Review of Trusted Community Representation in Root Zone DNSSEC Key Signing Ceremonies

Public Consultation

Review of Trusted Community Representation in Root Zone DNSSEC Key Signing Ceremonies

Since July 2010, the DNS Root Zone has been secured using DNSSEC[1]. 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[2].

Each ceremony is attended by ICANN staff, the TCRs, representatives of the Root Zone Maintainer (Verisign), representatives of an independent audit firm retained by ICANN to monitor the process, and often additional external witnesses. Ceremonies are recorded by three audit cameras and webcast online. A typical ceremony lasts approximately four hours, and involves a process of temporarily removing the key signing key from a safe and performing key-signing operations in a secure manner following a formal script. The script is designed to perform each operation in a transparent manner to ensure the key signing key is only used for its proper purpose, and there is no ability for its contents to be disclosed for other purposes. Materials from each ceremony — such as the scripts, video recordings, and system output — are posted online[3].

De-briefings and discussions are conducted post-ceremony, where participants discuss how to improve future ceremonies. This feedback helps inform the evolution of the KSK ceremony to be both efficient and effective, while ensuring maximum trust in how ceremonies are performed.

The TCRs were selected[4] from the global community based on a number of criteria[5]. These selection criteria relate to the volunteers ability to travel to ceremonies, conscientiously oversee the process, ensure transparency in its operation, and ultimately contribute to the broader community's trust that the private component of the key signing key has not been compromised. The TCRs are privately funded volunteers who are not reimbursed or compensated by ICANN for their participation nor their expenses. The original TCR proposal was silent on the length of service of individual TCRs.

Of the 21 TCRs, seven are credentialed as "crypto officers" (COs) for each of the two facilities, and the remaining seven act as "recovery key shareholders" who only participate in ceremonies in the event the requisite number of COs are unable to participate or there is a need to rebuild the KSK following an unforeseen event. Of the seven COs for each facility, ICANN aims to have four attend each ceremony, with

[1] http://www.root-dnssec.org
[2] https://www.iana.org/dnssec/icann-dps.txt
[3] http://data.iana.org/ksk-ceremony/
[4] http://www.root-dnssec.org/tcr/selection-2010/
[5] http://www.root-dnssec.org/wp-content/uploads/2010/04/ICANN-TCR-Proposal-20100408.pdf

an absolute minimum of three required to successfully perform a ceremony. Each facility hosts two ceremonies per year, approximately once every six months. In practice, a TCR will attend at minimum one ceremony per year, and some will attend two in order to ensure sufficient attendance.

Of the initial pool of 21 TCRs, one has resigned and been replaced from the pool of recovery key shareholders. No TCR has been removed owing to the other three criteria for replacement in the TCR selection document, relating to lack of integrity or trustworthiness; assumption of a conflicting role within a root management organization; or being unable to serve in their position.

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 TCR participation.

Comments

Comments are welcome on any aspect of the consultation, and specifically on the following questions:

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?