Time to change registrar and/or DNS platform

torbjorn.eklov@interlan.se

2007

- Friday, 21/9 at 14:28, Interlan Gefle reported that there are routers and clients that cannot handle **DNSSEC** correctly and can therefore not reach **gavle.se** or **ockelbo.se.**

And the year is 2009

- I have trained 40 municipalities in
- Why DNSSEC
- How to sign your domain
- How to validate DNSSEC

- Any problems to deploy DNSSEC?

Problems

- Lack of DNSSEC support in most registries
- Lack of DNSSEC support in Linux and Windows as DNS-platform

Registrar

- 15 Swedish registrars with DNSSEC
- 27 from other countries

- > 140 total
- => ~ 30 % can do DNSSEC

Municipality and registrar

- 230 of 290 have a registrar that can DNSSEC
- SE Direkt > 200

290 municipalities

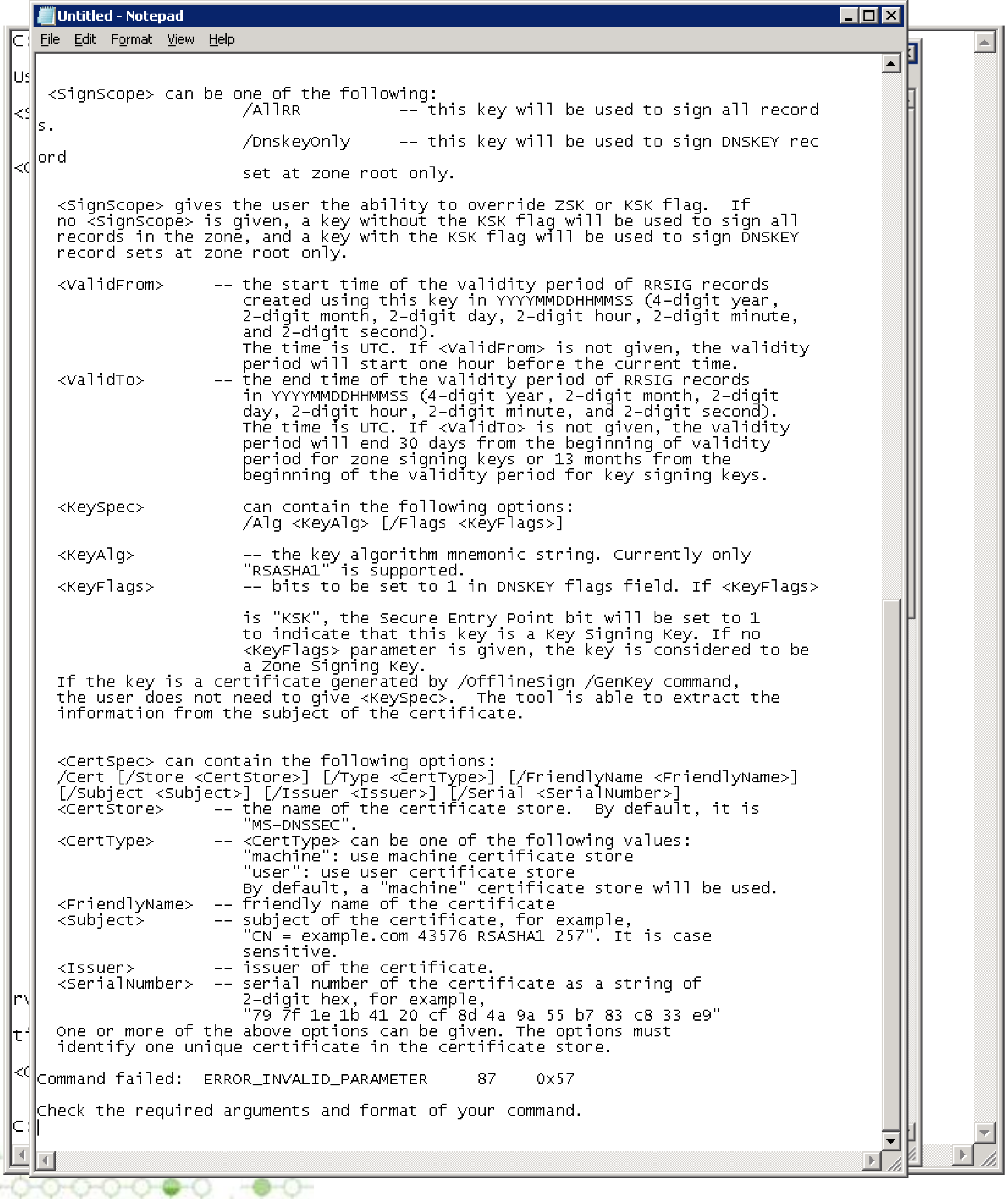
- 195 domains with glue records
- 689 DNS servers

DNS platforms

- Appliance?
- ”It’s to expensive”

DNS platforms

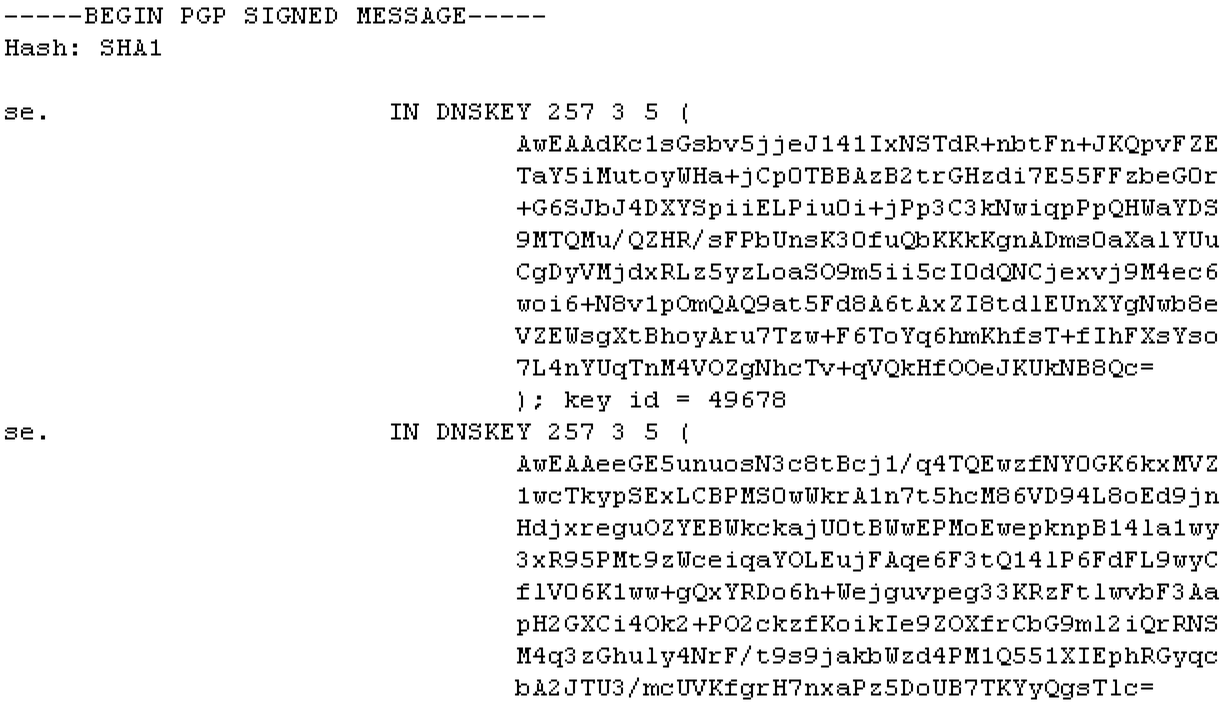
- Microsoft??
- Support for DNSSEC in Windows server 2008 R2
- DNSCMD.EXE
  Described in DNS SVR2008R2 DNSSEC.doc



```
 <SignScope> can be one of the following:
                    /AllRR          -- this key will be used to sign all record
s.
                    /DnskeyOnly     -- this key will be used to sign DNSKEY rec
ord
                    set at zone root only.

  <SignScope> gives the user the ability to override ZSK or KSK flag.  If
  no <SignScope> is given, a key without the KSK flag will be used to sign all
  records in the zone, and a key with the KSK flag will be used to sign DNSKEY
  record sets at zone root only.

  <ValidFrom>     -- the start time of the validity period of RRSIG records
                    created using this key in YYYYMMDDHHMMSS (4-digit year,
                    2-digit month, 2-digit day, 2-digit hour, 2-digit minute,
                    and 2-digit second).
                    The time is UTC. If <ValidFrom> is not given, the validity
                    period will start one hour before the current time.
  <ValidTo>       -- the end time of the validity period of RRSIG records
                    in YYYYMMDDHHMMSS (4-digit year, 2-digit month, 2-digit
                    day, 2-digit hour, 2-digit minute, and 2-digit second).
                    The time is UTC. If <ValidTo> is not given, the validity
                    period will end 30 days from the beginning of validity
                    period for zone signing keys or 13 months from the
                    beginning of the validity period for key signing keys.

  <KeySpec>         can contain the following options:
                    /Alg <KeyAlg> [/Flags <KeyFlags>]

  <KeyAlg>          -- the key algorithm mnemonic string. Currently only
                    "RSASHA1" is supported.
  <KeyFlags>        -- bits to be set to 1 in DNSKEY flags field. If <KeyFlags>

                    is "KSK", the Secure Entry Point bit will be set to 1
                    to indicate that this key is a Key Signing Key. If no
                    <KeyFlags> parameter is given, the key is considered to be
                    a Zone Signing Key.
  If the key is a certificate generated by /OfflineSign /GenKey command,
  the user does not need to give <KeySpec>.  The tool is able to extract the
  information from the subject of the certificate.


  <CertSpec> can contain the following options:
  /Cert [/Store <CertStore>] [/Type <CertType>] [/FriendlyName <FriendlyName>]
  [/Subject <Subject>] [/Issuer <Issuer>] [/Serial <SerialNumber>]
  <CertStore>     -- the name of the certificate store.  By default, it is
                    "MS-DNSSEC".
  <CertType>      -- <CertType> can be one of the following values:
                    "machine": use machine certificate store
                    "user": use user certificate store
                    By default, a "machine" certificate store will be used.
  <FriendlyName>  -- friendly name of the certificate
  <Subject>       -- subject of the certificate, for example,
                    "CN = example.com 43576 RSASHA1 257". It is case
                    sensitive.
  <Issuer>        -- issuer of the certificate.
  <SerialNumber>  -- serial number of the certificate as a string of
                    2-digit hex, for example,
                    "79 7f 1e 1b 41 20 cf 8d 4a 9a 55 b7 83 c8 33 e9"
  One or more of the above options can be given. The options must
  identify one unique certificate in the certificate store.

Command failed:  ERROR_INVALID_PARAMETER     87     0x57

Check the required arguments and format of your command.
```

Windows Server 2008 R2

- Validation
- dig +short dnskey se. @a.ns.se
- ”Make DNSKEY to one row”



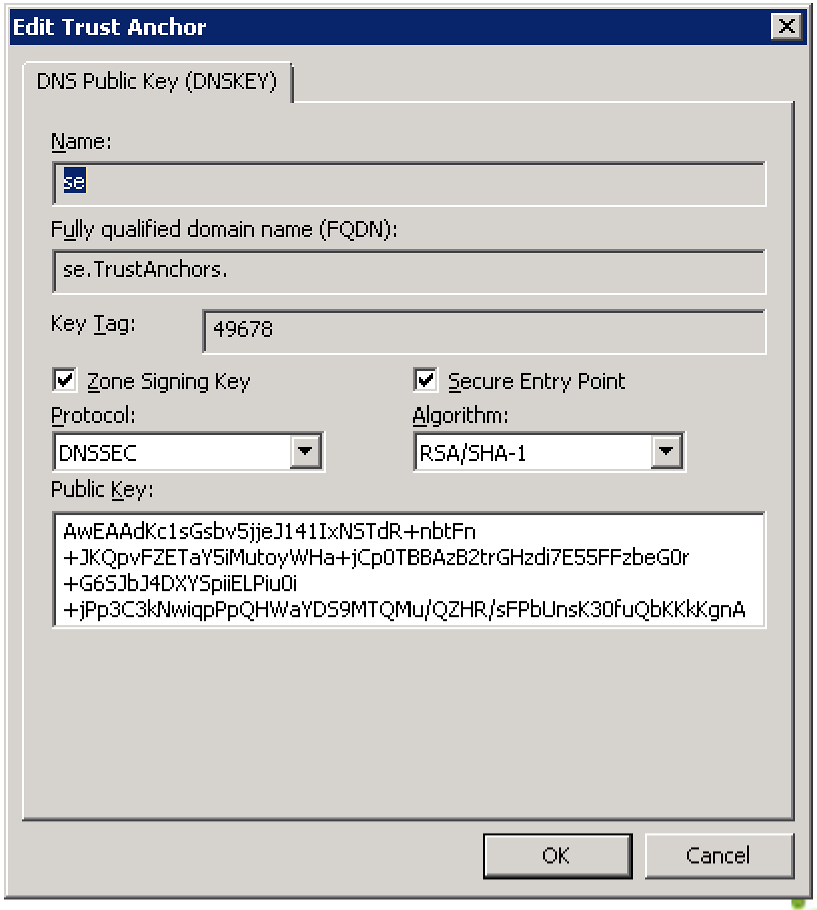
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

se.                     IN DNSKEY 257 3 5 (
                                AwEAAdKc1sGsbv5jjeJ141IxNSTdR+nbtFn+JKQpvFZE
                                TaY5iMutoyWHa+jCpOTBBAzB2trGHzdi7E55FFzbeGOr
                                +G6SJbJ4DXYSpiiELPiuOi+jPp3C3kNwiqpPpQHWaYDS
                                9MTQMu/QZHR/sFPbUnsK3OfuQbKKkKgnADmsOaXalYUu
                                CgDyVMjdxRLz5yzLoaSO9m5ii5cIOdQNCjexvj9M4ec6
                                woi6+N8v1pOmQAQ9at5Fd8A6tAxZI8tdlEUnXYgNwb8e
                                VZEWsgXtBhoyAru7Tzw+F6ToYq6hmKhfsT+fIhFXsYso
                                7L4nYUqTnM4VOZgNhcTv+qVQkHfOOeJKUkNB8Qc=
                                ); key id = 49678
se.                     IN DNSKEY 257 3 5 (
                                AwEAAeeGE5unuosN3c8tBcj1/q4TQEwzfNYOGK6kxMVZ
                                1wcTkypSExLCBPMSOwWkrA1n7t5hcM86VD94L8oEd9jn
                                HdjxreguOZYEBWkckajUOtBWwEPMoEwepknpB14la1wy
                                3xR95PMt9zWceiqaYOLEujFAqe6F3tQ14lP6FdFL9wyC
                                flVO6K1ww+gQxYRDo6h+Wejguvpeg33KRzFtlwvbF3Aa
                                pH2GXCi4Ok2+PO2ckzfKoikIe9ZOXfrCbG9ml2iQrRNS
                                M4q3zGhuly4NrF/t9s9jakbWzd4PM1Q551XIEphRGyqc
                                bA2JTU3/mcUVKfgrH7nxaPz5DoUB7TKYyQgsTlc=
```

Microsoft Windows Server 2008 R2

Create aTrust Anchor for se.

Paste the key and enable ”Zone Signing key” och ”Secure Entry Point”

But it’s a KSK you paste in there… ☺



Edit Trust Anchor

DNS Public Key (DNSKEY)

Name: se

Fully qualified domain name (FQDN): se.TrustAnchors.

Key Tag: 49678

☑ Zone Signing Key

☑ Secure Entry Point

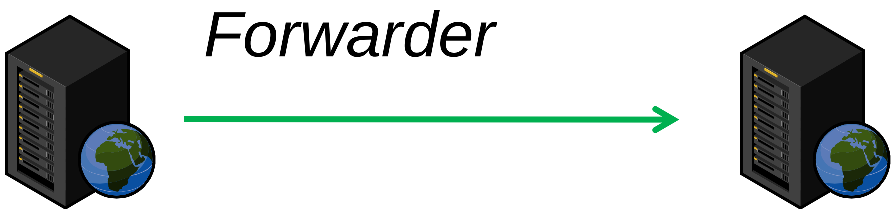
Protocol: DNSSEC

Algorithm: RSA/SHA-1

Public Key:

```
AwEAAdKc1sGsbv5jjeJ141IxNSTdR+nbtFn
+JKQpvFZETaY5iMutoyWHa+jCp0TBBAzB2trGHzdi7E55FFzbeG0r
+G6SJbJ4DXYSpiiELPiu0i
+jPp3C3kNwiqpPpQHWaYDS9MTQMu/QZHR/sFPbUnsK30fuQbKKkKgnA
```

Validation Windows Server 2008 R2



Windows Active Directory DNS

I recommend you to use a internal or external validating resolver and not your Windows DNS for validation

Expect problem above there is no NSEC3 support

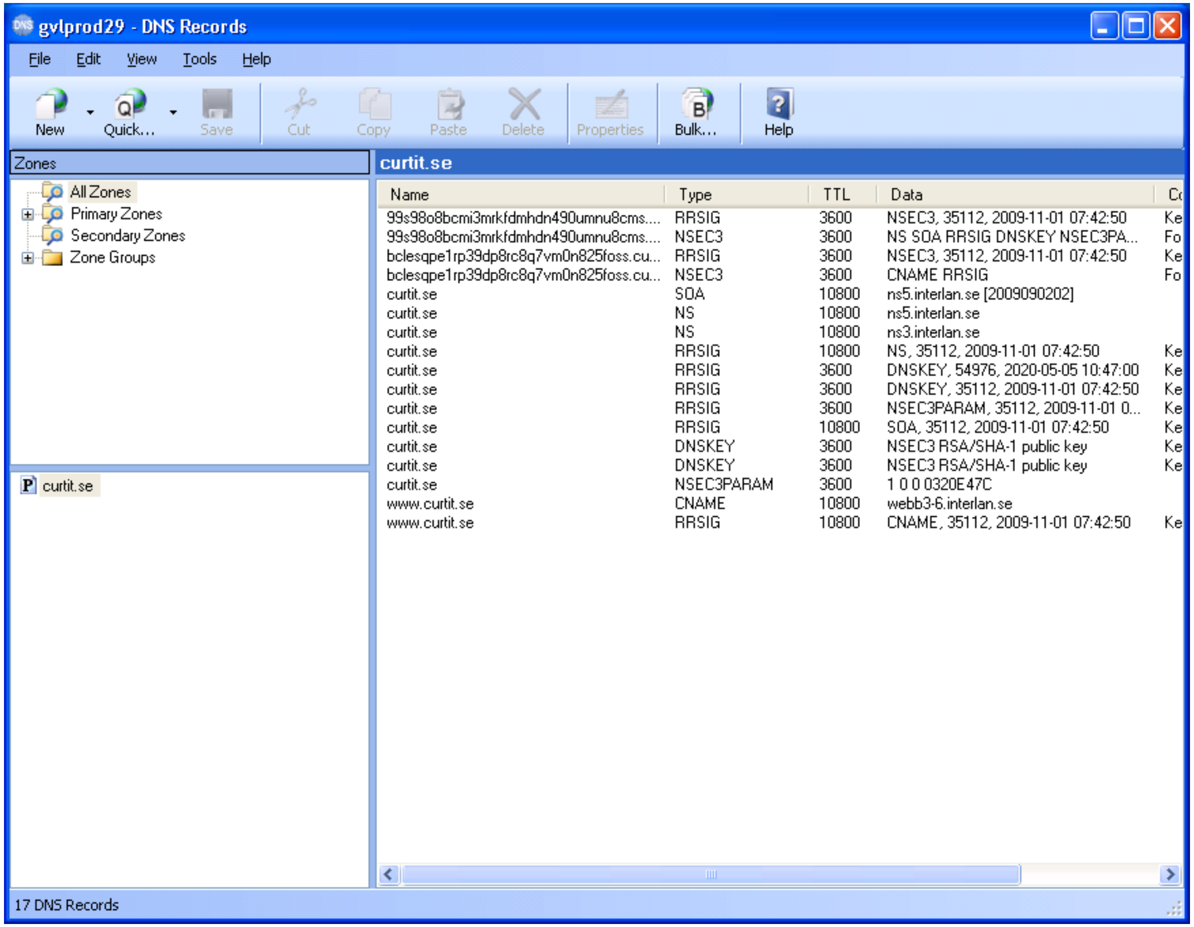
DNSSEC signing with Windows Server 2008 R2

- Dont do that!

DNS Simple plus

- *Easy to sign zones in Windows!!!*

- *NSEC3 support*
- *Cheap*
- *Automatic resigning is coming*



curtit.se

Name	Type	TTL	Data	Co
99s98o8bcmi3mrkfdmhdn490umnu8cms....	RRSIG	3600	NSEC3, 35112, 2009-11-01 07:42:50	Ke
99s98o8bcmi3mrkfdmhdn490umnu8cms....	NSEC3	3600	NS SOA RRSIG DNSKEY NSEC3PA...	Fo
bclesqpe1rp39dp8rc8q7vm0n825foss.cu...	RRSIG	3600	NSEC3, 35112, 2009-11-01 07:42:50	Ke
bclesqpe1rp39dp8rc8q7vm0n825foss.cu...	NSEC3	3600	CNAME RRSIG	Fo
curtit.se	SOA	10800	ns5.interlan.se [2009090202]	
curtit.se	NS	10800	ns5.interlan.se	
curtit.se	NS	10800	ns3.interlan.se	
curtit.se	RRSIG	10800	NS, 35112, 2009-11-01 07:42:50	Ke
curtit.se	RRSIG	3600	DNSKEY, 54976, 2020-05-05 10:47:00	Ke
curtit.se	RRSIG	3600	DNSKEY, 35112, 2009-11-01 07:42:50	Ke
curtit.se	RRSIG	3600	NSEC3PARAM, 35112, 2009-11-01 0...	Ke
curtit.se	RRSIG	10800	SOA, 35112, 2009-11-01 07:42:50	Ke
curtit.se	DNSKEY	3600	NSEC3 RSA/SHA-1 public key	Ke
curtit.se	DNSKEY	3600	NSEC3 RSA/SHA-1 public key	Ke
curtit.se	NSEC3PARAM	3600	1 0 0 0320E47C	
www.curtit.se	CNAME	10800	webb3-6.interlan.se	
www.curtit.se	RRSIG	10800	CNAME, 35112, 2009-11-01 07:42:50	Ke

17 DNS Records

Linux (Bind / Unbound)

- If you like ./configure almost every distribution is ok
- Many is still at BIND 9.4 or 9.5 level

- I think we need minimum BIND 9.6 for NSEC3 support

Ex. Ubuntu and Redhat

- Standard repositories
- Ubuntu 8.04 LTS
  BIND 9.4
  No Unbound

- Redhat Enterprise 5
  BIND 9.3 (!!!!)
  No Unbound

Ubuntu and Fedora

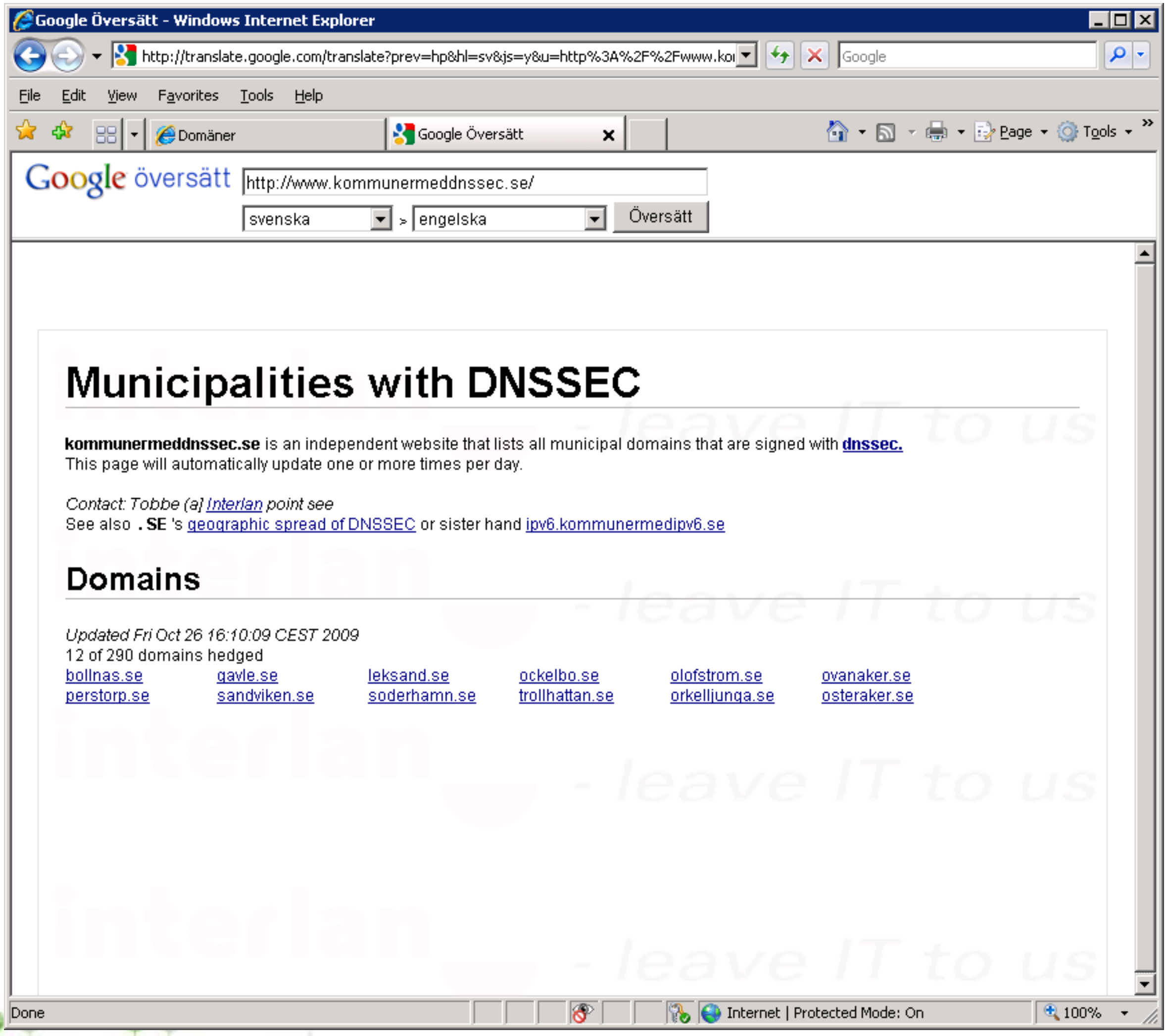
- Ubuntu 9.10 =>
  Bind 9.6
  Unbound 1.2.1

- Fedora 11 =>
  Bind 9.6
  Unbound 1.2.1

290 municipalities

- 195 domains with glue records
- 689 DNS servers
- Some is still running BIND 8.? (!!!)
- Many many with Bind <= 9.4
- A few with Bind 9.5 och 9.6
- 10% is running 2000 and 2003
- + others

Municipalities with DNSSEC


Google Översätt - Windows Internet Explorer
File Edit View Favorites Tools Help
Domäner
Google Översätt
Page
Tools
Google översätt
Översätt
Done
Internet | Protected Mode: On
100%

http://translate.google.com/translate?prev=hp&hl=sv&js=y&u=http%3A%2F%2Fwww.ko

http://www.kommunermeddnssec.se/

svenska > engelska

Municipalities with DNSSEC

kommunermeddnssec.se is an independent website that lists all municipal domains that are signed with **dnssec.**
This page will automatically update one or more times per day.

Contact: Tobbe (a) Interlan point see
See also **. SE** 's geographic spread of DNSSEC or sister hand ipv6.kommunermedipv6.se

Domains

Updated Fri Oct 26 16:10:09 CEST 2009
12 of 290 domains hedged

bollnas.se gavle.se leksand.se ockelbo.se olofstrom.se ovanaker.se
perstorp.se sandviken.se soderhamn.se trollhattan.se orkelljunga.se osteraker.se