



# DNSSEC the .SE way: Overview, deployment and lessons learned

Anne-Marie Eklund Löwinder  
Quality & Security Manager

**.se**



# My agenda

- Getting Started
  - Finding out about .se
  - Finding out what DNS does for you
- Why DNSSEC?
  - The arguments for DNSSEC
  - What can happen without DNSSEC
- How do we do DNSSEC in .se?
  - Lessons learned
  - DNSSEC the .se way
- What is in the crystal ball?
- Q&A?

**.se**



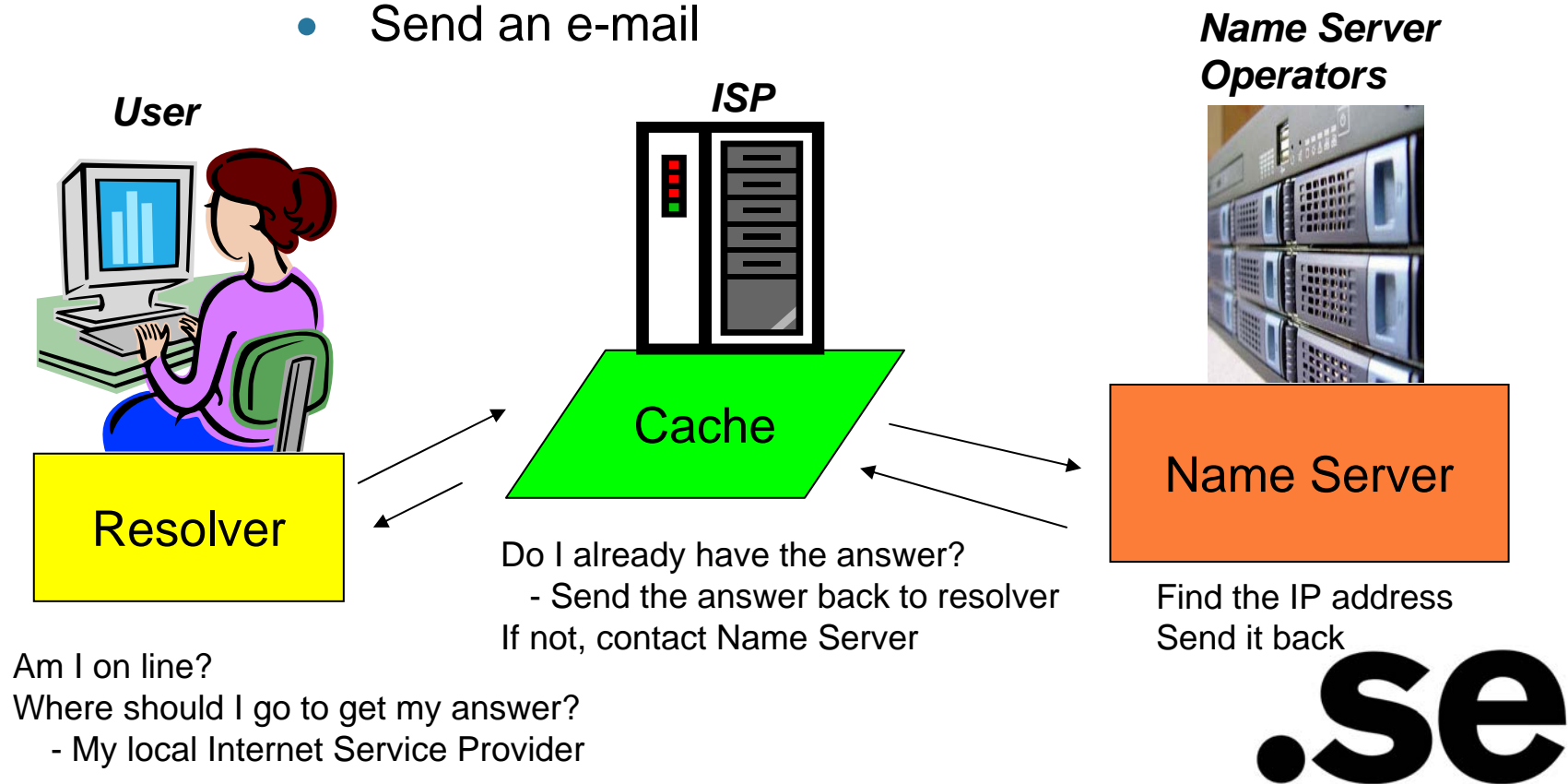
# What is .se?

- The ISO 3166-1 Alpha 2-code element for the Kingdom of Sweden.
- TLD operated by the Foundation of Internet Infrastructure ([www.iis.se](http://www.iis.se)).
  - 759 612 registered domains (2008-09-10; 13:31).
  - A daily growth with >600 domains.
  - 7 Unicast servers + 3 Anycast clusters.
  - Almost 800 signed delegations.
  - ~40 employees

**.se**

# What does DNS do for you?

- Tells devices where to go when you:
  - Type in a web address
  - Send an e-mail





# Why did .SE deploy DNSSEC?

- It increases the data integrity in DNS.
- It increases security for .SE's Registrants and the Internet community.
  - It's a measure against pharming and other
  - It's reinforcing the Internet infrastructure
  - Moreover, a possible extended use of DNSSEC is for safe distribution of attributes in other security protocols and solutions.
- Called upon by the responsible Swedish authority, the Post and Telecom Agency.
- Required to be able to trust new and critical applications.

**.se**



# What is DNSSEC good for?

## **China Netcom falls prey to DNS cache poisoning (The Kaminsky-bug)**

By Jeremy Kirk , IDG News Service , 08/21/2008

One of China's largest ISPs (Internet service providers) has fallen victim to a dangerous vulnerability in the Internet's addressing system, according to security vendor Websense.

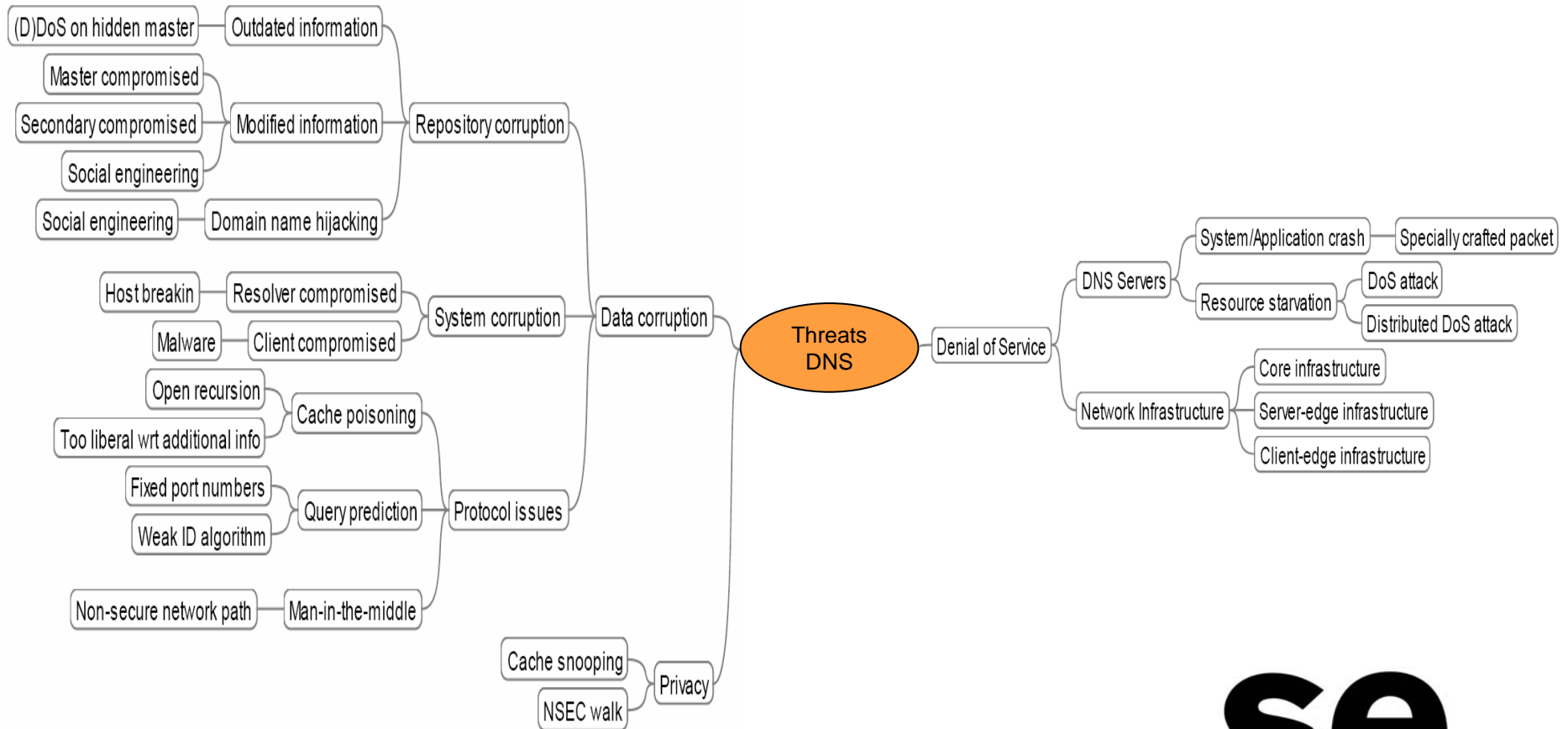
The flaw, which has been described as one of the most serious ones to ever affect the Internet, can cause Web surfers to be redirected to fraudulent Web sites even if the URL (Uniform Resource Locator) has been typed correctly in a browser's address bar.

Discovered by security researcher Dan Kaminsky, the problem is rooted in the DNS (Domain Name System). When a user types a Web address into a browser, the request goes to a DNS server or a cache, which returns the corresponding numerical IP (Internet protocol) address for a Web site.

But the flaw allows the DNS server to be filled with wrong information and direct users to malicious Web sites.

**.se**

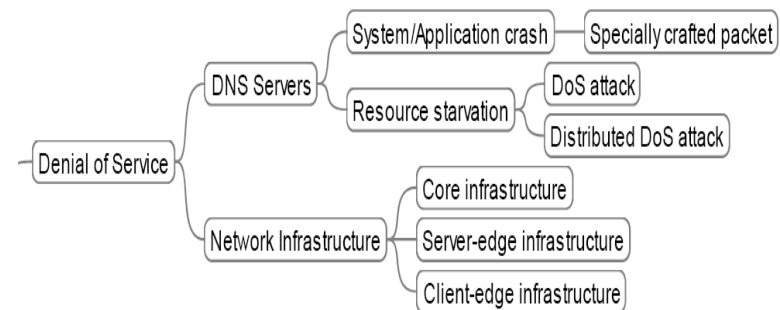
# Threats against DNS



**.se**

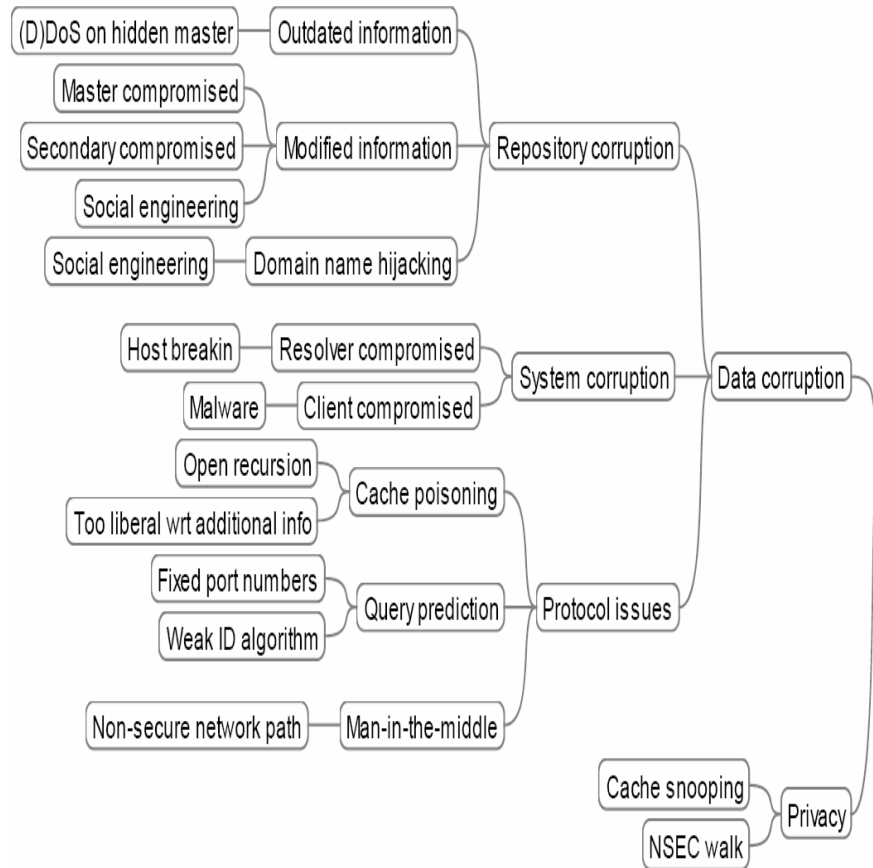
# Threats against DNS

- Protect the infrastructure
  - Anycast
  - Load balancing
  - Diversification of platforms
    - NSD
    - BIND
    - FreeBSD
    - Linux
- Management and surveillance



**.se**

# Threats against DNS



DNSSEC protects from some – but not all!

**.se**



What did we learn?

Quite a lot!

**.se**

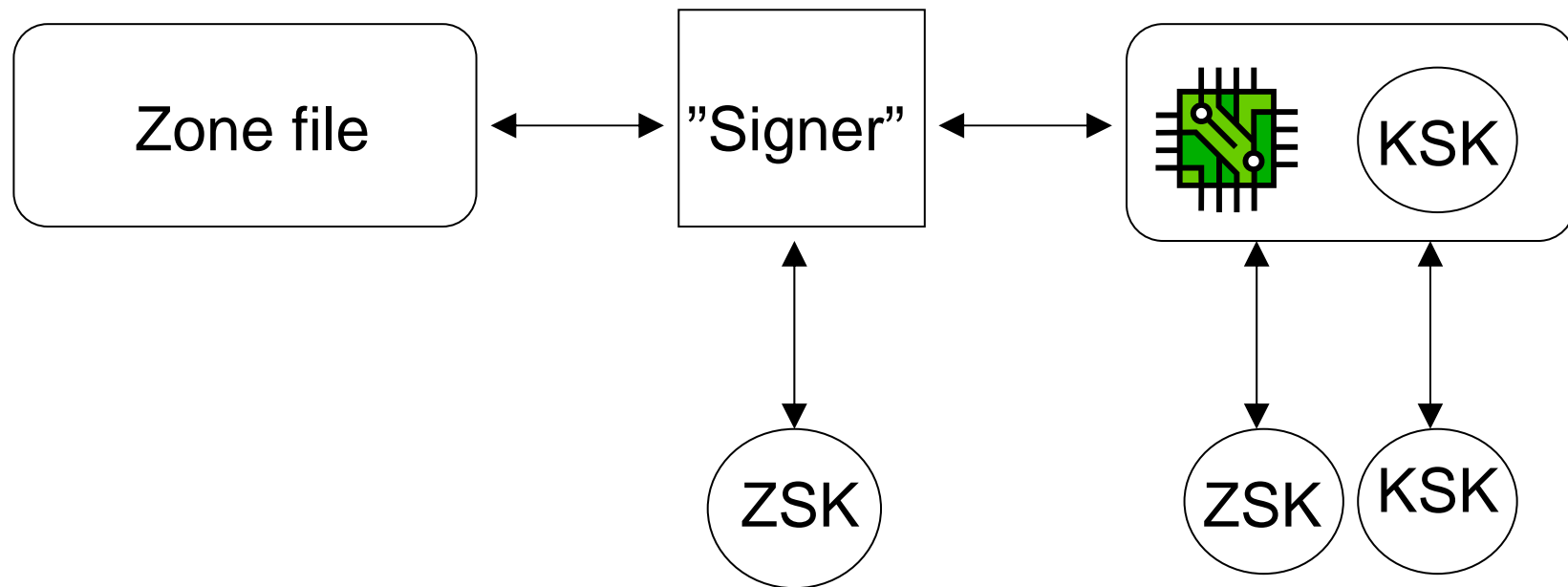


# Important considerations

- The deployment of DNSSEC necessitate a legal analysis. What risk exposure will the deployment imply? To what extent will we need contractual restrictions of the responsible against customers and third parties?
- A self evident ambition is that the level of responsibility should be percieved as reasonable of any partner involved.
- .SE will for instance take no responsibility for the subdomains keys or the administration thereof.
- Stated in .SE DPS – DNSSEC Policy and Practice Statement.

**.se**

# Key administration is essential



**.se**



# Key management in the .se zone

- Technical environment for key management
- Set up routines for:
  - Key generation
  - Key storage
  - Key usage
  - Key rollover (routinely and emergency)
  - Key distribution and publishing

**.se**



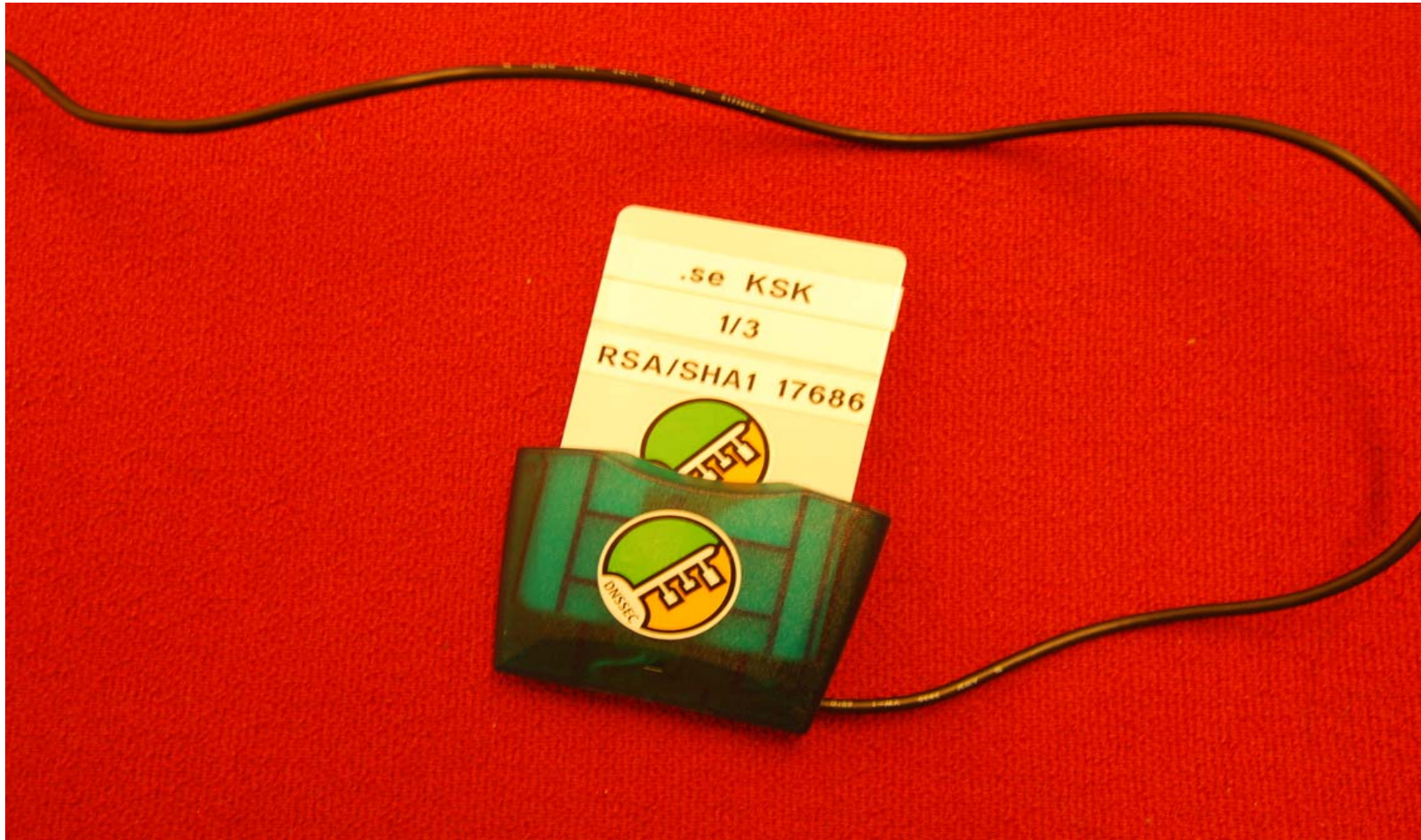
Servers involved... Lockable rack is nice to have.

**.se**



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

**.se**



Smart card and smart card reader.

**.se**



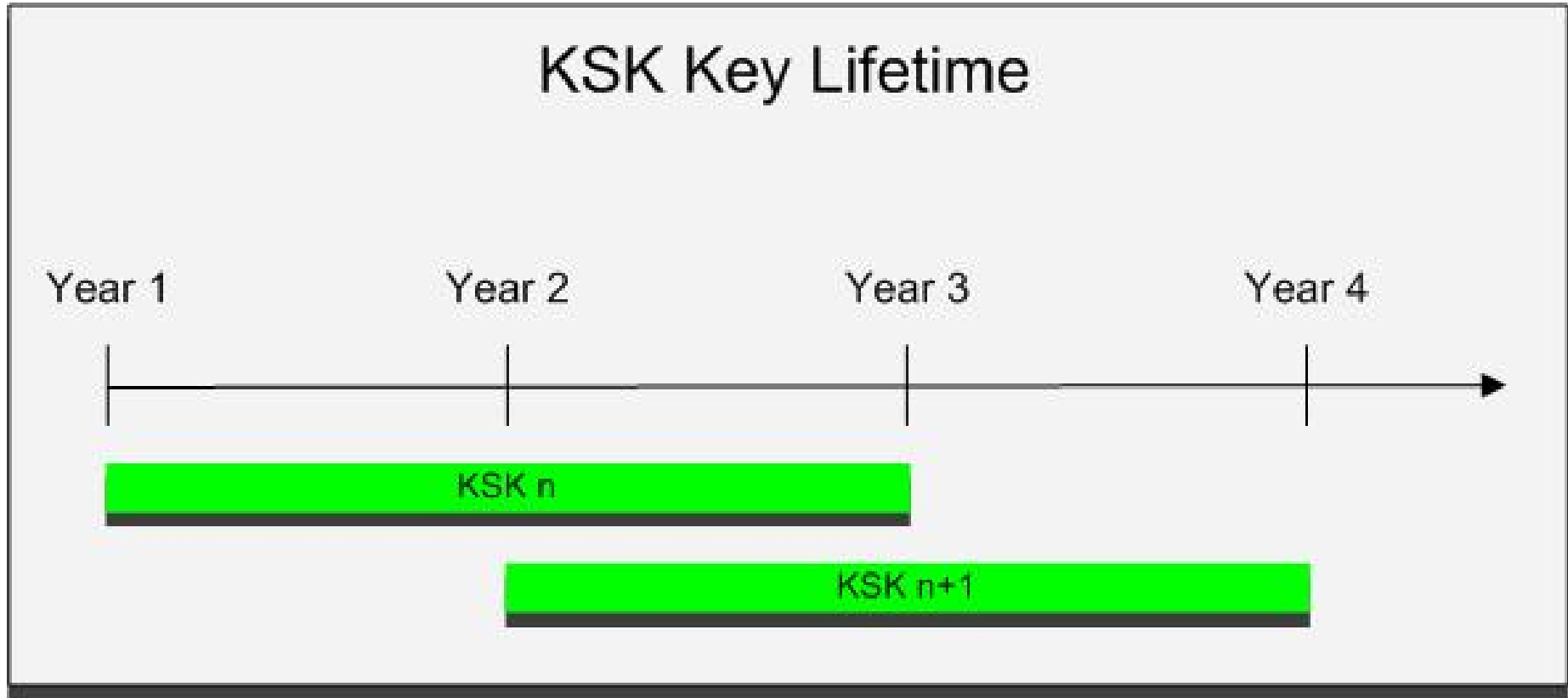
Random Number Generator.

**.se**



## Frequency – Key signing key - KSK

- KSK is only used for signing zone signing keys (ZSK). Generation of KSK takes place once a year.
- Key parameters:
  - RSA
  - 2048 bits key length
- Storage: smart card (FIPS certified)
- Validity period: 2 years. This means that we always have keys with a one year overlap in validity.
- Public KSK is the keys published and distributed to the Internet community.



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

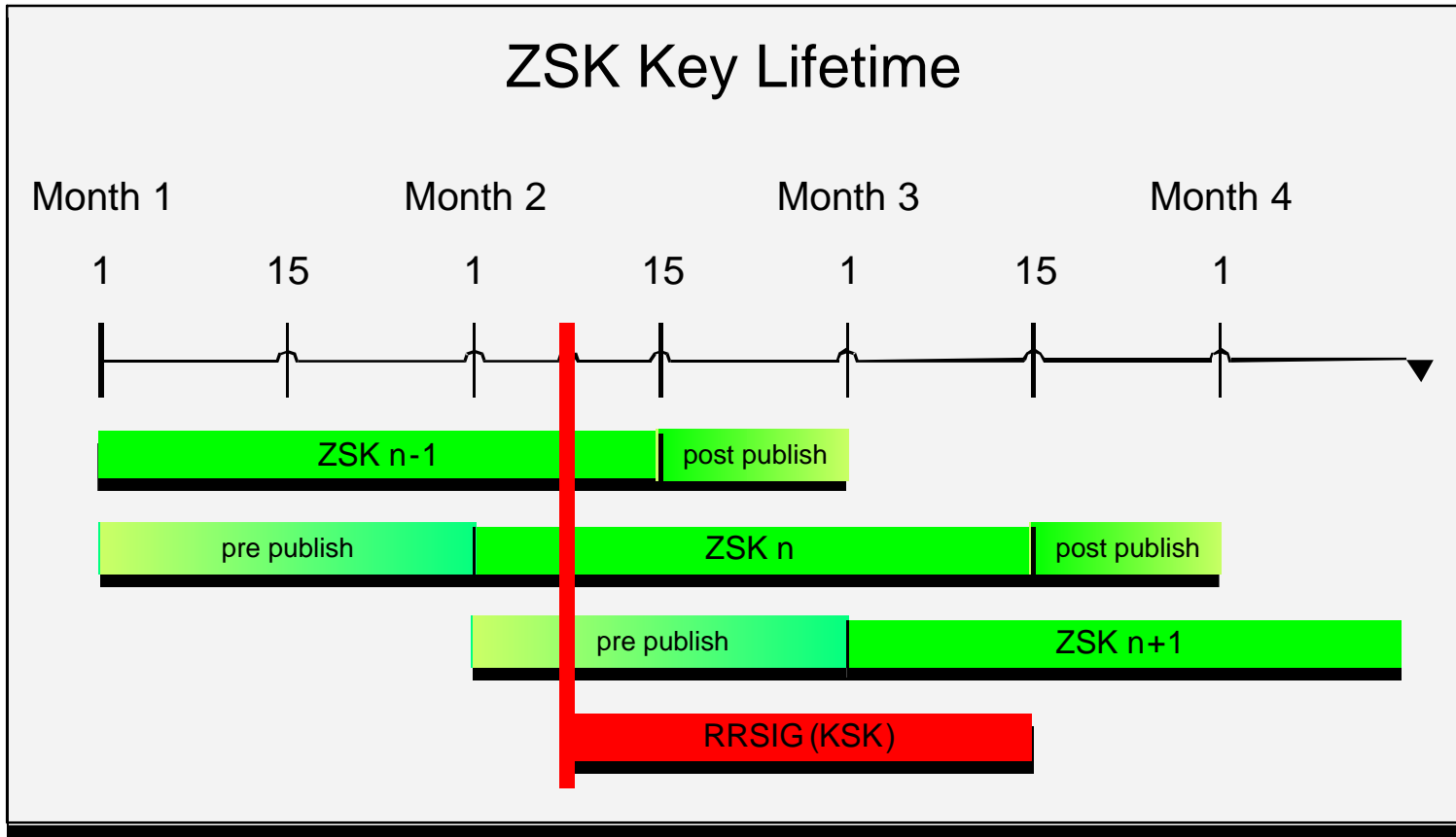
**.se**



# Frequency – Zone Signing Key - ZSK

- The ZSK is solely used to sign data in the .se-zone.
- Generation of ZSK takes place once a month.
- Key parameters:
  - RSA/SHA-1
  - 1024 bits key length.
- Storage: portable storage media (USB).
- Validity period of ZSK is 1 month.

**.se**



**.se**



# Emergency key rollover

- It is very important to have routines for an emergency key rollover! It will occur.
- ZSK has an unsecure window of opportunity of 5 days.
- KSK has an unsecure window of opportunity of 6 weeks, that is as long as the KSK is in use.
- To be able to change KSK in an effective manner we need the root to be signed.

**.se**



# Signing of .SE's own zones

## How to proceed?

- Make someone responsible for the administration of the inhouse domain name management.
- Map all domains available within the organization.
- Check name servers – DNS basic configuration must be up to date and compliant to standard RFC's.
- Choose what domains to start and decide on a progress plan.
- Specify requirements (system, resources, competence).
- Make up a time schedule.
- Strive to achieve automatization.

**.se**



# Monitoring is important

- .SE's monitoring system has been supplemented to maintain basic DNSSEC checking:
  - Warns about signatures on its way to get invalid.
  - Performs tests of the extra DNSSEC-procedures in the production system to be proved correct.
  - Controls the authenticity of certain signatures.

**.se**



# There's more into DNSSEC than just signing a zone...

- You need tools for Key administration and management.
- You need Registrars who offers name services that supports DNSSEC.
- You need Resolver operators to support and enable DNSSEC in the resolvers so signatures will be validated.
- You need applications that supports DNSSEC.

**.se**



# .SE-projects 2008 - DNSCHECK

DNSCHECK - A tool for investigating the quality of DNS-delegations in .SE. Relaunched September 8th – with DNSSEC support in code.

Try it on: <http://dnscheck.iis.se>

Code shared through:

<http://opensource.iis.se/trac/dnscheck>

Nagios has been extended to perform basic DNSSEC checks:

Warn for signatures close to expire

Test for correct DNSSEC additional processing

Checks the integrity of some signatures

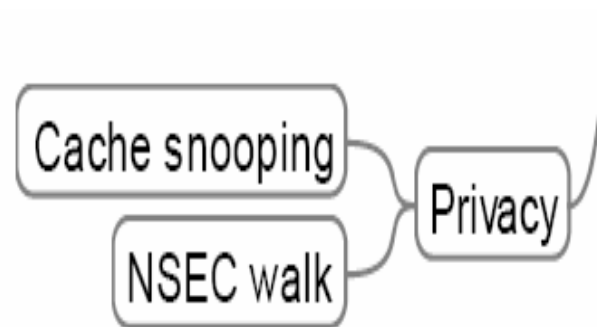


**.se**



# Implementing NSEC3

- Replaces NSEC (that allows zone walking).
- Complicated migration.
- Software support needed, NSD och BIND.



**.se**



# AKM

- Automatic Key Management for .SE
- ...supporting DNSSEC-Policy-XML (KASP, Key and Signing Policy)
- And supporting Automated updates of Trust Anchors according to RFC 5011.

**.se**



# What else is in the Chrystal ball?

- The [US] Federal Government will deploy DNSSEC to the top level .gov domain by January 2009.  
<http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf>
- More and more TLD's will be signed. Root soon to be signed?  
[http://www.iis.se/docs/brev\\_iana\\_pdf.pdf](http://www.iis.se/docs/brev_iana_pdf.pdf)

**.se**



# Find out more about DNSSEC

<http://www.dnssec.net/why-deploy-dnssec>

<http://www.dnssec-deployment.org/>

- RFC 4033, 4034 & 4035 (DNSSEC bis) published in March 2005.
- RFC 5011 Automated Updates of DNS Security (DNSSEC) Trust Anchors published in September 2007.
- RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence (NSEC 3) published in February 2008.

**.se**



Questions?  
Maybe later?  
[amel@iis.se](mailto:amel@iis.se)  
+46 8 4523517  
<http://www.iis.se>

**.se**