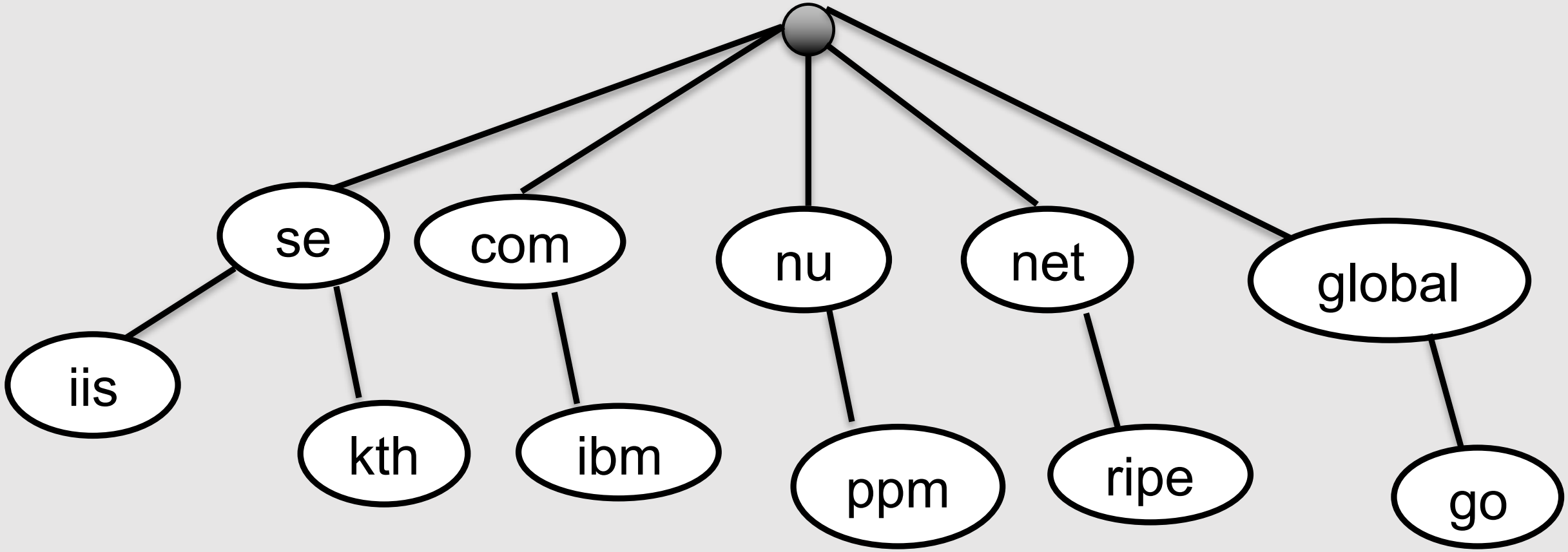

se
com
nu
net
global
iis
kth
ibm
ppm
ripe
go

INTERNET STIFTELSEN

Internets domännamnssystem*

Föreläsning FL08, HT 2023

Mats Dufberg

* Se “Internets domännamnssystem”

Innehåll

▶DNSSEC

[Till Innehåll]

Vad tillför DNSSEC?

- Ger signerade DNS-poster (eller snarare RRset).
  - Använder kryptografiska signaturer.
- Ger signerade svar på icke-existens (NXDOMAIN och NODATA).
- Förhindrar möjligheten till att skjuta in ”spoofad” data, ”man-in-the-middle attack”.

Hur påverkas DNS av DNSSEC?

- Nya posttyper, bl.a. DNSKEY, RRSIG och NSEC.
- Nya flaggor, bl.a. AD och DO.
- Nya tillstånd som kan leda till SERVFAIL.
- Ökad komplexitet.
- Begränsad livslängd (på RRSIG) innan underhåll måste göras på zonen (omsignering).

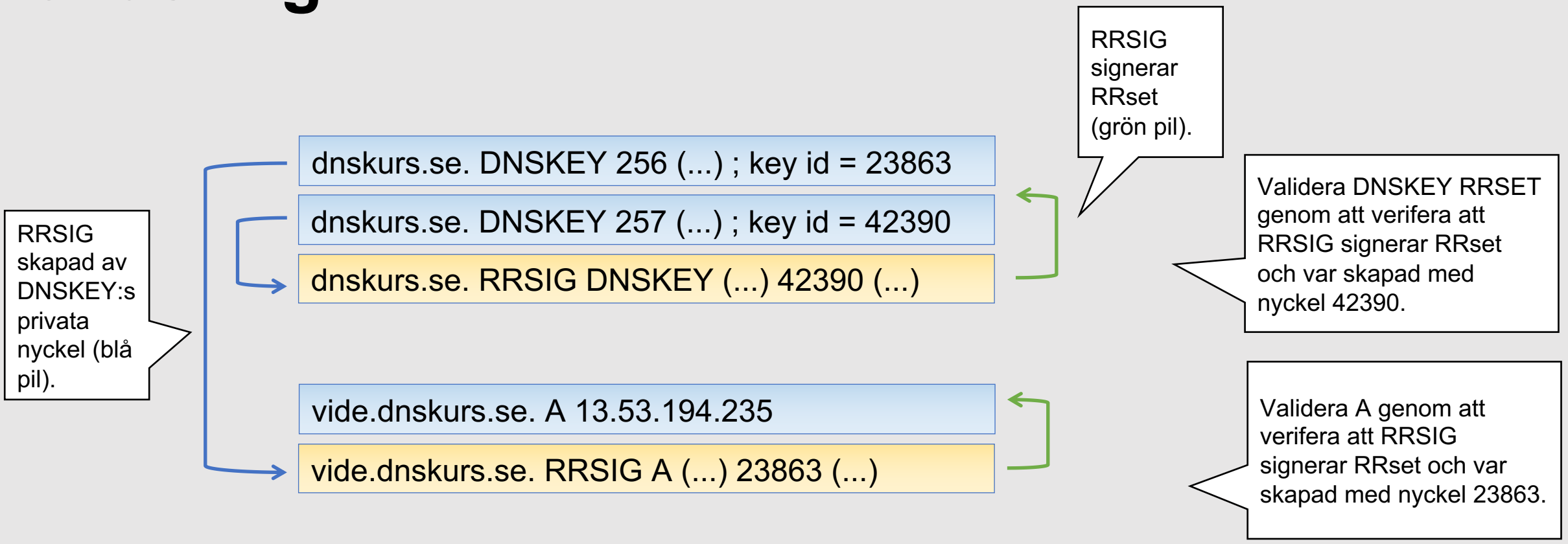
Mer om DNSSEC

Denna föreläsning är fortsätter att presentera DNSSEC.

Förra föreläsningen slutade när vi hade börja titta på hur vi ska validera i DNSSEC.

Validering

Bild från FL07



Hur kan vi lita på DNSKEY 42390?
Måste jag ha den från början?

[Till Innehåll]

Tillit till DNSKEY

DNSSEC skulle inte skala om vi behöver skaffa oss DNSKEY för alla zoner i förväg. Det måste finnas något säkert sätt att hämta DNSKEY genom DNS, när de behövs. På samma sätt som RRSIG hämtas genom DNS.

För detta så behöver vi en ny posttyp som binder ihop de signerade zonerna.

Zonerna är förbundna i delegeringen, där den nya posttypen kommer in.

DS

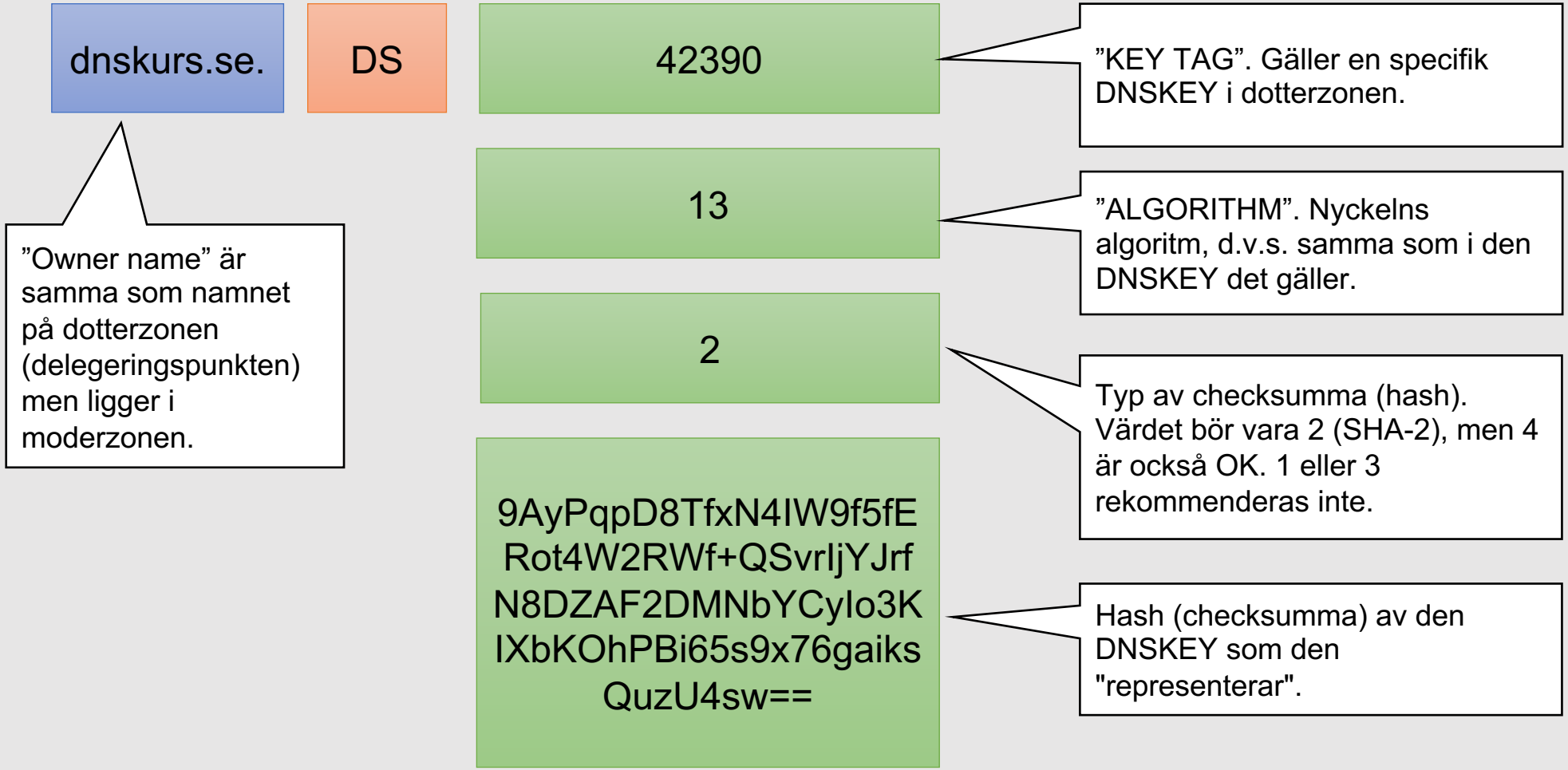
Checksumma (hash) av DNSKEY för en dotterzon.

```
dnskurs.se.     3600 IN  DS 42390 13 2 (
                DB1C7AA9E98AD9E38D0D59DB1E289DAA8A288835A93A
                96955AD432DC8498C3BA )

dnskurs.se.     3600 IN  DS 42390 13 1 (
                5773F953FD852F43AF85AF93F150F65BA0B38AFA )
```

DS

DS ligger tillsammans med NS-posterna i moderzonen och kan sägas utgöra en del av delegeringen. I fallet *dnskurs.se* så ligger DS-posterna i **.se**-zonen.

DNSKEY ligger i zones apex tillsammans med SOA- och NS-posterna. I fallet *dnskurs.se* så ligger DNSKEY-posterna i **dnskurs.se**-zonen.


dnskurs.se.
DS
42390
”KEY TAG”. Gäller en specifik DNSKEY i dotterzonen.
”Owner name” är samma som namnet på dotterzonen (delegeringspunkten) men ligger i moderzonen.
13
”ALGORITHM”. Nyckelns algoritm, d.v.s. samma som i den DNSKEY det gäller.
2
Typ av checksumma (hash). Värdet bör vara 2 (SHA-2), men 4 är också OK. 1 eller 3 rekommenderas inte.
9AyPqpD8TfxN4IW9f5fE Rot4W2RWf+QSvrIjYJrf N8DZAF2DMNbYCyIo3K IXbKOhPBi65s9x76gaiks QuzU4sw==
Hash (checksumma) av den DNSKEY som den "representerar".
Hashen är okrypterad, d.v.s. det är ingen signatur. Det behövs ingen DNSKEY för att verifiera den.
DS signeras av RRSIG som andra DNS-poster. DS-posterna ligger i moderzonen och signeras av moderzonens DNSKEY (dess privata nyckel).

Hash för DS

RFC 8624 specificerar vilka hash-algoritmer som bör användas och vilka som inte bör användas:

https://tools.ietf.org/html/rfc8624#section-3.3

DS

Finns i moderzonen i delegeringspunkten och håller en checksumma (hash) av DNSKEY som finns i dotterzon vars namn är DS-postens *owner name*.

”KEY TAG” för DNSKEY-posten i dotterzonen.

```
dnskurs.se.     3600 IN DS 42390 13 2 (
                DB1C7AA9E98AD9E38D0D59DB1E289DAA8A288835A93A
                96955AD432DC8498C3BA )

dnskurs.se.     3600 IN DS 42390 13 1 (
                5773F953FD852F43AF85AF93F150F65BA0B38AFA )
```

DS

- Om delegeringen innhåller DS så måste dotterzonen vara signerad.
- DS signeras med en RRSIG (i moderzonen).

▶KSK och ZSK

[Till Innehåll]

KSK och ZSK

Normalt så har vi minst två DNSKEY och vi använder dem för två olika roller:

- KSK = Key Signing Key (flags = 257)
- ZSK = Zone Signing Key (flags = 256)

DNSKEY med olika flaggor

```
$ dig se dnskey +mult @a.ns.se
(...)
;; ANSWER SECTION:
se.          3600 IN DNSKEY 256 3 8 (
                AwEAAa1CCGgWPeOoYclpgyPGuauo2savH2qm6vOEp6nh
                VqA3ABZZelkAZBN1du3vFXLmvYILWfKDoiSwzQsylRiV
                k82RgCMfa5q0aF+0ZJhX658Kb6i0Z3HQ1dL8lb7mkDin
                sHRPPqXvOA63Rzcy9L42jqOxUNAL1OjmO99tqjNectQq
                dxkmx2FDxSMlcDj4iGN6M0g6gKvB6/OYawyTlEkAWDxR
                n8opLYA74AfeET7nKmrBZscZWOAqhwAo2EjvW24y7nAp
                fNTBYtdaA2nF6AvQB0v6ThJDuv9+xt/qhOmOnAlcajWC
                zWgafPb1ket3uNhOl7sC7WKwq2IzqKTmzFJZTpk=
                ) ; ZSK; alg = RSASHA256 ; key id = 7906
se.          3600 IN DNSKEY 257 3 8 (
                AwEAAccqQMsh1rhvB3IWXmWZpCrug9MEGCKGteLIvwpp
                yHeHgeBBm3M0p5FV9ImquvxFCnBd6Eey3Vf8SzoTodZ3
                YrGF9WFve7bmie2MIBhFDoCep16v9lon0ZsKrOvoCkPb
                TT0iFCdrbdyikYcCfvvh303anvQeTCf3jy+bHOTleaqV
                aNRJiGv5NBsPKpfnnqBpqqKyZymSpwQXHtTeyv7iWwGl
                3cfP3U6sp711WvKkXy7Y2DJnC5T5owHWUy1ZPl4s+9Dt
                uC2A9AWhOpDicguHYRfmyscjCbPOB8/tO5j+uECo67i7
                JjsiLjQTRyHuigUUBRag3Z3FaTXZBg/myaoUL0U=
                ) ; KSK; alg = RSASHA256 ; key id = 59407
```

KSK

- KSK används för att signera DNSKEY RRset.
- DS pekar på KSK.
- KSK är ibland längre och byts mera sällan.
- Den är svårare att byta genom kopplingen till DS.

ZSK

- ZSK används för att signera all annan data i zonen, ibland även DNSKEY RRset.
- ZSK används bara internt i zonen och har ingen extern koppling.
- ZSK är ibland kortare och byts oftare.
- Den är lätt att byta eftersom det inte finns några direkta externa kopplingar.

CSK istället för ZSK och KSK

Uppdelningen mellan ZSK och KSK är en rekommendation snarare än ett ”måste”. Man kan ha en nyckel för båda rollerna istället. Då kallar man den CSK (”Common Signing Key”).

Om man stöter på en zon med bara en DNSKEY är det inte fel. Dock är det vanligaste att ha KSK och ZSK.

För CSK används normalt flags = 257.

▶Tillitskedja

[Till Innehåll]

Tillitskedja

Tillitskedja = ”chain of trust”

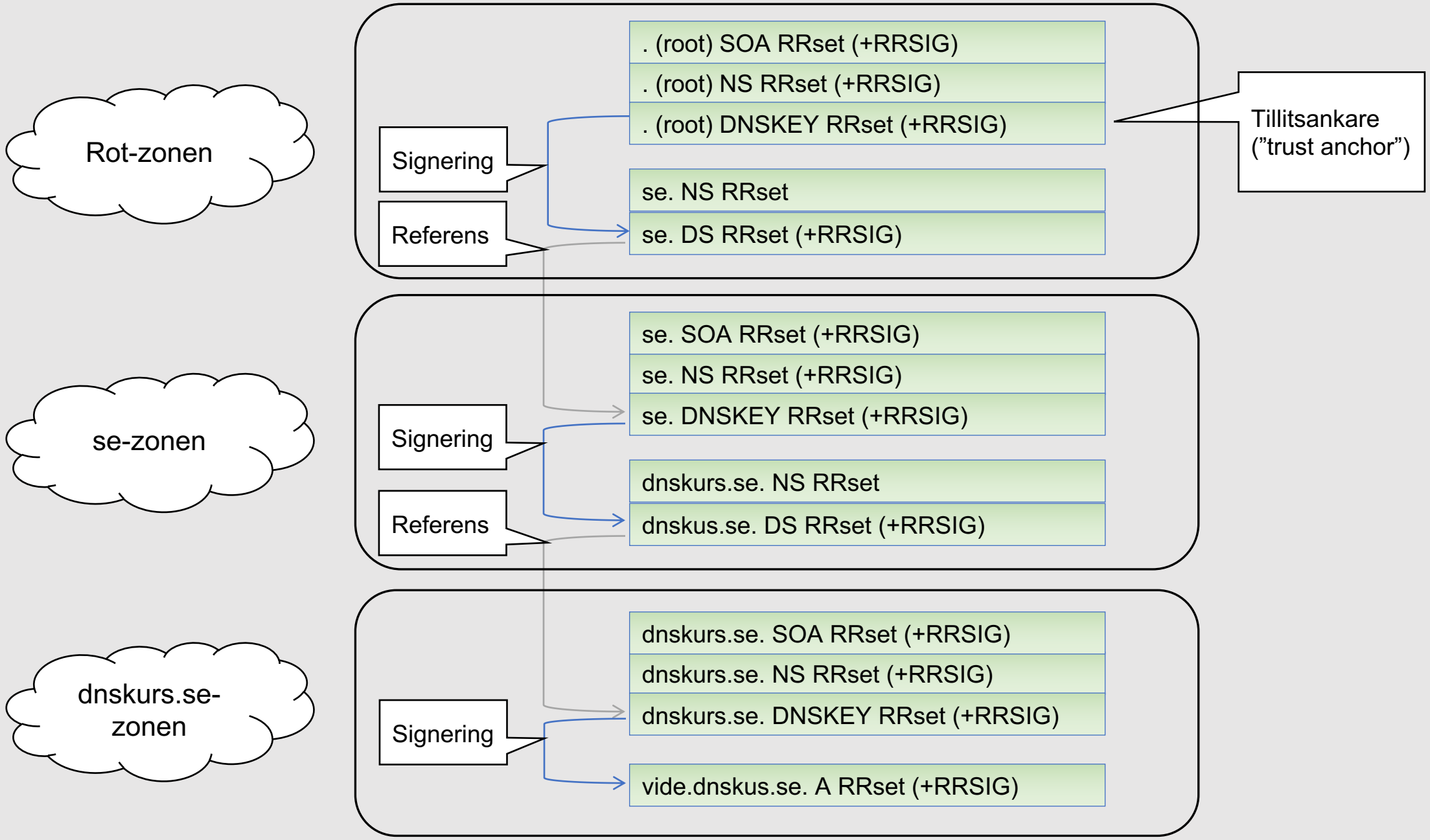
Tillitsankare

Vi måste ha en ingång till DNS-trädet (DNSSEC-trädet), en nyckel som vi litar på.

Normalt DNSKEY för rot.

Den är en tillitsankare, ”trust anchor”, för DNSSEC. Den gäller för rot och nedåt.

Man kan välja annan DNSKEY, på en lägre nivå, men den gäller bara nedåt, inte uppåt.


Rot-zonen
. (root) SOA RRset (+RRSIG)
. (root) NS RRset (+RRSIG)
. (root) DNSKEY RRset (+RRSIG)
Tillitsankare
(”trust anchor”)
Signering
Referens
se. NS RRset
se. DS RRset (+RRSIG)
se-zonen
se. SOA RRset (+RRSIG)
se. NS RRset (+RRSIG)
se. DNSKEY RRset (+RRSIG)
Signering
Referens
dnskurs.se. NS RRset
dnskus.se. DS RRset (+RRSIG)
dnskurs.se-
zonen
dnskurs.se. SOA RRset (+RRSIG)
dnskurs.se. NS RRset (+RRSIG)
dnskurs.se. DNSKEY RRset (+RRSIG)
Signering
vide.dnskus.se. A RRset (+RRSIG)

▶Delegering och validering

[Till Innehåll]

DS i delegeringen

Om delegeringen inkluderar DS betyder det att den delegerade zonen **måste** vara signerad. En validerande resolver kommer annars att returnera **SERVFAIL**.

Ett återkommande fel är att man tar bort signeringen på en zon utan att **först** ta bort DS.

Validering av RRset

Vi kan inte validera enskilda DNS-poster utan bara hela RRset. Ett RRset kan bestå av en eller flera DNS-poster.

- Utan fullständigt RRset så kan vi inte validera.
- Utan RRSIG för RRset så kan vi inte validera.
- Utan DNSKEY som använts för RRSIG så kan vi inte validera.
- Utan tillitskedja till DNSKEY (DS-post eller "trust anchor") så kan vi inte validera.

Steg för validering av RRset

- Hämta hela RRset
- Hämta RRSIG för RRset
- Verifiera att tiden ”nu” är inom starttid/sluttid i RRSIG
  - Annars avbryt ➔ **ej OK.**
- Hämta DNSKEY för RRSIG
- Sortera RRset i kanoniskt ordning
- Skapa samma typ av hash av RRset som RRSIG använt
- Dekryptera hash i RRSIG m.h.a. DNSKEY
- Båda ska ge samma hash.
  - Om olika ➔ **ej OK.**

Steg för validering av DNSKEY

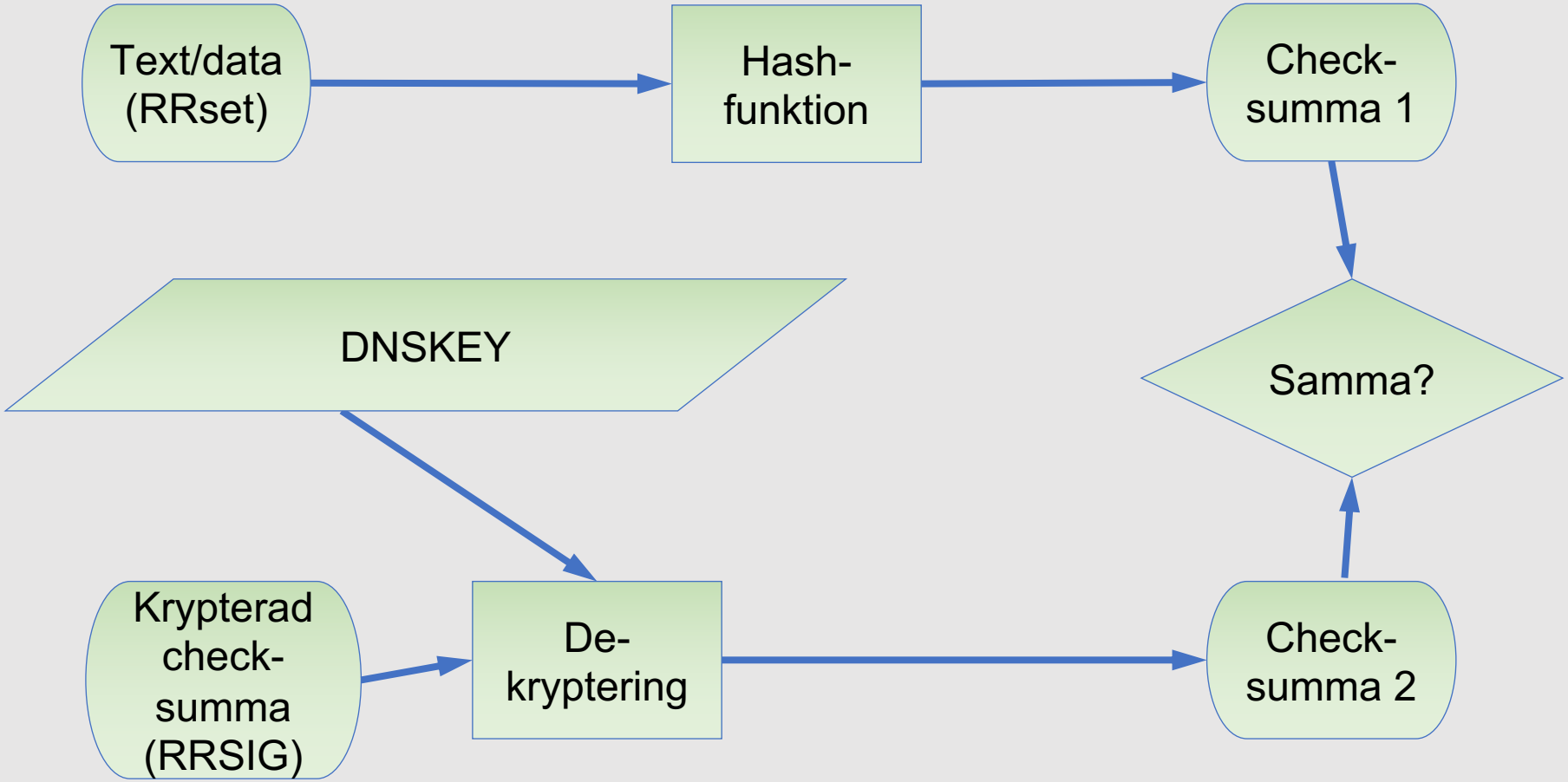
- Hämta hela DNSKEY RRset
- Hämta RRSIG för DNSKEY RRset
- Verifiera att tiden ”nu” är inom starttid/sluttid i RRSIG
  - Annars avbryt ➔ **ej OK.**
- Sortera RRset i kanoniskt ordning
- Skapa samma typ av hash av RRset som RRSIG använt
- Dekryptera hash i RRSIG m.h.a. DNSKEY från DNSKEY RRset
- Båda ska ge samma hash.
  - Om olika ➔ **ej OK.**
- Hämta DS RRset
- Verifiera att någon DS motsvarar en DNSKEY som har signerat RRset

Validring av DS RRset

DS RRset valideras som annat RRset, men nu i moderzonen.

Om vi har en inbyggd eller nedladdad ”trust anchor” så behöver den inte valideras.

Verifiera krypterad ”signatur”



Ställa frågor till validerande resolver

En resolver kan utföra alla steg i DNSSEC för att returnera att validerat svar.

- Om klienten inte indikerar stöd för DNSSEC så kommer resolvern inte att returnera någon indikering om DNSSEC (bakåtkompatibel).
- Resolvern returnerar alltid SERVFAIL, oavsett om klienten har stöd för DNSSEC eller inte, om
  - aktuell zon är felaktigt signerad, eller
  - aktuell zon är osignerad trots att det finns DS i delegeringen.

▶DNSSEC-frågor med ”dig”

[Till Innehåll]

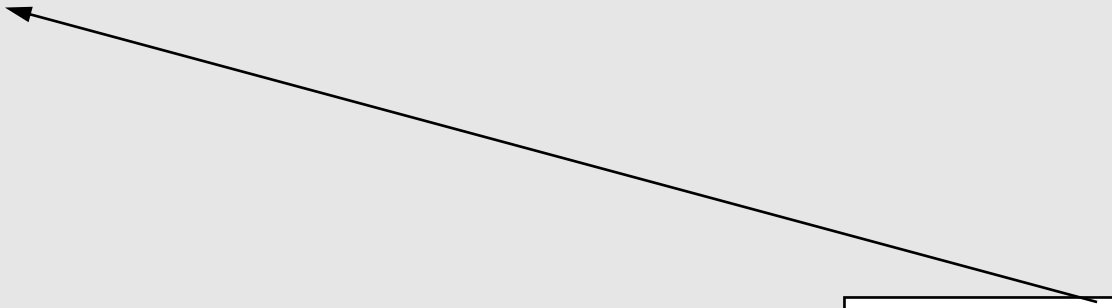
Ställa DNSSEC-frågor

Frågor om en signerad zon blir besvarade utan DNSSEC om man inte slår på DNSSEC. ”Utan DNSSEC” betyder utan DNSSEC-poster.

DNSSEC slår man på genom flagga i EDNS.

Fråga med DNSSEC

```
; <<>> DiG 9.10.6 <<>> @bill.ip.se dnskurs.se +mult +norec +qr +dnssec
; (1 server found)
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42137
;; flags: ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnskurs.se.            IN A
```



DO-flaggan (”DNSSEC OK”) satt i OPT/EDNS.
Signalerar att klienten stödjer DNSSEC.

Svar med DNSSEC

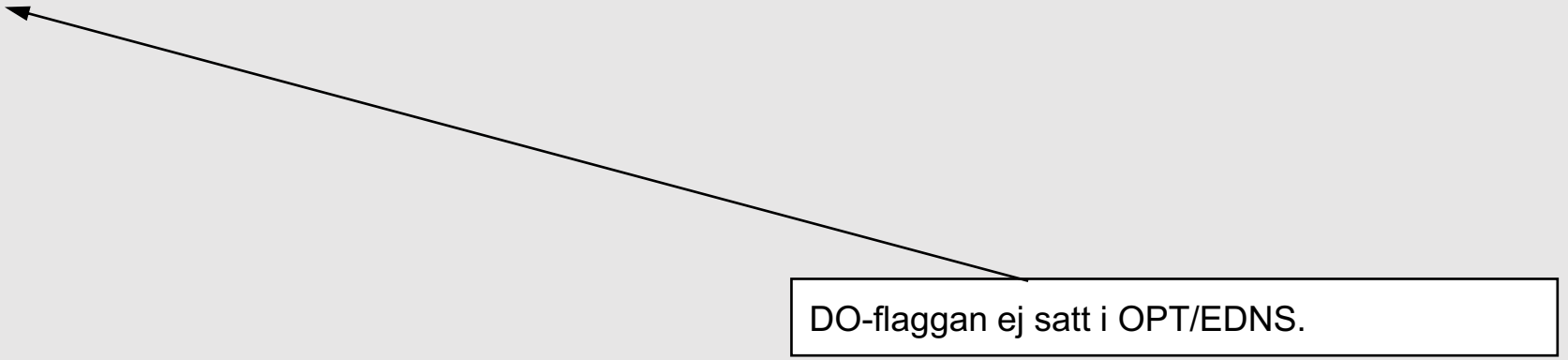
```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42137
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnskurs.se.            IN A

;; ANSWER SECTION:
dnskurs.se.         600 IN A 46.21.96.58
dnskurs.se.         600 IN RRSIG A 13 2 600 (
                    20190214090448 20190131090448 23863 dnskurs.se.
                    5baOtS9X753D+f60Oh+vmHlw1KuGGvOuaukuTH0YT8+D
                    IJWrsbEvr1WkT6HAz+7vaoDDOO0mtS3AmA8aRvhWAw== )

;; Query time: 44 msec
;; SERVER: 46.21.96.58#53(46.21.96.58)
;; WHEN: Thu Feb 07 00:07:16 CET 2019
;; MSG SIZE  rcvd: 161
```

DO-flaggan (”DNSSEC OK”) satt i OPT/EDNS. Signalerar att servern också stödjer DNSSEC.

Svaret är signerat.

Fråga utan DNSSEC

```
; <<>> DiG 9.10.6 <<>> @bill.ip.se dnskurs.se +mult +norec +qr
; (1 server found)
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1746
;; flags: ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnskurs.se.            IN A
```



Svar utan DNSSEC

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1746
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnskurs.se.            IN A

;; ANSWER SECTION:
dnskurs.se.     600 IN A 46.21.96.58

;; Query time: 53 msec
;; SERVER: 46.21.96.58#53(46.21.96.58)
;; WHEN: Thu Feb 07 00:03:50 CET 2019
;; MSG SIZE  rcvd: 55
```

DO-flaggan ej satt i OPT/EDNS eftersom klienten inte hade satt den.

Inga DNSSEC-poster.

Fråga utan DNSSEC

Om DO-flaggan inte sätts i frågan så kommer namnservern inte att inkludera DNSSEC-poster i svaret.

Undantag:

- Om frågan är om en specifik DNSSEC-post (”query type”) så kommer den att inkluderas (om den finns), men inget mer.

Svar på fråga utan DNSSEC om DNSKEY

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12311
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnskurs.se.            IN DNSKEY

;; ANSWER SECTION:
dnskurs.se.     600 IN DNSKEY 256 3 13 (
                9AyPqpD8TfxN4IW9f5fERot4W2RWf+QSvrIjYJrfN8DZ
                AF2DMNbYCyIo3KIXbKOhPBi65s9x76gaiksQuzU4sw==
                ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 23863
dnskurs.se.     600 IN DNSKEY 257 3 13 (
                oIy29iz9vH5eE+4KhZGXFf3FsLK93rkgeghCuUGDh4Dm
                TTO6XH/d/Z0x50vFw4ZBfvoXm+83Z8U+8DHnAtDGQw==
                ) ; KSK; alg = ECDSAP256SHA256 ; key id = 42390
(...)
```

DO-flaggan (”DNSSEC OK”) **ej** satt i OPT/EDNS. Svaret är **ej** signerat. RRSIG **ej** inkluderat.

Svar på fråga med DNSSEC om DNSKEY

```
(...)
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8872
;; flags: qr aa; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnskurs.se.            IN DNSKEY

;; ANSWER SECTION:
dnskurs.se.     600 IN DNSKEY 256 3 13 (
                9AyPqpD8TfxN4IW9f5fERot4W2RWf+QSvrIjYJrfN8DZ
                AF2DMNbYCyIo3KIXbKOhPBi65s9x76gaiksQuzU4sw==
                ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 23863
dnskurs.se.     600 IN DNSKEY 257 3 13 (
                oIy29iz9vH5eE+4KhZGXFf3FsLK93rkgeghCuUGDh4Dm
                TTO6XH/d/Z0x50vFw4ZBfvoXm+83Z8U+8DHnAtDGQw==
                ) ; KSK; alg = ECDSAP256SHA256 ; key id = 42390
dnskurs.se.     600 IN RRSIG DNSKEY 13 2 600 (
                20190214090448 20190131090448 42390 dnskurs.se.
                HWn6wbVlxOCVhXVuB51G/QJDTj7nbRtSyH9mJwF4hhrJ
                k2tZYOkr8vPMASNnrrd3MUWLsx4CVBNynDVhUmwwbA== )
(...)
```

DO-flaggan (”DNSSEC OK”) satt i OPT/EDNS.
Svaret är signerat. RRSIG inkluderat.

Fråga utan DNSSEC till resolver

```
; <<>> DiG 9.10.6 <<>> www.sunet.se +mult +qr +noadflag @8.8.8.8
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19061
;; flags: rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sunet.se.      IN A

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19061
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.sunet.se.      IN A

;; ANSWER SECTION:
www.sunet.se.      102 IN CNAME webc.sunet.se.
webc.sunet.se.     218 IN A 192.36.171.231
(...)
```

DO-flaggan **ej** satt i OPT/EDNS.

Notera att **AD-flaggan** inte är satt i ”response” (mer kommande bild).

Fråga med AD-flaggan satt till resolver

```
; <<>> DiG 9.10.6 <<>> www.sunet.se +mult +qr @8.8.8.8
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61099
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sunet.se.      IN A

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61099
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.sunet.se.      IN A

;; ANSWER SECTION:
www.sunet.se.       46 IN CNAME webc.sunet.se.
webc.sunet.se.      80 IN A 192.36.171.231
(...)
```

DO-flaggan ej satt i OPT/EDNS. AD-flaggan satt i vanliga flaggfältet.

AD satt i ”response” betyder att det är validerat med DNSSEC.

Om AD är satt i ”query” så kan AD sättas i ”response” men utan DO inga extra DNSSEC-poster som RRSIG.

AD

AD = Authenticated Data

AD-flagga till resolver

AD-flaggan i frågan (”query”):

- Klienten kan hantera AD-flagga i svaret (”response”).

AD-flaggan i svaret (”response”):

- AD-flaggan satt == svaret validerat (DNSSEC är OK)
- AD-flaggan osatt == ingen DNSSEC eller resolver validerar inte

*Om resolvern validerar och DNSSEC inte är OK (fel vid validering) så blir det **SERVFAIL** istället.*

Fråga med DO-flaggan satt till validerande resolver

```
; <<>> DiG 9.10.6 <<>> www.sunet.se +mult +qr +dnssec @8.8.8.8
(...)
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50487
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.sunet.se.          IN A

;; ANSWER SECTION:
www.sunet.se.          230 IN CNAME webc.sunet.se.
www.sunet.se.          230 IN RRSIG CNAME 8 3 300 (
                    20190216094347 20190206084347 7636 sunet.se.
                    CsQ2UKABmZg1s0sMiOsE1Gac3HfQN6mK7rjfkJfVVMa6
                    PMFfcww4idMAHMPBW9ROI6tdXd74aZRfA6Z91HEYzeXb
                    AG0DZAGh3S8JaHH4NsCuxRrRn5K2TGSqLXkpqzGXFdpJ
                    DrJ8B3xDNcMTJUtEsotw/ZYPi386rRoVmaU1rMo= )
webc.sunet.se.         230 IN A 192.36.171.231
webc.sunet.se.         230 IN RRSIG A 8 3 300 (
                    20190215214344 20190205204344 7636 sunet.se.
                    PPlz9B+1G6QS4wYBph1XGqtgK3hSb2oelN0lxoL9E/0C
                    NjHmAzAYvMJsoQvUkSIwhcZAWljC2Q8emGEI6cSD2yg1
                    iMiXruCmG+G4pE/ZatA/nDcaGvmYCvMWrpLfY6hYY9vt
                    0qRXE6XAYsN6TSW0eD0aJ/n9RL7mBLhp/Ik9m3w= )
(...)
```

Sätt DO-flaggan i frågan med +dnssec till ”dig”.

AD satt i ”response” betyder att det är validerat med DNSSEC.

Svaret är signerat och RRSIG-posterna är inkluderade.

Validerat eller inte?

”Query” har satt AD eller DO. Alternativ för en öppen resolver som validerar:

1. Alla inblandade zoner är signerade och det finns DS-poster i delegeringarna. Och **allt validerar**. ”Response” med **AD-flaggan satt**. NOERROR eller NXDOMAIN.
2. Zonerna ska vara signerade – och korrekt signerade – men det finns **något fel i DNSSEC**. ”Response” med **SERVFAIL**.
3. Zonerna m.m. är **OK men utan DNSSEC**. ”Response” **utan AD-flagga**. NOERROR eller NXDOMAIN. *(”Vanlig” DNS.)*
4. Andra fel oavsett DNSSEC, t.ex. oåtkomlig zon. ”Response” med **SERVFAIL**.

Validerat eller inte?

Om ”query” varken har satt AD-flagga eller DO-flagga så får inte AD-flaggan vara satt i ”response”.

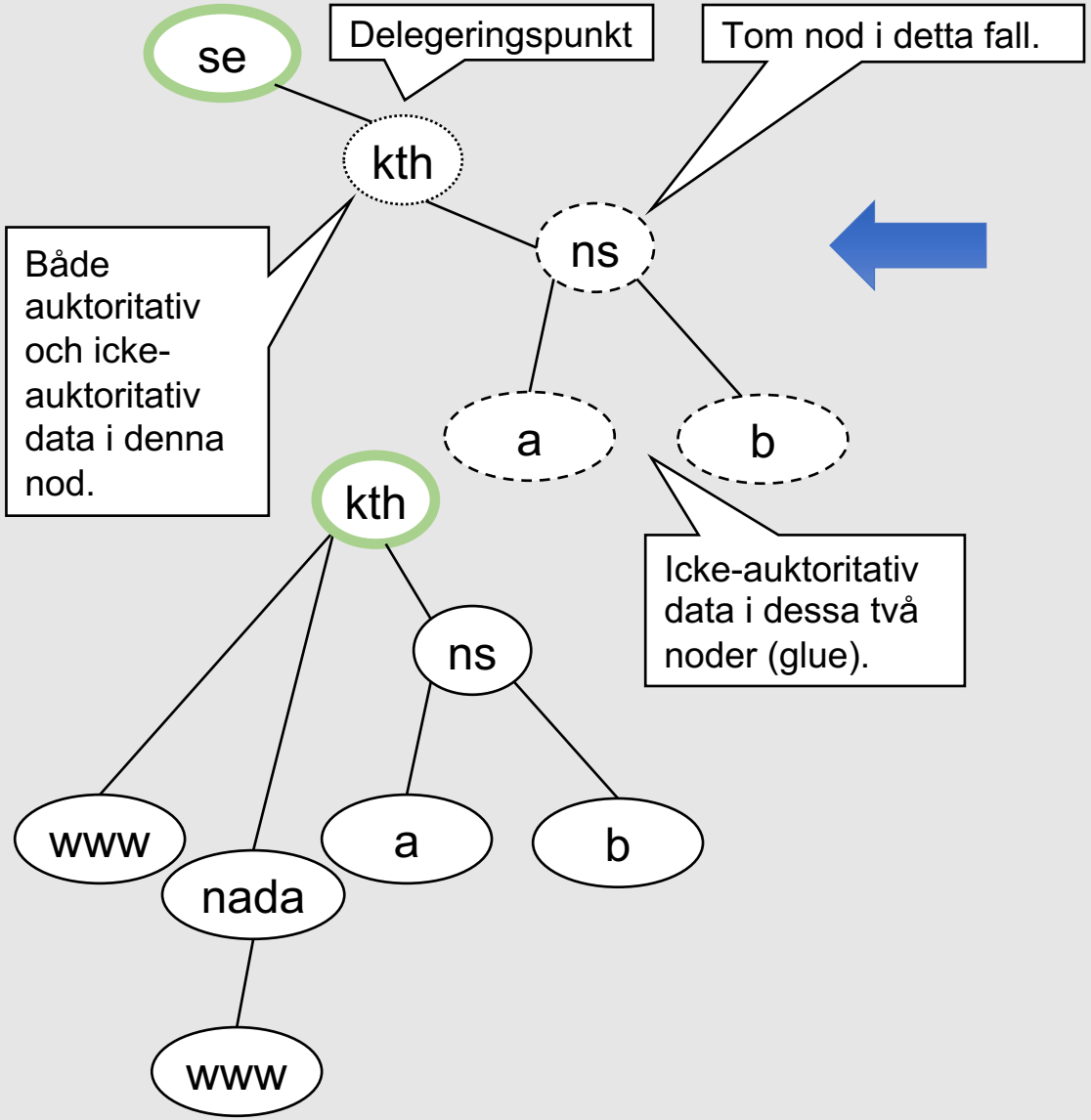
Notera: *En validerande resolver kommer att validera ändå*, men inte signalera till klienten.

En validerande resolver kommer att returnera SERVFAIL om den hittar fel i DNSSEC oavsett om klienten har har satt AD-flaggan, DO-flaggan eller ingen av de två. – SERVFAIL kan också returneras av andra orsaker, som vi har sett tidigare.

▶Delegering och DS

[Till Innehåll]

Delegering med DS

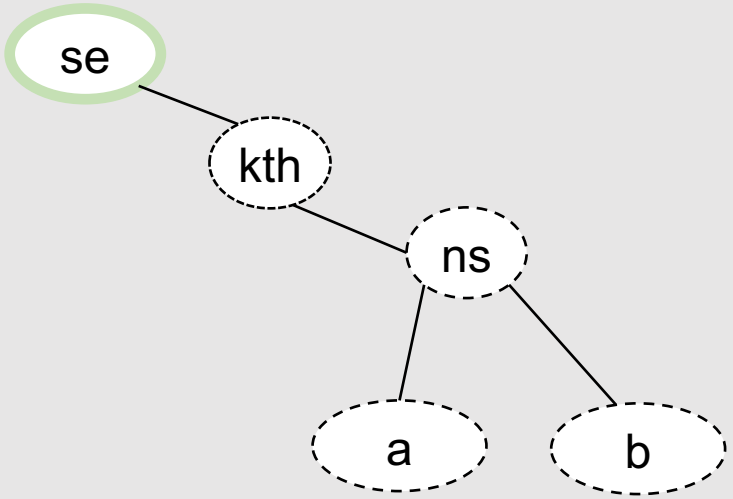


I eventuella noder under delegeringspunkten, i moderzonen, så kan det finnas glue-poster, men inget annat.

De icke-auktoritativa posterna är kopior av motsvarande poster i dotterzonen. Se nästa bild.

Delegering av kth.se. DNS-poster i se-zonen.

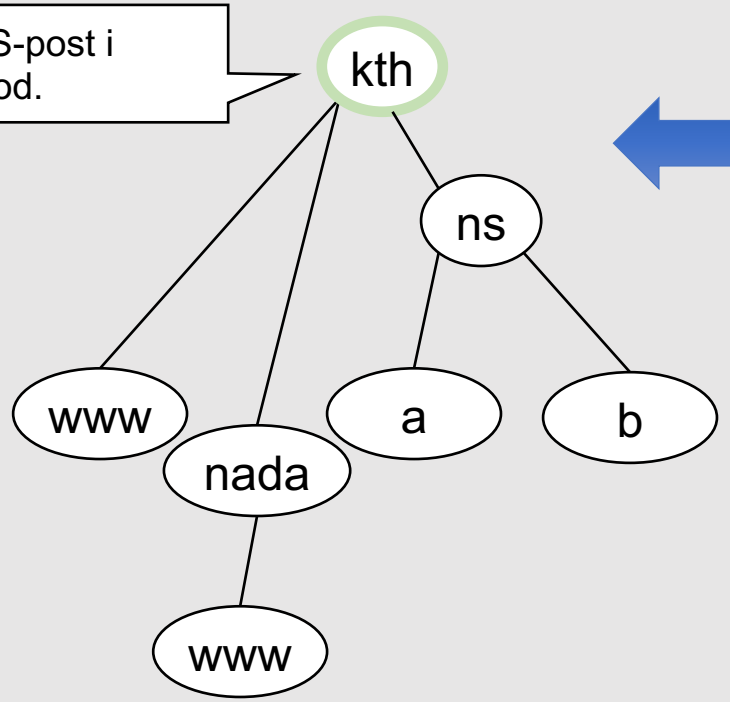
```
;; Icke-auktoritativ data:
kth.se.          NS      nic2.lth.se.
kth.se.          NS      b.ns.kth.se.
kth.se.          NS      a.ns.kth.se.
kth.se.          NS      ns2.chalmers.se.
b.ns.kth.se.     AAAA    2001:6b0:1::250
a.ns.kth.se.     AAAA    2001:6b0:1::246
b.ns.kth.se.     A       130.237.72.250
a.ns.kth.se.     A       130.237.72.246

;; Auktoritativ data:
kth.se.      DS      52831 8 1 (...)
kth.se.      DS      52831 8 2 (...)
kth.se.      RRSIG   DS 8 2 3600 (...)
kth.se.      NSEC    kth-edu.se. NS DS RRSIG NSEC
kth.se.      RRSIG   NSEC 8 2 7200 (...)
```



NSEC-posterna har utelämnats från denna bild.

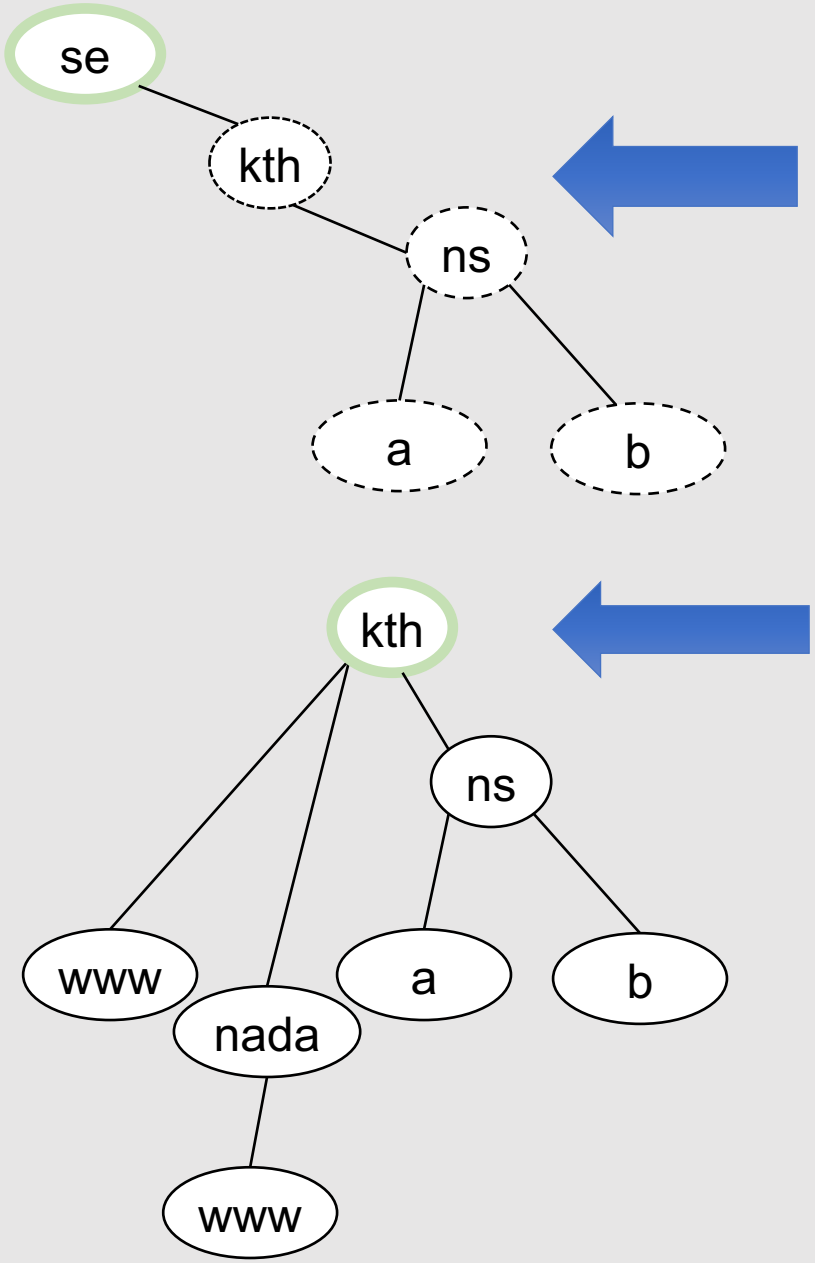
DS-posten hör till moderzonen, inte till dotterzonen.

Ingen DS-post i denna nod.



DNS-poster i kth.se-zonen.

```
;; Auktoritativ data:
kth.se.          NS      ns2.chalmers.se.
kth.se.          NS      a.ns.kth.se.
kth.se.          NS      b.ns.kth.se.
kth.se.          NS      nic2.lth.se.
kth.se.          RRSIG   NS 8 2 1800 (...)
a.ns.kth.se.     AAAA    2001:6b0:1::246
a.ns.kth.se.     RRSIG   AAAA 8 4 1800 (...)
b.ns.kth.se.     AAAA    2001:6b0:1::250
b.ns.kth.se.     RRSIG   AAAA 8 4 1800 (...)
a.ns.kth.se.     A       130.237.72.246
a.ns.kth.se.     RRSIG   A 8 4 1800 (...)
b.ns.kth.se.     A       130.237.72.250
b.ns.kth.se.     RRSIG   A 8 4 1800 (...)
kth.se.          DNSKEY  257 3 8 (...) ; KSK; key id = 52831
kth.se.          DNSKEY  256 3 8 (...) ; ZSK; key id = 25833
kth.se.          RRSIG   DNSKEY 8 2 1800 (...) 25833 (...)
kth.se.          RRSIG   DNSKEY 8 2 1800 (...) 52831 (...)
```



DS för kth.se i se-zonen.

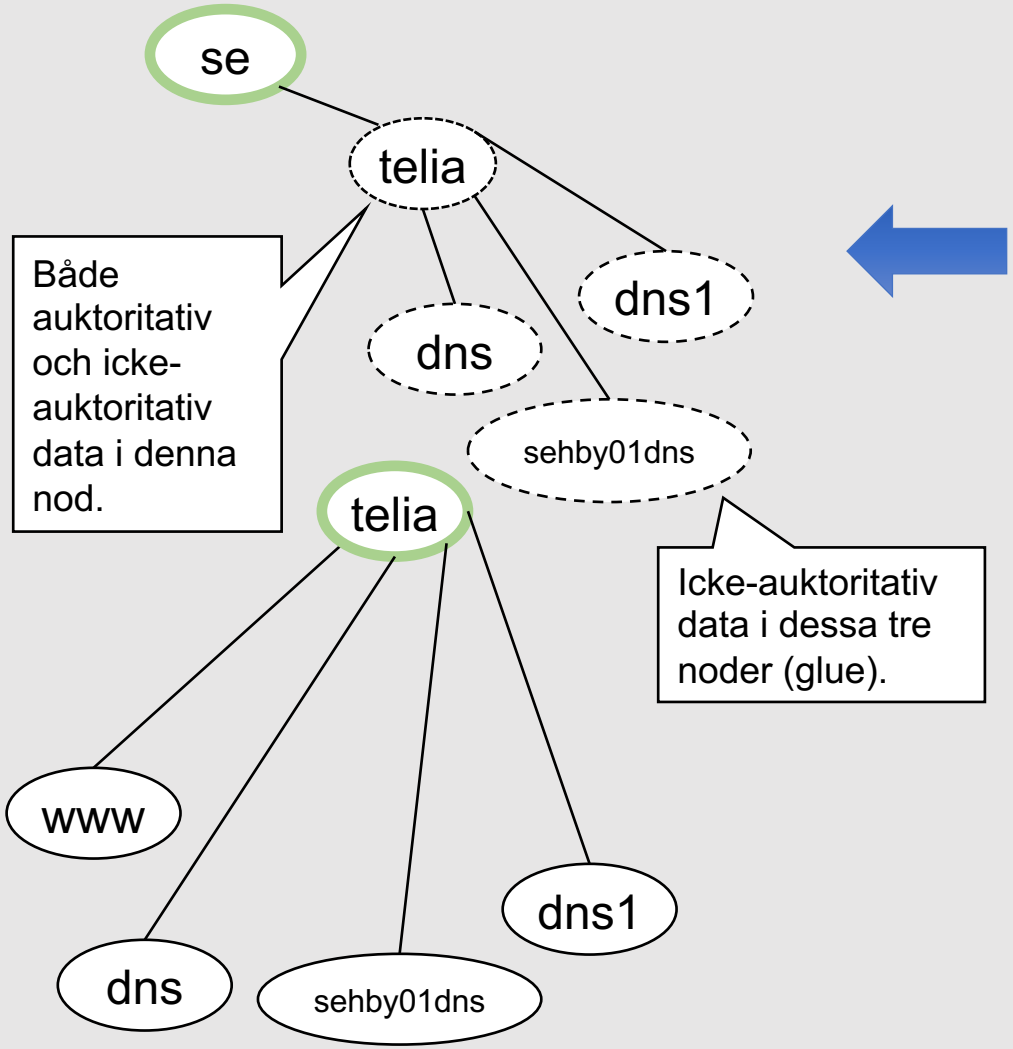
```
kth.se.     DS      52831 8 1 (...)
kth.se.     DS      52831 8 2 (...)
```

DS ovan ska stämma med rätt DNSKEY i kth.se-zonen.

DNSKEY för kth.se i kth.se-zonen.

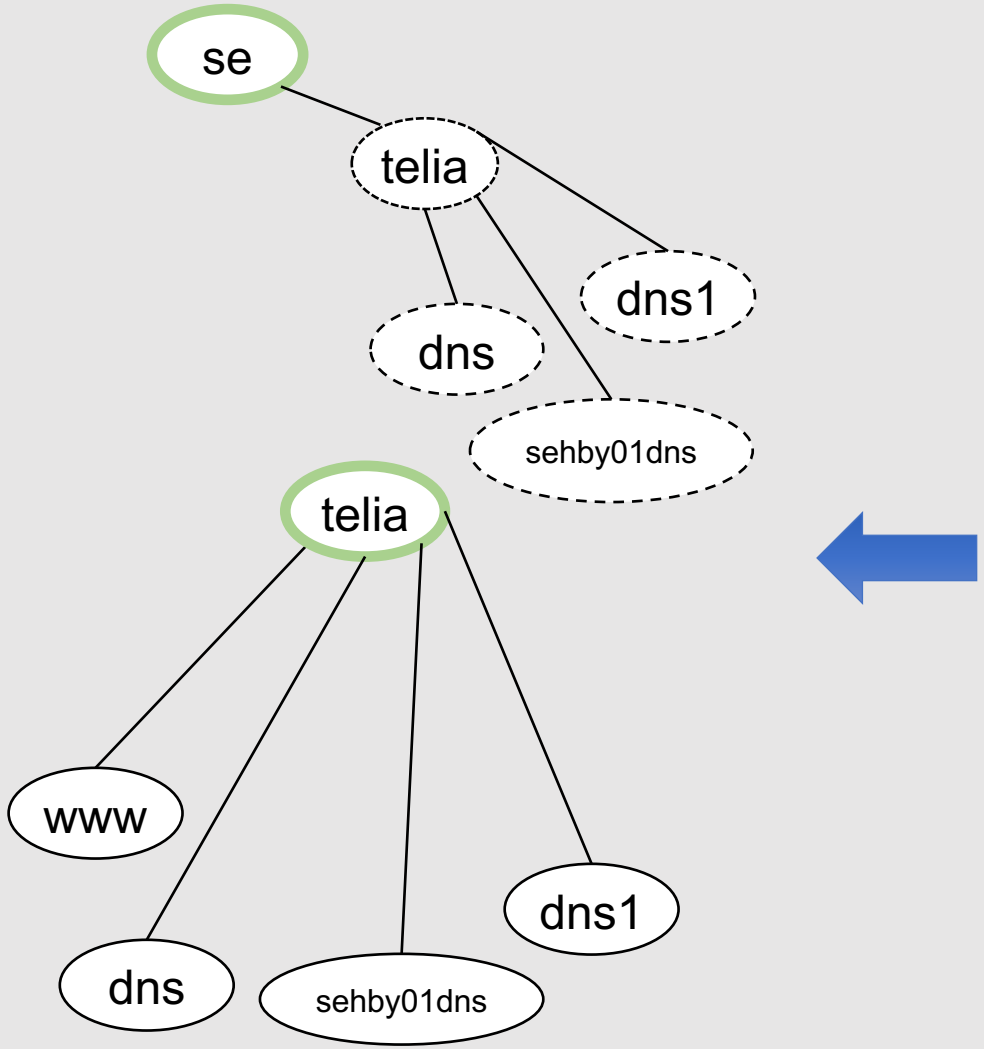
```
kth.se.     DNSKEY  257 3 8(...) ; KSK; key id = 52831
```

Delegering utan DS från signerad moderzon



Delegering av kth.se. DNS-poster i se-zonen.

```
;; Icke-auktoritativ data:
telia.se.                NS   dns.telia.se.
telia.se.                NS   dns1.telia.se.
telia.se.                NS   sehby01dns.telia.se.
sehby01dns.telia.se.     A    193.44.164.165
dns1.telia.se.           A    81.236.34.35
dns.telia.se.            A    193.44.165.16

;; Auktoritativ data:
telia.se.            NSEC    telia-5g.se. NS RRSIG NSEC
telia.se.            RRSIG   NSEC 8 2 7200 (...)
```



DNS-poster i telia.se-zonen

```
;; Auktoritativ data:
telia.se.                NS   dns.telia.se.
telia.se.                NS   dns1.telia.se.
telia.se.                NS   sehby01dns.telia.se.
sehby01dns.telia.se.     A    193.44.164.165
dns1.telia.se.           A    81.236.34.35
dns.telia.se.            A    193.44.165.16
```

▶DS kräver signerad zon

[Till Innehåll]

DS kräver signerad zon

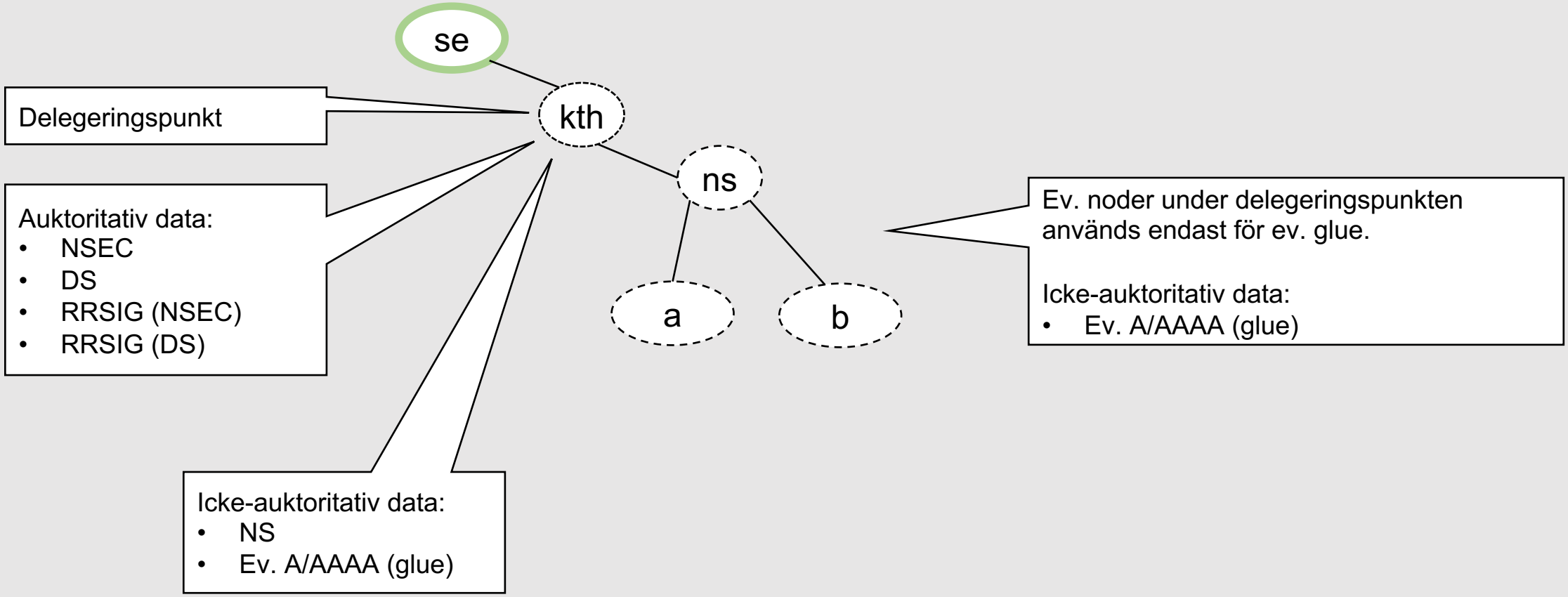
	Dotterzonen korrekt signerad	Dotterzonen felaktigt signerad*	Dotterzonen är osignerad
Korrekt DS i moderzonen	Dotterzonen är DNSSEC-valid	SERVFAIL	DS i moderzonen ger alltid SERVFAIL
Felaktig DS i moderzonen	SERVFAIL	SERVFAIL	
Ingen DS i moderzonen	Dotterzonen DNSEC-valideras inte	Dotterzonen DNSEC-valideras inte	Dotterzonen DNSEC-valideras inte

*) Gäller fråga som berör det som är felaktigt signerat.

Utan DS har signering inget värde, men signering först och sedan DS.

▶DNS-poster i delegeringen

[Till Innehåll]


se
kth
ns
a
b
Delegeringspunkt
Auktoritativ data:
• NSEC
• DS
• RRSIG (NSEC)
• RRSIG (DS)
Icke-auktoritativ data:
• NS
• Ev. A/AAAA (glue)
Ev. noder under delegeringspunkten används endast för ev. glue.
Icke-auktoritativ data:
• Ev. A/AAAA (glue)

NSEC

NSEC finns i varje nod (för varje "owner name") med andra poster.
NSEC pekar mot nästa nod ("owner name") med data.

- NSEC struntar i noder som bara har glue-poster (A, AAAA) i delegeringen (i moderzonen).
- NSEC finns i delegeringspunkten – där NS ligger.

NSEC

NSEC listar alla posttyper som finns noden ("owner name" till NSEC-posten) inklusive ev. NS och DS. Men...

- NSEC-posten som ligger tillsammans med NS-posterna i delegeringen inkluderar **inte** ev. glue (A, AAAA) i samma nod.

I en zon med i stort sett bara delegeringar, t.ex. .se och de flesta TLD:er, så pekar NSEC-posterna från en delegering till nästa.

Från NSEC-posten så kan man se ifall det finns någon DS-post för den delegerade zonen (dotterzonen).

RRSIG

RRSIG finns för varje RRset i zonen, men bara när zonen är auktoritativ för datat.

- Det finns ingen RRSIG för NS i delegeringen (i moderzonen).
- Det finns ingen RRSIG för glue-poster i delegeringen (i moderzonen).

Motsvarande NS- och adressposter är auktoritativa i dotterzonen, och där finns det RRSIG.

RRSIG och NSEC i delegeringen

	Auktoritativ data?	NSEC i samma nod?	RRSIG för posten?
Glue	nej	nej (*)	nej
NS	nej	ja	nej
DS	ja	ja	ja
NSEC	ja	ja (sig själv)	ja
RRSIG	ja	ja	nej, ingen RRSIG för RRSIG

*) Om glue-posten har samma "owner name" som NS så finns det en NSEC-post i samma nod, men NSEC-posten refererar inte till glueposten.

▶Nyckelbyte och uppdatering av DS

[Till innehåll]

Byte av ZSK

ZSK används bara inom zonen, men bytet måste göras med överlappning mellan gammal och ny nyckel och med hänsyn till cachningen av DNSKEY RRset och RRSIG.

1. Lägg till en ny ZSK.
2. Signera uppdaterad DNSKEY-RRset med KSK.
3. Ladda om zonen med nytt serienummer.
4. Vänta tills DNSKEY RRset propagerad med hänsyn till zonöverföring och cachning (TTL).
5. Signera om zonen med ny ZSK, tag bort gammal ZSK och ladda om zonen med nytt serienummer.

Byte av KSK

Byte av KSK i dotterzonen måste samordnas med byte av DS i moderzonen. Bytet måste göras med överlappning mellan gammal och ny nyckel och med hänsyn till cachningen av DNSKEY RRset, RRSIG och DS.

"Chain of trust" får aldrig brytas och då måste man ta hänsyn till TTL och cachning.

Byte av KSK

1. Lägg till en ny KSK i dotterzonen.
2. Signera uppdaterad DNSKEY RRset med ny och gammal KSK.
3. Vänta tills DNSKEY RRset har propagerat med hänsyn till zonöverföringar och cachning (TTL).
4. Skapa DS från ny KSK.
5. Byt till ny DS i moderzonen.
6. Vänta tills DS RRset har propagerat med hänsyn till zonöverföringar och cachning (TTL).
7. Tag bort gammal KSK och signaturer gjorda av den från dotterzonen.

Uppdatera DS

Moderzon (t.ex. .se) och dotterzon (t.ex. dnskurs.se) hanteras oftast av olika organisationer. Uppdatering av DS beställs av från dotterzon men utförs i moderzon. Uppdatering betyder här:

- Stoppa in DS för en zon (delegering) som inte har DS, d.v.s. introducera DNSSEC.
- Byt DS från en till en annan, antingen att den pekar på en ny DNSKEY eller att algoritmen för DS byts.
- Tillägg av ytterligare DS-post, t.ex. annan DNSKEY eller annan algoritm på DS.
- Ta bort DS, men inte alla.
- Ta bort alla DS, d.v.s. koppla bort dotterzonen från DNSSEC.

DS-posten måste alltid gälla en DNSKEY i dotterzonen och den DNSKEY måste alltid signera DNSKEY RRset

Uppdatera DS

Det finns många olika lösningar och rutiner för hur uppdateringen av DS i moderzonen ska gå till, och det är alltid administratören av moderzonen som fastställer det. Eller ombud (”registrar”) som fastställer det, när det gäller de flesta toppdomäner.

Domännamnsinnehavaren får själv söka efter hur reglerna ser ut för moderzonen.

Själva uppdateringen ligger utanför själva DNS, men är avgörande för DNSSEC.

▶CDS och CDNSKEY

[Till innehåll]

Uppdatera DS

Det finns två speciella DNS-poster för att underlätta byte av DS-post.

Namnserverprogramvarorna, som Bind, har lagt in stöd för att automatiskt skapa dessa när en ny KSK skapas.

De nya posttyperna är:

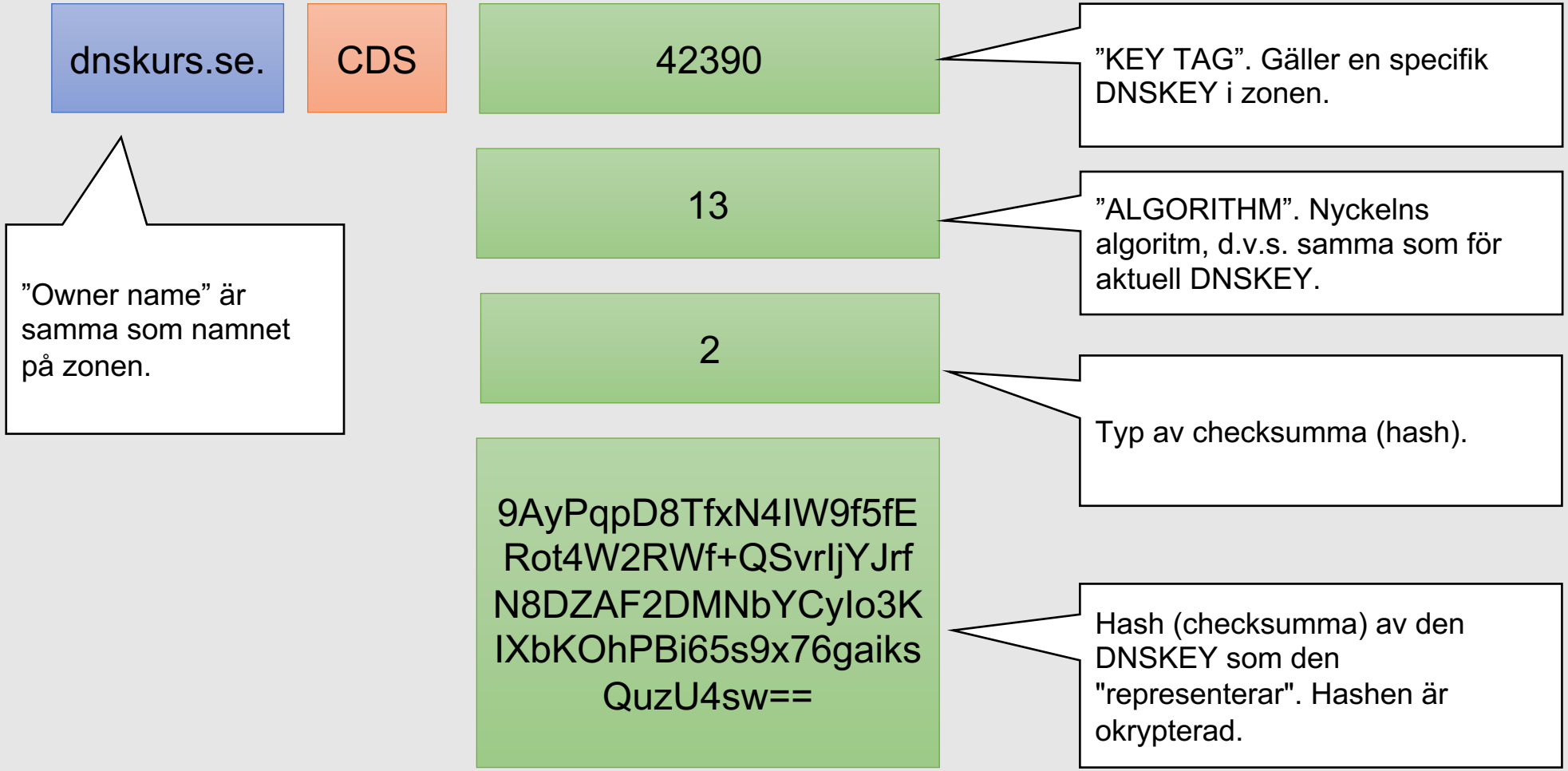
- CDS
- CDNSKEY

CDS

En CDS-post har exakt samma **format** på RDATA som en DS-post. T.ex.

```
dnskurs.se.       DS  42390 13 2 (
                      DB1C7AA9E98AD9E38D0D59DB1E289DAA8A288835A93A
                      96955AD432DC8498C3BA )

dnskurs.se.       CDS 42390 13 2 (
                      DB1C7AA9E98AD9E38D0D59DB1E289DAA8A288835A93A
                      96955AD432DC8498C3BA )
```

DS och CDS har samma "owner name" men finns i olika zoner och betyder olika saker.


dnskurs.se.
CDS
42390
”KEY TAG”. Gäller en specifik DNSKEY i zonen.
”Owner name” är samma som namnet på zonen.
13
”ALGORITHM”. Nyckelns algoritm, d.v.s. samma som för aktuell DNSKEY.
2
Typ av checksumma (hash).
9AyPqpD8TfxN4IW9f5fE Rot4W2RWf+QSvrIjYJrf N8DZAF2DMNbYCyIo3K IXbKOhPBi65s9x76gaiks QuzU4sw==
Hash (checksumma) av den DNSKEY som den "representerar". Hashen är okrypterad.
Verifieras av RRSIG som andra DNS-poster.

DS och CDS

DS och CDS har identisk RDATA, men betyder olika saker och har olika funktion.

	DS	CDS
Placering	Delegeringspunkten i moderzonen	Apex i dotterzonen
Ingår valideringskedjan?	Ja	Nej
Resolver hämtar den automatiskt?	Ja, om resolvern validerar	Nej
Obligatorisk för DNSSEC?	Ja	Nej

Samma "owner name", men olika zoner.

CDS för DS uppdatering

Modellen för CDS är att registry för moderzonen ska kunna plocka upp förändringar av DS direkt via DNS och att alla skulle kunna göra på samma sätt.

CDS vid byte av DS

CDS får bara finnas i en signerad zon och CDS RRset måste vara signerad som alla andra DNS-poster i zonen och det ska gå att validera CDS RRset via befintliga DS (om sådan finns) och DNSKEY, och CDS måste peka på DNSKEY i dotterzonen.

Policy hos administratören av moderzonen avgör om CDS ska accepteras eller ignoreras.

Om CDS accepteras så ska hela det befintliga DS RRset bytas ut det som hela CDS RRset anger.

CDS vid tillägg av DS

Om det inte finns något DS så går det inte att validera CDS RRset med DNSSEC. Policy hos administratören av moderzonen avgör om CDS ska accepteras, och i så fall om extra verifiering krävs eller inte.

Fortfarande är det så att CDS bara får finnas i en signerad zon och CDS RRset måste peka på befintlig DNSKEY.

Hela CDS RRset måste läggas in som DS, eller inget.

CDS vid borttag av DS

DS plockas bort ifall administratören av dotterzonen vill tillfälligt eller permanent ta bort DNSSEC från dotterzonen, i alla fall validering av den. Det finns olika skäl till det, t.ex.:

- Byte till DNS-operatör som inte stödjer DNSSEC.
- Nyckelbyten eller annat som är enklare att göra utan DNSSEC.

CDS vid borttag av DS

Det finns ett specialdata för CDS (som aldrig kan finns i DS) som betyder att DS-posterna ska plockas bort.

```
namn.se.        CDS     0 0 0 00
```

Återigen, det är policy hos administratören av moderzonen som avgör om den ska accepteras eller om administratören av dotterzonen måste använda andra rutiner.

CDNSKEY istället för CDS

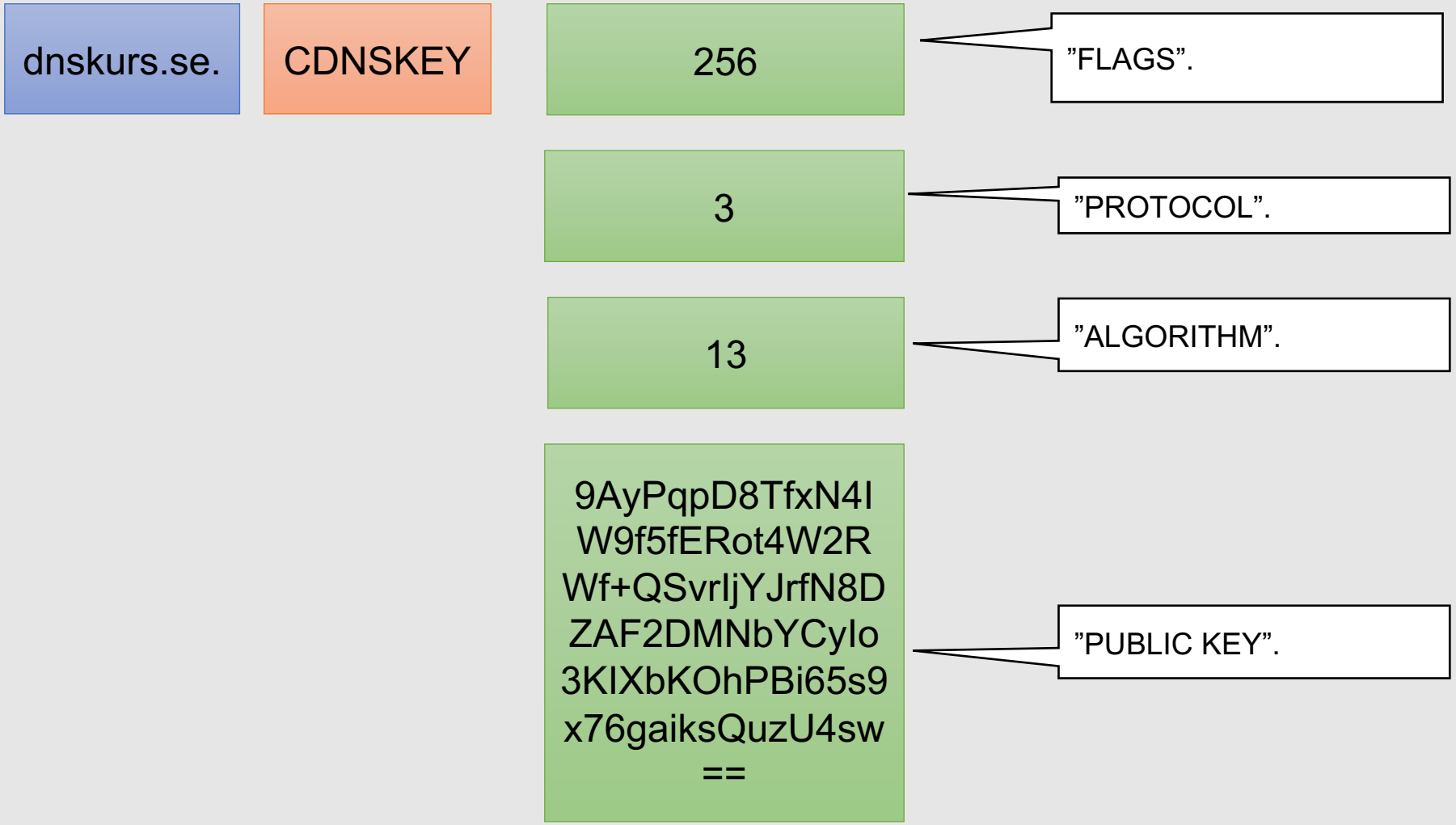
Istället för CDS så kan dotterzonen publicera CDNSKEY. CDNSKEY är en kopia av den DNSKEY som administratören av dotterzonen vill ska vara underlag för en ny DS-post.

Där CDS är en ”färdig” DS-post så ska den kommande DS-posten skapas ur CDNSKEY. Eftersom det finns flera, i alla fall två, algoritmer för DS-poster att välja mellan så kan administratören för moderzonen välja vilken det ska vara, eller båda.

CDNSKEY

En CDNSKEY-post har exakt samma **format** på RDATA som en DNSKEY-post.
T.ex.

```
dnskurs.se.   DNSKEY     256 3 13 (
                         IOD9VyozTjs7woYD3QK97miM4TCkeK0TnNZdgmvNtH0M
                         mmPOtAVKWjAkL/urwf70+nLxLMNLktC9XujWZ0ASjQ==)

dnskurs.se.   CDNSKEY    256 3 13 (
                         IOD9VyozTjs7woYD3QK97miM4TCkeK0TnNZdgmvNtH0M
                         mmPOtAVKWjAkL/urwf70+nLxLMNLktC9XujWZ0ASjQ==)
```


dnskurs.se.
CDNSKEY
256
”FLAGS”.
3
”PROTOCOL”.
13
”ALGORITHM”.
9AyPqpD8TfxN4I
W9f5fERot4W2R
Wf+QSvrIjYJrfN8D
ZAF2DMNbYCyIo
3KIXbKOhPBi65s9
x76gaiksQuzU4sw
==
”PUBLIC KEY”.

DNSKEY och CDNSKEY

De har samma "owner name" och finns i samma zon (dotterzonen), men är olika RRset och betyder olika saker. Alla poster i CDNSKEY måste motsvara en post i DNSKEY, men inte omvänt. Oftast är det bara vissa poster ur DNSKEY som ska motsvaras av en DS.

	DNSKEY	CDNSKEY
Placering	Apex i dotterzonen	Apex i dotterzonen
Ingår valideringskedjan?	Ja	Nej
Resolver hämtar den automatiskt?	Ja, om resolvern validerar	Nej
Obligatorisk för DNSSEC?	Ja	Nej

CDNSKEY vid borttag av DS

Det finns ett specialdata för CDNSKEY (som aldrig kan finns i DNSKEY) som betyder att DS-posterna ska plockas bort.

```
namn.se.     CDNSKEY    0 3 0 AA==
```

Användning av CDS och CDNSKEY

Det är policy hos administratören för moderzonen (eller dess registrarer, återförsäljare) som avgör om det är CDS eller CDNSKEY som ska användas. – Eller inte alls.

Kontrollera med moderzonen om stöd finns och vad som gäller för att få in DS-post när det inte finns någon.

Det skadar aldrig att alltid lägga in både CDS och CDNSKEY så länge de är korrekta.

Toppdomäners stöd för CDS och CDNSKEY

Sedan 2021 så har .se och .nu stöd för CDS. Varje natt kontrolleras alla dotterzoner för CDS-poster.

Även toppdomänerna .ch, .li, .sk och .cz har stöd för CDS eller CDNSKEY.

Vissa registrarer för olika toppdomäner hanterar också CDS och CDNSKEY för domäner som den är registrar för.

DS i apex istället för CDS

Vissa registrarer använder – eller har använt – en DS-post i dotterzonens apex istället för CDS.

Sådana DS-poster ingår inte i DNSSEC-kedjan. Användningen är inte standardiserad utan det är upp till registraren att beskriva hur den används.

DS-poster hör inte hemma i dotterzones apex och kan skapa missförstånd vid felsökningar. Det är alltså en olämplig användning.

Specificering av CDS och CDNSKEY

Om man vill läsa mer om CDS och CDNSKEY så finns det specificerat i följande RFC:er (extraläsning):

https://tools.ietf.org/html/rfc7344

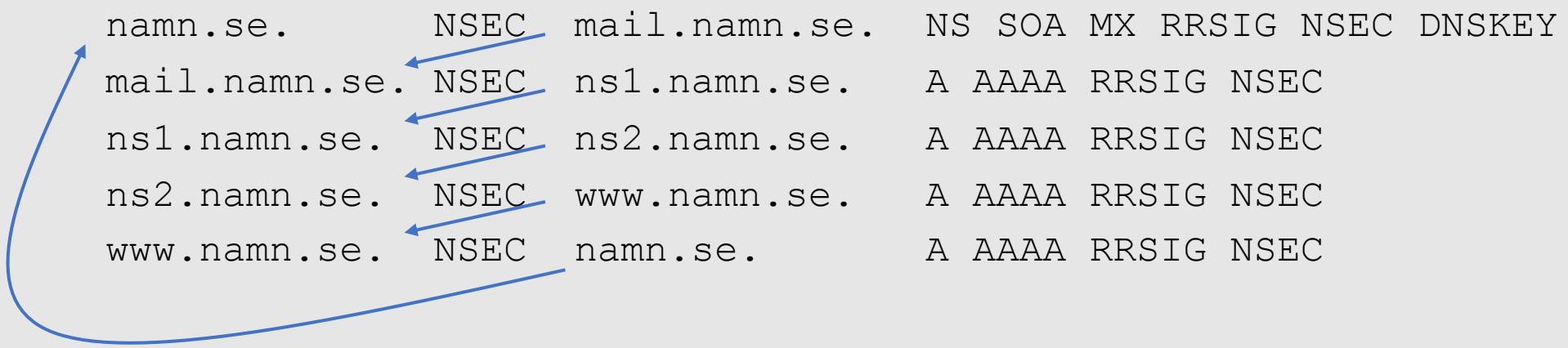
https://tools.ietf.org/html/rfc8078

▶Zone walking

[Till innehåll]

NSEC

NSEC pekar från ett domännamn med data till nästa domännamn med data:



```
namn.se.        NSEC  mail.namn.se.  NS SOA MX RRSIG NSEC DNSKEY
mail.namn.se.   NSEC  ns1.namn.se.   A AAAA RRSIG NSEC
ns1.namn.se.    NSEC  ns2.namn.se.   A AAAA RRSIG NSEC
ns2.namn.se.    NSEC  www.namn.se.   A AAAA RRSIG NSEC
www.namn.se.    NSEC  namn.se.       A AAAA RRSIG NSEC
```

Vad hjälper det då att begränsa zonöverföring?

Zone walking

”Zone walking” betyder att man använder NSEC-posterna i en DNSSEC-signerad zon för att plocka ut all data ur zonen utan att ha tillgång till zonöverföring.

Zone walking

- Man börjar i apex och fråga efter NSEC.
- Man får alla posttyper i apex och kan fråga efter dem.
- Man får nästa namn och kan fråga efter NSEC.
- Sedan fortsätter man tills man har gått igenom hela zonen.

I praktiken så innebär det samma sak som att zonöverföring är tillåten även om det kan ta lite längre tid för en stor zon. Det kan kräva många frågor. Det kan finnas gränser för hur många frågor som accepteras per tidsenhet så man får fråga över en längre tid. Alla namnservrar för zonen kan användas.

OFF-line signing

”Off-line signing” betyder att zonen signeras i förväg och är färdig när den skickas ut till slavarna. Vid ”off-line signing” så måste hela NSEC-kedjan finnas.

En DNSSEC-zon som är signerad med ”off-line signing” så kan man utnyttja ”zone walking” för att hämta zonen.

"Off-line signing" är det vanliga sättet att hantera signering.

OFF-line signing

Vid ”off-line signing” så kommer hela zonen inklusive alla NSEC- och RRSIG-poster att skapas innan zonöverföring. Den som kör slavtjänst för en sådan zon behöver inte ha något nyckelmaterial för DNSSEC, och inga ”falska” RRSIG kan skapas på slaven.

Det är lättare och förmodligen billigare att hitta en operatör som kör slavtjänst med ”off-line signing”.

ON-line signing

”On-line signing” betyder att RRSIG skapas på namnservern först när DNS-posterna efterfrågas. Det gäller även på alla slavar, som måste ha tillgång till den hemliga nyckeln.

RRSIG kan då skapas med kort giltighetstid eftersom de skapas om vid varje förfrågan.

ON-line signing

Även NSEC-poster, och dess RRSIG, kan skapas vid behov om ”on-line signing” används. Då kan man skapa en NSEC-post ”runt” det efterfrågade namnet som inte avslöjar nästa namn. Om A, men inte AAAA, finns för "name.example.com" (NODATA) så kan följande NSEC-post skapas, "on the fly", för att förneka existensen.

```
name.example.com. NSEC name-.example.com. A RRSIG NSEC
```

Man kan tycka att då borde "name-.example.com" finnas, men NSEC är bara till för att förneka existensen, inte för att lova att något annat finns.

Man kan läsa mer i https://tools.ietf.org/html/rfc4470 (överkurs).

ON-line signing

För att kunna göra ”on-line signing” så måste den privata nyckeln för någon ZSK finnas tillgänglig på alla auktoritativa servrar (master eller slav).

Det är inte alltid en möjlig eller acceptabel lösning om slavtjänsten upphandlas av annan operatör.

▶Om presentationen

[Till innehåll]

Internets domännamnssystem

Denna presentation är framtagen 2019–2023 av Mats Dufberg (mats.dufberg@internetstiftelsen.se) på Internetstiftelsen (https://internetstiftelsen.se/). Den är en del av undervisningsmaterialet för kursen ”Internets domännamnssystem” vid Kungliga tekniska högskolan, KTH (kurskod HI1037) resp. Karlstads universitet, KAU (kurskod DVGC28).

Licens

Dokumenthistorik

- Rev A: Ursprunglig version HT 2023

Slut.