DNSSEC Validators Requirements

draft-mglt-dnsop-dnssec-validator-requirements-00.txt

D. Migault

07/03/2014- IETF89- London

Table of Contents

Motivations & Goals

Motivations of the document:

- Bringing DNSSEC to the end points (EU, CPEs...)

Currently DNSSEC Validation works as follows:

```
if DNSSEC Validation is properly performed:
     show a smiley
else:
    switch to DNS
```

Goals of the document:

- Listing requirements so DNSSEC Validation is always-on

Coming document will define DHCP Options to address these requirements:

- update of draft-mglt-homenet-dnssec-validator-dhc-options-02.txt

Requirements

Time derivation and absence of Real Time Clock

- REQ1: DNSSEC validator MUST be provided means to appropriately update their time.

Unplugged devices during Trust Anchor KSKs roll over

- REQ2: DNSSEC Validator MUST be able to check the validity of their Trust Anchor KSKs.
- REQ3: DNSSEC Validator MUST be able to retrieve their Trust Anchor KSKs.

Requirements

Emergency Key rollover

- REQ4: DNSSEC Validator MUST be able to be informed a ZSK MUST be flushed from cache
- REQ5: DNSSEC Validator MUST be able to be informed a KSK MUST be flushed from cache
- REQ6: DNSSEC Validator MUST be able to be informed a KSK SHOULD be trusted as a Trust Anchor KSK.
- REQ7: DNSSEC Validator MUST be able to be informed that a KSK or a ZSK MUST NOT be used for RRSIG validation. (Neg Trust Anchors)

Private KSK

- REQ9: DNSSEC Validator MUST be able to be provided KSK for private use.

Requirements

Any missing Requirement you see?

Thank you for your attention