DRAFT

Placing TLD trust anchors in the root zone

The DNS root zone supports the listing of DS records to facilitate DNSSEC-signed domains through a chain of trust from the root. Operators of top-level domains are able to submit these trust anchors for inclusion in the DNS root zone in a similar way to how changes to the authoritative name servers are managed.

Submitting trust anchors

Top-level domain (TLD) operators who use DNSSEC to sign their zone are welcome to submit trust anchors. They need to be submitted using the same process for changes to the authoritative name servers. This involves filling out a change template, available at <URL>.

For the purpose of transmitting requests, they must be submitted to ICANN IANA staff via email, post or fax; although email is strongly encouraged. All email is to be transmitted to root-mgmt@iana.org. All requests transmitted by facsimile must be transmitted to +1 310 823 8649 and marked to the attention of "IANA Root Zone Management." All requests transmitted by post are to be directed to *IANA Root Zone Management, 4676 Admiralty Way #330; Marina del Rey CA 90292; USA.*

All the trust anchors the submitter wishes to have listed in the root zone should be listed on this form. For example, if there are already two trust anchors listed, and you wish to remove one and add a new one, list the 2 trust anchors you wish to remain after the change. If you wish to remove the trust anchors altogether, submit a form with no trust anchors and the explanatory text "Delete all trust anchors".

Trust anchors must be provided each with the four attributes of a DS record — the key tag, the key algorithm, the digest hash type, and the digest hash. For example, if the DS record looks like this:

```
EXAMPLE. DS 39286 5 1 7E43E0891843984900A5A03AA01883EB37A20F5A
```

It should be listed in the root zone change template like this:

```
Delegation Signer Record
7a. Key Digest.....................:
7E43E0891843984900A5A03AA01883EB37A20F5A
7b. Key Tag........................: 39286
7c. Key Algorithm..................: 5
7d. Key Digest Type................: 1
```

Once a TLD operator submits a DS resource record change request, it will be processed in the same manner as other change requests. That is, the request will be vetted

and processed by the IANA Functions Operator (ICANN), authorized by the Root Zone Administrator (U.S. Department of Commerce), and then incorporated into the root zone by the Root Zone Maintainer (VeriSign). See DNSSEC Practice Statement for the Root Zone KSK Operator, section 1.3 available at <URL>.

Technical requirements for trust anchors

Trust anchors are subject to a few technical requirements:

— They must be provided with legal values for each of the DS record fields.

— For the hash digest, ICANN supports two types — SHA1 (value 1), and SHA256 (value 2).

— At the time of the trust anchor request, there must be a DNSKEY that matches the DS record present in the child zone. This will be tested for the presence of a matching DNSKEY record as part of the implementation of the record. As with most technical conformance criteria for the root zone, if a top-level domain operator has a situation where this is not the case, but this is by design and can be demonstrated not to affect the stability of the TLD or the root zone, it is possible to request that the trust anchor be listed regardless.

Performing key rollovers

Top-level domain operators can reflect key rollovers in the root simply by submitting updates to their DS records on an appropriate schedule in the same manner as described above.

If the top-level domain operator needs to revoke usage of a trust anchor in the event of an emergency, the TLD operator should submit a change request clearly marking it as an emergency change. ICANN's emergency 24x7 service may be utilized for this purpose.

The emergency change process will be completed and reflected in the root zone within 48 hours from the reception of a valid emergency removal request.

Transition Arrangements

During the launch phase of DNSSEC in the root zone, a method of publishing a "deliberately unvalidatable root zone" is being used for a transitional period. During this time, the root zone will be signed, but the signatures used cannot be validated using the DNSSEC protocol. It is anticipated that once testing is complete on the impacts of DNSSEC in the root zone, that trust anchors will be published that can be verified.

During this transition period, DS records can be listed in the root zone. Once trust anchors are published for the root zone and this transition period is over, the submitted DS records will remain in the root zone and will be validatable as a chain from the trust anchors of the root.

For more information on the transition to a DNSSEC-signed root zone, see http://www.root-dnssec.org/