2 study about the nature of the relationship between RSSAC and ICANN and the ACs and SOs?

It may be worth some comment at a generic level with respect to this, and the next topic about the difference between devolved and centralised systems. The risks of a devolved system is that the components may not provide uniform responses from every element of the devolved system, and this may cause issues for users. On the other hand the devolved system allows each component to use different approaches to some common challenges, and these different approaches may ensure that a persistent client can get the answer they are seeking if they are persistent in querying across all elements of the system.

Deleted:

The other are of comment here is that the modes of community engagement differ between the two bodies. RSSAC tend to operate with little in the way of public consultation and the soliciting of advice and comment on aspects of their operation, whicvh appears to be quite distinct to the mode of operation undertaken by ICANN.

Respective roles of ICANN, PTI and Verisign over root zone contents

Each iteration of the root zone is produced as the outcome of a multi-party process, where the zone file is the result of records managed by PTI (NS, DS and glue records) and records provided by Verisign DNSSEC RRSIG records (generated through the use of the ZSK).

- Is this separation of roles appropriate?

  Does this multi-step process introduce vulnerabilities, or do they remove potential single points of failure by having multiple parties with oversight on the root zone as it is generated?

  The case in point here is the inordinate delay in the signing of the zone used to name the root server instances.

Comment [3]: Can we get some background on the intuition behind this question?

Formatted: Indent: Left: 0.5"

Formatted: Font:10 pt

2. Change Management

With respect to the root zone of the DNS, the list of delegated labels is not considered to be a static list, and the current mode of management of the root zone is to periodically open the zone for the inclusion of new top level labels. The general motivation behind this is that this expanded set of top level labels promotes diversity and competition in the domain name space, and this competition works to the benefit of the consumer in terms of reduced prices and improved focus on customer service for holders of second level name registrations. It is unclear if these changes and the increased diversity of top level names and top level name registries promote or detract from the overall security and integrity of the domain name system.

- Introduction of new TLDs

  Is the phased introduction of TLDs into the root zone, resulting in a zone that is in a state of constant flux better or worse than a single introduction of a set of new top level labels in a single event, or is the mode of introduction of new labels neutral to the security and stability of the root zone management function?

- Aside from ccTLDs (below) is there any consideration of the retirement of TLDs from the root zone?

- Coordination with ISO3166 or both introduction and retirement of ccTLDs

  What is the nature of the interaction between ISO 3166 and the root zone? Are all two letter TLDs reserved? What about Exceptionally reserved, traditionally reserved and indeterminately reserved names? Does ISO3166 provide for CC name retirement in an acceptable manner?

Comment [4]: Is this an SSR issue?

- Coordination with IETF over Special Use Names Registry

  There is none at the moment! See SSAC 090

- Coordination between IETF and Unicode Consortium over IDNA standards and practice

  See SSAC 095 for the specific case with emojis, but the general observation holds true as well.

- Evolution of the Root Service

  Does the future security of the DNS root service rely solely on the current root server operators and the infrastructure that they operate? Should the model of distribution of root zone data evolve to include consideration of the opportunities offered by DNSSEC, such as local root secondary servers and recursive resolvers DNSSEC NSEC caching. How can ICANN assist in these measures to assist tin scaling the root and making it more resilient to known attack vectors?

Comment [5]: Is this a suggestion to investigate? It seems to presume a problem in scaling that I'm not aware of.

- Consistency of the Identifiers

  The DNS resolution protocol is not the only protocol that performs a mapping from a domain name to a IP address (or other 'attached' attribute. To what extent should the ICANN community take steps to ensure that a domain name has a consistent meaning irrespective of the method of name resolution? i.e. is ICANN's remit solely concerned with domain names as resolved by the DNS protocol. Or does it extent to domain names as resolved by any protocol in the context of the public Internet? Or domain names irrespective of the name's manner and context of use?

Comment [6]: The name collisions issue (not to mention any others) demonstrates that there can be an interaction between namespaces, despite intentions. That, imho, makes this an SSR issue.

3. Roles and Responsibilities

There are many bodies who have an interest in the DNS and its operation. ICANN and its SOs and ACs bring many of these interests together, but not all. The broader DNS ecosystem includes aspects of applicable technical standards and their evolution, security and threat analysis, and modes of use of identifiers by applications and services. The observation is that this is not a static space and changes are anticipated. The consideration from security and stability is to ensure that such changes are considered carefully and the motivations that are driving such change are balanced against what is prudent and safe in terms of operational practice and use of available technology.

- Has ICANN achieved an effective balance relating to community policies, applicable standards, and SSR concerns?

- Are there checks and balances in the process, and do they have a voice?

4. Abuse and Threats

What are ICANN's responsibilities in this space?

<more material needed here!>

Notes about DNSSEC.

DNSSEC is the chosen mechanism to support security in the DNS, in so far that the resolution process itself is not protected, but the result can be validated to assure the client that the resolution response is genuine and complete. Being such a central part of DNS Security in general, should it be a topic of study in this sub-topic?

DNSSEC is largely under the control of the IETF as a piece of technology. If a party wants to alter the operation of DNSSEC or any other aspect of the way in which its operation if defined then the IETF is the place to undertake such a conversation. This implies that such technical aspects are beyond ICANN's remit.

DNSSEC, as seen by ICANN, is firstly a set of DS delegation records, similar in almost every respect to NS records. There are some operational questions in this process, noted in section 1.2. Secondly, DNSSEC is a root zone signing operation. This area includes the management of the KSK key which appears to fall under the subtopic of ICANN operations as it not a generic DNS topic. The question of the choice of protocol and key length and the scheduling of periodic KSK rolls appears to also be an ICANN operational topic rather than a generic DNS stability issues.

Notes about the KSK roll - DNS Review Team Call 8 August

Formatted: Font:Italic

The "largest" issues at the time of preparing this report is the forthcoming roll of the Key-Signing Key of the DNS. This is a major issue for the DNS, or at least the DNSSEC-aware part of the DNS in so far as the roll is not a "standard" part of the operation of DNSSEC. In this hierarchical key structure subordinate keys derive their validity by being "signed over" by the ley's immediate superior. This has lead to a wealth of operational practice related to rolling keys, and part of this is the established practice of rolling the Zone-Signing Key of the root zone every quarter. The KSK has only been "rolled" once, when in 2010 the original unvalidatable KSK was rolled to the first production "valid" key.

ICANN, and its advisory bodies, notably SSAC, have been aware of the challenges in this area. The commitment to roll the original KSK some 5 years after the original introduction of this key has resulted in a significant body of effort to design a process that minimizes the risks to the DNS, and at this stage there is some level of confidence that to the extent that such risks can be mitigated, every reasonable effort has been taken to ensure that outcome.

At the same time we are aware that there are still some uncertainties in the process, principally concerned with the unknown level of use of clients using manually managed local copies of the public part of the KSK. These concerns cannot be alleviated by taking further measures within the specifications of the DNS and DNSSEC as they stand. This leaves the somewhat unsatisfying assertion that "we are doing the best we can do with the tools we have available to us, but we are aware that this does not address all known risks."

We anticipate that the actual roll of the KSK will be instrumented in the DNS at large, and the impacts of the roll, and the subsequent revocation of the original KSK, will be analysed, both by OCTO staff and interested DNS researchers.

The open question is then one: "How can we use the findings of this analysis to improve this process?" The regular rolling of the ZSK at three month intervals has made this process a standard operational practice and both the operators of the ZSK and client DNSSEC validating resolvers are aware of the procedures and the implications of this regular roll on their behaviours in validation. The current intuition is that performing a KSK roll every roll is sufficiently infrequent that it becomes an exceptional event that must be carefully managed every time, and the operational responses are sufficiently infrequent that they do not become an integral part of the operation of the DNS. However, the current lack of DNS integration for this KSK roll implies that the risks of stranding client resolvers is not necessarily improved by performing this every more frequently. It could be argued that increased disruption is a disincentive for DNSSEC adoption rather than an enabling factor. The open question at this point is how to take the outcomes of the analysis of this roll and feed it into a larger process that inevitably involves stakeholders that include DNS infrastructure operators, DNS resolver vendors, and the IETF, as well as others, to investigate ways to improve the resilience of KSK rolls in the future.

We cannot assume that KSK keys maintain their integrity for the indefinite future, and it seems unwise to perform KSK rolls so infrequently that accommodating these key rolls are an exception event each and every time.

In looking at this topic we would also encourage further consideration of emergency procedures involving the unforeseen events of either key compromise or an inability to access the key. it would be appropriate for procedures relating to such "emergency" key rolls to be widely promulgated, so that relying parties are clearly aware of the distinctions between a legitimate emergency key roll and a hostile attack on the key.

Formatted: Font:10 pt, Italic