DNSSEC Validators Requirements

draft-mglt-dnsop-dnssec-validator-requirements-06

Daniel Migault, Edward Lewis, Dan York

Scope of the document

Requirements related to validation exist in [RFC4033], [RFC4034] and [RFC4035]. However, the specification of the validation is not sufficient to enable a wide deployment of DNSSEC validators

There are a number of situations where the necessary condition are not met by the DNSSEC validator to perform DNSSEC validation.

This document is focused on the necessary mechanisms that DNSSEC validators should implement in order to make DNSSEC validation output accurate.

The document requires mechanisms for an administrator to ensure the validity of the DNSSEC validation output, i.e.:

- provisioning mechanisms
- Monitoring mechanism
- management mechanisms

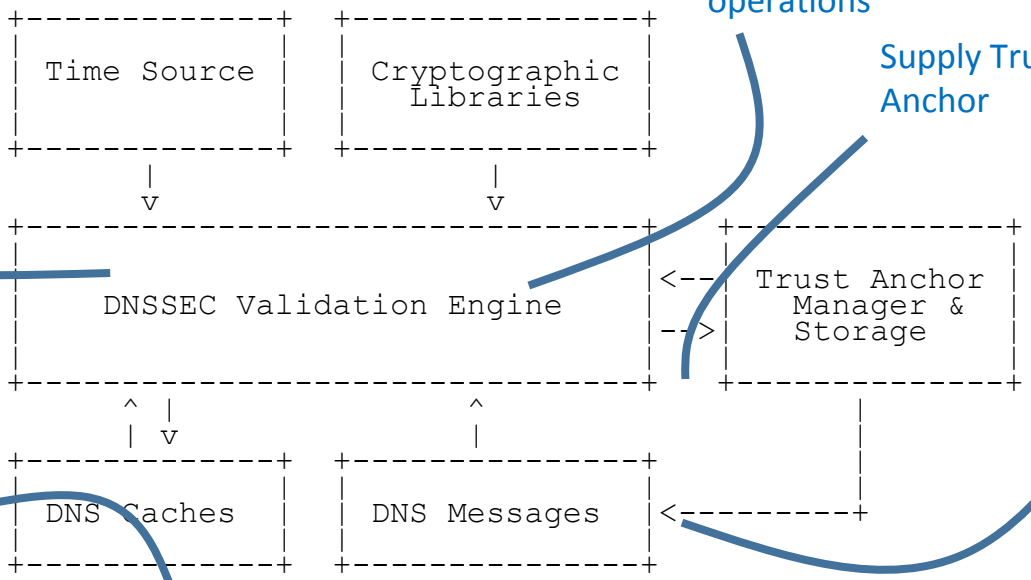
Draft Content

We have currently listed 20 requirements: https://tools.ietf.org/html/draft-mglt-dnsop-dnssec-validator-requirements-06

Current discussions concern finding the right balance between over managing the cache versus letting the protocol work.

4. DNSSEC Validator Description 4
5. Time derivation and absence of Real Time Clock 5
6. Trust Anchor 5
6.1. Trust Anchor Bootstrapping 6
6.2. Trust Anchor Data Store 7
6.3. Interactions with the cached RRsets 8
7. ZSK / KSK 8
7.1. KSK/ZSK Data Store 8
7.2. KSK/ZSK Data Store and Trust Anchor Data Store 10
7.3. Interactions with cached RRsets 11
8. DS 12
9. Cryptography Deprecation 12
10. Reporting 13

Validator Description



Crypto operations

Supply Trust Anchor

Current Time

Information about Trust Anchor update

Result of a Validation

ZSK / KSK for chain of Trust

Message to manage Trust Anchors

Questions

RFC7583 defines the following status for KSK/ZSK: Generated, Published, Ready, Active, Retired, Dead, Removed, Revoked.

Operations on KSK / ZSK are based on their associated trust.

What are the conditions for key be untrusted ?

- Signatures of an untrusted KSK/ZSK are rejected as errors.
- A KSK, ZSK may be revoked after the key roll over – different type of roll over, time ?
- Should an untrusted key contaminates the keys below ?

Questions

Can/Should a validator purge the cache of data accepted in part because of a suddenly revoked or untrusted key?

- Retroactively untrusted data

Do caches retain chain of trusts for data in the [validated-positive or validated-negative] cache?

Next step ?

- The draft has received several feed backs
- We believe the draft is ready for adoption by the WG