.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
- Commercial launch of .SE-DNSSEC: Sept. 2007
- Soft launch of service: Feb 16, 2007
- Step 2: automation, marketing
The market – the value chain

Registrants -> Registrars -> ICANN/IANA -> .SE registry -> DNS Name Service Provider

DNS the Domain Name tree

DNS Resolver -> Applications -> Internet users

.se
A first step – DNSSEC validation made by Resolvers

Registrants → Registrars → .SE registry → DNS Name Service Provider → ICANN/IANA

DNS the Domain Name tree

Applications → i.e. ISP’s → DNS Resolver

Internet users
<table>
<thead>
<tr>
<th>STATUS for .SE February 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrants</td>
</tr>
<tr>
<td>.SE Registrars</td>
</tr>
<tr>
<td>DNS Name Service Providers</td>
</tr>
<tr>
<td>.SE</td>
</tr>
<tr>
<td>Resolvers</td>
</tr>
<tr>
<td>Applications</td>
</tr>
<tr>
<td>Internet Users</td>
</tr>
</tbody>
</table>
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

- Registry (CORE)
- Registry (SERVICES)

EPP

Web (the Domain Manager)

E-mail (Electronic form)

Holder and its Contact persons

Registrars (resellers)
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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Key tag</th>
<th>Algorithm</th>
<th>Fingerprint (SHA-1)</th>
<th>Key type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published</td>
<td>18476</td>
<td>RSA/SHA-1</td>
<td>E17C7BE6C006A439B2</td>
<td>ZSK</td>
</tr>
<tr>
<td></td>
<td>20283</td>
<td>RSA/SHA-1</td>
<td>8DFB057319B44F10DB1</td>
<td>ZSK</td>
</tr>
<tr>
<td></td>
<td>32672</td>
<td>RSA/SHA-1</td>
<td>DE9C034275C50118B19</td>
<td>ZSK</td>
</tr>
<tr>
<td></td>
<td>38554</td>
<td>RSA/MD5</td>
<td>EDA8E8CB20F58D7E77</td>
<td>KSK</td>
</tr>
<tr>
<td></td>
<td>38577</td>
<td>RSA/SHA-1</td>
<td>5242B348E36954ECA4C</td>
<td>KSK</td>
</tr>
<tr>
<td>Unpublished</td>
<td>47940</td>
<td>RSA/SHA-1</td>
<td>BAD85B2FAFEE265C7F</td>
<td>KSK</td>
</tr>
<tr>
<td>Unpublished</td>
<td>57551</td>
<td>DSA/SHA-1</td>
<td>24AD595DEA4EC86C4F</td>
<td>KSK</td>
</tr>
</tbody>
</table>
Interfaces for .SE-DNSSEC 2009

Registry (CORE)

Registry (SERVICES)

EPP

A new protocol?

DNS Name Service Providers

Webb (Domain Manager)

E-mail (Electronic Form)

Registrar

Holder and its Contact persons

Resellers
Hidden Master
Name Server

Zone
generator

Zone
signer

SE's
customer
data base

KSK
Random
number
generator

ZSK
Key
generator

Hidden Master
Name Server

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>DISI</th>
<th>ZKT</th>
<th>DNSSEC-Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key generation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single domain</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>- Several domains</td>
<td>Good</td>
<td>Good</td>
<td>Bad</td>
</tr>
<tr>
<td><strong>ZSK rollover</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single domain</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>- Several domains</td>
<td>Bad</td>
<td>Absent</td>
<td>Acceptable</td>
</tr>
<tr>
<td><strong>KSK rollover</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single domain</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>- Several domains</td>
<td>Bad</td>
<td>Absent</td>
<td>Absent</td>
</tr>
<tr>
<td><strong>Status report, keys</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single domain</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>- Several domains</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Scriptable</strong></td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Export of keys</strong></td>
<td>Absent</td>
<td>Absent</td>
<td>Absent</td>
</tr>
<tr>
<td><strong>Import of keys</strong></td>
<td>Absent</td>
<td>Absent</td>
<td>Absent</td>
</tr>
<tr>
<td><strong>Choice of random source</strong></td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Signing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single domain</td>
<td>Acceptable</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>- Several domains</td>
<td>Bad</td>
<td>Good</td>
<td>Bad</td>
</tr>
<tr>
<td><strong>Status report, signing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Single domain</td>
<td>Absent</td>
<td>Absent</td>
<td>Good</td>
</tr>
<tr>
<td>- Several domains</td>
<td>Absent</td>
<td>Absent</td>
<td>Good</td>
</tr>
<tr>
<td><strong>Automatic update of SOA</strong></td>
<td>Absent</td>
<td>Acceptable</td>
<td>Acceptable</td>
</tr>
<tr>
<td><strong>Log</strong></td>
<td>Bad</td>
<td>Absent</td>
<td>Bad</td>
</tr>
<tr>
<td><strong>Monitoring and alarms</strong></td>
<td>Absent</td>
<td>Absent</td>
<td>Bad</td>
</tr>
</tbody>
</table>
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
DNSSEC enabled Resolver with the “Bind bug”

DNS query

DNS answer

AD=1

Low entry Router/Firewall

.se
KSK Key roll over for .SE


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?