DNSSEC in Sweden: Five Years of Practical Experience

Anne-Marie Eklund Löwinder
Quality and Security Manager
Amel@iis.se
http://www.iis.se

.se

What’s the problem

- Up until recently, DNSSEC looked like a solution looking for a problem…
  - Kudos Dan Kaminsky, for showing DNSSEC’s real value.
  - http://www.kaminskybug.se/movie_en/

What risks?

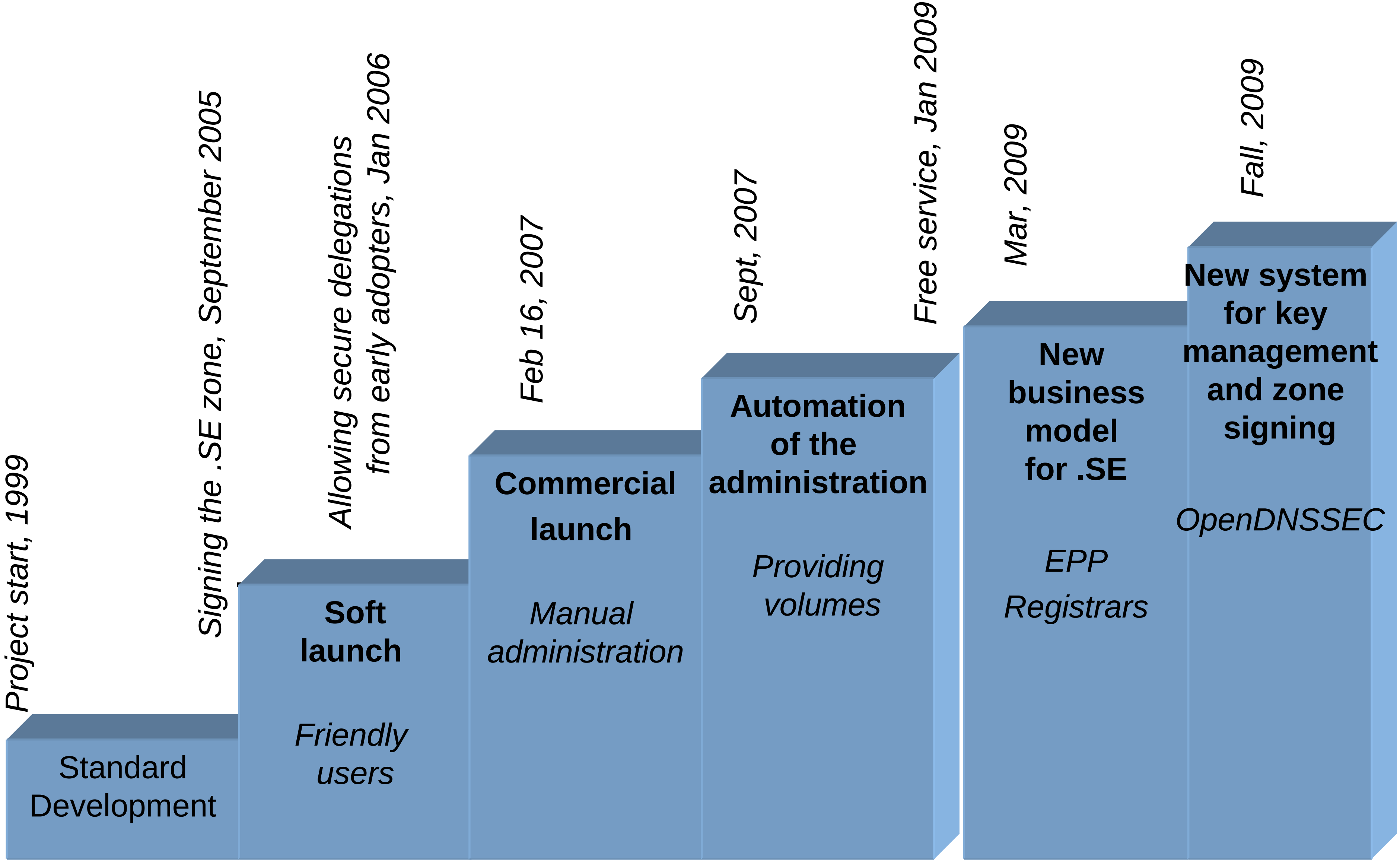
- MANY case scenarios
- Scary things like:
  - MX hijacking
  - Entire domain redirection
  - Take a large domain off line
  - Complete spoofing of a bank's DNS info

Long term solution

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.

Knowledge based on experience



Project start, 1999

Standard Development

Signing the .SE zone, September 2005

Allowing secure delegations from early adopters, Jan 2006

Soft launch

Friendly users

Feb 16, 2007

Commercial launch

Manual administration

Sept, 2007

Automation of the administration

Providing volumes

Free service, Jan 2009

Mar, 2009

New business model for .SE

EPP

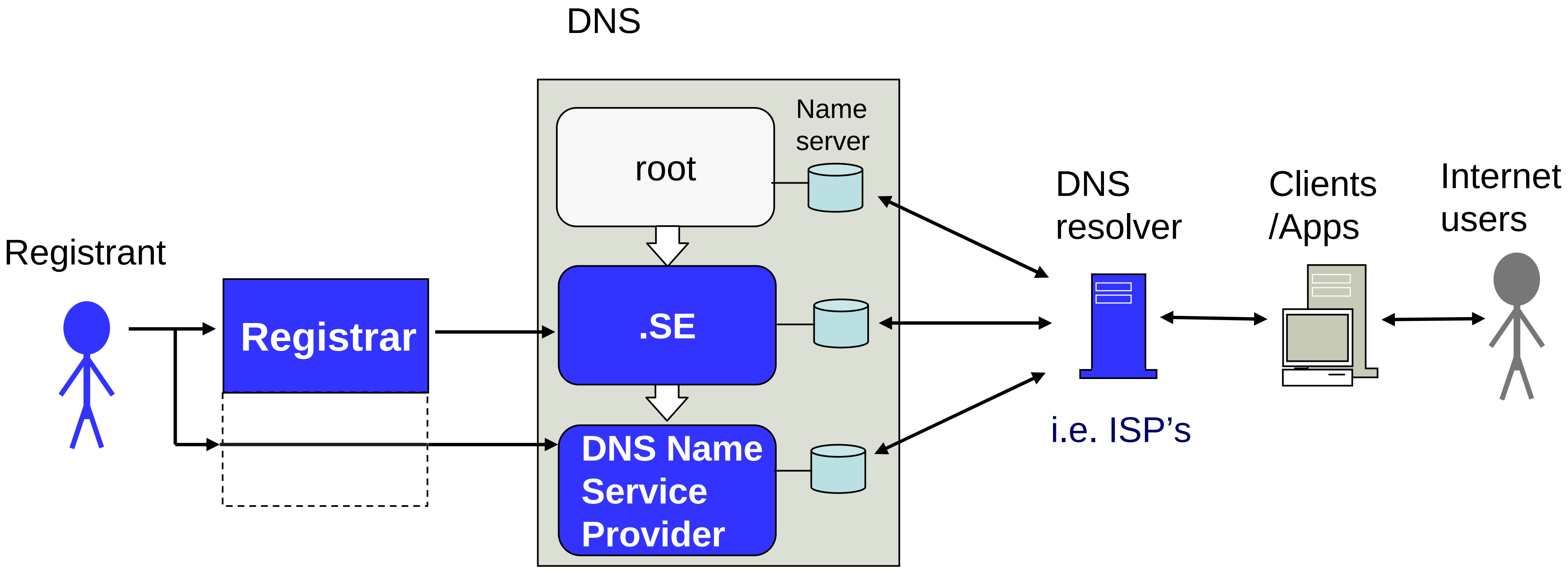
Registrars

Fall, 2009

New system for key management and zone signing

OpenDNSSEC

Try to get ALL on board from start!



Key findings from survey

Registrants	A greater demand than expected.
.SE Registrars	With few exceptions, unused and unwilling to handle new domain services.
DNS operators	The service is often taken for granted and bundled. It is very important that it is properly managed.
.SE	The first add on service, needs development of system, organisation and routines.
Resolvers (ISP’s)	A willingness to introduce DNSSEC in resolvers.
Applications	Immature area.
Internet users	Ignorant and unaware of risks.

Some figures (2010-01-22)

- DNSSEC ready Registrars – 12
- DNSSEC signed zones in .SE – ~2000 (940 000)
- ISP's validating signatures in resolvers – a majority of the largest broadband service providers in Sweden
- A number of signed TLD's in the world .cz .pr .museum(-) .nu .li .ch .se .org .gov .th .bg .na
- And more will follow…

Key management is important

- Technical environment for key generation
- Routines defining the operation:
  - Key generation (strictly and well defined routines).
  - Key storage (smart cards, HSM, soft HSM).
  - Key usage (KSK + ZSK).
  - Key rollover (frequency and routines).
  - Key publishing (who needs to know).
  - Plans for roll back while deploying DNSSEC and for emergency key roll over when in operation.

A DNSSEC Practice statement - DPS

- Defines the quality of the system.
- Explains what is agreed and decided.
- No legal status of the document, serve as guidelines to the user as a leyman to decide on how to do DNSSEC.
- To clarify the operation of DNSSEC in terms of what it offers and what people can expect from it.
- Offers liability.

What is important to put in a practice statement?

- The roles of the different parties involved, who will do what, and the workflow of how to get it done.
- Threat analysis, version of software, which party is responsible for what when a domain holder gets problem.
- Limitation of liability.
- How to handle keys, frequence of replacement of keys, algorithm(s) used, key length, how many people and who can (and may) handle keys, where and how to publish
  public keys.

RFC Draft - DNSOP wg

- https://datatracker.ietf.org/drafts/draft-ietf-dnsop-dnssec-dps-framework/
- Presents a framework to assist writers of DNSSEC Signing Policy and Practice Statements such as Regulatory Authorities and Registry Managers on both the TLD and secondary level, who is operating a DNS zone with Security Extensions (DNSSEC) implemented.

Key rollover

- How to handle key rollover?
  - How can you ensure that when the key has to be changed,
    it is propagated securely, safely, and quickly?
- RFC 5011
- Tools for automation.
- IANA’s ITAR

Methods for distribution of current public Key Signing Keys (KSK)

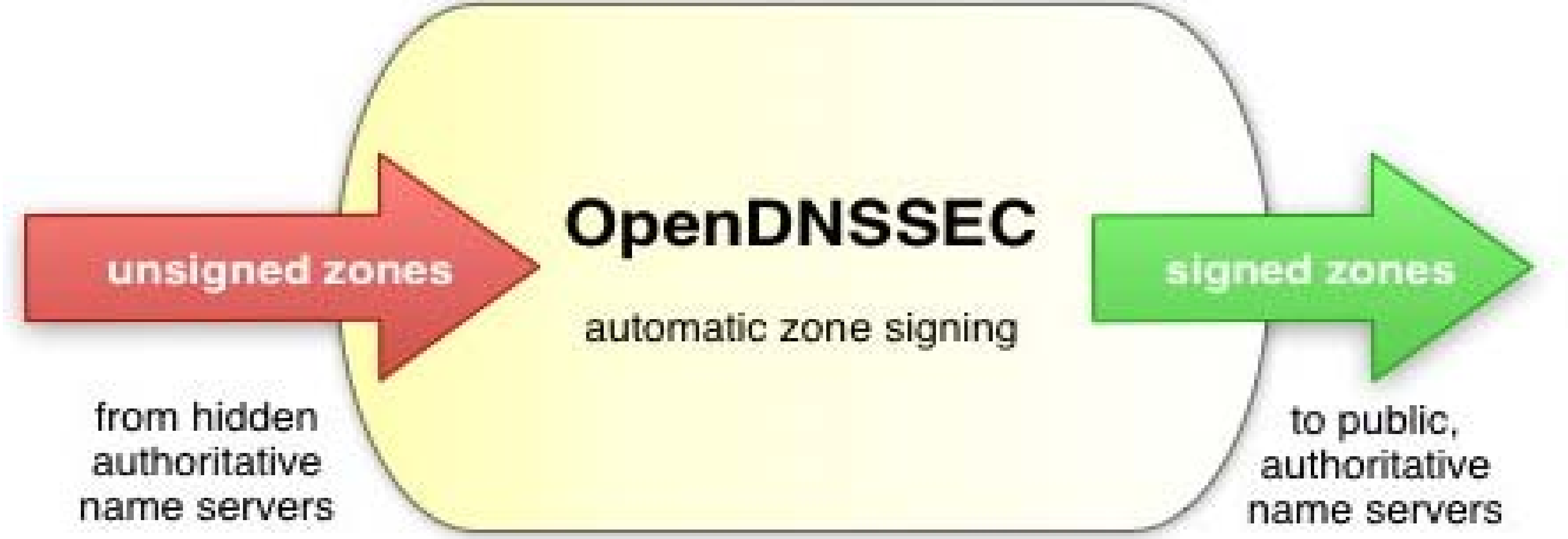
- Through a ssl-protected web site.
- Signed with PGP and .SE's official PGP key.
- KeyID of the PGP key.
- .SE's official PGP key: http://subkeys.pgp.net:11371/pks/lookup?op=get&search=0xFCEC5128F440EE9B
- Mailing list for important announcements.
- Advertisement in computer related magazines.
- Use ICANN's Interimistic Trust Anchor Repository (ITAR)

Tools for self-help

- DNSCheck http://dnscheck.iis.se
  - Tool for checking delegation in DNS
  - Also tests for DNSSEC

- The Kaminskytest http://thekaminskybug.se
  - Test your domain
  - Test your resolver

Developing a turn key system



unsigned zones

from hidden authoritative name servers

OpenDNSSEC

automatic zone signing

signed zones

to public, authoritative name servers

Open DNSSEC

Open source solution for a fast and easy DNSSEC deployment

OpenDNSSEC is a co-operation between .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei and John Dickinson.
http://opendnssec.se

Moving forward

- Root must be signed – in the meantime we have put .SE:s public keys in ICANN’s (IANA) ITAR.
- Evangelize the need for DNSSEC at industry – companies – organizations – making them interested and show them why DNSSEC is needed.
- Offer support and assistance to colleague TLD’s among others who wants to implement DNSSEC.
- Policies must be established.
- Registrars, network operators, registries, ICANN, root server operators … such large network will have to coordinate and interact.
- DPS IETF RFC Draft - work in progress.

Thank you…

Questions?