



DNSSEC – Policy and Practice Statement

Anne-Marie Eklund Löwinder
Quality and Security Manager
amel@iis.se

.se



What is a DNSSEC Policy and Practice Statement (DPS)?

- A document that contains the DNSSEC Policy and Practice Statement for establishing and managing keys to be used by TLD in conjunction with DNSSEC.
- A DPS may describe how the TLD verifies the link between a domain, a public key and a physical individual or legal entity that is the registrant for a domain, as well as the technical contact for the domain.
- A DPS contains a brief description of the verification procedures, the procedures followed by the TLD and how it handles its keys.
- The document is intended to enable trusting parties to determine the level of trust they wish to grant to the TLD's DNSSEC management.

.se



What does the .SE DPS contain (1)?

- .SE's area of responsibility
 - Signing of the .se-zone
 - Secure delegation of underlying zones in the .se zone
- Key administration for the .se zone
 - Technical environment for key generation
 - Procedures for generating keys
 - Storage of keys
 - Use of keys
 - Replacement of keys

.se

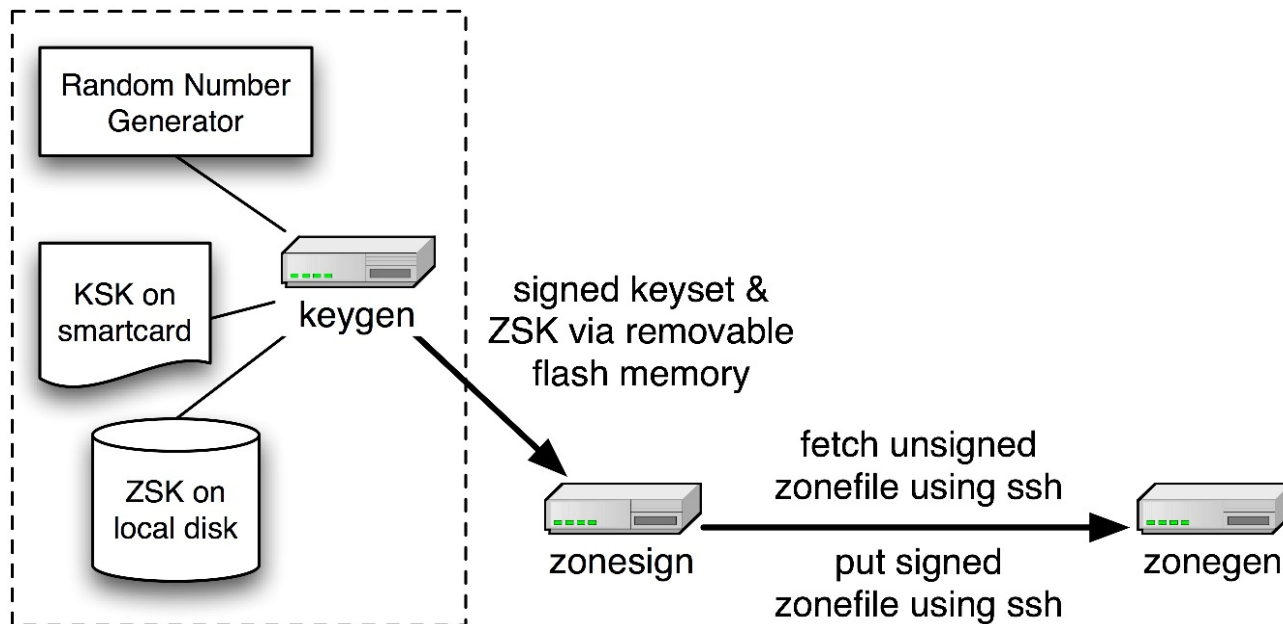
What does the .SE DPS contain (2)?

- Description of methods for distribution of current public Key Signing Keys (KSK)
 - through a ssl-protected web site.
 - signed with PGP and .SE's official PGP key.
 - KeyID of the PGP key.
 - url for .SE's official PGP key:
<http://keyserv.nic.se:11371/pks/lookup?op=get&search=0x97BE17CCC65FA7B0>.
 - mailing list address for announcements.

.se

What does the .SE DPS contain (3)?

- An overall description of key generation and zone signing



.se



Getting acceptance for the DSP

- Referral to
 - registrars (if you are a TLD)
 - resolving name server operators (ISP's)
 - the local internet community
- They will always come up with aspects you didn't think of...

.se



Public KSK distribution

Why use a SSL-protected web site?

The public in general does not automatically trust PGP without trusting any other already known signature on the PGP-key. It does not come easy to verify a PGP-signature. In this case it is much easier to trust a SSL certificate.

.se



Public KSK distribution – other options?

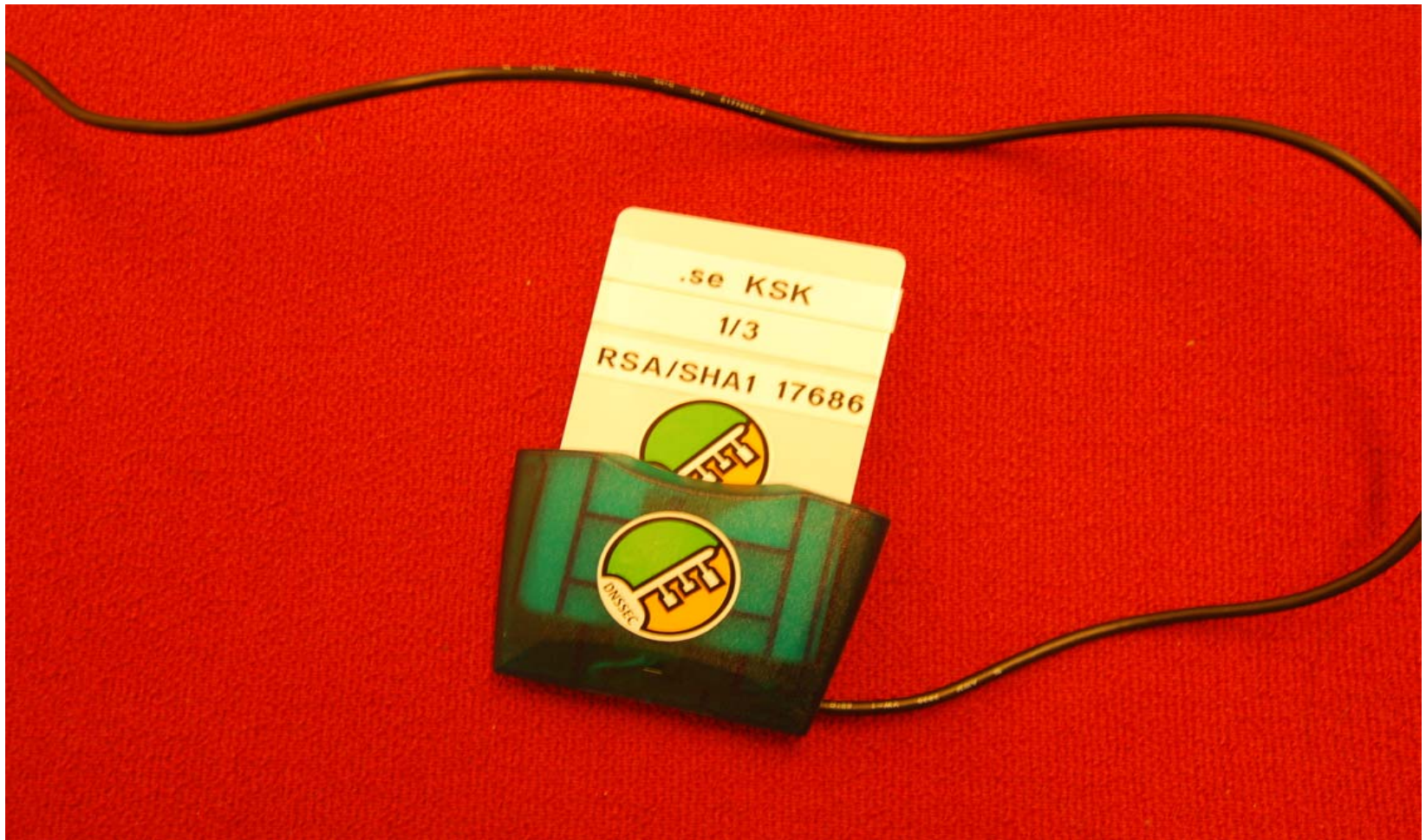
- .SE could urge some other organisation(s) to publish the current KSK's of .SE.
- .SE will not be able to guarantee the validity of these keys, the user's are responsible of verifying the validity.
- .SE may be able to make an agreement with external organisations for publishing .SE:s current KSK. The actual organisations name and link will be published on .SE:s web site and .SE is obliged to supply updates when there is a KSK rollover taking place.
- A precondition to make such an agreement is that the organisation fulfills .SE:s requirement on accurate administration and stability.

.se



Safe for the storage of the keys on smart cards and other equipment required (the safe locked in, in a locker, sited in the server room with very restricted access)

.se



Smart card and smart card reader.

.se



Random Number Generator.

.se

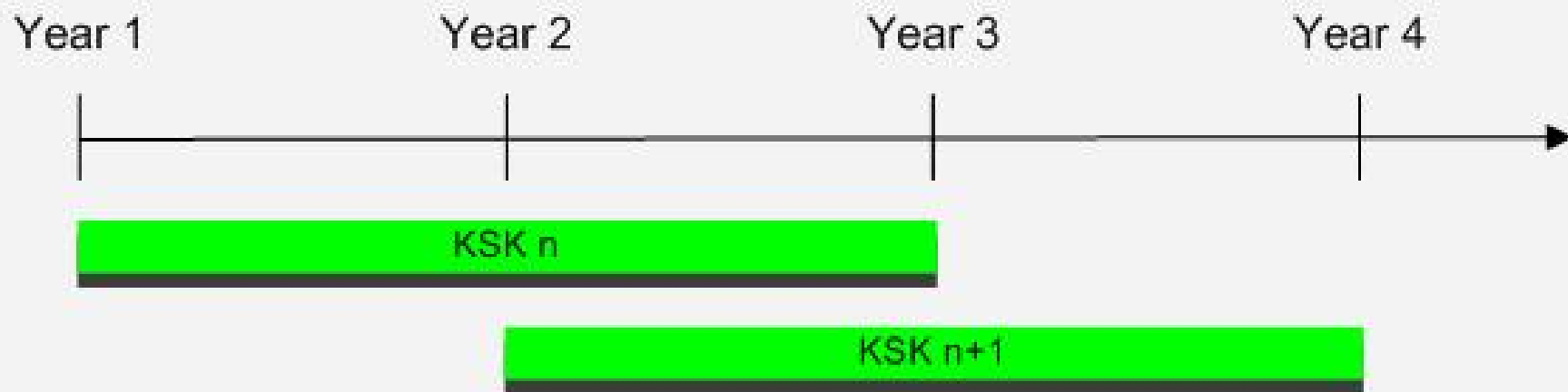


Key lifetime

- This is currently under reconsideration...
- Why should we change DNSSEC key signing keys every other year, when other types of PKI root keys is valid for 20-30 years?
- We need a frequency that prevent us from forgetting how...
- We need a frequency that prevent us from putting a heavy work load to the organization.

.se

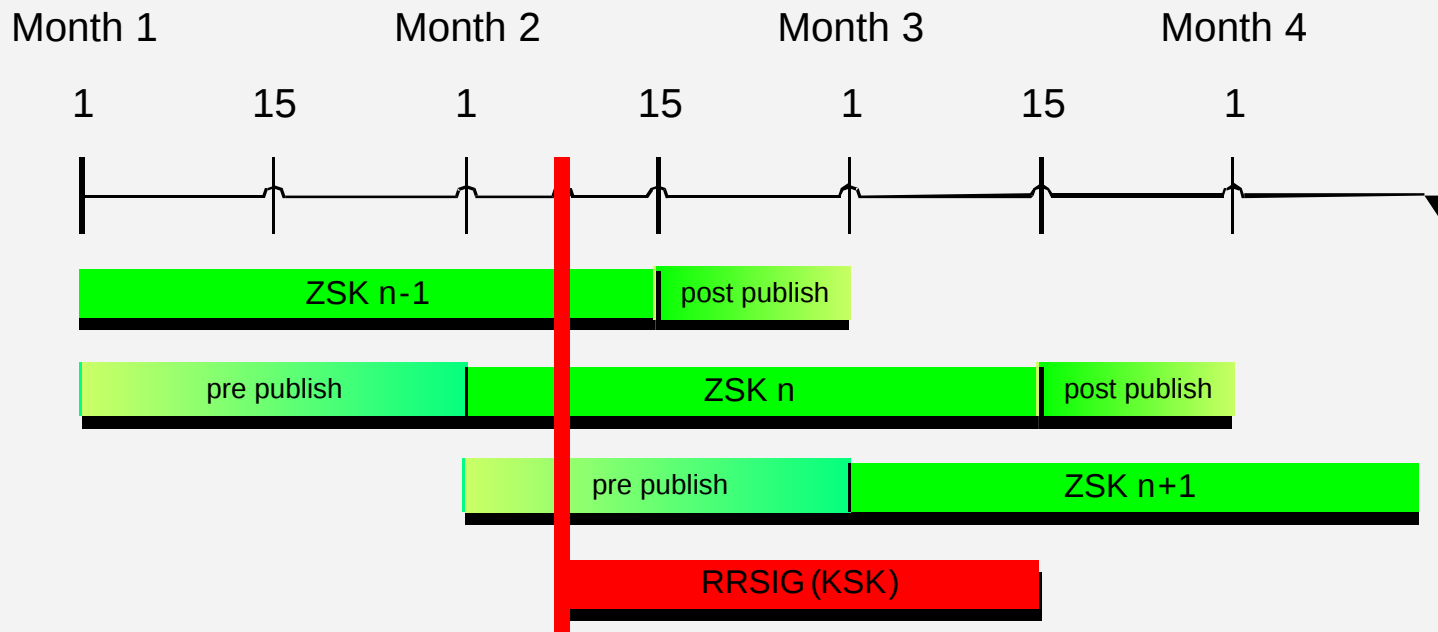
KSK Key Lifetime



Two KSK's always in use, with one year of overlap.

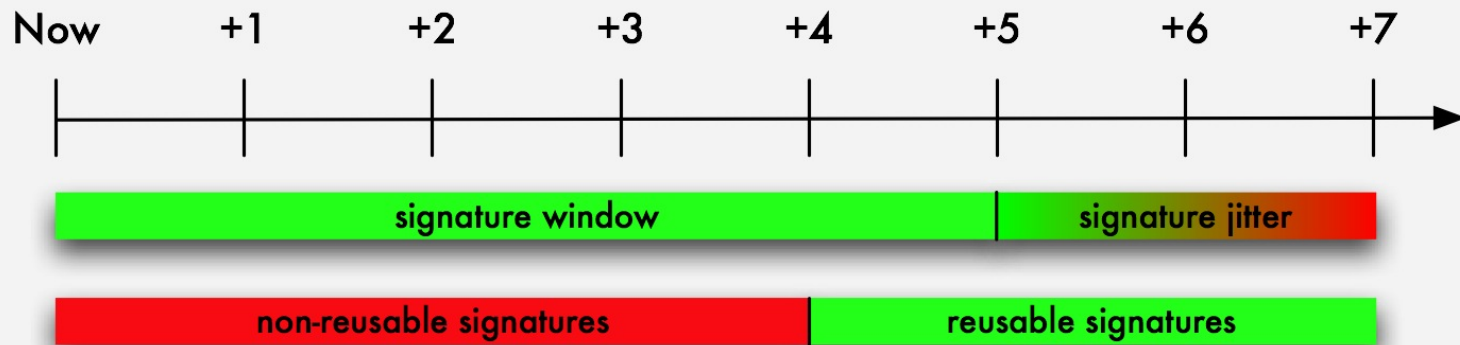
.se

ZSK Key Lifetime



.se

ZSK Signature Lifetime



Jakob Schlyter
Mon Sep 11 2006

.se



Servers involved... Lockable rack is nice to have.

.se



Server configuration

- Each DNS operator are strongly recommended to always check the current key - not only to copy and paste without verification.
- They need to be aware that the .SE Key Signing Key (KSK) will be changed from time to time.
- Everyone who configures this key into their resolver are strongly recommended to subscribe to the **dnssec-announce@lists.nic.se** mailing list where we notify key rollovers and make other important DNSSEC related announcements.

.se



We need an AKM

Automatic Key Management for .SE

...supporting DNSSEC-Policy-XML (KASP, Key and Signing Policy)

...and supporting RFC 5011

.se



Sign the root....

- to realize the greatest benefits from DNSSEC, there needs to be an uninterrupted chain of trust from the zones that choose to deploy DNSSEC back to the root zone.
- The only way to make that happen is to sign the root.

.se



Signing child domains – what is secured delegations?

- The domain must be a sub domain of the parent.
- The domain holder must provide parent with a technical contact person.
- The parent must be able to authenticate the technical contact person for instance by using a certificate signed by a certificate authority trusted by the parent.
- The domain must be delegated to one or more name servers, all of them supporting DNSSEC according to RFC 4033, 4034 and 4035.

.se



Verification

- How to carry out the verification of the link between key – Registrant – domain – technical contact?
- What needs to be verified?
- What attributes are needed to verify?
- How far do we want to go?

.se



Other examples of policies

- <http://www.ripe.net/ripe/draft-documents/dnssec-keyproc.html>
- <http://registro.br/info/dnssec-policy-en.html>

.se



More things needed...

- Automated Updates of DNS Security (DNSSEC) Trust Anchors RFC 5011.
- Publish .SE KSK in ISC DLV? Not decided. We rather think of IANA TAR or, even better, a signed root.
- Standardized API for key exchange with .SE.
- Go deeper into key management in DNS.
- More signing tools for NS service providers.

.se



Thank you for your attention!

amel@iis.se

.se



Exercises! Three different tasks

1. What, in your opinion, is the aim of having a DNSSEC policy and practice statement?
Discussion. Take notes and prepare a short presentation.
2. What, in your opinion, is necessary to put in a policy?
Discussion. Take notes and prepare a short presentation.
3. Critical review of .SE DPS!
Prepare a presentation with the pros and cons with the .SE way.

.se