



DNSSEC in .SE

Patrik Wallström
Project Manager, R&D

.se

.SE DNSSEC History

Procect start

1999 - 2005

Dry run

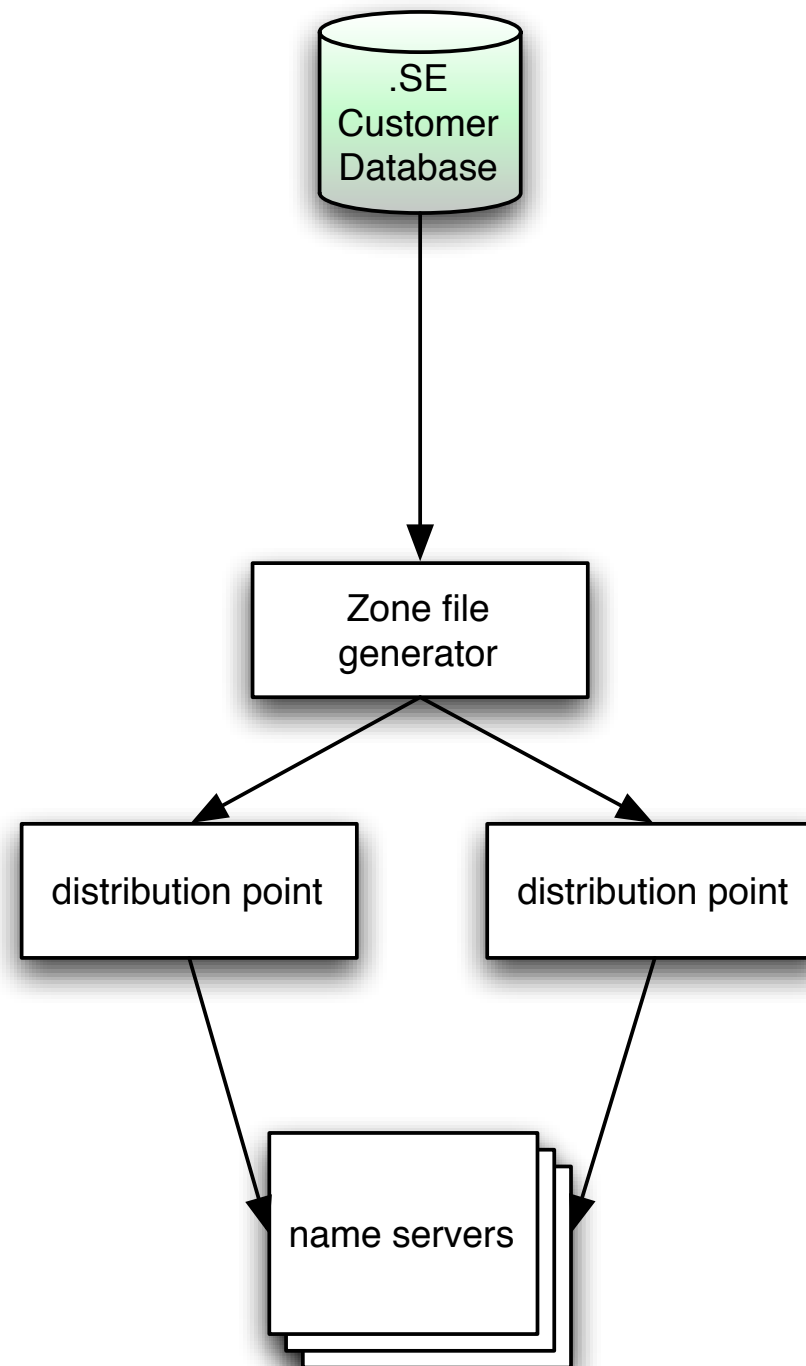
2006

Commercial deployment - .SE DNSSEC

2007 -

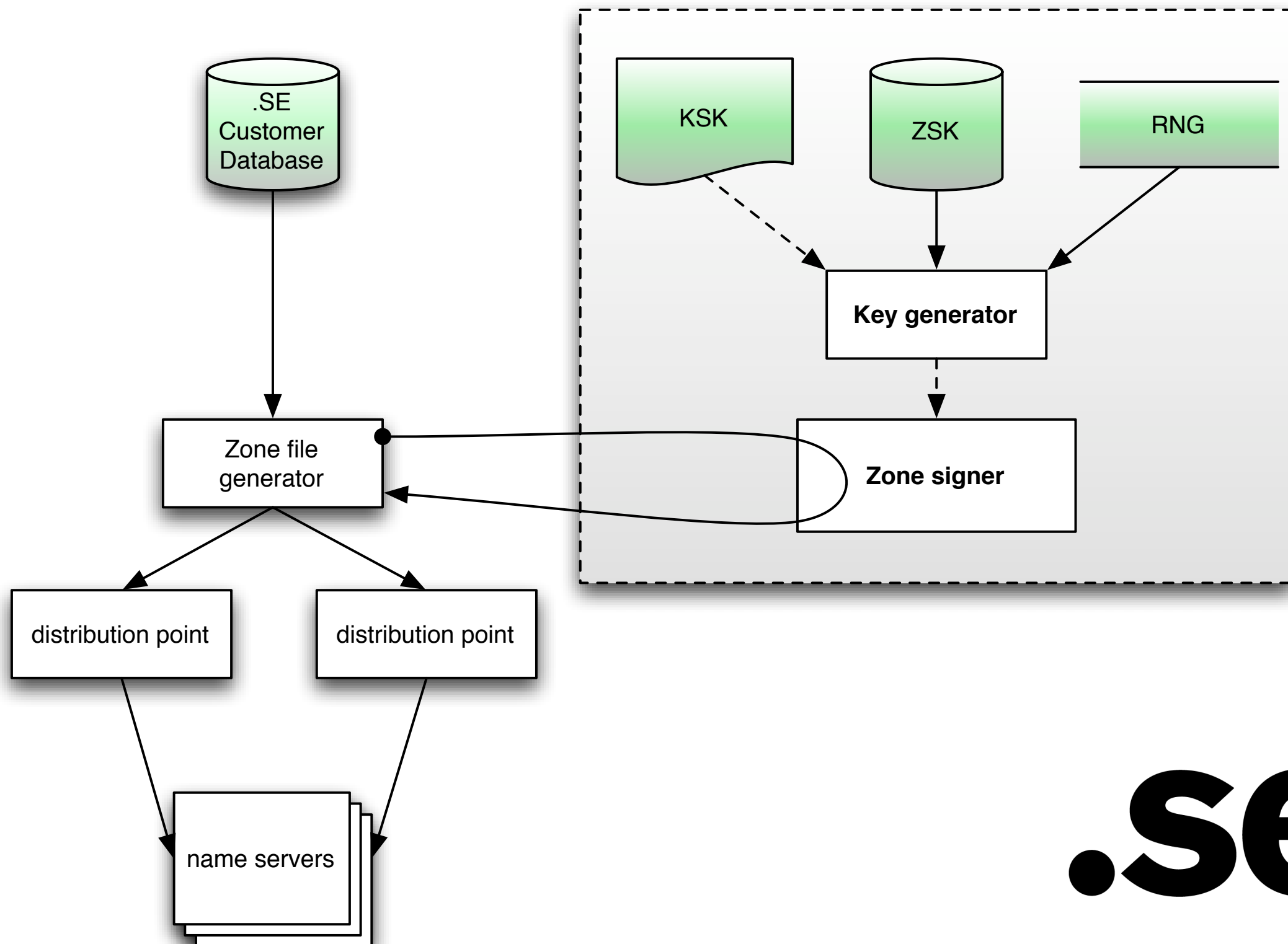
.se

System overview without DNSSEC



.se

System overview with DNSSEC



.se

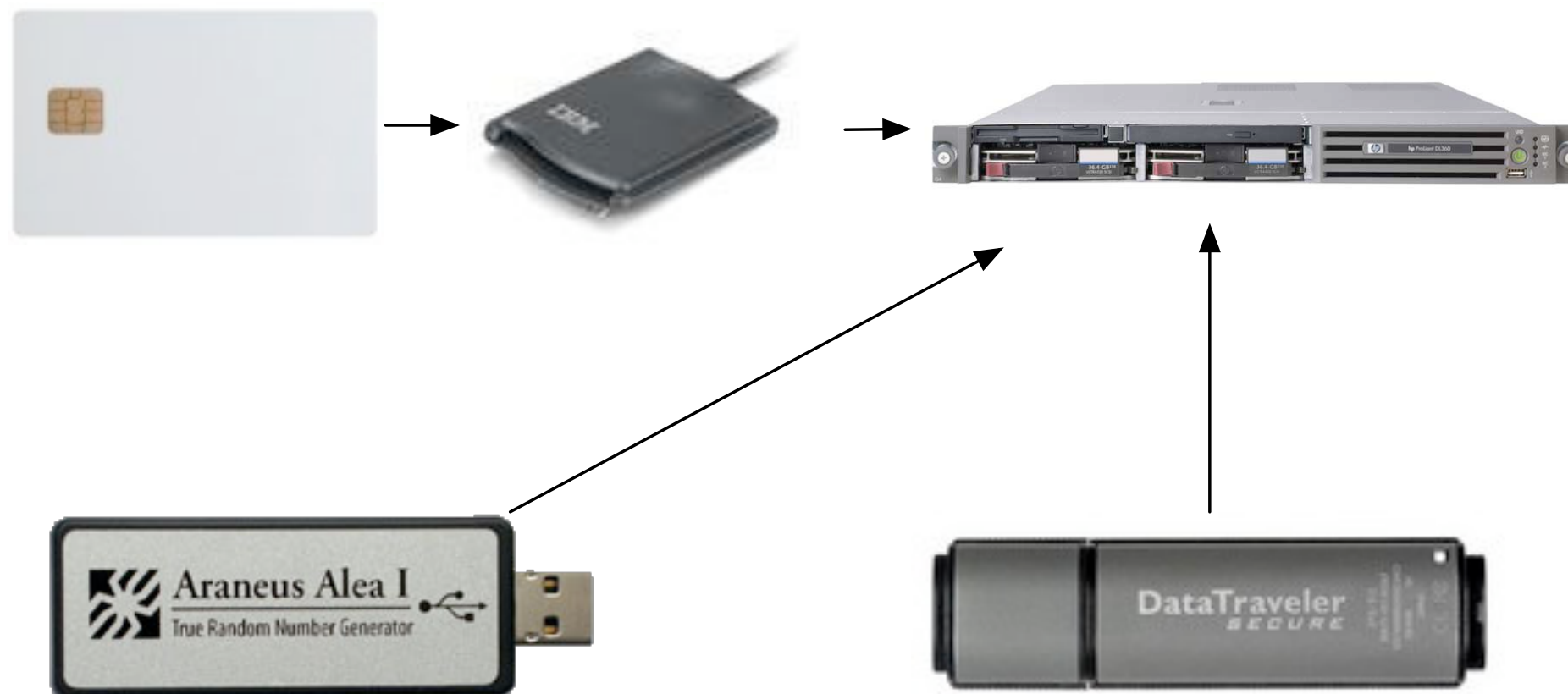


Checklist for generating new keys

- The smartcard(s) with the current key(s)
- A USB cardreader
- A USB random number generator
- A USB memory
- The logbook for logging the event

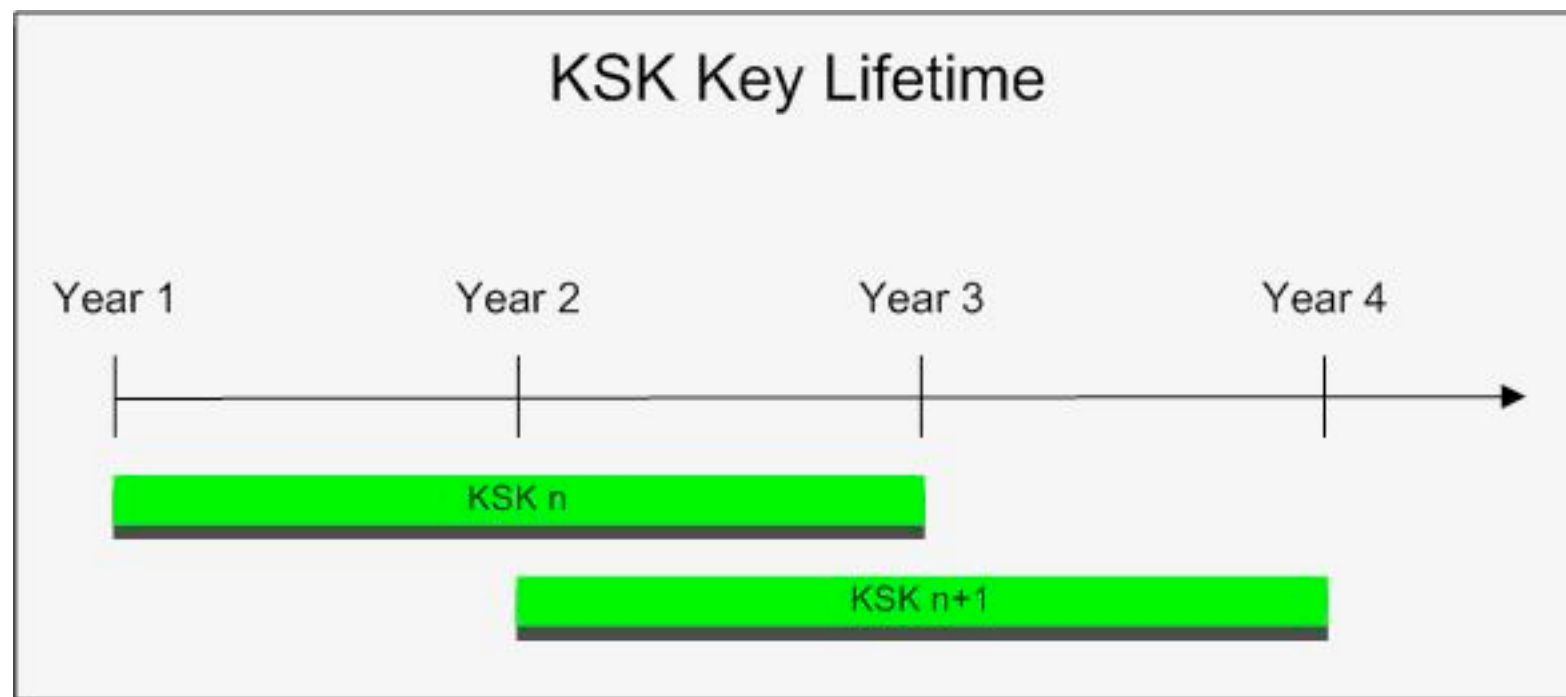
.Se

DNSSEC Key Generator



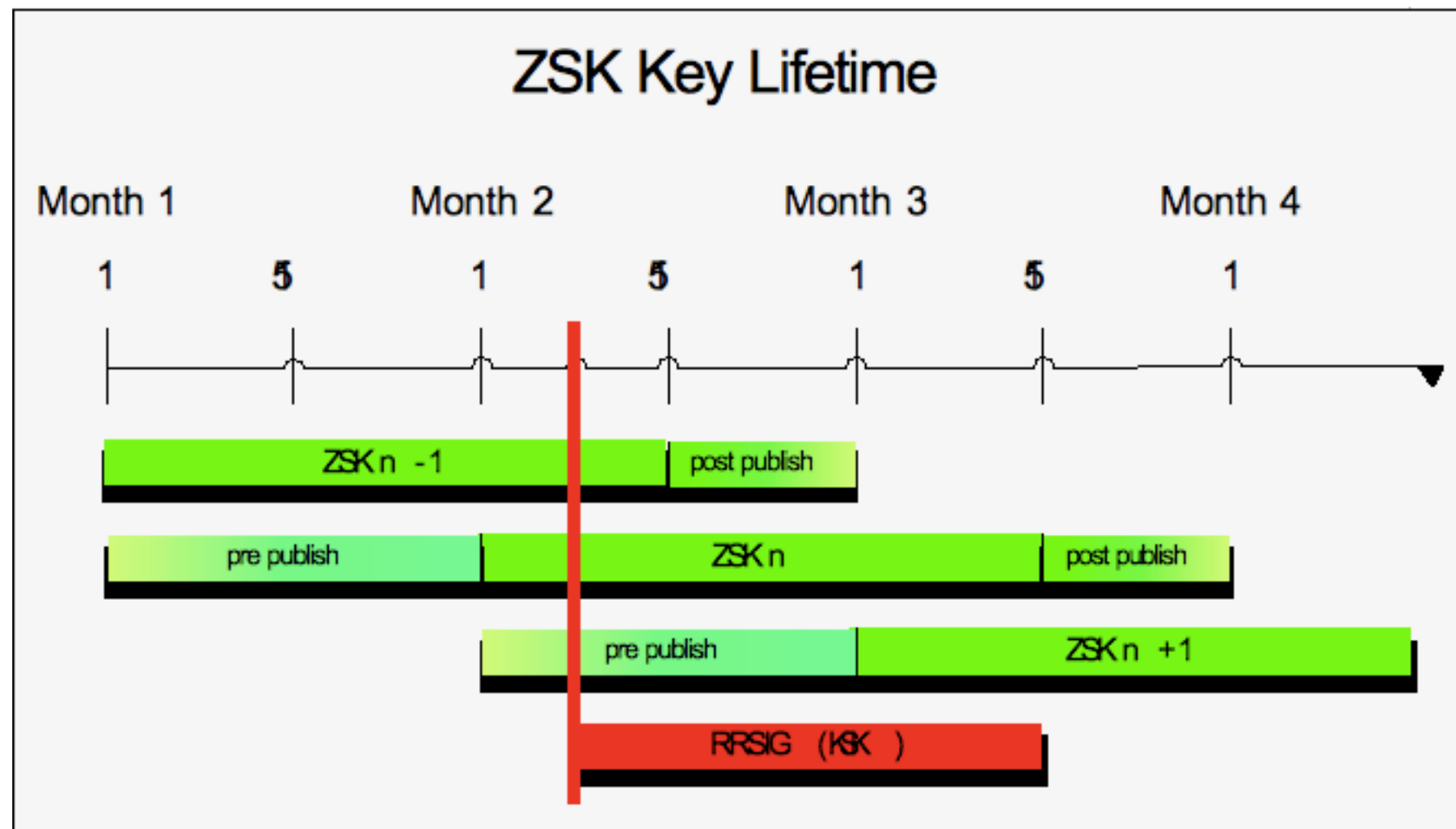
.se

KSK lifetime



.se

ZSK lifetime



.se



The INDEX file

```
se  KSK 5  12345  20060101  20060101  20071231  20071231
se  KSK 5  23456  20070101  20070101  20081231  20081231

se  ZSK 5  34567  20070301  20070401  20070514  20070601
se  ZSK 5  45678  20070401  20070501  20070614  20070701
se  ZSK 5  56789  20070501  20070601  20070714  20070801
...
```

.se

Creating the Key Bundle

The Key Bundle is a set of the current

- public keys
- private ZSK keys

Transferred from Key Generator to Zone Signer with this:



.se



Signing the zone

Using the Key Bundle with online keys

Using ISC BIND 9.4

Wrapper script - mksigned.pl

.se

Signing the zone

```
Oct 17 07:10:02 zonesign mksigned[30760]: alive
Oct 17 07:10:02 zonesign mksigned[30760]: starting zone fetch
Oct 17 07:10:04 zonesign mksigned[30760]: zone fetch done
Oct 17 07:10:04 zonesign mksigned[30760]: starting zone prepare
Oct 17 07:10:06 zonesign mksigned[30760]: zone prepare done
Oct 17 07:10:06 zonesign mksigned[30760]: starting zone merge
Oct 17 07:10:06 zonesign mksigned[30760]: merge zsk 53211
Oct 17 07:10:06 zonesign zonesign.info: loading "se" from "/var/dnssec/tmp/se..UNSIGNED" class "IN"
Oct 17 07:10:32 zonesign zonesign.info: zone se/IN: loaded serial 2008101703
Oct 17 07:10:32 zonesign zonesign.info: dumping "se" to "/var/dnssec/tmp/se..MERGED"
Oct 17 07:10:38 zonesign zonesign.info: OK
Oct 17 07:12:45 zonesign mksigned[30760]: zone merge done
Oct 17 07:12:45 zonesign mksigned[30760]: starting zone signing
Oct 17 07:16:17 zonesign mksigned[30760]: signzone success = 736811
Oct 17 07:16:17 zonesign mksigned[30760]: signzone dropped = 31067
Oct 17 07:16:17 zonesign mksigned[30760]: signzone unsuccess = 59
Oct 17 07:16:17 zonesign mksigned[30760]: signzone runtime = 212.924
Oct 17 07:16:17 zonesign mksigned[30760]: signzone speed = 146.385
Oct 17 07:16:17 zonesign mksigned[30760]: signzone retained = 705642
Oct 17 07:16:17 zonesign mksigned[30760]: signzone generated = 31169
Oct 17 07:16:17 zonesign mksigned[30760]: zone signing done
Oct 17 07:16:17 zonesign mksigned[30760]: starting zone delivery
Oct 17 07:16:24 zonesign mksigned[30760]: zone delivery done
```

.se



Published tools

PKCS15-DNSSEC - For smartcards

DNSSEC-monitor - Nagios monitoring

<http://opensource.iis.se>

.se



Thank you

patrik.wallstrom@iis.se

.se