Questions and Answers on COVID-19 mitigations for KSK Ceremony 41

The root zone key-signing key ceremony scheduled for 23 April 2020 is being planned with a reduced agenda and with minimal in-person participation to limit risks associated with the COVID-19 pandemic. These questions and answers reflect the key considerations that went into the ceremony's planning and the common questions we have been receiving.

How will this ceremony be conducted differently?

- Only a minimum number of staff will be present in the ceremony room. These essential staff members will use personal protective equipment while on site, and will maintain physical distance from one another as much as possible.

- The ceremony is being held in the key management facility in El Segundo, California instead of the originally scheduled location of Culpeper, Virginia. These two key management facilities are duplicates of one another and either can be used, although normally we alternate between the two facilities.

- Four trusted community representatives (TCRs) who fulfil Cryptographic Officer roles in the ceremony have transmitted their safe deposit keys to separate ICANN and PTI staff. These staff will act as surrogates, but the TCRs will participate in the ceremony remotely and monitor their credential's use.

- Verisign, whose role during the ceremony is to verify the authenticity of the key signing requests, will conduct their role remotely.

- RSM, the independent auditor, will monitor the ceremony remotely, and be availed of all the materials from the ceremony in order to conduct its assessment against the SOC 3 framework.

- Typically a key signing ceremony generates a single calendar quarter of signatures used to sign the root zone, whereas this ceremony will generate signatures for three calendar quarters. The additional generated signatures will be initially withheld, and then transmitted to Verisign at the time required per the DNSSEC Practice Statement.

- Non-essential work that was planned for the ceremony will not be performed. This additional planned work was to induct a new hardware security module (HSM) as part of our normal hardware renewal process, and replacing two TCRs who were planning to retire from their roles. This work will be deferred.

What is not changing for this ceremony?

- The ceremony will still be held at the same date and time (23 April 2020, 1700 UTC).

- The ceremony will be conducted in a manner that ensures the fundamental security objectives are still met. For example, the critical elements like the HSM and the smart cards will be under full camera supervision from multiple angles for the duration of being removed from their protective enclosures.

- The ceremony will be livestreamed for anyone to watch in real time on Youtube.

- A ceremony script will be published online for anyone to review before the ceremony date, and an annotated script will be published post-ceremony for audit purposes.

- Artefacts such as the operating system DVD, key signing software, audit logs and raw audit camera footage will be posted online after the ceremony.

Why has the ceremony been relocated to a different facility?

Our location in El Segundo allows us to hold a ceremony without any of our staff needing to fly to the facility, as it is close to ICANN's Los Angeles office. This option reduces the risk of staff exposure to contracting COVID-19 by avoiding unnecessary exposure through air travel.

How will the safe deposit keys sent by the TCRs be protected?

The TCRs have wrapped their deposit keys with opaque material, and then transmitted them in tamper-evident bags. This bag will not be opened until within the ceremony so that each TCR can witness their key is in the same condition as when they released it. At the conclusion of the ceremony, the four keys will be similarly wrapped and then entrusted to four staff members who will independently arrange for them to be couriered back to their respective TCRs. Our objective is to return them to the TCRs as quickly as possible, allow the TCRs to remotely witness all usage of their keys, and to be able to account for the complete chain-of-custody throughout the entire process.

How will communication with remote trusted witnesses be conducted in the ceremony?

In addition to our normal method of broadcasting the ceremonies live on Youtube, we will additionally be providing the personnel who would normally be physically present at the ceremony a side channel to communicate with the ceremony administrator during the ceremony. Our goal is to provide the normal capability for the trusted community representatives, the auditors and others to interject, make recommendations, and so on.

Why are you signing additional key signing requests?

This allows for greater flexibility in planning ceremonies for the remainder of the year, or circumventing them entirely if health advisories continue to recommend avoiding gathering people together. The additional signatures that are generated will not be disclosed until needed.

How will the signed key responses be stored post-ceremony?

Our security controls result in us only supplying Verisign with the signatures they need in three month increments. As this ceremony will generate nine months of signatures, the additional six months of key material will be securely stored in ICANN facilities and released to Verisign during the normal time window when the ceremonies would have been held later in the year. ICANN maintains a small-form key management facility in its Los Angeles office with similar controls (such as requiring dual occupancy and segregation of duties) that can be used to store these assets until they are needed.

Are there any implications for the SOC 3 audit?

We have discussed our plans with our independent auditor to ensure that the changes we are making continue to meet our requirements against the trust service principles.

What is the impact on the DNSSEC Practice Statement (DPS)?

The only element of our revised approach that was inconsistent with the DPS was signing additional quarters of KSRs during the ceremony. The Policy Management Authority, an internal committee that reviews changes to the DPS, convened on 6 April and approved revisions that allow for signing additional quarters of KSRs as a disaster recovery response.

Why will there be no TCRs present in the room?

There are no trusted community representatives for the El Segundo facility that were located close enough to allow unrestricted and safe travel to the facility. The TCRs for El Segundo are located in Mauritius, Spain, Russia, Tanzania, Uruguay and east-coast United States.

Could new TCRs have been inducted for this ceremony only?

This was considered, but it was deemed impractical to identify qualified experts that could meaningfully oversee the ceremony that were located in Los Angeles and that could go through the background check process conducted for trusted community representatives. We are confident that the TCRs can meaningfully discharge their responsibilities remotely, and are augmented by many other controls including oversight by the independent audit firm RSM.

Can you access your secure facility given the restrictions on movement?

We have received a special waiver to enable access to the facility despite it being contrary to limits that have been put in place by our vendor. Relevant government agencies have been briefed on our need to hold the key signing ceremonies, and processes are available to us to enable access should it be needed. We have faced no difficulties in having our vendors recognize the need for us to perform the ceremony, however.

Could the ceremony have been rescheduled?

Yes, but not by a sufficient amount that would give us confidence that the ceremony could be held in a normal manner. While there is flexibility inherent in the schedule to allow moving the ceremony a few weeks in either direction, a ceremony still needs to be held sooner than it is expected COVID-19 restrictions will be lifted. The last of the signatures generated at the previous ceremony will expire at the start of July 2020.

Will additional ceremonies be held later in 2020 if circumstances improve?

This is not decided. Should conditions improve and allow us to safely hold ceremonies later in 2020, we will consult with the potential attendees to make an assessment on whether to hold the ceremonies. While such ceremonies would not be strictly necessary for key signing purposes, they would allow us to implement the other deferred ceremony items.

Do you need to drill into the safe deposit boxes?

No. The first version of our contingency plan assumed the trusted community representatives would not transmit their safe deposit box keys for performance of the ceremony. In such a scenario, a trained locksmith would drill and replace the locks to three safe deposit boxes during the ceremony in order to retrieve the smart cards needed to activate the hardware security module. This is no longer being contemplated as the trusted community representatives indicated they broadly supported transferring their safe deposit keys by international courier as the preferred approach.

What outreach was performed on the changes you’ve made?

In preparing this approach, staff engaged with:

- those scheduled to take part in the April 2020 ceremony;

- the third-party auditor;
- the root zone maintainer;
- the vendors that support the key ceremonies;
- the trusted community representatives and former ceremony attendees;
- ICANN’s Root Zone Evolution Review Committee, comprised of representatives of ICANN’s various sponsoring organizations and advisory committees;
- the DNS-OARC operations mailing list;
- the KSK Rollover project mailing list; and
- the ICANN Board of Directors

General notice of this approach was also provided to our public announcement mailing list, comprised of around 700 subscribers interested in Root KSK management.

Discussions focused on the viability of elements of the proposal, their impacts on operations and the control environment, and steps necessary to retain the high levels of trust that ICANN enjoys with respect to how it manages the KSK.