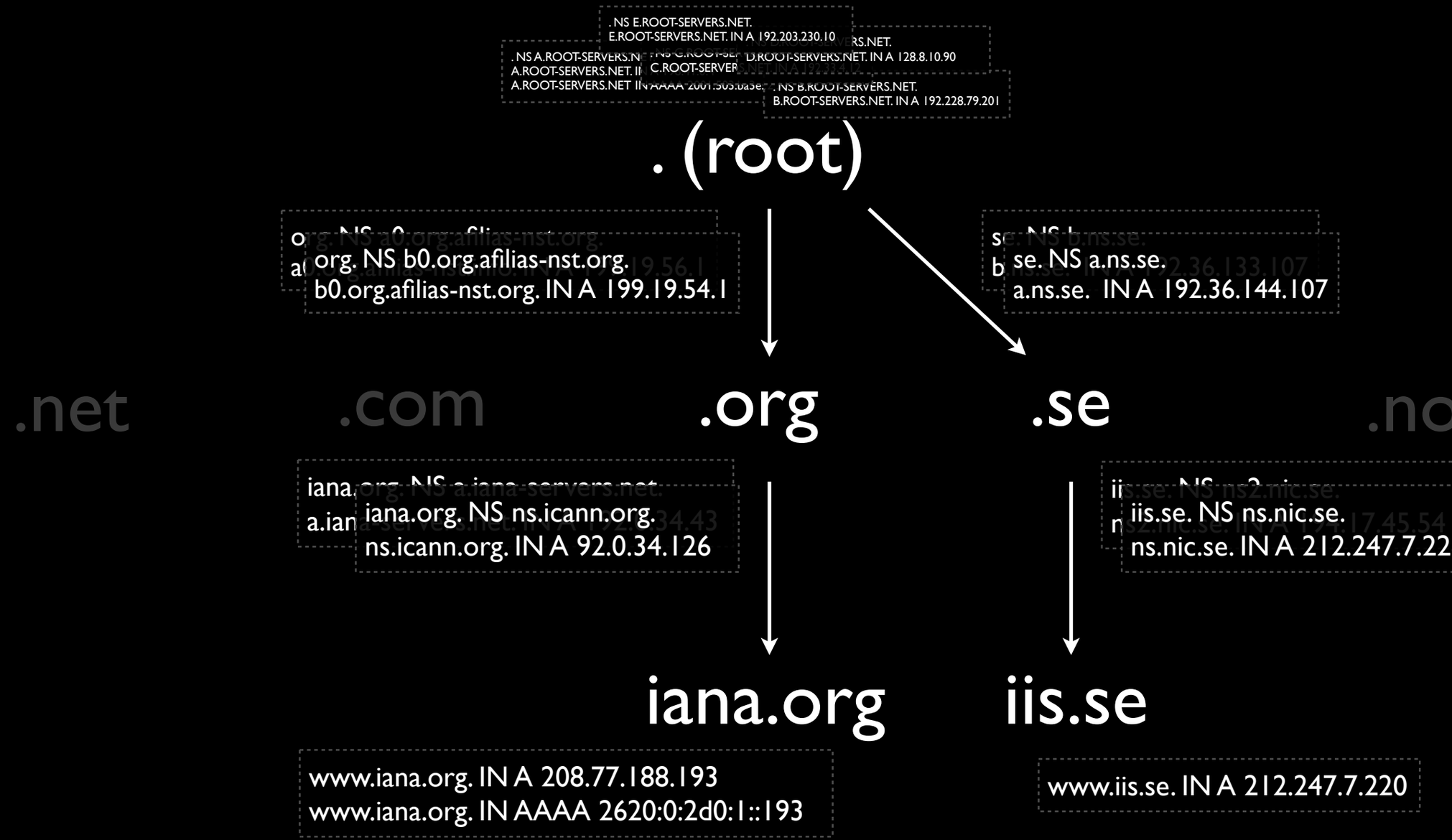
DNSSEC Basics

Patrik Wallström, R&D @ .SE

The DNS Hierarchy



Resolving DNS

Adding crypto to the mixture

Assymetric crypto:

- Assymetric *key pairs* have a **public** and **private** key
- **Protect** the **private** keys
- **Publish** the **public** keys

KSK:

- The Key Signing Key - what you **trust**
- Signs the Zone Signing Keys, ZSK

ZSK:

- The Zone Signing Key
- Creates **signatures** of **records** in the zone - **RRSIG**

DNSKEY and RRSIG

KSK

iis.se. IN DNSKEY 257 3 5 wEAAcq5uqe5VibnyvSnGU20panweAk2QxfIGVuVQhzQABQV4SIdAQs
LNVHF61Icxe504jhPmjeQ656X6tdHpRz1DdPOukcIITjIRoJHqSXXyL6gUluZoDUK6vpxkGJx5m5n4boRTKCT
UAR9rw2+IQRRTtb6nBwsC3pmf9IlJQjQMb1cQTb0UO7fYgXDZIYVul2LwGpKRrMJ6UI1nepkSxTMwQ4H9iK
E9FhqPeIpzU9dnXGtJZCx9tWSZ9VsSLWBJtUwoE6ZfIoF1ioq qxfGI9JV1/6GkDxo3pMN2edhkp8aqoo/R
+mrJYi0vE8jbXvhZ12151Dy wuSxbGjAIxk=

ZSK

iis.se. IN DNSKEY 256 3 5 AwEAAdancK9+0Il/tuXCBylBiUpNq4RGzDE2uQ6+nb6Un0myCJFzaN3
bzSMjAU5xlt6vnAfFZkRNKANu06j2zYjRbQucYfLEq69GIKOBnSHA46H 7uUDqM32KEL+KfIIlQvFpXW2/
r835mP9+dtlsa860Kf1n2ye/77I9QtC gBeZ5okF

RRSIG

iis.se. IN RRSIG DNSKEY 5 2 3600 20090205084501 20090126084501 18937 iis.se.
DiNYYelgXcgli6+xevjgqSy/ilcWmu52LkcKk9AwoWbcBrf1Zag8gowv 8S0LWJjKUO2aYRy53VvU/nkl20AJBuec/
PYtEw7pK8Z3fMFspQZeqR8Z kTQv6+I5w1n1UUKIzRNtFG5FEH5zSdb5sOL8YEylUVScuHewmtkwoN+M
dWkoB5IEb3IuT57LgiQPxMogFRH9xoR/DrP299pvBQ78dgmbCwHxQCVG
orGY1XHbvfwndsqrnFmBxrxu6DwZitXSCVHWgsiMMVE/rhKpdlCwl3uZ
WJ4vipACelaqjdqpZG2sLbfKpeK44WeMTiaSgypDQVnXdDaP0g7mMk3o 0xGLXQ==

RRSIG

iis.se. IN RRSIG DNSKEY 5 2 3600 20090205084501 20090126084501 27345 iis.se.
DLAB4SbzYw9YEs3rj0vE3eXmA6J3HiFIi0jgO3wVtnwnCzn9J5iSuTUn b1iUjsk4TpwuF6tf4udo9L1IAQPGyw
+qLzEKdfQ+G02n1rvcSBDU8pPT MsgyCz6DV+TJ/oGkCVi4grUycj4q5rtCRToL4Icdx+F91moY0yW2LO6T
qMw=

Signatures?

A signature is an encrypted hash of data.
The key used for encryption is the private key, and the signature can be verified by decrypting the hash with the public key.

A hash is a checksum of a set of data. Typical checksum algorithms are MD5, SHA-1 and SHA-256. MD5 is considered **vulnerable**.

DNSSEC signatures

```
g.ns.se.                172682 IN A 130.239.5.114
g.ns.se.                172682 IN AAAA 2001:6b0:e:3::1
g.ns.se.                172682 IN RRSIG A 5 3 172800 20100311000326 (
                                20100304101819 40935 se.
                                IbCqCAa63j6uf0o52b4JDCvkl/VHlXJCcbwpfxiizySY
                                qBXkHSHJw/vDn9he8EApSzJehfXQoUa2oySukuCHssdv
                                IayAonD1LG1RP1SQnxTe3iwWPcNQjMIofBn0cY2/FlVR
                                W4H5WIeS2DwZpLRr7IAM51OZRGIg8aUnzfrnML8= )
g.ns.se.                172682 IN RRSIG AAAA 5 3 172800 20100310041411 (
                                20100304101819 40935 se.
                                Qo4JViec7dgJY1+LcpYqVoJA65Gxf9xRyCGlkZW2Xf3n
                                +tO6/6jsdK+OWF9tWrtJH0xlRdeiiEu2FJU4iV+EBtZN
                                1zEiy7Gyehe6UA+oAZ4s3CRfYrD+QKoZ4D6uoIucAN5g
                                3H96l+Ad++tEniQtuqCzbgFVSzsBl+hMUaMEJrg= )
```

Fingerprints

A fingerprint is a checksum of a key. Fingerprints are often published instead of a key because it is much shorter than a key, and more easy to read.

AwEAAcq5u+qe5VibnyvSnGU20panweAk2QxflGVuVQhzQABQV4SIdAQs
+LNVHF61lcxe504jhPmjeQ656X6t+dHpRz1DdPO/ukcIITjIRoJHqS+X XyL6gUluZoD
+K6vpxkGJx5m5n4boRTKCTUAR9rw2+IQRRTtb6nBwsC3pmf9IIJQjQMb1cQTb0U
O7fYgXDZIYVul2LwGpKRrMJ6Ul1nepkSxTMwQ4H9iKE9FhqPeIpzU9dnXGtJZCx9t
WSZ9VsSLWBJtUwoE6ZfloF1ioqqxfGI9JV1/6GkDxo3pMN2edhkp8aqoo/R
+mrJYi0vE8jbXvhZ12151DywuSxbGjAlxk=

↓

10DD1EFDC7841ABFDF630C8BB37153724D70830A

DS records

DS - Delegation Signer.

A DS record (the hash of the DNSKEY) is published at the parent zone to delegate trust to the child zone.

This is what is published for iis.se at .se:

```
iis.se.     IN   DS   18937 5 2 B5C422428DEA4137FBF15E1049A48D27FA5EADE64D2EC9F3B58A994A6ABDE543
iis.se.     IN   DS   18937 5 1 10DD1EFDC7841ABFDF630C8BB37153724D70830A
```

Two DS records - two algorithms are used for .SE, SHA-1 and SHA-256.
The DS and NS are signed by the parent.

The DS delegation

.se:

DS

```
iis.se.     IN    DS    18937 5 2 B5C422428DEA4137FBF15E1049A48D27FA5EADE64D2EC9F3B58A994A6ABDE543
iis.se.     IN    DS    18937 5 1 10DD1EFDC7841ABFDF630C8BB37153724D70830A
```

iis.se:

KSK

```
iis.se.    IN    DNSKEY  257 3 5 AwEAAcq5u
e5VibnyvSnGU20panweAk2QxflGVuVQhzQABQV4SIdAQs +LNVHF61Icxe504jhPmjeQ656X6t
HpRz1DdPO/ukcIITjIRoJHqS+X XyL6gUluZoDU+K6vpxkGJx5m5n4boRTKCTUAR/9rw2+IQRRTtb6nBwsC
3pmf9IIJQjQMb1cQTb0UO7fYgXDZIYVuI2LwGpKRrMJ6UI1nepkSxTMw Q4H9iKE9FhqPeIpzU9dnXGtJ
+ZCx9tWSZ9VsSLWBJtUwoE6ZfloF1ioq qxfGI9JV1/6GkDxo3pMN2edhkp8aqoo/R
+mrJYi0vE8jbXvhZ12151Dy wuSxbGjAlxk=
```

If you have more KSK keys, you will have more DS records in the parent zone.

NSEC

Proof of non-existance.

You might want to protect anybody from performing a DoS-attack against a name in DNS. That is done with NSEC.

iis.se. **IN NSEC iis07.se.** NS DS RRSIG NSEC
iis.se. IN RRSIG NSEC 5 2 7200 20090131230405 20090126101756
28770 se. GK6JQNDTsHII3z8v1QR2jHr2VNpzhyB2UYFCEASJJBINnRpaUpmnsE4
iF9AoyS4g50Lly1zJb659bY76hkmaJDO6Xwl0+IlefX8ZN9iv0snfd2GUJyGyJzlu9txg
ZTsfC7HQcX1gZPjnq9BgE1YDHifJNZAqijBG83rtj 9Wc=

NSEC points to the next label (domain name) in the zone.

NSEC3

Can be both opt-in and opt-out.

Opt-out differs from opt-in in the way that signatures are not generated for the whole zone but only for the authoritative data and for delegations to signed zones.

If NSEC3 is chosen a decision will need to be made on the number of hash iterations. The number of iterations has an impact on both the recursive resolver and the authoritative nameserver.

NSEC3 data

```
;; QUESTION SECTION:
;uk.                    IN NSEC3PARAM

;; ANSWER SECTION:
uk.                    3522 IN NSEC3PARAM 1 0 0 -
uk.                    3522 IN RRSIG NSEC3PARAM 8 1 3600 20100427211130 (
                            20100413201130 16134 uk.
                            WCCPrHhS+PZlnaKeTPaHJEH2HYM7Sgkv8QdtuvR/Xq6M
                            JPHqR6kgzczbbFiNU2RMWXlYi2EhCU22gZe8q7b4tSnQ
                            01Nfb8T52LvjpU/Ibrsng1yhFPB1VRyY4vWZsifDrgkJ
                            jZjaXaZjivjj1UQO9JtjB3LAFT8miPl1tPPz1bo= )
```

NSEC3PARAM have the following data elements:

- **Hash Algorithm**: The cryptographic hash algorithm used.
- **Flags**: "Opt-out" (indicates if delegations are signed or not).
- **Iterations**: How many times the hash algorithm is applied.
- **Salt**: Salt value for the hash calculation.

NSEC3 hashing

```
org.                    835 IN SOA a0.org.afilias-nst.info. noc.afilias-nst.info. (
                                2009097238 ; serial
                                1800       ; refresh (30 minutes)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
org.                    835 IN RRSIG SOA 7 1 900 20100428191626 (
                                20100414181626 47948 org.
                                AHIsfmsvsrgYdaNr8NLO5k6nQXdsUEIcNIW+PYK1dhFm
                                mrsxcs0rK8i1oqQzSOxL10rwHdEXD+3TuIyIfkrDkVIn
                                E6NFL6hSq/S7oh7NdlKVwHZEmM2dYTnxZpbIVFvfxYSU
                                plu0kDud26a9sT8ndYMam6deMDqvSpQvvPC2hqg= )
h9p7u7tr2u91d0v0ljs9l1gidnp90u3h.org. 86335 IN NSEC3 1 1 1
D399EAABH9RSFB7FPF2L8HG35CMPC765TDK23RP6 NS SOA RRSIG DNSKEY NSEC3PARAM
h9p7u7tr2u91d0v0ljs9l1gidnp90u3h.org. 86335 IN RRSIG NSEC3 7 2 86400 20100428191626
(
                                20100414181626 47948 org.
                                jCJqFzC/nF2MI51WOEk8d40kxHfjgs/DkOtRbqdsLBD/
                                tiOW5uFroOGSaRW2LgIpjE8BM7hNvz8YW3aoMr5CUXQC
                                hI7kwSTeZLW3kRxYtyim1+WQ+Je7Mdgv90MRO2NqifKA
                                s1HQQvuy6TLNgRSe+GsZ7hROimpXaiOsu6xaBUc= )
```

Zonefile without DNSSEC

```
@       IN SOA  ns.nic.se. hostmaster.iis.se. (
                2009012701 ; serial
                10800      ; refresh (3 hours)
                3600       ; retry (1 hour)
                604800     ; expire (1 week)
                86400      ; minimum (1 day)
        )
        NS      ns.nic.se.
        NS      ns2.nic.se.
        NS      ns3.nic.se.
        MX      10 cleaner.prod.iis.se.
$ORIGIN iis.se.
www     IN A    212.247.7.210
```

A signed zone

```
@       IN SOA  ns.nic.se. hostmaster.iis.se. (
                 2009012501 ; serial
                 10800      ; refresh (3 hours)
                 3600       ; retry (1 hour)
                 604800     ; expire (1 week)
                 86400      ; minimum (1 day)
        )
 RRSIG   SOA 5 2 86400 20090131030501 (
                 20090125030501 53069 iis.se.
                 BGZ3AMUQ3GL3yowBrrLhV9Sa8s47nmXm2ci6ZjC4kCickw5Wo1d+zSPpV9SL4hVF0XwYOtP
                 fNAcGh7BaasK/jhDLMBzoI4O5ZujV0erUj/U2or27WEinUu+q5zeLiPrPy4pG654dZ+0y9aT
                 7NwvCkxliKoaVlweyU4UafyxA8U= )
NS      ns.nic.se.
NS      ns2.nic.se.
NS      ns3.nic.se.
RRSIG   NS 5 2 86400 20090131030501 (
                 20090125030501 53069 iis.se.
                 sPbCYM62YiB0ciIBev+As97d/oTXVy/97EV6JITcod4xUWMjAIcuAyoFdYpGTEddAfe8xK+w
                 D1nwSJLAleA7uefzOOClCxS/pIJq8Hbh92nZ0VN30wTEHk8mb97ivWrRxAqUQaeINSOei5Zh
                 /J8ymfL9X639SvO2y5jHiXeZ0JM= )
MX      10 cleaner.prod.iis.se.
RRSIG   MX 5 2 86400 20090131030501 (
                 20090125030501 53069 iis.se.
                 L+EZ/NDc5/PTDx6PLOkAUJOUdbd50bYAqNpA/WQq3s8I6g5she6A5IpgtR7BQ4zF2XtnDX0G
                 vE7Zxqi6iWE/Pyd1iVxChi7NmgzK7siazfYI
                 R7fFE+ZPSAfIHjAafD5scmk2OOIMaZzvhkk8
                 nYzqbCCC0gVgurXsx8nycOUZbTM= )
DNSKEY  257 3 5 (
                 BQEAAAABuM9XroBb7Qrrz3winhL2vgNOEKDqTwiajUt/IYn9Z6GlPjd2hAsubgm+tXGKs2qo
                 kdfsvCOVljiyRA885uI2o2S5ELLFICw4LiJbedAAuJXNDvwwB8Xf8tYwxxh82fZ9JqwqD+n6
                 E31w/aL0UlGuIh7PWE/IMj+O8iMv3croHScHkfVxtz9aF2fRI2QwXCjcrvS5i06Ss14Af2bB
                 BUrX0y8cXKI9AuIrWZIniWLIce6b88yzxPuqJaNjOg8LFC1tMsSm6aeEKErQgJaeMJheRo4P
                 WFitdMB9FpCH/6ylVEbZJpm/hKOZp2uedh8AmxmSDhUM7bMngQmXD/qpgrApqQ==
                 ) ; key id = 27840
RRSIG   DNSKEY 5 2 3600 20090131030501 (
                 20090125030501 53069 iis.se.
                 Kco8fH1BINR2xVe4kTtFBbjKtLe0BFvhP9iZWxgR9DCqKVK5VzxnTcLAJGF8xjwq0W8IUZws
                 GSgWyOsx7bzrfoMNlkutYP14nTJio5zjX4heSx2C4Dx33egg0IIM/iur52O7KWEF7AC7l+ra
                 RP3GGTCu7Ls0kGc2GDGNxothr8A= )
NSEC    www.iis.se. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
RRSIG   NSEC 5 2 86400 20090131030501 (
                 20090125030501 53069 iis.se.
                 KOFHUf1ZB+e/AxGdMkTkq9W461AjFjxLHBrMRt5ULZ4+IfMsYHw5VSecMq61VabhXO5ziOC
                 B1vK4BYrUeC+xAMFWJzn6xsLMDj/MMjM5d2iZhjE1zPc2sX42M6er1fjF9rw3qjWCFTLdy8Z
                 CTsiw0Ou7ESX6afYwkb7QkTdL9g= )
```

RRSIG

RRSIG

RRSIG

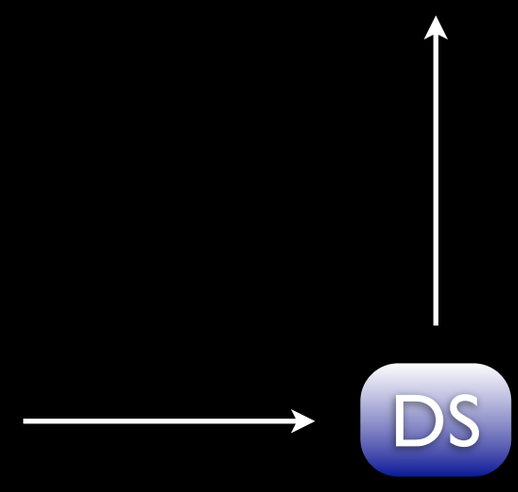
KSK

RRSIG

NSEC

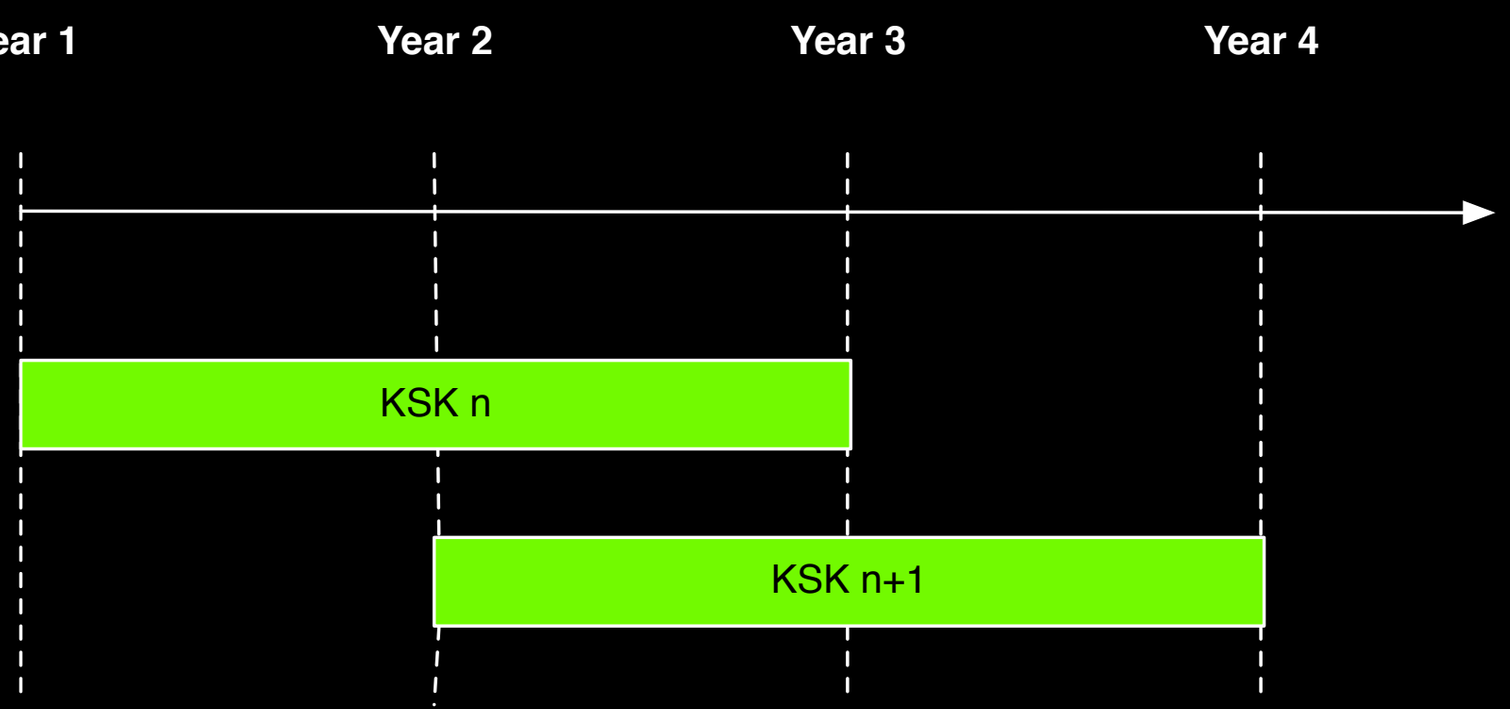
RRSIG

KSK is published as DS in the parent



Keys in the resolver

A resolver needs at least one key to validate DNSSEC records. For .SE we are using two overlapping KSK, each valid for two years.



Getting the keys from .SE

http://iis.se/domains/sednssec/publickey

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

se.             IN DNSKEY 257 3 5 (
                      AwEAAdKc1sGsbv5jjeJ141IxNSTdR+nbtFn+JKQpvFZE
                      TaY5iMutoyWHa+jCp0TBBAzB2trGHzdi7E55FFzbeG0r
                      +G6SJbJ4DXYSpiiELPiu0i+jPp3C3kNwiqpPpQHWaYDS
                      9MTQMu/QZHR/sFPbUnsK30fuQbKKkKgnADms0aXalYUu
                      CgDyVMjdxRLz5yzLoaSO9m5ii5cI0dQNCjexvj9M4ec6
                      woi6+N8v1pOmQAQ9at5Fd8A6tAxZI8tdlEUnXYgNwb8e
                      VZEWsgXtBhoyAru7Tzw+F6ToYq6hmKhfsT+fIhFXsYso
                      7L4nYUqTnM4VOZgNhcTv+qVQkHfOOeJKUkNB8Qc=
                      ); key id = 49678
se.             IN DNSKEY 257 3 5 (
                      AwEAAeeGE5unuosN3c8tBcj1/q4TQEwzfNY0GK6kxMVZ
                      1wcTkypSExLCBPMS0wWkrA1n7t5hcM86VD94L8oEd9jn
                      HdjxreguOZYEBWkckajU0tBWwEPMoEwepknpB14la1wy
                      3xR95PMt9zWceiqaYOLEujFAqe6F3tQ14lP6FdFL9wyC
                      flV06K1ww+gQxYRDo6h+Wejguvpeg33KRzFtlwvbF3Aa
                      pH2GXCi4Ok2+PO2ckzfKoikIe9ZOXfrCbG9ml2iQrRNS
                      M4q3zGhuly4NrF/t9s9jakbWzd4PM1Q551XIEphRGyqc
                      bA2JTU3/mcUVKfgrH7nxaPz5DoUB7TKYyQgsTlc=
                      ); key id = 8779

-----BEGIN PGP SIGNATURE-----
Version: PGP Desktop 9.8.3 (Build 4028)
Charset: utf-8

wj8DBQFJQmz4/OxRKPRA7psRAqKyAKCqzF2oamv1kwY3/5f27ioxicVMZACfX8By
sKp405q8KBbheYVYKb5gE7k=
=T8Is
-----END PGP SIGNATURE-----
```

BIND example

In your named.conf:

```
trusted-keys {
    "se." 257 3 5 "AQOfYGgsIqyVeES+J9JWQ/
xZdK92sZVN2tTXlJeDm5DgIQM0qfvC3Cd6T3unHQf7pTQv8hf3qP/
50yFEVttiGPVL4ctm3KFhaybJGz/1/AGkCdqmGPymAcVVvdBICCx165gusSsK5fF70j
+Zm6r4NBsFMyUiIPLiMkKHPQE2pWDMLw==";
};

options {
    dnssec-enable yes;
    dnssec-validation yes;
};
```

Resolving DNS with DNSSEC