

# At-Large Review of Trusted Community Representation in Root Zone DNSSEC Key Signing Ceremonies Workspace

Comment Close Date	Statement Name	Status	Assignee (s) and RALO(s)	Call for Comments	Call for Comments Close	Vote Announcement	Vote Open	Vote Reminder	Vote Close	Date of Submission	Staff Contact and Email
11.02.2014	<a href="#">Review of Trusted Community Representation in Root Zone DNSSEC Key Signing Ceremonies</a>	ADOPTED 12Y, 0N, 0A	<a href="#">Salanieta Tamanikawai maro</a> (APRALO)	31.01.2014	07.02.2014	11.02.2014	11.02.2014	16.02.2014	17.02.2014	18.02.2014	Kim Davies <a href="mailto:kim.davies@icann.org">kim.davies@icann.org</a>

For more information about this PC, please click [here](#) >>

## Comment / Reply Periods (\*)

Comment Open Date: 21 January 2014

Comment Close Date: 11 February 2014 - 23:59 UTC

Reply Open Date: 12 February 2014

Reply Close Date: 4 March 2014 - 23:59 UTC

## Important Information Links

[Public Comment Announcement](#)

[To Submit Your Comments \(Forum\)](#)

[View Comments Submitted](#)

## Brief Overview

Originating Organization:

ICANN Staff

Categories/Tags:

- Security/Stability

## Purpose (Brief):

Based on feedback from the current TCRs and our experience from the first 14 ceremonies, we are reviewing what changes, if any, should be made to the current model of Trusted Community Representative participation.

Current Status:

Initial public consultation

Next Steps:

Review consultation input

Staff Contact:

Kim Davies

[Email Staff Contact](#)

## Detailed Information

Section I: Description, Explanation, and Purpose:

Based on feedback from the current TCRs and our experience from the first 14 ceremonies, [we are reviewing](#) [PDF, 321 KB] what changes, if any, should be made to the current model of Trusted Community Representative participation.

Section II: Background:

Since July 2010, the DNS Root Zone has been secured using DNSSEC. The model of using DNSSEC in the DNS Root Zone revolves around a "key signing key" (KSK) that is managed by ICANN in two secure facilities. Four times a year, a ceremony is conducted at these facilities to perform operations involving the KSK. As a key part of this process, a minimum of three from a pool of 21 trusted community representatives (TCRs) attend each ceremony to enable access to the secure materials, to witness the procedure, and to attest that the ceremony was conducted properly.

Section III: Document and Resource Links:

- [Consultation document](#) [PDF, 321 KB]
- [Information about DNSSEC for the Root Zone](#)
- [DNSSEC Practice Statement for the Root Zone KSK Operator](#)
- [Archive of ceremony audit bundles](#)
- [TCR Selection 2010](#)
- [Trusted Community Representatives – Proposed Approach to Root Key Management](#) [PDF, 102 KB]

Section IV: Additional Information:

N/A

(\*) Comments submitted after the posted Close Date/Time are not guaranteed to be considered in any final summary, analysis, reporting, or decision-making that takes place once this period lapses.

## FINAL VERSION TO BE SUBMITTED IF RATIFIED

Please click [here](#) to download a copy of the PDF below.

---

## FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

### Background

The [Affirmation of Commitment](#) describes the Internet as a transformative technology that empowers people around the globe, spurs innovation, facilitates trade and commerce, and enables the free and unfettered flow of information[1]. One of the elements of the Internet's success is a highly decentralized network that enables and encourages decision-making at a local level. Notwithstanding this decentralization, global technical coordination of the Internet's underlying infrastructure - the Domain Name System[2] (DNS) - is required to ensure interoperability[3].

DNS Security Extensions[4] (DNSSEC) is a protocol that is currently being deployed to secure the Domain Name System (DNS), the Internet's global phone book. DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names.

In DNSSEC a secure response to a query is one which is cryptographically signed and validated. An individual signature is validated by following a chain of signatures to a key which is trusted for some extra-protocol reason. ICANN, as IANA Functions Operator, is responsible for the publication of [trust anchors](#)[5] for the root zone of the Domain Name System.

Since July 2010, the DNS Root Zone has been secured using DNSSEC. The model of using DNSSEC in the DNS Root Zone revolves around a "key signing key" (KSK) that is managed by ICANN in two secure facilities. Four times a year, a ceremony is conducted at these facilities to perform operations involving the KSK. As a key part of this process, a minimum of three from a pool of 21 trusted community representatives (TCRs) attend each ceremony to enable access to the secure materials, to witness the procedure, and to attest that the ceremony was conducted properly.

### Introduction

The At Large Community recognizes the role and significance that the DNS plays in ensuring interoperability. We recognize the importance of DNSSEC in the security, stability and resiliency of the Internet in the root zone and the subsequent deployment in DNS Infrastructure. Noting that at the time this statement was written there were [427 TLDs in the root zone of which 235 are signed and that 229 have trust anchors published in the DS records in the root zone whilst 4 TLDs have trust anchors published in the ISC DLV Repository](#), we hope that in time more TLDs will move towards having trust anchors published.

The Root Zone Key Signing Ceremony points to one of ICANN's important functions of preserving accountability and transparency in the manner in which it conducts its DNSSEC Key Signing Ceremonies.

We recognize the unique combination the key-signing and TCRs make of broad participation, transparency and accountability in order to serve the central function of preserving and enhancing the stability, security and resilience of the DNS, thus engendering widespread trust.

We would like to congratulate all the stakeholders involved in the KSK management process on the services since the first KSK signing ceremony till to date. We welcome the opportunity to contribute to the Review of Trusted Community Representation in Root Zone DNSSEC Key Signing Ceremonies. Following consultations with the At Large community along the questions that was raised, we found that on some issues there was divergence of views and we have captured both views.

**1. Is the current TCR model effectively performing its function of ensuring trust in the KSK management process?**

The current Trusted Community Representative (TCR) model has been effectively performing its functions of ensuring trust in the KSK management process; however, we make the following observations.

The Abbreviation Draft of the Key Signing Ceremony Annotated Scripts, which provides a permanent trusted record of the Ceremony, does not include a definition for "EV" when these appear to be sometimes the largest number of category of people at the Ceremony. The Key Signing Ceremony Annotated Scripts do not clearly state whether there are no other participants (including Camera person) present apart from those listed.

**2. Is the current size of the TCR pool appropriate to ensure sufficient participation in the ceremonies, while not overburdening the availability of specific volunteers?**

There are two different views on this. The first view is that the current size of the TCR pool is sufficient. The second view is that the current size needs to be expanded to cater for unforeseen circumstances (includes but is not limited to terrorist attacks, flight disruptions, state of emergency, civil war, etc) that could render a majority of the 21 TCRs unable to attend to their responsibilities. The possibility of having signing at the same time in either the same country or different countries or frequency of signing could also exhaust reserves leading to overburdening these volunteers. There might be some merit in expanding the pool and retaining the TCRs whilst rotating them from within the pool of candidate TCRs.

**3. Should there be a minimum level of participation required of a TCR in order to be considered to be successfully discharging their duties?**

The community believes that TCRs should meet the existing criteria merited of what would comprise a responsible TCR. TCRs should actively engage by writing reports which are made public. Minimum participation should include, attendance, engagement, carrying out responsibilities, writing full and thorough reports and listing concerns if any.

**4. There is no standard provision to refresh the list of TCRs except when they are replaced due to inability to effectively perform their function. Should there be a process to renew the pool of TCRs, such as using term limits or another rotation mechanism?**

There are two views on this matter. The first view is that the existing pool and their indefinite terms are sufficient and that the 21 TCRs are more than enough to meet possible contingencies that may arise. That there is no need for process to renew the pool neither of TCRs nor to use term limits or introduce a rotation mechanism.

The other view is that there is a need for term limits as the original TCR mechanism is silent on the term. Given the Internet reaches an estimated 2.6 billion users all over the world, there should be enough candidates able to meet the criteria of being a TCR. The number of candidate or backup TCRs can also be increased. Regardless, where there is an assumption of indefinite service as a TCR, there should be a constant requirement to disclose any and all potential conflicts of interest to disable the risk of "capture" by any stakeholder or interest.

**5. The current model does not compensate TCRs for their services in order to**

**ensure their independence from ICANN.**

**a. Should the model of TCRs paying the costs of their participation be retained?**

**b. Would some form of compensation to offset the expenses incurred by the TCRs detract from their independence in performing the role?**

**c. If you support compensating TCRs for their expenses, are there requirements or limitations on whom the funding organization should be?**

There are two divergent views in relation to this. The first view holds that the current model where TCRs pay the costs should be retained. TCRs should be cost-neutral for those not supported by firms or other entities should suffice. To create another source of travel funds for TCRs is poor and unwarranted.

The second view acknowledges the financial burden placed on TCRs. Although TCRs are volunteers, a system should be set in place that guarantees independence yet allows them to carry out their duty. A fund should be managed externally that is independent that can cater for the expenses of the TCRs. There should be limitations on those who can contribute to this fund. Any funds or gifts being awarded to the TCR should be promptly and formally disclosed through appropriate avenues. One of the suggestions for possible funding model is where ICANN sets up the fund as in the case of the Office of the Independent Objector (IO) where ICANN does not interfere with the decisions of the (IO).

## **FIRST DRAFT SUBMITTED**

### **Background**

The [Affirmation of Commitment](#) describes the Internet as a transformative technology that empowers people around the globe, spurs innovation, facilitates trade and commerce, and enables the free and unfettered flow of information[1]. One of the elements of the Internet's success is a highly decentralized network that enables and encourages decision-making at a local level. Notwithstanding this decentralization, global technical coordination of the Internet's underlying infrastructure - the Domain Name System[2] (DNS) - is required to ensure interoperability[3].

DNS Security Extensions<sup>[4]</sup> (DNSSEC) is a protocol that is currently being deployed to secure the Domain Name System (DNS), the Internet's global phone book. DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names.

In DNSSEC a secure response to a query is one which is cryptographically signed and validated. An individual signature is validated by following a chain of signatures to a key which is trusted for some extra-protocol reason. ICANN, as IANA Functions Operator, is responsible for the publication of [trust anchors](#)<sup>[5]</sup> for the root zone of the Domain Name System.

Since July 2010, the DNS Root Zone has been secured using DNSSEC. The model of using DNSSEC in the DNS Root Zone revolves around a "key signing key" (KSK) that is managed by ICANN in two secure facilities. Four times a year, a ceremony is conducted at these facilities to perform operations involving the KSK. As a key part of this process, a minimum of three from a pool of 21 trusted community representatives (TCRs) attend each ceremony to enable access to the secure materials, to witness the procedure, and to attest that the ceremony was conducted properly.

#### Questions for the At Large

1. **Is the current TCR model effectively performing its function of ensuring trust in the KSK management process?**
2. **Is the current size of the TCR pool appropriate to ensure sufficient participation in the ceremonies, while not overburdening the availability of specific volunteers?**
3. **Should there be a minimum level of participation required of a TCR in order to be considered to be successfully discharging their duties?**
4. **There is no standard provision to refresh the list of TCRs except when they are replaced due to inability to effectively perform their function. Should there be a process to renew the pool of TCRs, such as using term limits or another rotation mechanism?**
5. **The current model does not compensate TCRs for their services in order to ensure their independence from ICANN.**
  - a. **Should the model of TCRs paying the costs of their participation be retained?**
  - b. **Would some form of compensation to offset the expenses incurred by the TCRs detract from their independence in performing the role?**
  - c. **If you support compensating TCRs for their expenses, are there requirements or limitations on whom the funding organization should be?**

#### DRAFT ALAC STATEMENT

##### Introduction

The At Large Community recognizes the role and significance that the DNS plays in ensuring interoperability. We recognize the importance of DNSSEC in the security, stability and resiliency of the Internet in the root zone and the subsequent deployment in DNS Infrastructure. Noting that to date there are [427 TLDs in the root zone of which 235 are signed and that 229 have trust anchors published in the DS records in the root zone whilst 4 TLDs have trust anchors published in the ISC DLV Repository](#), we hope that in time more TLDs will move towards having trust anchors published.

The Root Zone Key Signing Ceremony points to one of ICANN's most sacred functions of preserving accountability and transparency in the manner in which it conducts its DNSSEC Key Signing Ceremonies. We would like to congratulate all the stakeholders involved in the KSK management process on the services since the first KSK signing ceremony till to date. We welcome the opportunity to contribute to the Review of Trusted Community Representation in Root Zone DNSSEC Key Signing Ceremonies.

We believe that the current Trusted Community Representative (TCR) model has been effectively performing its functions of ensuring trust in the KSK management process. We would like to suggest a few additional processes that could complement the existing process. The original TCR proposal is silent on the term. Where there is an assumption of indefinite service as a TCR, there should be a constant requirement to disclose any and all potential conflicts of interest to disable the risk of "capture" by any stakeholder or interest.

We note that there is a financial burden placed on the TCR although they are volunteers and a system should be set in place that guarantees independence yet allows for ease in carrying out their duty. A fund should be managed externally that is independent that can cater for the expenses of the TCRs. There should be limitations on those who can contribute. Any funds or gifts being awarded to the TCR should be promptly and formally disclosed through appropriate avenues.

The At Large community is curious as to whether the TCR who resigned did so because of an inability to continue in his or her role due to arising conflict, lack of finances etc. The current size of the TCR pool needs to be expanded to ensure that there is sufficient participation in ceremonies as ICANN should account for the remote possibility of mass unavailability due to random unforeseen circumstances. There might be some merit in expanding the pool and retaining the TCRs whilst rotating them from within the pool.

---

[1] <http://www.icann.org/en/about/agreements/aoc/affirmation-of-commitments-30sep09-en.htm>

[2] [RFC 1034] and [RFC1035]

[3] *ibid*

[4] [RFC4033], [RFC4034], [RFC 4035]

[5] <http://data.iana.org/root-anchors/>