Trusted Community Representatives – Proposed Approach to Root Key Management

ICANN, as the IANA functions operator, seeks to improve confidence and acceptance in the DNSSEC security mechanism among the wider Internet community by inviting recognized members of the DNS technical community to be part of the key generation, key backup and key signing process for the root.

As part of the joint effort to secure the domain name system (DNS) and the Root DNSSEC key management process currently under consideration, a number of persons acting as trusted representatives of the Internet community will be sought to participate in the root key generation and signing ceremonies. These persons are called Trusted Community Representatives (TCRs).

ICANN will select 21 TCRs and a number of candidate TCRs. Initially, this will be done on a provisional basis to determine the approach's viability based on the success of the first Hardware Security Module (HSM) initialization and key generation that is scheduled for June 2010. The selection will be based on Statements of Interest, solicited from the Internet community. Persons considered affiliated with ICANN, VeriSign or the U.S. Department of Commerce may not become a Trusted Community Representative.

Functions

There are two TCR functions - a "Crypto Officer" and a "Recovery Key Share Holder". A single person may not hold both functions at the same time.

Crypto Officer

A Crypto Officer participates in activating (enabling) the Hardware Security Module (HSM) containing the private half of the DNSSEC root KSK before that module may be used for cryptographic operations. Each Crypto Officer will hold a physical key to a safe deposit box that is located within a secure facility operated by ICANN. The safe deposit box contains the actual credentials needed to enable the use of the HSM.

Initially, the Crypto Officer role will be on a provisional basis. This is to ensure that the role is viable based on the first HSM initialization and key generation that is scheduled to take place in June 2010. Assuming the Crypto Officer's role in first initialization and key generation process proves successful, the Crypto Officer may be considered for serving an annual term.

Seven (7) individuals are designated for each ICANN-operated secure facility, one facility on the U.S. East Coast and another facility on the U.S. West Coast, for a total of 14 Crypto Officers. It is expected that each TCR will be required to travel to an ICANN facility in the US up to four (4) times a year.

Recovery Key Share Holder

A Recovery Key Share Holder is responsible for protecting a part of a key used to encrypt backup copies of the HSM contents. Each share holder is responsible for keeping a smart card (in a tamper-evident bag) in a safe deposit box at a bank accessible by them.

If the provisional Crypto Officer role proves viable based on first HSM initialization and key generation process, Recovery Key Share Holders will be instituted and serve annual terms.

Seven (7) individuals are required. After HSM initialization, the share holder is not expected to participate in any scheduled ceremonies, but must be able to travel to an ICANN facility in the US on relatively short notice at any time when requested. Share holders must participate in the annual inventory by providing proof of possession of their smart card.

TCR Selection Criteria & Selection Process

While strong technical knowledge of the Internet is not the determining factor in TCR selections, the selected TCRs are expected to be committed to the security of the DNS and knowledgeable, or committed to becoming knowledgeable, about the environment in which ICANN operates and the technical functions for which ICANN has responsibilities. ICANN will apply the criteria and eligibility factors defined in the attached to develop a pool of qualified candidates.

ICANN encourages wide participation in this process, and is grateful for the valuable input it will receive from those who volunteer for the positions available.

Attachment

Section A. Criteria, Core Values, and Timing for Positions

Criteria

1. Persons of integrity, objectivity, and intelligence, with reputations for sound judgment and open minds;
2. Persons with an understanding of the domain name system and the potential impact of DNSSEC operations on the global Internet community;
3. Persons who can help ICANN represent the broadest cultural and geographic diversity consistent with meeting the other criteria set forth in this Section;
4. Persons who, in the aggregate, have personal familiarity with the operation of gTLD and ccTLD registries and registrars; with IP address registries; with Internet technical standards and protocols; with policy-development procedures, legal traditions, and the public interest; and with the broad range of business, individual, academic, and non-commercial users of the Internet;
5. Persons who are willing to serve as volunteers, without compensation; and
6. Persons who are able to work and communicate in written and spoken English.

Although Candidates should be able to both work and communicate well in English, there is no requirement that English be the candidate's first language.

Core Values

In making its selections, ICANN will look for persons who can improve confidence in the DNSSEC security mechanism among the wider Internet community, and who

1. Seeks and supports broad adoption of the DNSSEC technology,
2. Remains accountable to the Internet community for the security function.

Section B. Position Roles, Eligibility Factors, and Time Commitments

TCRs serve as individuals who have the duty to act in what they reasonably believe are the best interests of the security of the DNS and the Internet Community.

ICANN will use the Selection Criteria for TCRs for these positions.

TCRs shall receive no compensation for their services as TCRs.

Eligibility Factors for TCRs

1. ICANN shall seek to ensure that the TCRs are composed of members who in the aggregate display diversity in geography, culture, skills, experience, and perspective, by applying the Selection Criteria set forth above in this document.

2. No individual from an organization affiliated with the root zone management process (ICANN, VeriSign, or the US Department of Commerce) may serve as a TCR.

Time Commitment and Working Practice

The basic responsibilities of a TCR in the role of Crypto Officer require a maximum commitment of time of roughly equivalent to two days, four (4) times a year at key ceremonies. The time spent in these basic responsibilities is typically clustered around the turn of a quarter. For the Recovery Key Share Holder, there is no regular time requirement but they must be able to travel to an ICANN facility in the US with relatively short notice when requested.

Role of the TCR

TCRs are not the representatives of any specific organization, though they may choose to represent the interests of groups.

C. Replacement Criteria for TCR

ICANN will use one (or more) of the following criteria for replacing a TCR if necessary:

1. TCR performs an action that leads ICANN to question their integrity or trustworthiness.
2. TCR assumes a position with an organization that plays a role in the root management process (i.e. ICANN, VeriSign or the US Department of Commerce).
3. TCR explicitly states desire to be replaced.
4. TCR is rendered incapable of serving.