**Subject:** Business Constituency (BC) comment on the Proposal for Future Root Zone KSK Rollovers
**Date:** Wednesday, January 29, 2020 at 5:34:34 PM Eastern Standard Time
**From:** Steve DelBianco
**To:** comments-proposal-future-rz-ksk-rollovers-01nov19@icann.org
**CC:** BC List

Below (and attached) is the comment of ICANN's Business Constituency (BC), on the Proposal for Future Root Zone KSK Rollovers.

Understandably, the Root Zone KSK serves as the trust anchor for DNSSEC and is managed as part of the IANA functions, performed by ICANN through its affiliate, the Public Technical Identifiers (PTI).

Having commented on 2-Apr-2018 on the need for a comprehensive KSK Rollover Plan, the BC is pleased with the detailed plan outlined in the Proposal, noting that:

1. A three-year rollover interval strikes a responsible balance between ensuring that procedures and software remain sufficiently agile to adopt new keys as they are commissioned.

2. A three-year rollover interval will also assist in developing institutional memory of all participants in the process.

3. A new KSK should be generated well before it signs the zone and is published.

We have some concern with risk associated with publication of the new KSK algorithm, which is 2-years before it is used. In this regard, we recommend that the recipients of the publication should be those that are most concerned with the KSK process and that a Memorandum of Understanding (MOU) be signed in this respect.

On the KSK lifecycle, we observed that a fourth cycle might be missing and that is the Key **Replication** process after the Key has been Created. We note that if the Key is Created and it is not Replicated, there can be no Signing, hence a proposed improvement in the lifecycle as follows:

Creation
**Replication**
Signing
Destruction

**Endorsement of the 8 Distinct KSK Phases**

KSK rollover refers to the process of switching the active KSK from one key to another, and includes pre-publication of the new key in a manner that allows it to be trusted, processing updates to the root zone trust anchor, introducing a new KSK in the root zone, and retiring the previous KSK. As such, the BC endorses the retention of the eight distinct phases (A-H) which constitute the current approach. We further recommend that the need to keep to the phased timelines be a subject of the MOU earlier proposed for signature of concerned parties.

Finally, the BC appreciates the high level of transparency embedded in the process which includes third party audit; notes as currently safe the 2048-bit RSA keys that are used; and anticipates the continuation of the periodic community engagement process associated with the KSK Signing process.

--
This comment was drafted by Jimson Olufuye and was approved in accord with our charter.

--
Steve DelBianco
Vice Chair for Policy Coordination
ICANN Business Constituency (BC)