.SE-DNSSEC
one year of experiences

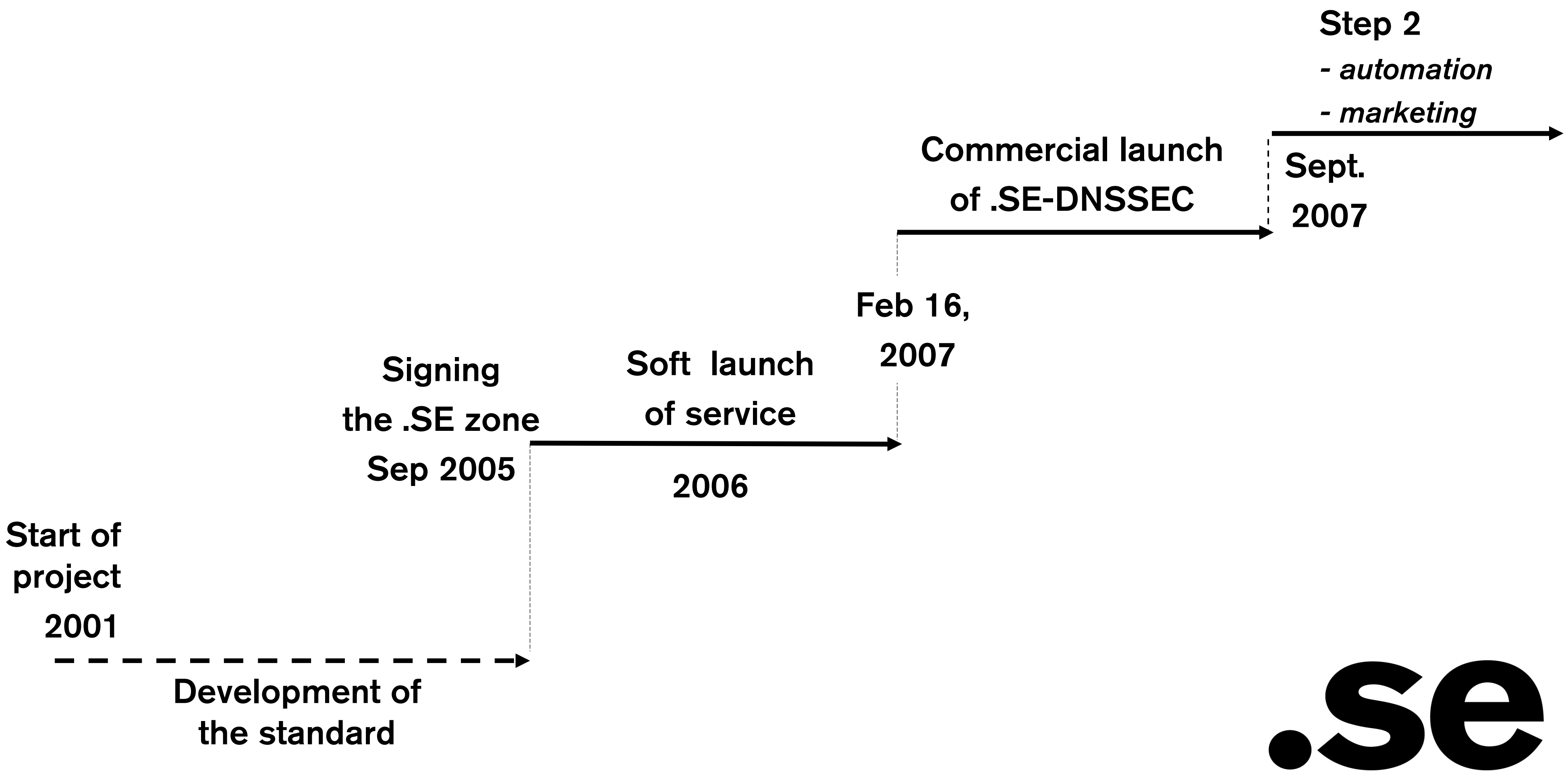
- Background
- The market
- .SE's service
- Operational experience
- Future plans

Staffan.Hagnell@iis.se

Why DNSSEC?

- DNSSEC to assure correct DNS data
  - do not protect against all kind of frauds, (PC's and Users are more vulnerable)!
- .SE wants DNSSEC!
  - it is our responsibility to provide a high quality DNS-service (not only available but also correct)
  - as a repository for other security information (certificates and keys for IPsec, SSH, PGP, DKIM …?)
  - recommended by our supervisory agency

.SE-DNSSEC History



Start of project

2001

Development of the standard

Signing the .SE zone

Sep 2005

Soft launch of service

2006

Feb 16, 2007

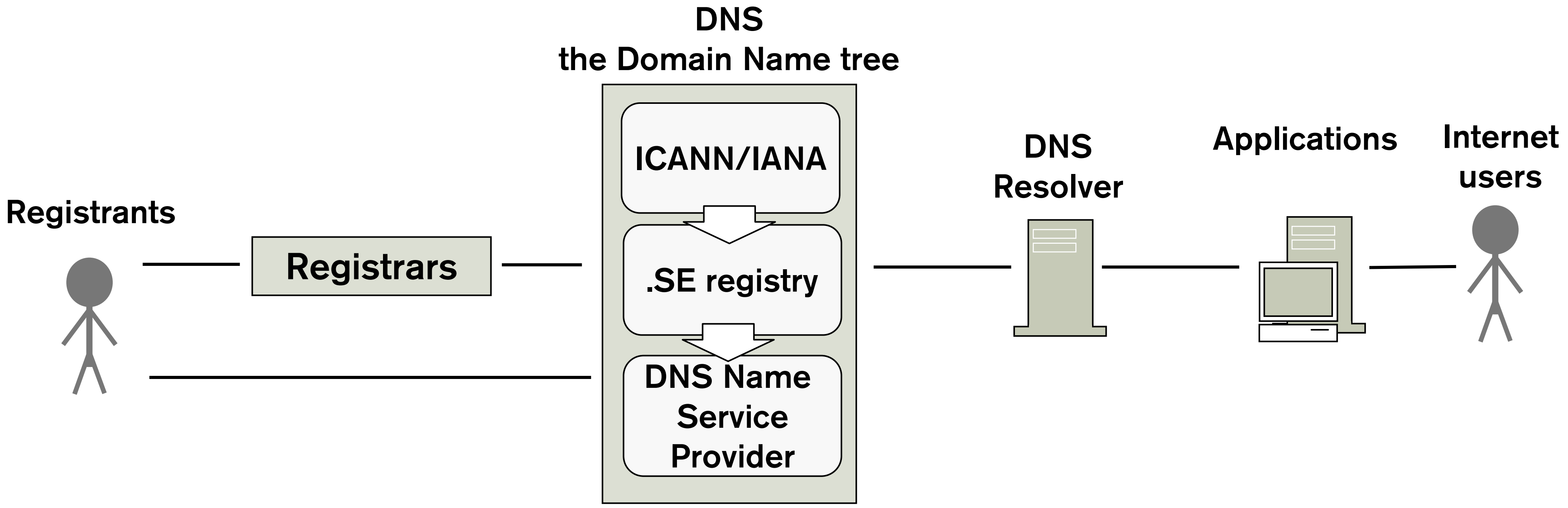
Commercial launch of .SE-DNSSEC

Sept. 2007

Step 2

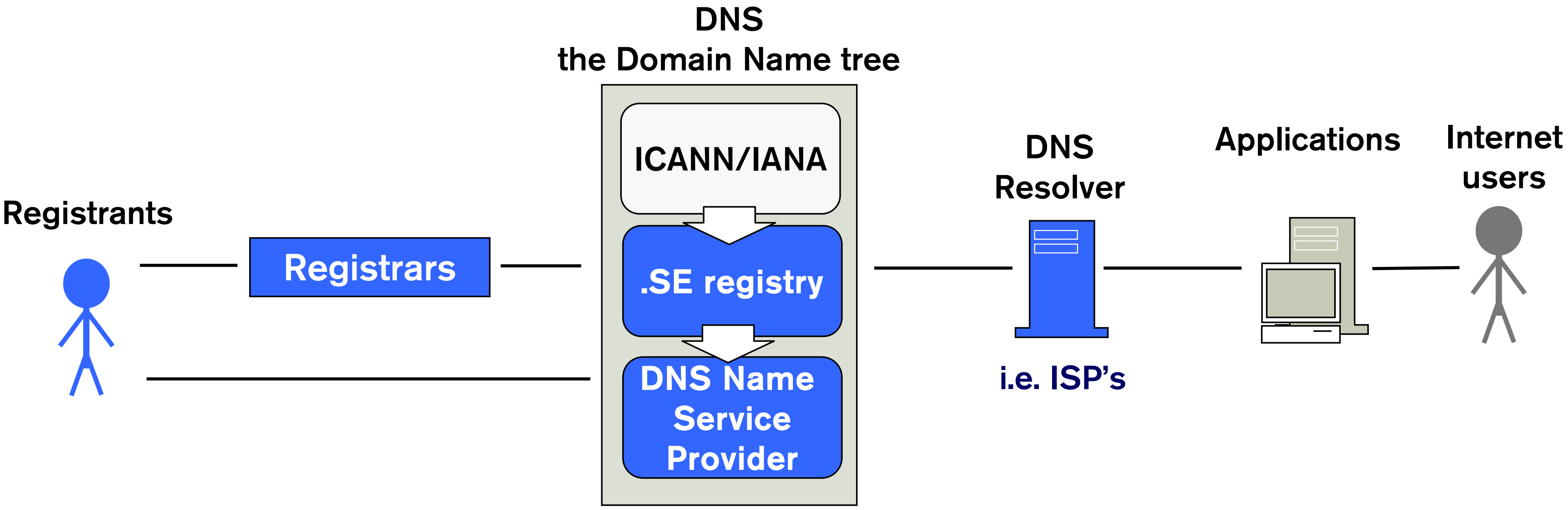
- *automation*
- *marketing*

The market – the value chain



.se

A first step – DNSSEC validation made by Resolvers

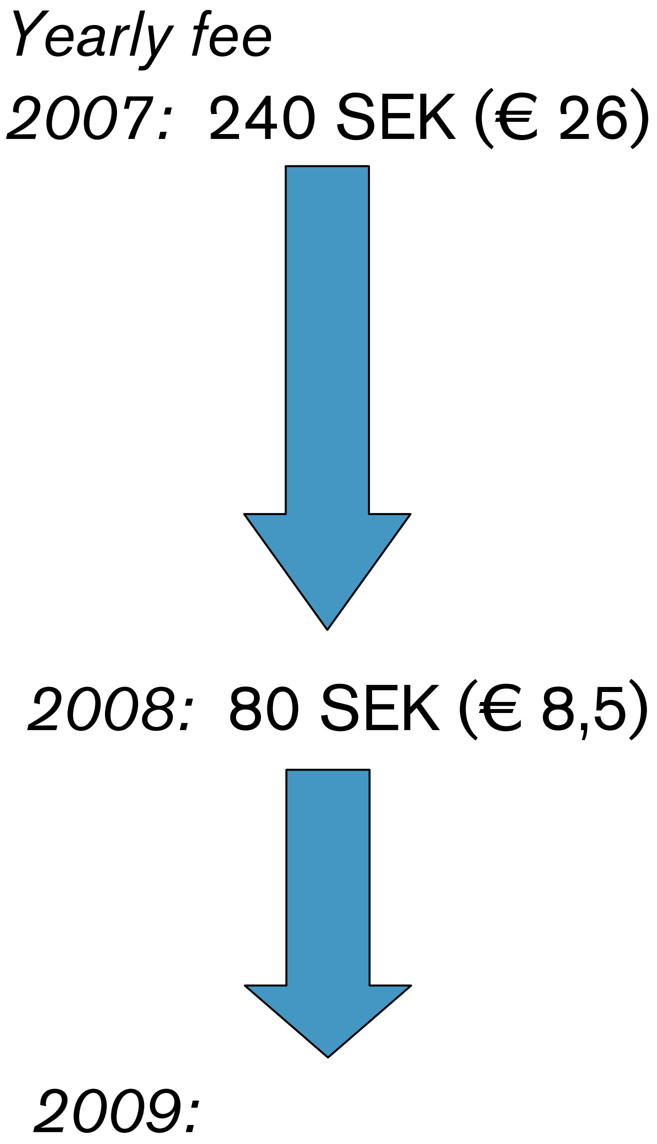


STATUS for .SE February 2008

Registrants	There is a demand to get DNSSEC!
.SE Registrars	It has taken us some time to get them interested. It has taken them time to prepare their marketing effort, technique, and administration
DNS Name Service Providers	Lack of administrative tools for DNSSEC. This is a major problem!!!
.SE	Our first additional service, some automations in place but more is needed, still a need to coordinate the value chain
Resolvers	A good start by the largest ISP's
Applications	*Not yet*
Internet Users	*Not yet*

Pricing strategy

- An additional service
- Kick-backs and establishment subsidiaries to registrars



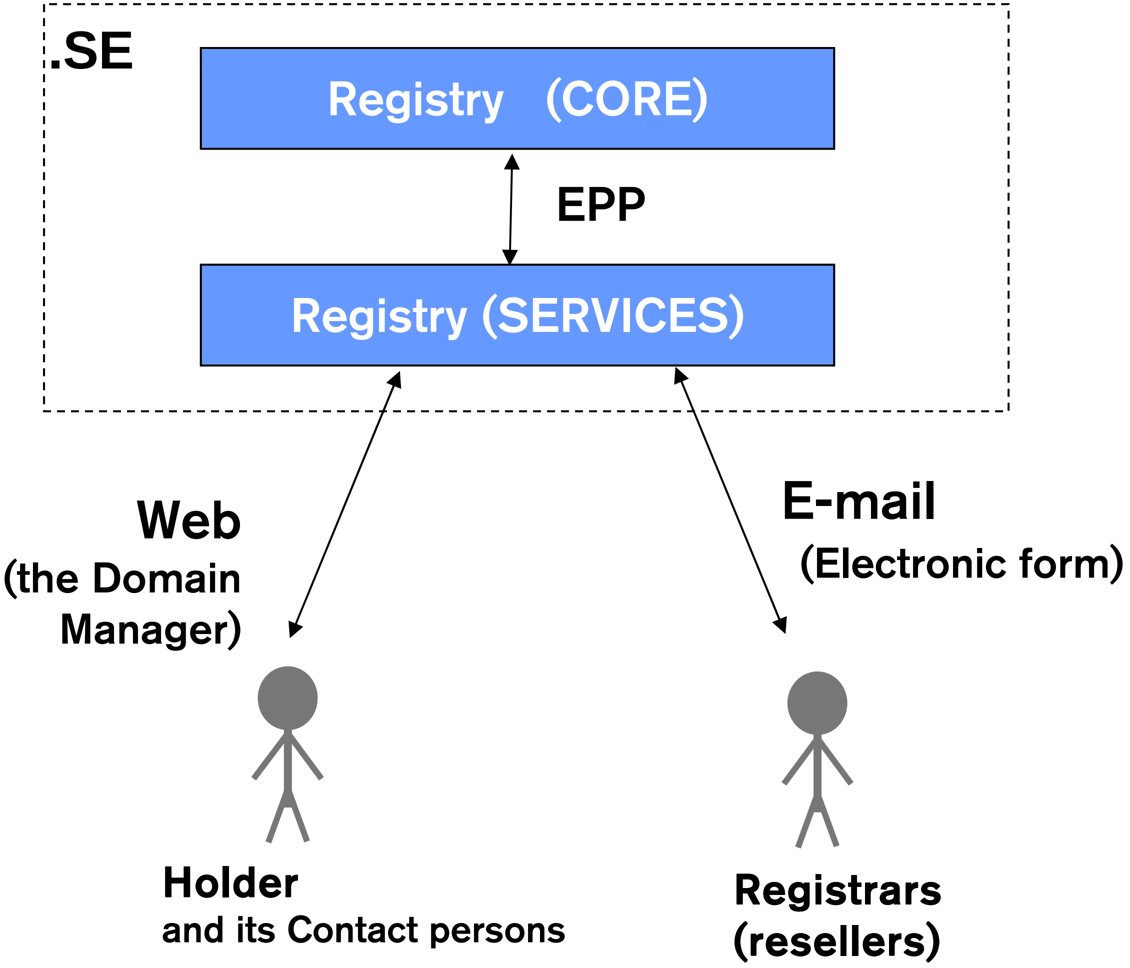
Yearly fee

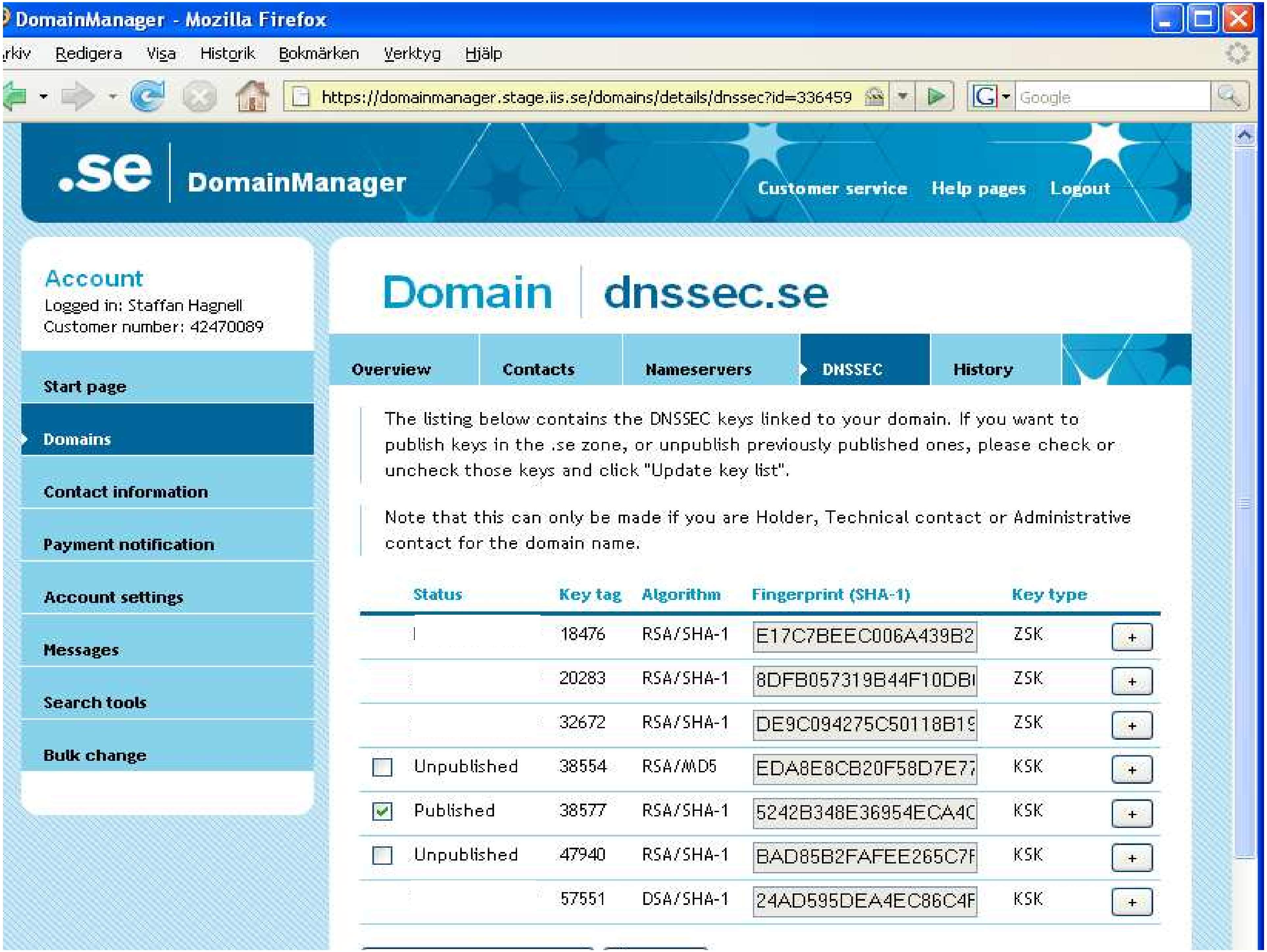
2007: 240 SEK (€ 26)

2008: 80 SEK (€ 8,5)

2009:

.SE's service - user interfaces





https://domainmanager.stage.iis.se/domains/details/dnssec?id=336459

Account

Logged in: Staffan Hagnell
Customer number: 42470089

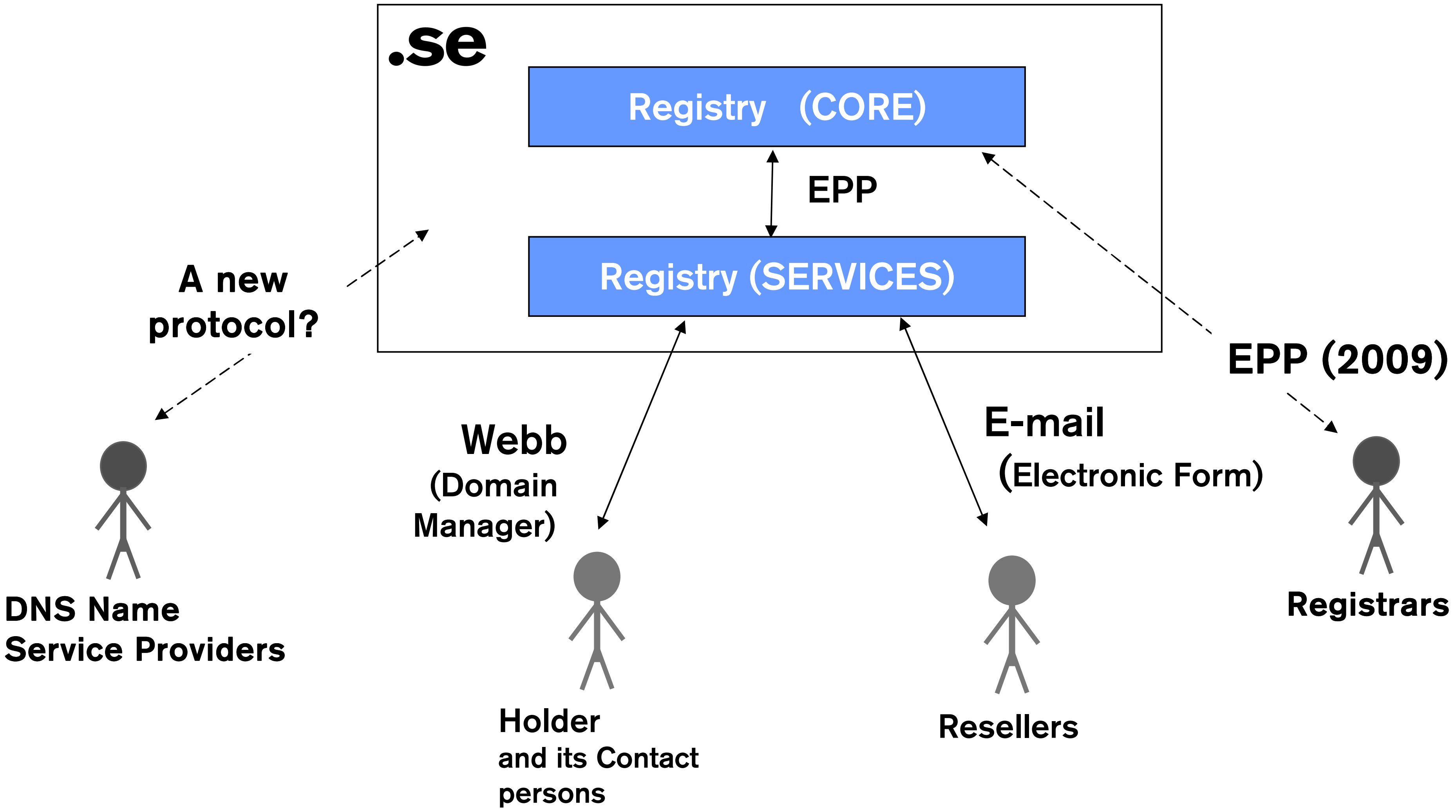
Domain | dnssec.se

The listing below contains the DNSSEC keys linked to your domain. If you want to publish keys in the .se zone, or unpublish previously published ones, please check or uncheck those keys and click "Update key list".

Note that this can only be made if you are Holder, Technical contact or Administrative contact for the domain name.

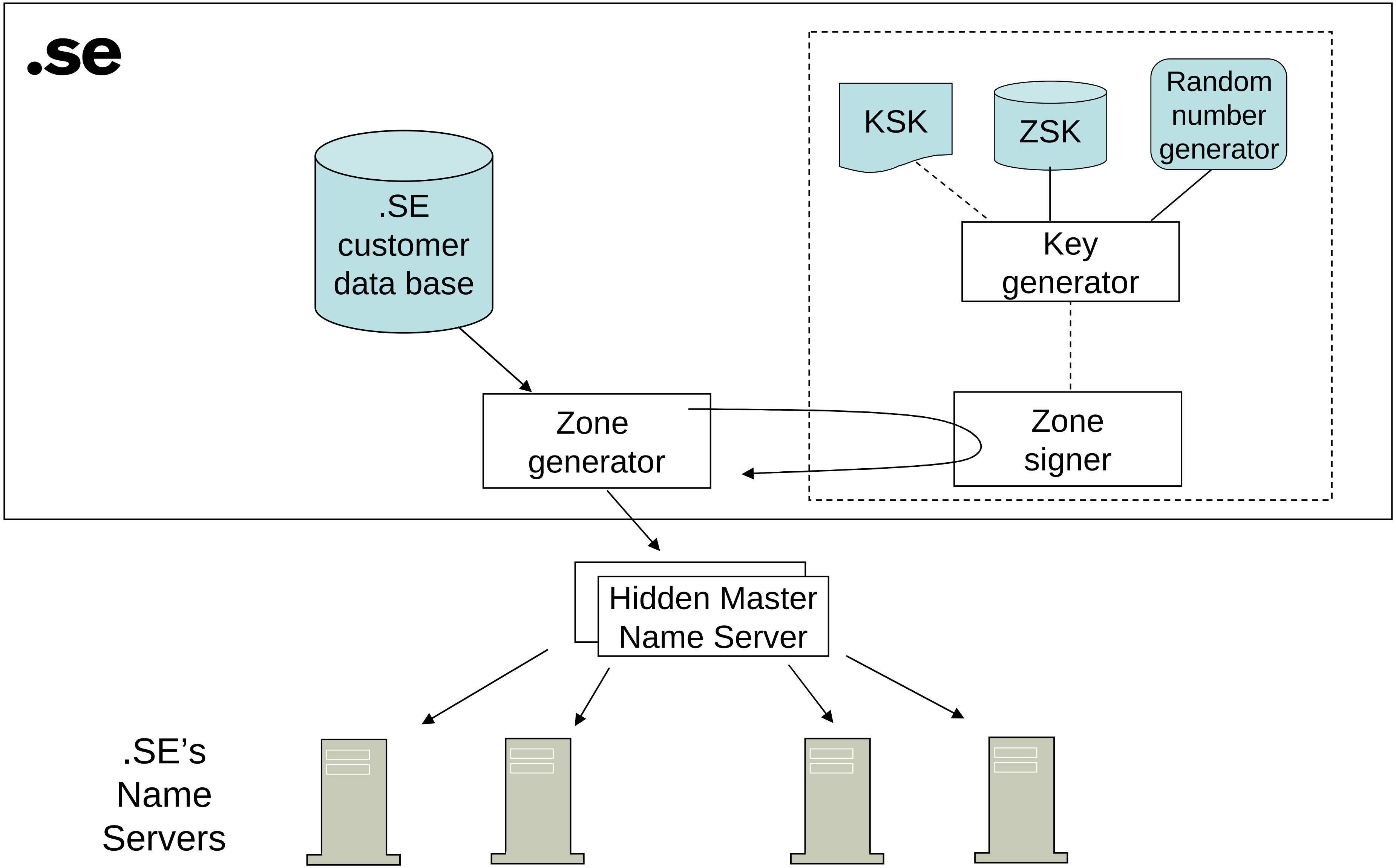
	Status	Key tag	Algorithm	Fingerprint (SHA-1)	Key type	
		18476	RSA/SHA-1	E17C7BEEC006A439B2	ZSK	+
		20283	RSA/SHA-1	8DFB057319B44F10DBI	ZSK	+
		32672	RSA/SHA-1	DE9C094275C50118B1	ZSK	+
☐	Unpublished	38554	RSA/MD5	EDA8E8CB20F58D7E7	KSK	+
☑	Published	38577	RSA/SHA-1	5242B348E36954ECA4C	KSK	+
☐	Unpublished	47940	RSA/SHA-1	BAD85B2FAFEE265C7F	KSK	+
		57551	DSA/SHA-1	24AD595DEA4EC86C4F	KSK	+

Interfaces for .SE-DNSSEC 2009



se KSK
1/3
RSA/SHA1 17686

Araneus Alea I


.se
.SE customer data base
KSK
ZSK
Random number generator
Key generator
Zone generator
Zone signer
Hidden Master Name Server
.SE's Name Servers

Selection of a tool for signing .SE's own domain (spring 2007)

		DISI	ZKT	DNSSEC-Tools
Key generation	- Single domain	Good	Good	Good
	- Several domains	Good	Good	Bad
ZSK rollover	- Single domain	Good	Good	Good
	- Several domains	Bad	Good	Acceptable
KSK rollover	- Single domain	Good	Good	Good
	- Several domains	Bad	Absent	Absent
Status report, keys	- Single domain	Good	Good	Good
	- Several domains	Good	Good	Good
Scriptable		Good	Good	Good
Export of keys		Absent	Absent	Absent
Import of keys		Absent	Absent	Absent
Choice of random source		Good	Good	Good
Signing	- Single domain	Acceptable	Good	Good
	- Several domains	Bad	Good	Bad
Status report, signing	- Single domain	Absent	Absent	Good
	- Several domains	Absent	Absent	Good
Automatic update of SOA		Absent	Acceptable	Acceptable
Log		Bad	Absent	Bad
Monitoring and alarms		Absent	Absent	Bad

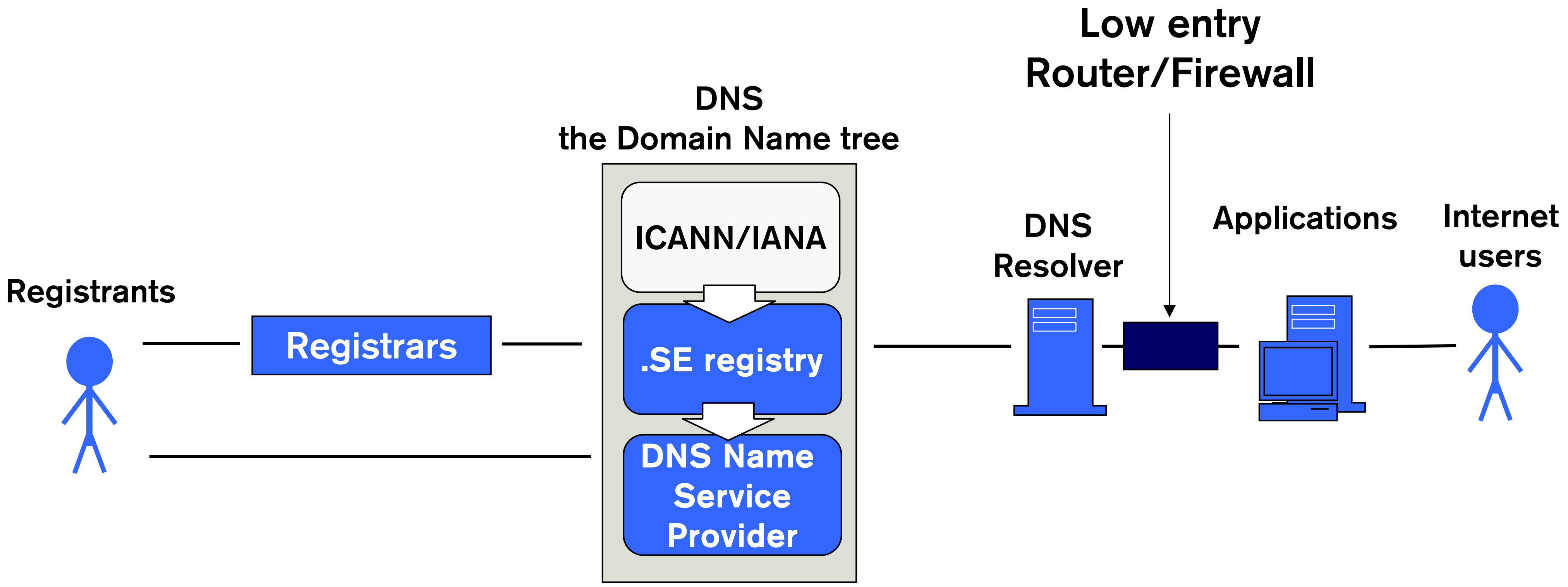
AKM, Automatic Key Management for .SE

- Make a new requirement specification
  - Buy or develop (.SE alone or a joint project)?
- Support for
  - Fully automatic for the daily routines
  - KASP, Key and Signing Policy (DNSSEC-Policy-XML)
  - RFC 5011
  - …
- Project start is now!

Operational experience

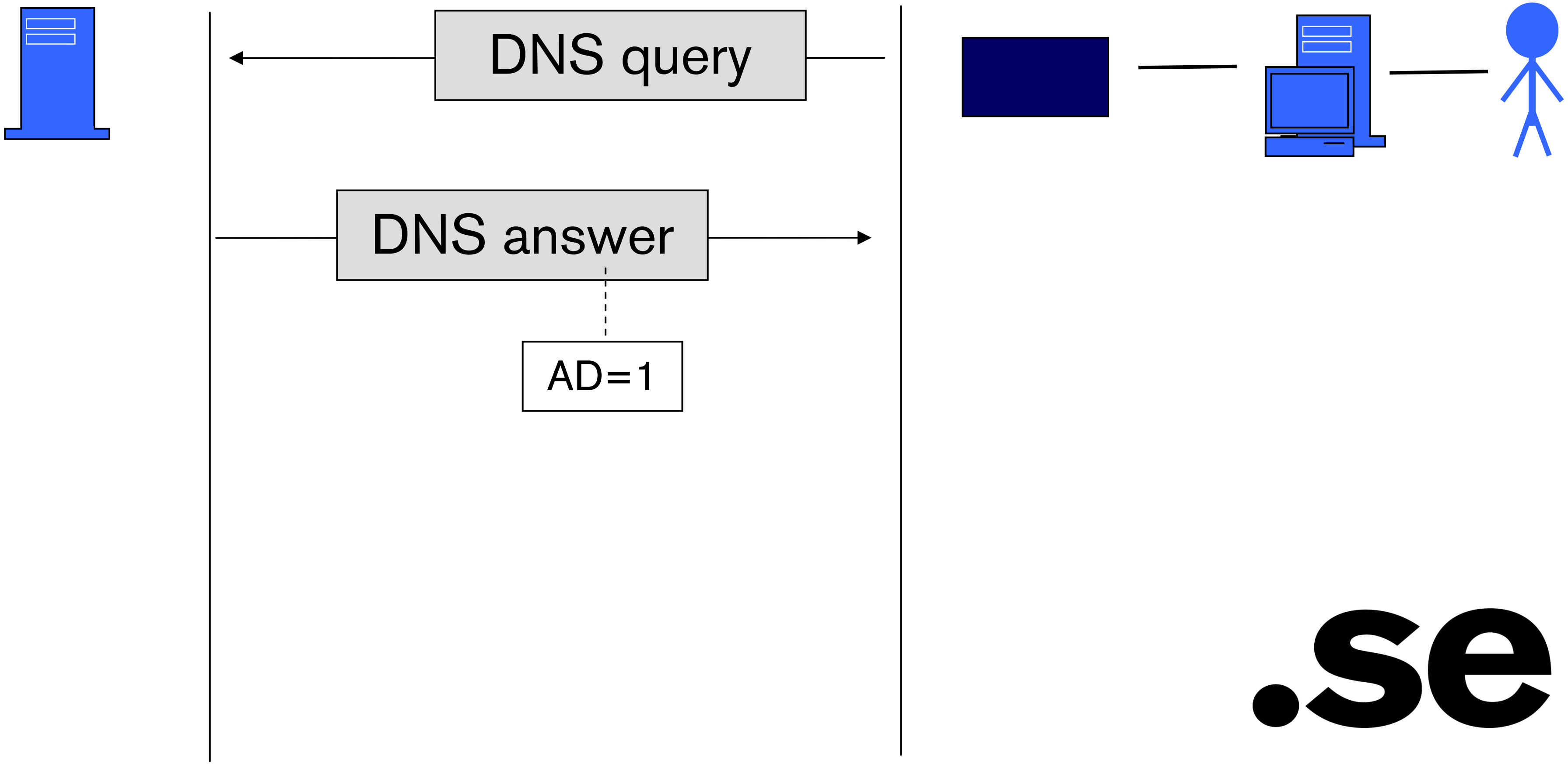
“The bind bug”

Sept 21	Error reports from gavle.se and ockelbo.se “Some users cant reach the citizens services”
Sept 22	Immediate deactivation of DNSSEC for gavle.se and ockelbo.se (DS records removed)
Sept 24	Testing
Sept 26	Patch for Bind
Oct 2	The ISP’s upgraded their resolvers


Low entry
Router/Firewall
DNS
the Domain Name tree
ICANN/IANA
.SE registry
DNS Name
Service
Provider
Registrants
Registrars
DNS
Resolver
Applications
Internet
users

DNSSEC enabled
Resolver with
the “Bind bug”

Low entry
Router/Firewall

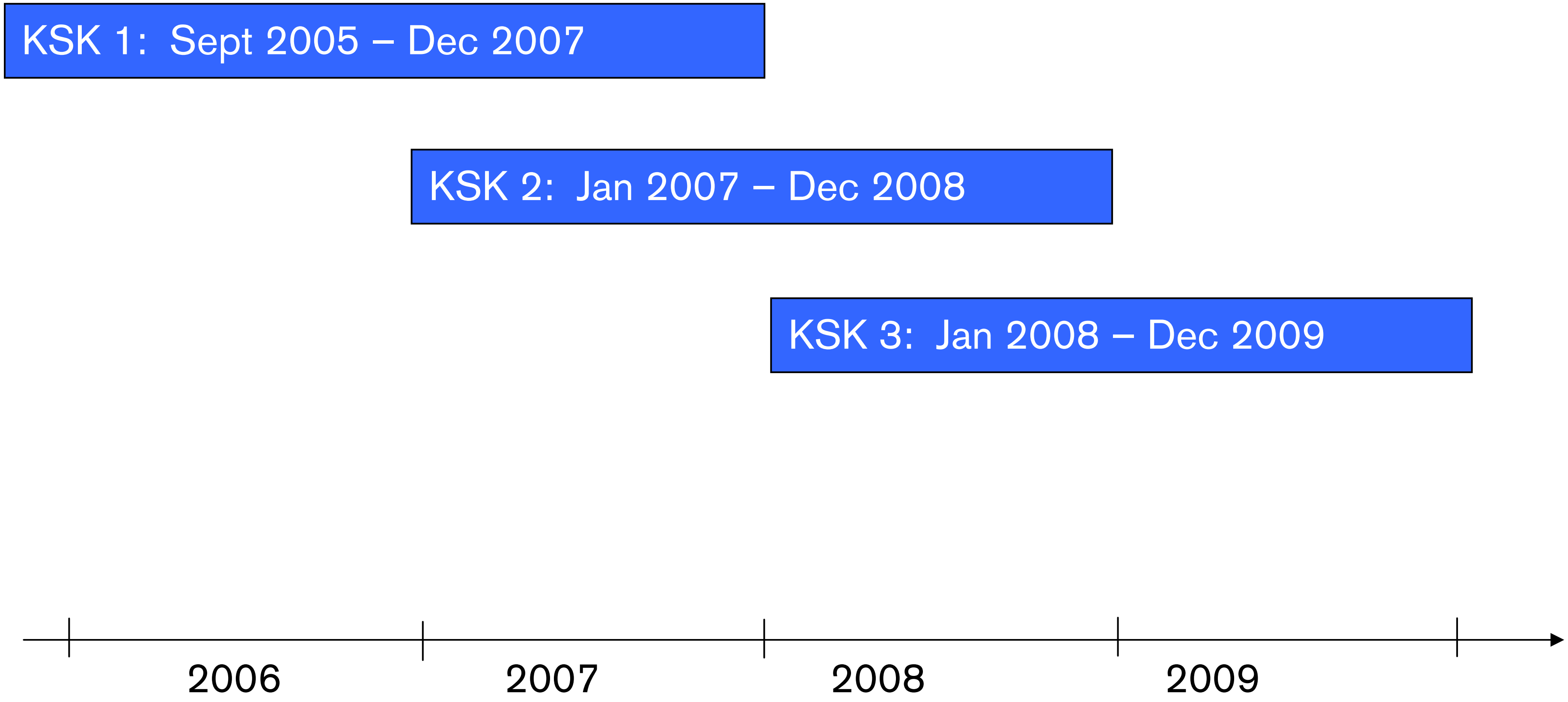


DNS query

DNS answer

AD=1

KSK Key roll over for .SE



KSK 1: Sept 2005 – Dec 2007

KSK 2: Jan 2007 – Dec 2008

KSK 3: Jan 2008 – Dec 2009

Plans for 2008

- Development
  - AKM, Automatic Key Management
  - Automatic Key roll over for resolvers (RFC 5011)
  - DNS testing of low entry routers
  - Promotion of DNSSEC aware Applications
  - Promotion of administrative tools for DNSSEC
  - Monitoring of DNSSEC in .SE supervision
- Marketing activities
  - Work together with our Registrars

Our vision 2011

- DNSSEC is considered a natural part of DNS, key management is fully automated
- DNSSEC is deployed
  - by many important domains
  - into many useful applications

Thank you!

Questions?

.se