DNSSEC operational practices for authoritative name servers

Matthijs Mekking

NLnet Labs

May 12, 2014

Why

We have:

RFC4641	DNSSEC Operational Practices
RFC6781	DNSSEC Operational Practices, version 2
RIPE64	Looking at TLD DNSSEC Practices (Edward Lewis)
AND	DNSSEC Deployment Guides (NIST, Kirei, ...)

I want:

BCP	DNSSEC Operational Practices

We want:

BCOP	actually GOP

BCP vs BCOP

BCP

A -bis of RFC6781 (aka RFC RFC4641-bis, so that would actually become RFC4641-bis-bis)

BCOP

A document that focuses more on operational guidance

What should be in it?

What should be in it?

Protocol default values (the BCP part) aka Policy values?

+ Cryptographical considerations?

What should be in it?

Protocol default values (the BCP part) aka Policy values?

- \+ Cryptographical considerations?
- \+ ZSK/KSK split or CSK?

What should be in it?

Protocol default values (the BCP part) aka Policy values?

- \+ Cryptographical considerations?
- \+ ZSK/KSK split or CSK?
- \+ When to rollover?

What should be in it?

Protocol default values (the BCP part) aka Policy values?

- + Cryptographical considerations?
- + ZSK/KSK split or CSK?
- + When to rollover?
- + Values for signature validities, re-sign, refresh, ...

What should be in it?

Protocol default values (the BCP part) aka Policy values?

- + Cryptographical considerations?
- + ZSK/KSK split or CSK?
- + When to rollover?
- + Values for signature validities, re-sign, refresh, ...
- + NSEC or NSEC3?

What should be in it?

Protocol default values (the BCP part) aka Policy values?

- + Cryptographical considerations?
- + ZSK/KSK split or CSK?
- + When to rollover?
- + Values for signature validities, re-sign, refresh, ...
- + NSEC or NSEC3?
- + If NSEC3, when to resalt?

What should be in it?

Available software?

- Standalone solutions: OpenDNSSEC, BIND, Knot, ...

What should be in it?

Available software?

- \+ Standalone solutions: OpenDNSSEC, BIND, Knot, ...
- \+ Combinations: ldnsutils + NSD, ...

What should be in it?

Available software?

- Standalone solutions: OpenDNSSEC, BIND, Knot, ...
- Combinations: ldnsutils + NSD, ...
- Closed source: Microsoft DNS, Nominum, ...

What should be in it?

Key management?

- Generation: Number of participants?

What should be in it?

Key management?

- \+ Generation: Number of participants?
- \+ Delivery: Integrity checks? Audit trail?

What should be in it?

Key management?

- Generation: Number of participants?
- Delivery: Integrity checks? Audit trail?
- Storage: Online or offline? HSM or not?

What should be in it?

Key management?

- Generation: Number of participants?
- Delivery: Integrity checks? Audit trail?
- Storage: Online or offline? HSM or not?
- Usage: Who can use? How to (de)activate?

What should be in it?

Many other topics:

- Good to have documentation: DPS, incident response procedures, ...
- Facility requirements: Power failover, area access control, ...
- Hardware and software: Diversity, maintenance, ...
- Did I miss something? Probably

Need consensus on

The content

+ Scope and detail

Need consensus on

The content

- \+ Scope and detail
- \+ Different scenarios have different practices

Need consensus on

The content

- Scope and detail
- Different scenarios have different practices
- Perhaps split up between TLD and hoster scenario

Questions

Is there interest?

And is there anybody willing to collaborate?

Are there opinions about what should be in it?

And what definitely not?

Do we need it all?

Or is existing documentation already sufficient?