Comments on the Design Team’s draft report on DNS Root Zone KSK Change

This comment is being submitted by me purely in an individual capacity.

I would like to thank the Design Team for their dedicated work, and for presenting a very complex topic in a concise and easily understood document.

I do have some concerns and comments, some of which are aimed specifically at the report, but the vast majority of which are aimed at the larger process. It is very likely that the KSK Roll will go seamlessly and with a minimum of disruption. On the grounds that prevention (or preparation) is better than cure, I do have several thoughts and recommendations on how to make the document and the process even more thorough and safe and likely to guarantee a higher success rate.

Summary:

1. There have been a number of previous documents and public comments. It is unclear from this document how much of the prior work was incorporated into this design and how much / what has been explicitly discarded. As appropriate, the document should note the reasons why such recommendations have not been included in this document.

2. The document acknowledges that some 13% of the population may be adversely affected, but does not discuss how to refine this number, evaluate whether this is acceptable, or who makes this determination.

3. Outreach and communications. The described communication plan is neither broad enough nor long enough. DNSSEC is much more widely deployed than when first launched, many people are relying on DNSSEC without knowing it. The outreach needs to reach them, not DNS insiders. The outreach should also begin early enough for both the public and DNS insiders to have time to prepare

4. The DPS states that the key will be rolled after 5 years. We have exceeded this point, and there is still no clear schedule for the keyroll. ICANN should acknowledge the fact that they are slipping behind the implicit schedule as per the DPS, and either provide a schedule for the roll, or note the particular activities that will lead to a schedule.

5. The document also does not discuss anything to do with emergency key rolls. I assume that this was outside the scope of the Design Team's charter, but it would be good to know what the plan is, especially regarding communications and distribution of the new key.

Detail:

Status and history.
Section "4 Abridged History" of the report contains a history of previous work.
For example, ICANN held "Consultation on Root Zone KSK Rollover" public comment period March 8, 2013 (https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en) (the same topic currently being discussed).
ICANN received feedback from six organizations and 15 individuals.The summary of responses (https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf), states seven recommendations (oddly, only six are listed in the document); however, there is no clear follow up of which have been accepted or implemented, which have been explicitly rejected, or what the status is of the feedback and recommendations received.

The "Advice to the ICANN Board" tracking system (https://features.icann.org/board-advice) says, in regards to SAC063, "ICANN staff is evaluating these recommendations as mandated in its 21 November 2013 resolution http://www.icann.org/en/groups/board/documents/resolutions-21nov13-en.htm#1.a and will share its results by 17 February 2014. In the instances where ICANN recommends that the advice be accepted - ICANN will evaluate the feasibility and costs of implementation, and provide an implementation plan with timelines and high-level milestones for review by the Board, no later than 21 March 2014."

It is difficult to understand the purpose or premise of this public comment period without knowing what happened with the last on the same topic. Comments would likely be more relevant and productive if there were some awareness of what has already been considered and accepted or rejected as well the as the rationale behind those decisions.

Example 1: The "ICANN Recommendations" section from the summary of the "Consultation on Root Zone KSK Rollover":

> 1. What prerequisites need to be considered prior to a first scheduled KSK rollover?
> A set of tests and measurements, with a test-bed, should be established before embarking on a RFC5011 KSK roll. Lines of communication need to be established during testing phases and methods for success evaluation constructed.

2. When should the first scheduled KSK rollover take place?
The KSK rollover should be performed as soon as practical with an emphasis on preparedness.

6. What public notification should take place in advance of a scheduled KSK rollover?
An effort of public notifications via multiple diverse stakeholder groups with significant advance notice, prior to a KSK rollover event, should be undertaken.

Example 2: The Internet Architecture Board (IAB), a committee of the Internet Engineering Task Force (IETF) provided (http://forum.icann.org/lists/comments-root-zone-consultation-08mar13/msg00022.html) :
"To this end, the IAB suggests the rollover of the Root Zone KSK before
the end of the year, with significant prior notice to all involved parties, including vendors, implementors, TLD operators, and end-users.

In addition, the IAB suggests that RFC 5011 be followed. The new KSK for the Root Zone should be published as widely as possible using mechanisms in addition to those specified in RFC 5011 to minimize surprises."

Dr Steve Crocker provided (in http://forum.icann.org/lists/comments-root-zone-consultation-08mar13/msg00002.html):
"My first comment is this test should have been carried out much earlier, preferably not long after the root was first signed. Key rollover is an integral part of the overall system, and to leave it untested is very odd, perhaps akin to not testing whether the landing gear on an airplane will work.
There's no question the key has to be changed, and when it is eventually changed, the process had better work."

Recommendation #7: While I understand that there is too much risk involved in changing the algorithm and key size for this key size, this is primarily due to a lack of foresight and testing, and not for a technical reason. I agree that, at this point, changing the algorithm and key size is, unfortunately, unrealistic. Recommendation 8 suggests that the algorithm and key size should be reviewed in the future for subsequent KSK rolls. We should ensure that we do not run into the same issues for the next keyroll, be that 2020 or "as required" prior.

The document should explicitly reference earlier activities and reports and respond in detail to the recommendations contained in those documents. It is unclear from this

document how much of the prior work was incorporated into this design and what has been explicitly discarded. As appropriate, the document should note the reasons why such recommendations have not been included in this document.

Breakage.

The document contains a very useful section to help understand the possible impact on validating resolvers (Section 7, Impact on Validating Resolvers). As noted in this section, it is difficult to predict the population of the Internet that will “break” (be unable to resolve any names). There are many possible reasons for the breakage, including large response, validating resolvers that do not implement RFC5011, and an unknown population of resolvers that have not enabled RFC5011 support. There are various numbers and metrics provided, but the conclusion drawn is that we cannot currently accurately predict the breakage with a high level of confidence. An upper bound of 13% of the population is derived. Most experts expect the impact to be much, much lower (for example, large validating resolvers who do not do RFC5011 style rollovers are expected to be paying attention and manually insert the new trust anchor, many validating resolvers will perform RFC5011 correctly, etc), but everyone seems to agree with the conclusion that we cannot currently accurately predict the likely affected population.

The document does not discuss:

- if this is an acceptable situation, or if the keyroll needs to be delayed until better measurement techniques can be created and deployed
- who is responsible for determining if the keyroll should proceed, and using what input and metrics
- how breakage is evaluated once the keyroll has begun, and what input and metrics are used.
- who is responsible for determining if the roll should be aborted / rolled back
- clear plans for aborting and rolling back if the breakage is determined to be unacceptable.

Many of these are related to:
SAC063 Recommendation 3: ICANN staff should lead, coordinate, or otherwise encourage the creation of clear and objective metrics for acceptable levels of “breakage” resulting from a key rollover.
SAC063 Recommendation 4: ICANN staff should lead, coordinate, or otherwise encourage the development of rollback procedures to be executed when a rollover has affected operational stability beyond a reasonable boundary.

It is very likely that the keyroll would proceed with minimal breakage, but making this decision with more than an informed guess seems prudent.

The problem in the room is one of feedback and measurement. It is acknowledged that there are a set of DNS resolvers that perform DNSSEC validation that do not use RFC5011 managed keys and these resolvers will fail if they are not updated manually with new key values in time when the outgoing key is no longer used to sign the ZSK.

The document should explicitly note the measurement and feedback problem, and canvas options that would allow measurement. Approaches such a sentinel record signed with the incoming key, self reporting of TAs by validating resolvers or staggered deployment are options here; but the document does not consider them, nor does it explicitly state if such approaches are infeasible.

Communications.

Recommendations #2, #3 and #9 all relate to communication. For example, "Recommendation 9: ICANN, in cooperation with the RZM partners, should design and execute a communications plan to raise awareness of the Root Zone KSK rollover, including outreach to the global technical community through appropriate technical meetings and to "channel partners" such as those identified in this document."

This is very similar to the first recommendation in SAC063, published in November 2013, which states, "Recommendation 1: Internet Corporation for Assigned Names and Numbers (ICANN) staff, in coordination with the other Root Zone Management Partners (United States Department of Commerce, National Telecommunications and Information Administration (NTIA), and Verisign), should immediately undertake a significant, worldwide communications effort to publicize the root zone KSK rollover motivation and process as widely as possible."

Section 6.5.1 expands on the recommendation, and says: "Awareness ought to be raised within technical forums such as those at which the original deployment of DNSSEC in the Root Zone was presented."

I believe that this is insufficient. Since the original deployment of DNSSEC there has been significant outreach (for example, the "DNSSEC Workshop" held at ICANN meetings, the very effective "Deploy360 Programme" (http://www.internetsociety.org/deploy360/dnssec/), the DNSSEC requirement in TLDs, the DNSSEC requiements in the 2013 RAA, significant outreach and presentations in operator meetings, the US "FCC DNSSEC Implementation Guidlines for ISPs" (http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf)). A number of Operating System distributions and Customer Premises Equipment include validation resolvers. This means that DNSSEC is much more widespread than just amongst a few DNS geeks who hang around in technical forums. Because DNSSEC is now so widespread, the outreach should be expanded as well.

SAC063 Recommendation 1 states that "Internet Corporation for Assigned Names and Numbers (ICANN) staff, in coordination with the other Root Zone Management Partners (United States Department of Commerce, National

Telecommunications and Information Administration (NTIA), and Verisign), should **immediately** undertake a **significant, worldwide** communications effort to publicize the root zone KSK rollover motivation and process as **widely as possible.**" (emphasis added).

ICANN and the root zone management partners need to publicly broadcast the message that when the KSK is rolled, companies' and individuals validating resolvers may stop working, how to determine if a validating resolver is being used, how to determine which trust anchor is being used, and how to make the necessary changes. This is a very big undertaking and a public awareness and understanding is key to the KSK rollover going smoothly and not creating mass outages.
While there are automated ways to update the root KSK, for example RFC5011, we have no way of knowing which systems implement these and subsequently no way of predicting the scale of systems on which this will not work.

Operating outside the DPS.
Definition of DPS: This is described as a document describing specifics of DNSSEC processing; I believe a better description of a DPS comes from RFC6841 (A Framework for DNSSEC Policies and DNSSEC Practice Statements) which says that a DPS provides "a means for stakeholders to evaluate the strength and security of the DNSSEC chain of trust, an entity operating a DNSSEC- enabled zone may publish a DNSSEC Practice Statement (DPS), comprising statements describing critical security controls and procedures relevant for scrutinizing the trustworthiness of the system.
…
The DP and DPS are not primarily aimed at users who rely on signed responses from the DNS ("relying parties"); instead, their audience is other stakeholders of the DNS infrastructure, a group that may include bodies such as regulatory authorities."
It is, in essence, a statement on the keys are stored and protected, and provides the basis for stakeholders to actually trust the keys.

The current root DPS says: "**6.5. Key signing key roll-over**
"Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.

"The current root key was generated 2010-06-16, more than 5 years ago, and we do not have a new key, nor a firm schedule on when it will be rolled. Not complying with such a simple part of the DPS, nor even clearly acknowledging that we are operating outside of its parameters, brings the entire document, and reason for trusting the key, into question. This fact was also noted in the IANA "Consultation on Root Zone KSK Rollover" (https://www.iana.org/reviews/ksk-rollover-201303), There is no specific urgency now, other than if one is going to publish a DPS (essentially a contract with people relying on the key's security), one should abide by it.

i.e. ICANN should acknowledge the fact that they are slipping behind the implicit schedule as per the DPS, and either provide a schedule for the roll, or note the particular activities that will lead to a schedule.

Other

Recommendations #11, #12 recommends that "ICANN should coordinate with RSSAC to request that the root server operators carry out data collection…" and that "When DNSSEC was initially deployed in the Root Zone, a substantial data collection exercise was carried out, and the resulting data proved useful in off-line analysis of the reaction of the DNS as a whole to the structural changes taking place in the Root Zone, including analysis by third parties, facilitated by DNS-OARC. A similar exercise is warranted for the first KSK rollover.”.
(This is almost identical to SAC063 “Recommendation 5: ICANN staff should lead, coordinate, or otherwise encourage the collection of as much information as possible about the impact of a KSK rollover to provide input to planning for future rollovers.”)
I am perturbed that since the publication of SAC063 there is not more detail provided about what specifically should be collected.

Recommendation #5: The current level of transparency has not been held to as high a standard as ideal. For example, most of the transparency is achieved through public key ceremonies, so that the public may observe that the key ceremonies are being properly performed. These have been announced publicly only a day or two prior to the ceremony[1]. This doesn’t give the community that may be interested in watching sufficient notice.
These ceremonies are archived, but until very recently the information was not very well organized or presented (e.g: from KSK Ceremony 1 (http://data.iana.org/ksk-ceremony/1/) to 16 (http://data.iana.org/ksk-ceremony/16/)).
This does not really give the impression that ICANN / the IANA wants the ceremonies to be observed. To improve public perception the following could be considered: documenting the number of external observers of the video stream, widely distributing the details of when the ceremony will be performed in advance, and continuing to use the HTML format for ceremonies 17 onwards (instead of the old non-HTML format for earlier ceremonies).

Summary:

Root key rollover is important (and needs to be performed at some point), but contains considerable risk. We do not wish the keyroll to be rushed, but are concerned that we have not seen continuous, focused progress on implementing the previous recommendations.

[1] This has since been improved.

Issues arising from the keyroll have the potential to create incredibly poor press for ICANN, and could significantly hurt the deployment of DNSSEC.

Understanding what feedback has been accepted or rejected, determining methods to better evaluate the impact before, during and after the keyroll, and publicize and educate both what the root key rollover means and when the ceremony will be, believed to be key to this project's success.

Warren Kumari
(as an individual, not as a Google employee, member of ICANN SSAC, RSSAC Caucus, IETF participant, ICANN Technical Liaison Group member, etc.).