DNSSEC Validators Requirements

draft-mglt-dnsop-dnssec-validator-requirements-05

Migault, Lewis, York IETF99

ToC

- Time Requirements
- Trust Anchor Requirements
  - Bootstrapping / configuration
  - TA Datastore
  - Interaction with other RRsets
- ZSK/KSK Requirements
  - KSK/ZSK Datastore
  - KSK/ZSK - TA Datastore
- Cryptography Deprecation Requirements

Goal

DNSSEC validation is based on:

- Matching a RRSIG resource record’s contents to a RRset
- Placing sufficient trust into a DNSKEY resource record

This document describes what an implementation is required to do to allow proper, accurate validation.

Time derivation and absence of real time clock

Devices may not be configured with real time clock:

- When replugged, these devices show January 1 1970
- Suffer from time derivation

REQ1: A DNSSEC validator MUST be provided means to update the time without relying on DNSSEC.

TA: Bootstrapping

Without Trust Anchor, A DNSSEC Validator will never be able to build a chain of trust.

REQ2: A DNSSEC validator MUST check the validity of its Trust Anchors when bootstrapping. When a Trust Anchor cannot be verified, the DNSSEC validator MUST send a warning and SHOULD NOT start validating traffic without manual validation.

REQ3: A DNSSEC validator SHOULD be able to retrieve a Trust Anchor with bootstrapping mechanism. Such mechanism' security MUST NOT be based on [only on] DNSSEC, but could instead include downloading a XML file from a trusted URL, or a PKIX certificate.

TA: Trust Anchor Data store

When a Trust Anchor roll-over is ongoing, the administrator may check the key roll over is properly ongoing or not before traffic is being rejected.

While TA not rolled appropriately will result in rejecting traffic, accepting a rogue TA may even be worst.

- Such operations must be cautiously [carefully] handled

TA provisioning may also include private deployment:

- Split-zone (careful with flip/flopping between private / public DNS)
- Homenet domain

TA: Trust Anchor Data store

REQ4: A DNSSEC validator MUST store its Trust Anchors in a dedicated Trust Anchor Data Base. Such database MUST store informations associated to each Trust Anchor status as well as the time the status has been noticed by the DNSSEC validator. Such database MUST be resilient to DNSSEC validator reboot.

REQ5: Trust Anchor states SHOULD at least consider those described in [RFC5011] (Start, AddPend, Valid, Missing, Revoked, Removed). Additional states SHOULD also be able to indicate additional motivations for revoking the Trust Anchor such as a Trust Anchor known to be corrupted, a Trust anchor miss published, or part of a regular roll over procedure.

TA: Trust Anchor Data store

REQ6: A DNSSEC validator MUST provide access to the Trust Anchor data base to authorized user only. Access control is expected to be based on a least privileged principles.

REQ7: A trusted party MUST be able to add, remove a Trust Anchor in the Trust Anchor Database.

TA: Interactions with the cached RRsets

Revocation of a TA may have various reasons, but when a TA is known to be corrupted data associated to that TA may be flushed.

REQ8: A DNSSEC validator MUST be able to flush the cached RRsets that rely on a Trust Anchor.

KSK/ZSK: ZSK/KSK Data store

KSK/ZSK:

- build the chain of trust but are not expected to be part of the configuration
- Subject to roll-over

REQ9: A DNSSEC validator MUST store its KSK/ZSK in a dedicated KSK/ ZSK Data Base. Such a database MUST store information associated to each KSK/ZSK status as well as the time the status has been noticed by the DNSSEC validator. Such database MUST NOT-strike be resilient to DNSSEC validator reboot.

REQ10: A validator's retained state for a KSK or ZSK must be available for inspection upon demand by an authorized operator. The state information must include time information. The information must be stored in a way that survives a reboot.

ZSK/KSK: ZSK/KSK Data store

REQ11: KSK/ZSK states SHOULD at least consider those described in section 3.1 of [RFC7583] (Generated, Published, Ready, Active, Retired, Dead, Removed, Revoked). Additional states SHOULD also be able to indicate additional motivations for revoking the KSK/ZSK such as a KSK/ZSK known to be corrupted, a KSK/ZSK miss published, or part of a regular roll over procedure.

REQ12: A DNSSEC validator MUST provide access to the KSK/ZSK data base to authorized user only. Access control is expected to be based on a least privileged principles.

REQ13: A trusted party MUST be able to add, remove a Trust Anchor in the KSK/ZSK Database.

KSK/ZSK: KSK/ZSK Data Store and Trust Anchor Data Store

A zone may have been badly signed

REQ14: A trusted party MUST be able to indicate a DNSSEC validator that a KSK or a ZSK as Negative Trust Anchor. Such Trust Anchors MUST NOT be used for RRSIG validation and MUST be moved to the Trust Anchor Database, so the information become resilient to reboot.

REQ15: A trusted party MUST be able to indicate a DNSSEC validator that a KSK/ZSK is known "back to secure".

Cryptography Deprecation

DNSSEC validator is not able to determine other than by trying whether a signature scheme is supported by the authoritative server.

REQ18: A DNSSEC validator SHOULD be able to request the signature scheme supported by an authoritative server.

Thanks!