ICANN BOARD PAPER NO. 2020.04.16.1a

TITLE: **Contingency Plans for Key Signing Key Ceremony**

PROPOSED ACTION: **For Board Consideration and Approval**

EXECUTIVE SUMMARY:

- ICANN, through PTI, must regularly generate cryptographic signatures that allow the root zone to be properly authenticated using DNSSEC. This work is currently performed every three months using "key ceremonies" involving trusted community representatives from throughout the world.

- The Coronavirus pandemic challenges our capability to perform these key ceremonies according to policy, predominantly due to travel restrictions, plus a desire to comply with guidance to limit gatherings of people.

- Staff recommends endorsing a graduated set of options based on the capability of parties to attend and ongoing monitoring of the evolving situation, with decision criteria for each of the options. We also recommend extending the period for which cryptographic signatures are generated to better guard against volatility.

- Inability to conduct the next key ceremony would result in widespread DNS resolution failure globally in July 2020 as DNSSEC would cease to function. A lack of timely cryptographic signatures would mean that DNSSEC-enabled devices could no longer resolve any domain names.

ICANN ORG RECOMMENDATION:

ICANN org recommends the Board endorse the proposed contingency plans for holding the KSK ceremony. We believe that the proposal strikes a responsible balance that best ensures the KSK ceremony can be held.

PROPOSED RESOLUTION:

Whereas, ICANN, through its affiliate PTI, must regularly generate cryptographic signatures that allow the root zone to be properly authenticated using DNSSEC. This work is currently performed every three months using "key ceremonies" involving trusted community representatives from throughout the world, governed by the DNSSEC Practice Statement.

Whereas, in December 2019, a new strain of coronavirus, causing a disease referred to as COVID-19, emerged and on 30 January 2020 was declared by the World Health Organization (WHO) as a public health emergency of international concern. On 11 March 2020, the WHO publicly characterized COVID-19 as a pandemic.

Whereas, the COVID-19 pandemic challenges ICANN's ability to perform the key ceremonies according to policy, due to global travel restrictions and guidance from governments and health authorities to limit gatherings of people.

Whereas, in the face of the COVID-19 pandemic, ICANN has developed contingency plans with a graduated approach to holding the key ceremony, initially providing for maximum participation, and incrementally deciding upon alternatives if participation is not possible.

Whereas, there is sufficient uncertainty whether a subsequent ceremony can be held in an orderly manner later in the year, and there are options under consideration that will reduce this risk by holding a ceremony that produces cryptographic signatures for an extended period of time.

Resolved (2020.04.16.xx), the Board finds the contingency plans to be in the best interests of ICANN and in the global public interest, and authorizes the President and CEO, or his designee(s), in consultation with the PTI President, to take all necessary steps to perform the key signing ceremonies as provided in the contingency plans.

PROPOSED RATIONALE:

1. Introduction

The Root Zone Key Signing Key (Root KSK) is managed using a system that deliberately disperses a number of trusted roles both logically and geographically as a security measure that is designed to reduce risk of collusion between parties to perform unplanned activity. In normal operations, many of these trusted role-players need to converge at one of two ICANN-managed sites (key management facilities, or KMFs) to perform "ceremonies" where each performs their role to perform essential KSK procedures, typically once every three months.

Due to the 2020 Coronavirus pandemic, ICANN org staff's mobility has been curtailed and other companies that supply these trusted roles are enacting similar policies. Further, governments have implemented travel restrictions that have a similar effect of reducing mobility. There is a significant risk that these events reduce participation below minimums that harm KSK management. Without effective contingency plans, the inability to perform successful KSK operations would ultimately mean a widespread catastrophic failure of the DNS.

2. Board Remit

The Board's action on this matter is in-line with precedent concerning significant decisions around the operations of the DNSSEC key signing key that could have widespread community impact. In the past, the ICANN Board adopted a resolution authorizing proceeding with the first key-signing key rollover.

3. Proposal

The Board's action today is to authorize the President and CEO, in consultation with the PTI President, to take all necessary steps to perform the key signing ceremonies as outlined in the following contingency plans. The ceremony management approach in the contingency plans contains two key components:

1. A graduated approach to holding the ceremony, initially providing for maximum participation, and incrementally deciding upon alternatives if participation is not possible.
2. Seek to implement a contingency to sign for additional quarters at the next ceremony, which will provide operational resilience against a period of anticipated high volatility.

The associated procedures and policies were updated to reflect these new procedures during a meeting of ICANN's Policy Management Authority on 6 April 2020. In particular, the DNSSEC Practice Statement[1] (DPS) formally governs how KSK management is performed, and has been revised to allow for implementation of the presented options following proper authorization by management.

3.1 Planned scenarios for holding KSK Ceremony 41

The graduated approach consists of four options, ranked from most desirable to least desirable. Each has associated conditions and approval processes for moving to the next option:

3.1.1 Option A: Hold the April 2020 Ceremony as planned

The 41st KSK ceremony is currently scheduled for 23 April in Culpeper, Virginia. The ceremony can continue to be held that date according to normal procedure if the minimum number of attendees are present, including three trusted community representatives.

Key risks: Holding the ceremony as planned relies on international mobility of trusted community representatives which is currently severely compromised, and the future evolution of these restrictions is unpredictable. Staff mobility is also impacted domestically.

[1] https://www.iana.org/dnssec/dps

Proceeding to Option B: If in the judgment of the President of PTI the situation does not stabilize with a high-level of confidence the ceremony can be held as scheduled, Option B shall become the preferred option.

3.1.2 Option B: Hold the ceremony with only US-based personnel

Three of the seven trusted community representatives for the Culpeper location are based in the US, two on the east coast and one on the west coast. Only two of the three can attend the ceremony scheduled for the selected date, so this option would identify an alternate date that can be attended by all three.

Key risks: This option relies upon ongoing domestic mobility of trusted community representatives and staff. It also assumes necessary personnel do not get sick or otherwise cannot attend, as there is no safety margin for non-attendance.

Proceeding to Option C: If in the judgment of the President of ICANN the ceremony cannot be committed to with a high level of confidence or otherwise cannot be executed by May 8, Option C becomes the preferred option.

3.1.3 Option C: Hold the ceremony only with Los Angeles based personnel and minimum in-person participation

The KMFs were expressly designed to allow for staff-only ceremonies in a disaster recovery ceremony to ensure key ceremonies are held as needed. The minimum essential personnel could perform a key ceremony in our El Segundo KMF on short notice. This would, however, not have the required number of trusted community representatives present in-person.

Key risks: This option requires a minimum number of staff and contractors to be available (i.e. not incapacitated or restricted in movement). It breaches the standard expectations on participation in key ceremonies, but is considered an option within scope of the disaster recovery procedure.

Proceeding to Option D: If the ceremony cannot be conducted by June 19, Option D becomes the ultimate option. The Board of ICANN shall make the final determination to move to Option D.

3.1.4 Option D: Suspend signing of the DNS root zone

This is the final option if there is no conceivable way to activate the KSK and perform signing operations. There would need to be a massive education campaign at short notice to have resolver operators disable DNSSEC validation. There is a high risk of widespread outages as it is not possible to ensure global implementation, and high risk this will fatally compromise trust in DNSSEC in general as a technology.

This is considered highly unlikely, but nonetheless the final option. Without exercising the option, in the absence of a successful key signing ceremony, DNSSEC validation would be unsuccessful starting in July 2020.

3.2 Sign key material covering two calendar quarters

A standard key ceremony generates signatures that cover one calendar quarter (3 months). Generating signatures that cover additional calendar quarters in this key ceremony will provide greater resilience to root zone operations during a period of ongoing uncertainty. Should a prolonged threat materialize, this additional time will allow for consideration of long-term changes to the current key ceremony model if necessary.

Based on the feedback from the trusted community representatives, we expect to generate signatures for three quarters, covering nine months. Such an action would relieve the need to hold a key signing ceremony for the remainder of 2020, therefore the next ceremony would be needed around February of 2021. The key material for the additional quarters would be held securely by ICANN and released to the Root Zone Maintainer in accordance with the normal schedule.

4. Stakeholder Consultation

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; and
- the DNS-OARC operations mailing list; and
- the KSK Rollover project mailing list.

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.

5. Fiscal Impact

This proposal is not anticipated to have a material fiscal impact beyond normal operational costs associated with KSK management.

6. Public Consultation Requirements

This matter relates to IANA Naming Functions operations, performed by PTI under contract from ICANN. Procedures that are used in KSK operations must be approved by the Policy Management Authority, an internal ICANN Org committee. There is no formal public comment requirement, however, IANA staff will continue to consult with the trusted community representatives and other stakeholders to implement and adapt these plans. A communications strategy will be developed to support awareness of any operational changes and impacts.

7. Public Interest

The Board's action is within the public interest and within ICANN's mission as it will help to continue to ensure the stable and secure operation of the Internet's unique identifier systems. The inability to conduct the next key ceremony would result in widespread DNS resolution failure globally in July 2020 as DNSSEC would cease to function. The Board's action will help ensure that DNSSEC-enabled devices will be able to resolve any domain names.

8. Key Risks

The following risk considerations were factored into the Board's deliberations on this action.

8.1 Travel of attendees is interrupted

The primary risk that this plan is designed to address is the inability of attendees to attend the key ceremony. The suggested mitigation is the graduated approach to different options to hold the ceremony, up to and including holding a ceremony only with staff in the Los Angeles metropolitan area, that will not require air or interstate travel.

8.2 Facility operator suspends access to facility

The company that provides the facilities in which the KMFs are based may suspend access as part of their response to the pandemic. The suggested mitigation would be to advocate to their senior management, through trusted proxies if necessary, to make an exception given the requirement to hold this ceremony to support critical Internet infrastructure and Internet operation. ICANN has been in discussion with the US Government about issuance of special guidance should it be necessary to retain the access needed to perform the key ceremony.

8.3 Government suspends access to the facility, and/or constrains travel

Governments at different levels may impose restrictions on travel or gatherings that impede the ability to hold the ceremony. ICANN can advocate for

exceptions to be made through the appropriate channels, as described in the previous section, noting the requirement to hold this ceremony to support critical Internet infrastructure and Internet operation. In particular, ICANN has existing relationships with governments that can be used to seek such exemptions.

8.4 Staff become ill or otherwise indisposed

The minimum essential personnel may be incapable of performing the ceremony because they themselves are ill, quarantined or otherwise unavailable. The primary mitigation is PTI staff and other support staff from ICANN Org have been implementing social distancing since the beginning of March 2020 to limit potential transfer of illness. Additionally, there is approximately a three-month window to traverse the options presented, with sufficient slack to allow the exact date within each option to be adjusted to allow for recovery and still be held.

8.5 Option C undermines community trust in KSK stewardship

Holding a ceremony without the standard protections, including third-party community witnesses physically in the KMF, may dilute trust in the management and stewardship of the KSK. To mitigate this, the ceremony would still be conducted to audit standards, under supervision of a third-party auditor, and all materials (including comprehensive audit footage and ceremony artefacts) would be posted online as is standard. Live streaming of the ceremony would be provided and enhanced to allow those not present to observe and interject with concerns or questions. TCRs and other stakeholders have been consulted on how to conduct an Option C ceremony so it is performed to their maximum satisfaction given the necessary constraints. We would strive to obtain buy-in from TCRs and other stakeholders that this would be the right compromise given the alternatives.

Signature Block:

Submitted by: Kim Davies

Position:	Vice President, IANA Services; President, PTI
Date Noted:	6 April 2020
Email:	kim.davies@iana.org

REFERENCE MATERIALS – BOARD PAPER NO. 2020.04.16.XX

TITLE: Contingency Plans for Key Signing Key Ceremony

The following provides additional background information regarding KSK Key Signing Ceremonies, including the participation requirements and roles of those participating.

1 Ceremony Participation Requirements

The roles needed to perform a routine key ceremony are as follows, along with the number required to be physically present (per the DPS and associated procedures):

Role	Standard	Minimum	
Cryptographic Officers	5	3	Community volunteers, geographically dispersed
Ceremony Administrator	2	1	ICANN staff (alternative procedures needed if only 1 due to dual-occupancy requirements)
Internal Witness	2	1	ICANN staff (alternative procedures needed if only 1 due to dual-occupancy requirements)
Safe Security Controller	2	2	ICANN staff.
System Administrator	2	0	ICANN staff. Other roles can do double duty as System Administrator in dire situations.
Root KSK Operations Staff	2	1	ICANN staff. Also serve as relief Ceremony Administrator and Internal Witness if needed.
Root Zone Maintainer staff	2	0	Verisign staff. May participate but can do so virtually, with prior preparation
Third party auditor	2	0	RSM (audit firm) staff. Potential for remote participation.

Physical Access Control Manager	1	0	ICANN staff. Work is performed remotely.

2 Breakdown of personnel locations

2.1 Cryptographic Officers

Three of seven cryptographic officers are needed to perform a ceremony in their respective facilities. Roles fulfilled by "trusted community representatives" (TCRs) may not be interchanged with those from another facility without a prior credential swap.

- KMF West (El Segundo, California): Mauritius, Portugal, Russia, Tanzania, Uruguay[1] (×2), United States (Maryland).
- KMF East (Culpeper, Virginia): Brazil, Netherlands, Togo[2], Sweden[3], United States (×3, Philadelphia, Seattle, Virginia)

2.2 Ceremony Administrator

There are qualified ceremony administrators on staff based out of the Los Angeles (LA) and Washington (DC) ICANN offices. There are former ceremony administrators on staff that could be re-provisioned into the role, plus PTI staff are capable of stepping into this role if emergencies dictate.

2.3 Internal Witnesses

There are qualified internal witnesses based out of the LA and DC ICANN offices. There are former internal witnesses on staff that could be re-provisioned into the role, plus PTI staff are capable of stepping into this role if emergencies dictate.

---

[1] One Uruguay-based TCR joined ICANN staff on 16 March 2020, and is therefore disallowed to act as a TCR due to conflict-of-interest, and will be replaced at the earliest opportunity.

[2] TCR has signaled their desire to retire from this position, and was originally scheduled to be replaced with a backup TCR from Sri Lanka during this ceremony.

[3] TCR has signaled their desire to retire from this position, and was originally scheduled to be replaced with a backup TCR from the Czech Republic during this ceremony.

2.4 Safe Security Controllers

Two are needed for a given facility, one for each safe. These roles are not interchangeable; however, exact personnel could be re-provisioned.

KMF West (El Segundo, California)		KMF East (Culpeper, Virginia)	
Safe 1	Safe 2	Safe 1	Safe 2
2 in Los Angeles metro area	2 in Los Angeles metro area	1 in Chicago 1 in Northern California	2 in Washington DC metro area

2.5 System Administrators

There are qualified ceremony system administrators on staff based out of the LA and DC offices.

2.6 Root Zone Maintainer

The RZM staff are based out of Reston, Virginia, proximate to KMF East. Participation by RZM staff can be virtual by prior arrangement.

2.7 Physical Access Control Managers

The two PACMs are both located in the LA office. They are not required to be physically present but must be available to arrange privileged access to the KMF for all other trusted roles.

3 Ceremony Timing Requirements

Each ceremony's baseline requirement is to sign key material that is valid for the subsequent calendar quarter. For example, the key ceremony held in the 1st Calendar Quarter of 2020 (around February) signs material that will be used in operations in the 2nd Calendar Quarter of 2020 (from April to June 2020).

The DNSSEC Practice Statement stipulates key ceremonies shall be conducted "no later than 33 days" before the start of the subsequent calendar quarter. While this window is

potentially adaptable through a change to the DPS, real-world logistics also inform the window in which the ceremony can be held. The Root Zone Maintainer requires time to process the key material and perform its own testing before using it in operations.

The selection of a quarterly cadence is a balance between limiting the duration of pre-generated signatures against the complexity of holding key ceremonies. Generating signatures for extended periods of time weakens security as there is a vector of compromise that cannot be contained if those signatures are disclosed.

4 Existing contingency procedures

One of the operational procedures is the "Root Zone KSK Operator Function Disaster Recovery and Business Contingency Procedure". This is reviewed at least once annually, and approved by the Root KSK Policy Management Authority (PMA)[4].

The procedure considers three scenarios in-scope, one being directly relevant:

"KSK Signing Disaster: Unable to produce a Signed Key Response (SKR) in time using either site within the 90-day quarter before the Resource Record Signature (RRSIG) on the Domain Name System KEY (DNSKEY) RRSIG expires"

The disaster recovery scenarios in this procedure spell out the steps that need to be taken, but do not define formal decision making processes around these events. It generally empowers the cryptographic key managers within PTI staff (formally known as the Root KSK Operations Security, or RKOS) to make the determination such a disaster has occurred, and to take the necessary steps. The current procedure contains no nuanced decision points that involve different levels of approval depending on the specific nature of the event, however adoption of this graduated contingency approach will be reflected in revised procedures.

5 Considered contingency options

[4] The PMA is a committee of representatives from multiple ICANN departments that meets at least once a year to, at a minimum, review and approve KSK management procedures.

This is not an exhaustive list of all possible options, but represents some key areas explored.

5.1 Ceremony rescheduling

Ceremonies are scheduled at an ideal time based on maximum availability of the trusted roles, within the prescribed policy window. They are normally scheduled to provide sufficient schedule slack such that they can be rescheduled successfully without adverse impact.

Advancement. The ceremony could potentially be held earlier, on the assumption there could be less impact on mobility due to the Coronavirus pandemic the sooner it is held.

Postponement. Short-term impacts (lasting no more than a few weeks) could be mitigated through simple postponement. To be compliant with the DPS, the ceremony must happen no later than 33 days before the start of the next quarter. Breaching that provision would still allow operational delivery much closer to the start of the quarter. Verisign has previously indicated that they need the key materials no later than a week before the start of a quarter.

5.2 Relocation of ceremonies to opposite facility

The key management facilities are practically replicas of one another, and while our standard operating procedures result in us using alternate facilities for each scheduled ceremony, this can be adjusted if necessary.

This would mitigate risk relating to the ability of specific individuals to attend to satisfy quorums at one facility only. It does not mitigate risks that impact both facilities. Notably, at present there are three US-based individuals capable of meeting the quorum for the East coast facility, although one is based in Seattle and therefore not proximate to the facility.

Not exercising alternate facilities increases the time between use of the KMF (currently each KMF is used with a 6-month interval), and there is a greater risk of undetected compromise or equipment failure in an individual KMF if it is used less often. Some

TCRs have recently focused on their role of regularly reviewing the chain-of-custody within each KMF as part of their responsibility, and not being able to witness the materials for an extended period means they cannot discharge this responsibility.

5.3 Signing of key material for extended period

Signing key material for a period beyond the subsequent quarter would alleviate the need for key ceremonies to happen as regularly. This would mitigate risk relating to general uncertainty concerning the ability to hold subsequent planned ceremonies.

A revision to the DNSSEC Practice Statement was approved by the PMA to allow for this during disaster recovery operations. Generating additional signatures with no compensating controls lowers the security in the current design which limits the amount of key material provided to the RZM to no more than those needed for a single quarter. However, this is mitigated through withholding the return of the additional signatures to Verisign until they would normally be needed.

5.4 Induct replacement Cryptographic Officers

If travel is prohibitive based on the geographic location of the cryptographic officers (COs), new COs could be inducted as replacements to fulfil the roles of those who cannot travel. There are two ways this can be facilitated:

- An orderly handoff via a trusted mechanism from the relinquishing CO to the new CO. We aim to perform this in a key ceremony context ideally (requires travel), but could be in a third-party locale that both COs can mutually visit with suitable witnesses.

- The relinquishing CO's credential is treated as lost/unavailable. Locksmith reprovisions a new lock assembly for the new CO in a key ceremony. This process has been used twice before when a retiring CO was unable to travel to a final ceremony to perform a hand-off.

There is a potential consideration of always having 3 US-based TCRs for at least one of the facilities that are likely to be able to travel within the country, independent of

international events. By circumstance (due to TCR relocation) this is the current situation, but it is not by design, and the current policies guide us to avoid this scenario due to collusion risk. Further, there is no guarantee that localized quarantines (either within parts of the US, or of the TCR individually) wouldn't cause this approach to fail.

5.5 Increase pool of Cryptographic Officers

The most central trust configuration of the KSK arrangements is the need for 3 of 7 COs to perform ceremonies. Both of these numbers are configurable, but have been selected as a balance of practicality versus risk. Increasing the pool of 7 increases collusion risk, as does decreasing the need for 3; but does provide greater resiliency and likelihood of success in performing ceremonies.

To reconfigure this arrangement requires all 7 of the existing COs plus the entire new class of COs to be present to regenerate all the key shares, therefore this cannot be done during an adverse event, it must be done in advance with maximum attendance (akin to Key Ceremonies 1 and 2 in 2010, when the two facilities were originally commissioned.)

Such a change must be carefully considered. Around five years ago, staff explored re-architecting the CO role to allow sharing of responsibilities between East and West coast COs, but this line of research was criticized by the TCRs and not pursued. Such a system was intended to allow a west coast CO to substitute for an east coast, and vice versa.

5.6 Increase staff pool to minimize travel requirements

Ideally, key ceremonies could be accommodated through only local travel for supporting staff. With sufficient staff roles available near each facility, air-travel would only be necessary for the TCRs performing the CO roles.

Whilst significant progress has been made in this direction, there is insufficient staff with suitable qualifications near both facilities to perform this at this time. Investment could be made to, for example, base PTI staff in the DC office to make it more resilient in this regard if this was considered a priority objective.

5.7 Remote participation by Root Zone Maintainer

Conventionally the root zone maintainer is physically present to perform their role. However, there is precedent for it being remote. Due to a weather emergency, the role has been performed remotely in the past. This does require prior exchange of trust materials before the ceremony, which can be done online.

5.8 Remote participation by auditors

While third-party auditors have been present at every ceremony, and we believe it is important for overall trust to seek this, it is not a fundamental requirement for them to be present. The auditors can satisfy their observations using audit materials tendered after the fact, with possible augmentation through monitoring of a live feed of proceedings.

5.9 Perform ceremony below participation minimums

Ceremonies could conceptually be held without having sufficient number of participants to meet minimums dictated by the policy and design of the system. While such changes would violate policies, this may be assessed as the least-worst option depending on the nature of the situation, and/or be cured through explicit disaster recovery scenarios being added to the policy with the trigger conditions being defined.

Role	What's involved
Cryptographic Officer (TCR)	Drill their individual lockbox to retrieve their secure credential. Have a surrogate use their credential. Mitigate potential risks through 100% audit camera coverage of key share at all times. Likely requires a locksmith to drill and remediate. Requires after-action plan to restore trusted state.
Ceremony Administrator	Can't perform a ceremony without a CA, as the CA does the 'work' of the ceremony.
Internal Witness	Unrealistic to hold a ceremony without an IW, as they perform dual occupancy with the CA. Theoretically, performing a ceremony without dual occupancy means subverting all logical security in the KMF (overriding door locks and ignoring alarms, reprogramming access control system, etc.)

System Administrator	PTI staff or suitably trained personnel could cover for this role, although professionalism of ceremony would be compromised due to regular cessation of activities to juggle responsibilities
Safe Security Controller	Drill safe, obtain materials, and remediate condition afterward. Requires a locksmith to drill and remediate, and will take several days based on February 2020 experience.

5.10 Additional key management facilities

Some risks are shared by both KMFs by virtue of both being in the United States of America. One or more additional KMFs could provide resilience against these risks if located extraterritorially.

The benefits of additional KMFs are offset to some degree by the increased attack surface of more KMFs, the need for additional staffing and significant costs it will incur. It is not a short-term option that can realistically address the immediate Coronavirus pandemic threat due to the extensive work to provision such a facility, and bootstrapping that would necessitate significant travel above and beyond that needed for standard ceremonies.