The ICANN GNSO "Business Constituency"

Comment on Plan to Restart the Root Key Signing Key (KSK) Rollover Process

Status: FINAL

Version: 3

2-Apr-2018

Business Constituency Submission

GNSO//CSG//BC

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter:

The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

BC comment on Plan to Restart the Root Key Signing Key (KSK) Rollover Process (the Draft Plan)[1]

We appreciate the cautious approach undertaken by ICANN in 2016, delaying initial plans for the Root KSK Rollover to study and address potential adverse impact to Internet users, as well as the inherent complexity in measuring and estimating that impact. The choice to further delay the rollover or proceed and accept current risk estimates is a challenging one, with risks on both sides. Further delay may risk erosion of trust in DNSSEC (as the rollover was initially targeted to occur in 2015).

However, the degree of impact is still uncertain. If significant breakage occurs and the rollover is perceived to have been rushed, then, in addition to the outages and enforced recovery of operations, there is the potential of negative press and a perception that these issues may have been avoidable.

Just as the risk to trust is impossible to quantify, the impact of the rollover not working for a large number of resolvers is also difficult to estimate. The number of resolvers impacted are a poor proxy, given dramatic differences in their end user reach, and it is grossly impractical to attempt to directly measure impact to an Internet population of over four billion users.

Taking these tradeoffs and considerations into account, we believe that further delay and analysis may be warranted, especially when better measurement methods become available to understand the risk, and more robust project planning is carried out.

Limitations of Available Data to Support Restart of Rollover

The three-page Draft Plan notes:

> *"Even after a concerted effort, ICANN org could often not determine which resolvers sent the message (such as when the resolver had a dynamic address), so there was no way to determine how many users would be affected by the rollover or why those resolvers had not updated their trust anchors. Additionally, even when ICANN org could identify the specific resolver, efforts to contact the operator were often unsuccessful."*

[1] See ICANN public comment page at https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en

In light of the fact that ICANN is unable, at this point, to assess the impact of the rollover, the BC would like to understand: Why is there is a rush to proceed with the restart?

Instead, why isn't further research into the state of resolvers and how many users would lose access to the DNS as a result of the rollover being done? The BC requests ICANN org fully consider and respond to these questions before taking further action.

Given the limitations of current research methods, we understand the challenges ICANN faces both in estimating potential breakage, as well as in establishing usable metrics for assessing the success or failure of a transfer once initiated. There are signs, however, that a future protocol is in development that could improve upon the current lack of understanding of the likely level of breakage, and provide clues for how to mitigate it. As noted in the Draft Plan:

> *"There was wide agreement during the discussion that there is no way to accurately measure the number of users who would be affected by rolling the root KSK, even though better measurements may become available for future KSK rollovers. There was also discussion of a future protocol, A 5 Sentinel for Detecting Trusted Keys in DNSSEC, that might give more valuable information for future root KSK rollovers. That in turn, prompted a discussion about how long it might take to standardize and deploy such a protocol."*

Based upon our preliminary review, we believe that allowing time to deploy the KSK sentinel and apply relevant learnings would be more prudent than proceeding with the current dearth of information. As far as is possible, the timing of the rollover should be a data-driven decision, although it appears neither the CTO's office nor the community is satisfied with the data that is currently available. At minimum, these options should be more fully outlined in the Draft Plan for meaningful community review and comment.

Comprehensive Updated Plan Needed

The incomplete nature of the Draft Plan in its current form also raises procedural concerns. While it is our expectation that ICANN would apply similar timelines and considerations as outlined in the 2016 KSK Rollover Plan, this is not explicitly stated. The Draft Plan does not endeavor to map the initial, detailed timeline to the rescheduled transition. Nor does it explicitly state whether similar processes for contingency planning will be applied. For example, the concept of rollback in the event that serious negative effects are realized is not even mentioned in the updated three-page Draft Plan. ICANN should provide a comprehensive updated plan to the community to ensure transparency and consistency of expectations, as well as to allow for robust community comment.

Lastly, while the report cites data from research carried out by the Office of the CTO, this data is not available for community review. This information should similarly be put forward for community review and comment. Alternatively, if there is a rationale for why the information has been withheld, that justification should be made known to the community.

We appreciate the complexity of the issue at stake and urge ICANN to continue to proceed with care in planning the Root KSK Rollover, including contemplating further delay.

--

This comment was drafted by Denise Michel and Stephanie Duchesneau.

It was approved in accord with the BC charter.