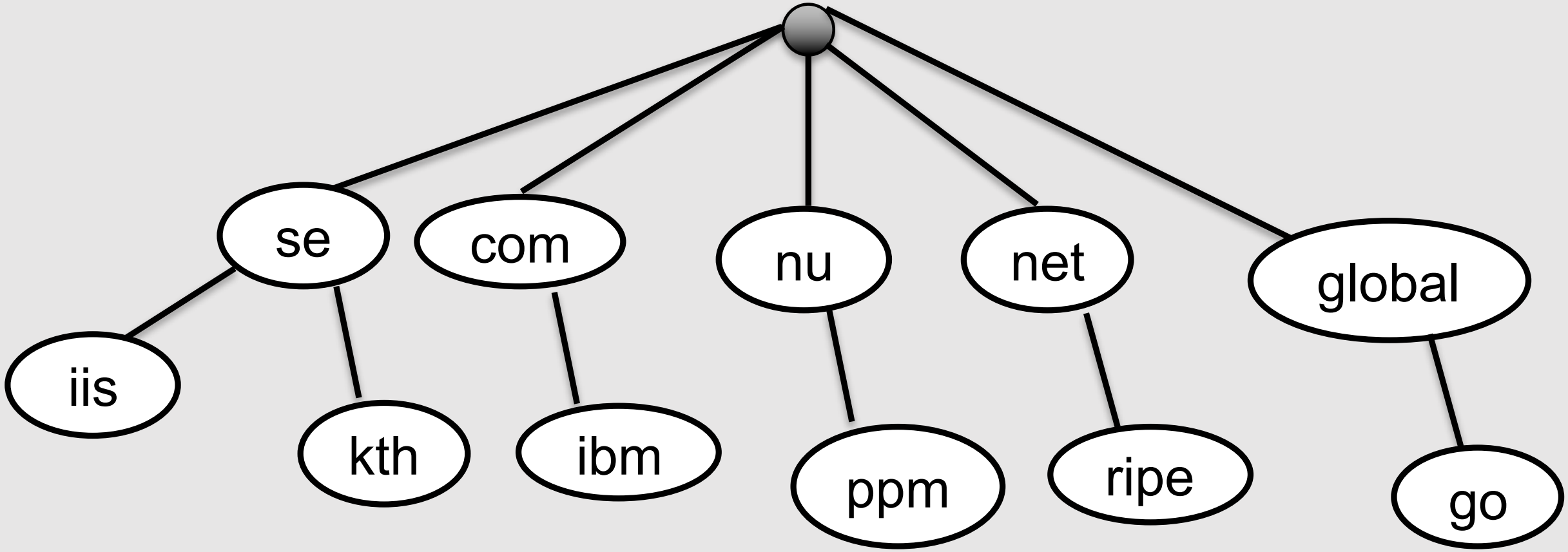

se
com
nu
net
global
iis
kth
ibm
ppm
ripe
go

INTERNET STIFTELSEN

Internets domännamnssystem*

Föreläsning FL07, HT 2023

Mats Dufberg

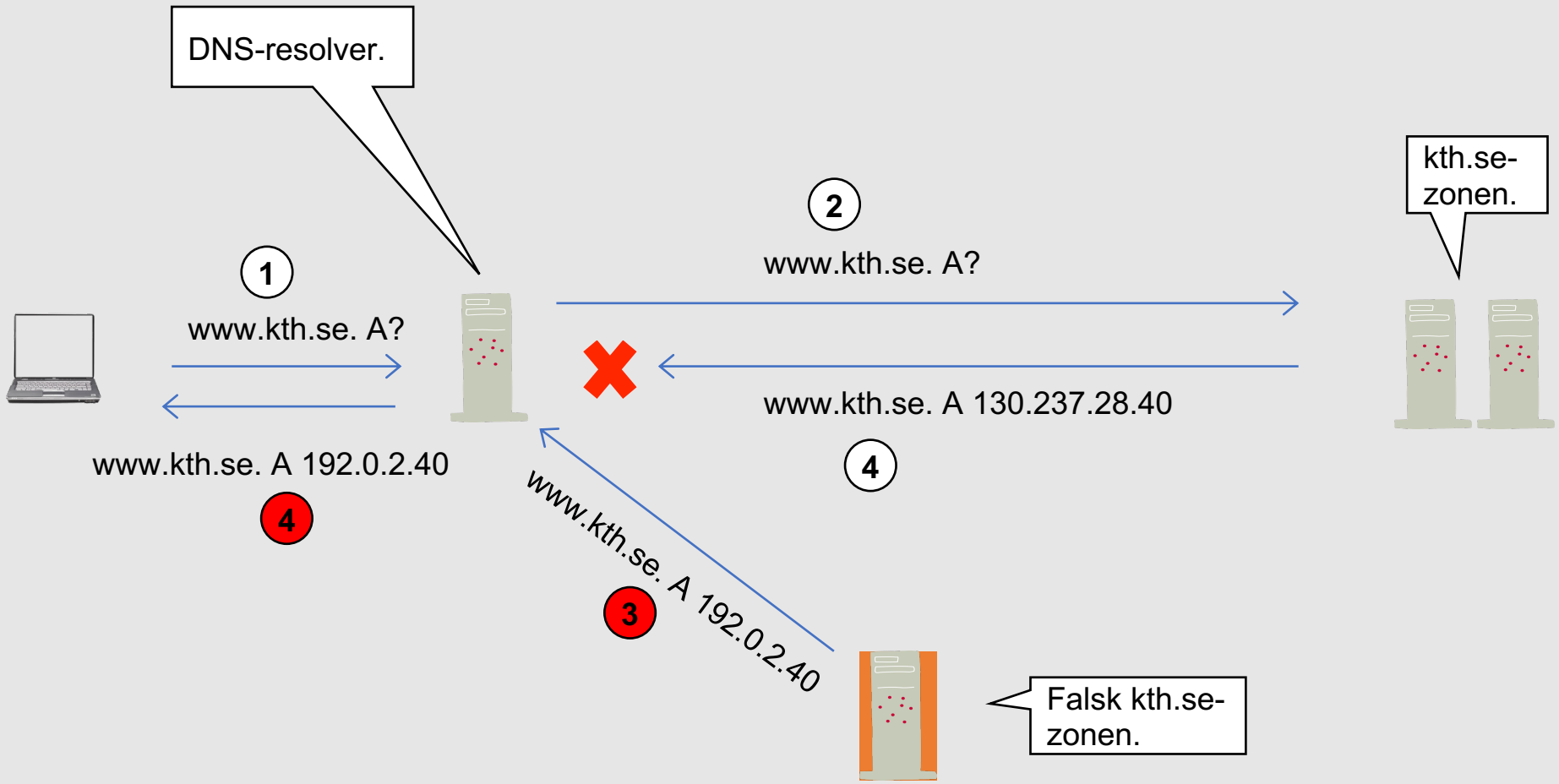
* Se “Internets domännamnssystem”

Innehåll

▶Vad DNSSEC skyddar mot

[Till Innehåll]

Uppslagning med ”man-in-the-middle”



Verifiering av innehåll

Traditionell DNS skickas utan kontroll och kan – som visats – förfalskas eller förvanskas på olika sätt.

- Det finns sedan 2005 en utökning av DNS-standarden som kallas DNSSEC.
- DNSSEC ska säkerställa att innehållet inte har förvanskats av någon.
- DNSSEC – DNS Security Extensions

Vad DNSSEC skyddar mot

- Med DNSSEC så går det att upptäcka ifall DNS-posterna har modifierats, med eller utan avsikter.
- DNSSEC ger mekanismer för att vi ska kunna verifiera att DNS-posterna vi får är samma som i den auktoritativa zonen.
- DNS-posterna kan mellanlagras på resolvrar (cachas) och kan därefter verifieras.

DNSSEC och "vanlig" DNS

- DNSSEC är bakåtkompatibelt med ”vanlig” DNS.

Om frågan (”query”) inte signalerar stöd för DNSSEC så kommer svaret (”response”) inte innehålla några DNSSEC-komponenter.

Vad DNSSEC inte skyddar mot

- DNSSEC krypterar inte datat. Allt går fortfarande i klartext.
- DNSSEC skyddar heller inte mot förvanskning som görs före eller på det system som signerar datat enligt DNSSEC.
  - Slavzonen är normalt färdigsignerad och är därmed skyddad mot förvanskning.
- DNSSEC skyddar heller inte de som inte utnyttjar skyddet som DNSSEC ger.
  - Man måste verifiera DNS-datat för att skyddas.

▶Krypto

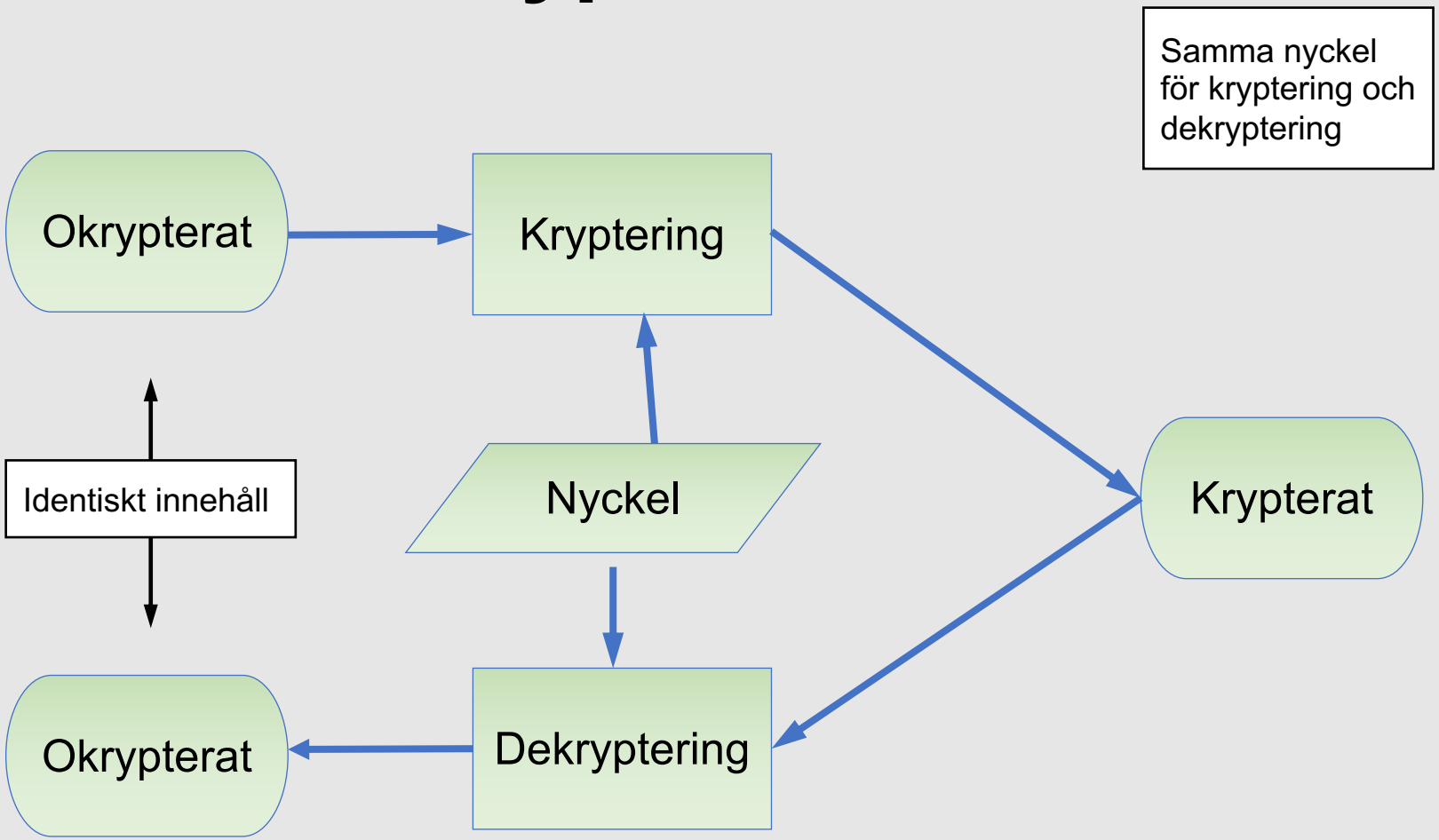
[Till Innehåll]

Krypto

Det finns två typer av krypton:

- Symmetriska krypton
- Asymmetriska krypton

Symmetriskt krypto



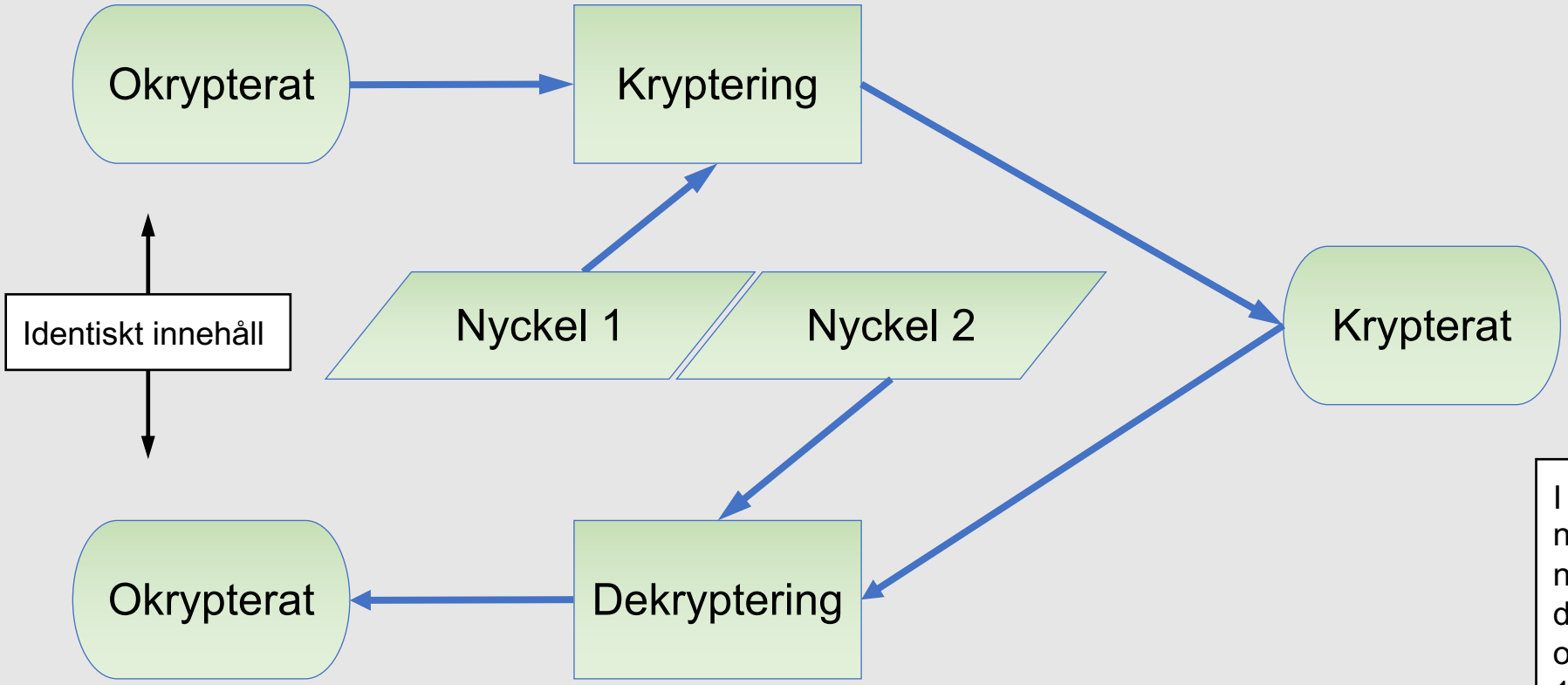
Symmetriskt krypto

Samma nyckel används för kryptering och dekryptering.

- Avsändare och mottagare måste ha tillgång till samma nyckel.
- Komplext när många är inblandade.
- Symmetriska krypton är snabba, effektiva och är säkra med små nycklar (jämfört med asymmetriska krypton).

Asymmetriskt krypto

De två nycklarna utgör ett nyckelpar där delarna hör ihop. jfr med SSH-nycklar.



I denna figur så krypterar vi med nyckel 1 och dekrypterar med nyckel 2, men vi kan vända på det och kryptera med nyckel 2, och då måste vi använda nyckel 1 för dekryptering.

Asymmetriskt krypto

Ett nyckelpar används för kryptering och dekryptering.

- Om den ena nyckeln i paret används för kryptering så används den andra för dekryptering. Och omvänt.
- Den ena nyckeln hålls hemlig, den andra görs ofta publik eller sprids till flera. T.ex. den publika SSH-nyckeln kan spridas till många.
- Fungerar väl när många är inblandade.
- Asymmetriska krypton är långsammare, mera resurskrävande och kräver längre (större) nycklar.

Kombinerat

I vissa tillämpningar så kombineras symmetriska och asymmetriska nycklar, t.ex. SSL/TLS.

- De asymmetriska nycklarna används initialt och i flera sessioner.
- De symmetriska nycklarna skapas per session och delas mellan deltagarna med hjälp av de asymmetriska nycklarna.
- De symmetriska nycklarna snabbar upp operationerna.

Krypto i DNS

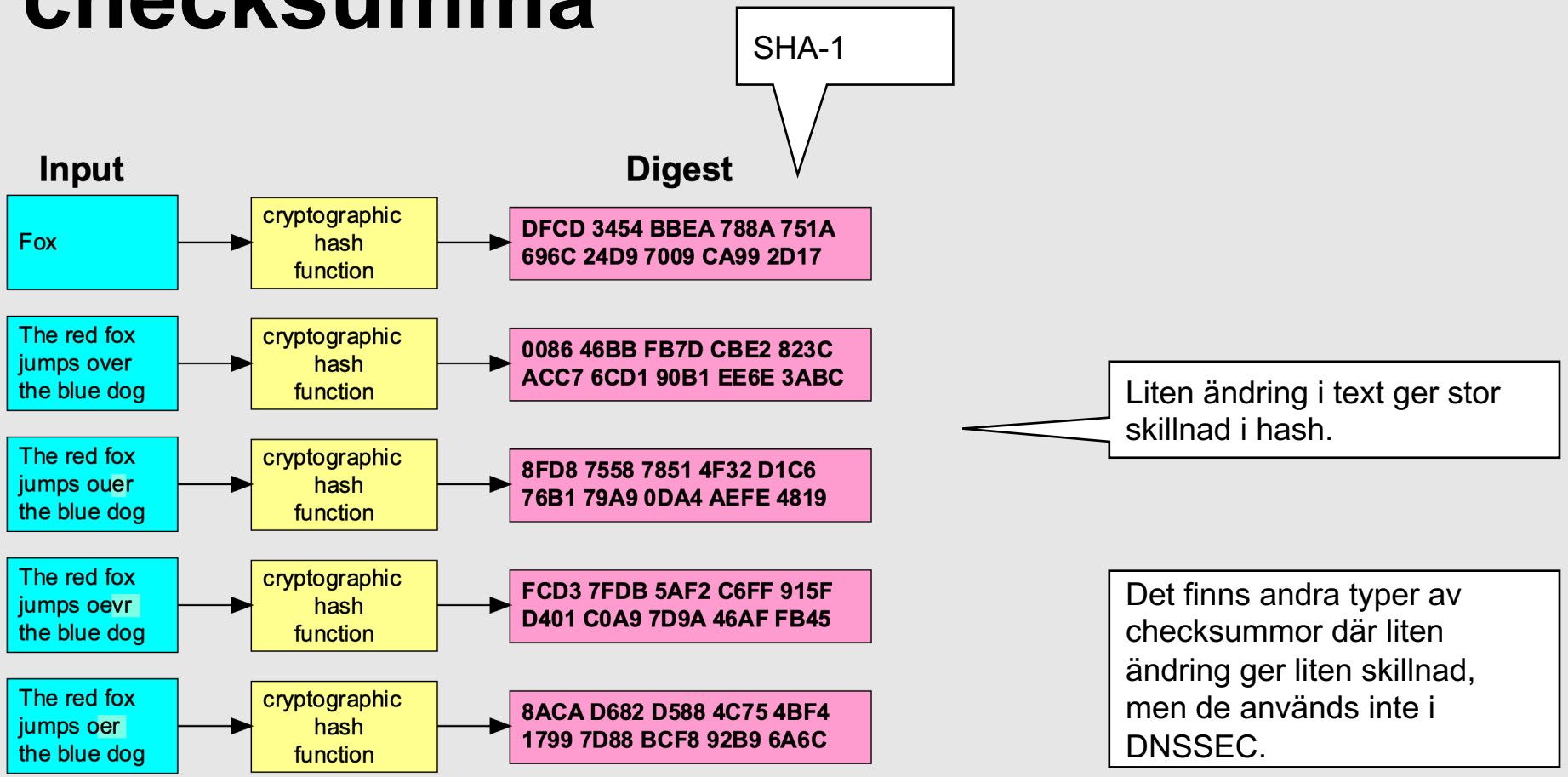
TSIG bygger på symmetriskt krypto. Samma nyckel används av klient och server.

DNSSEC bygger på asymmetriskt krypto.

▶Hash eller checksumma

[Till Innehåll]

Hash eller checksumma



”Summering” av data till en fast storlek.

Hash eller checksumma

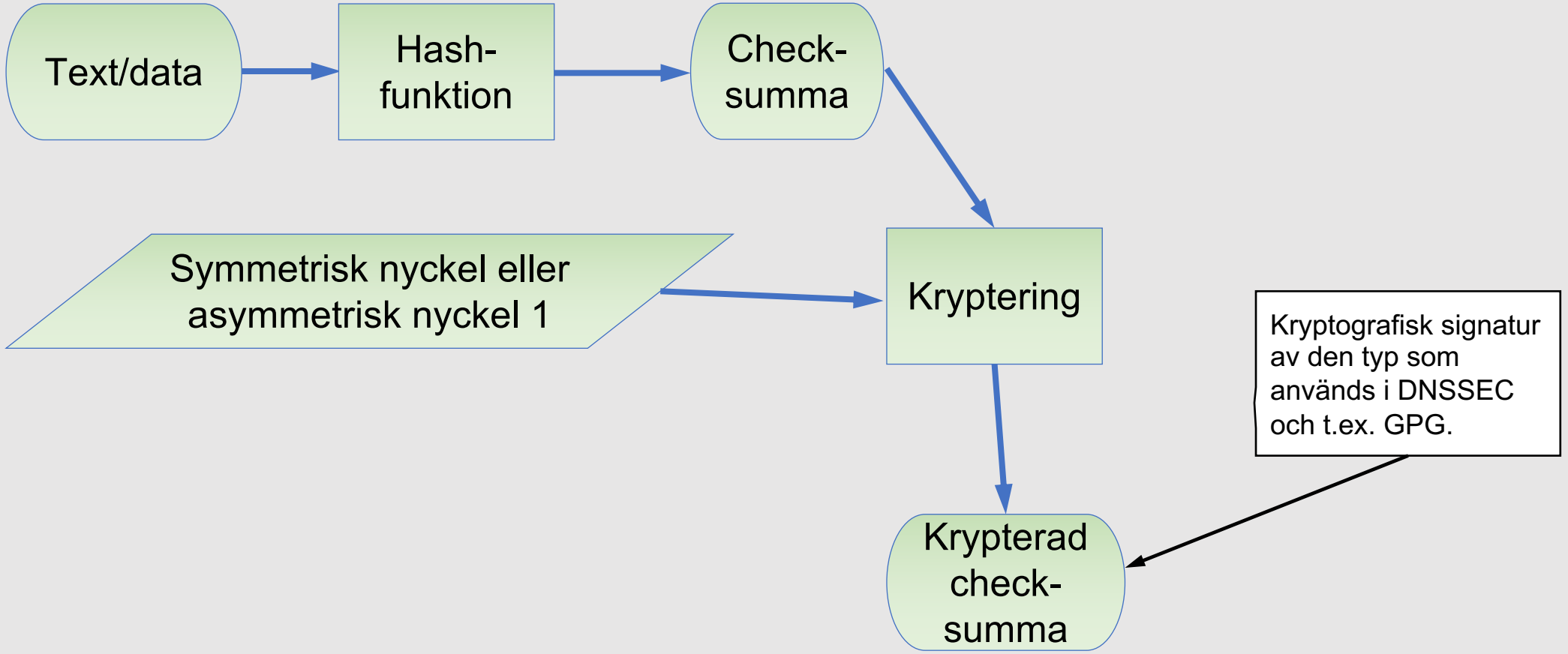
En checksumma går inte att vända, d.v.s. man kan inte återställa datat från checksumman.

- Om man har checksumman så kan man verifiera om datat har ändrats eller inte.
  - Men inte hur mycket det har ändrats.
- Checksumman kan kombineras med kryptering.

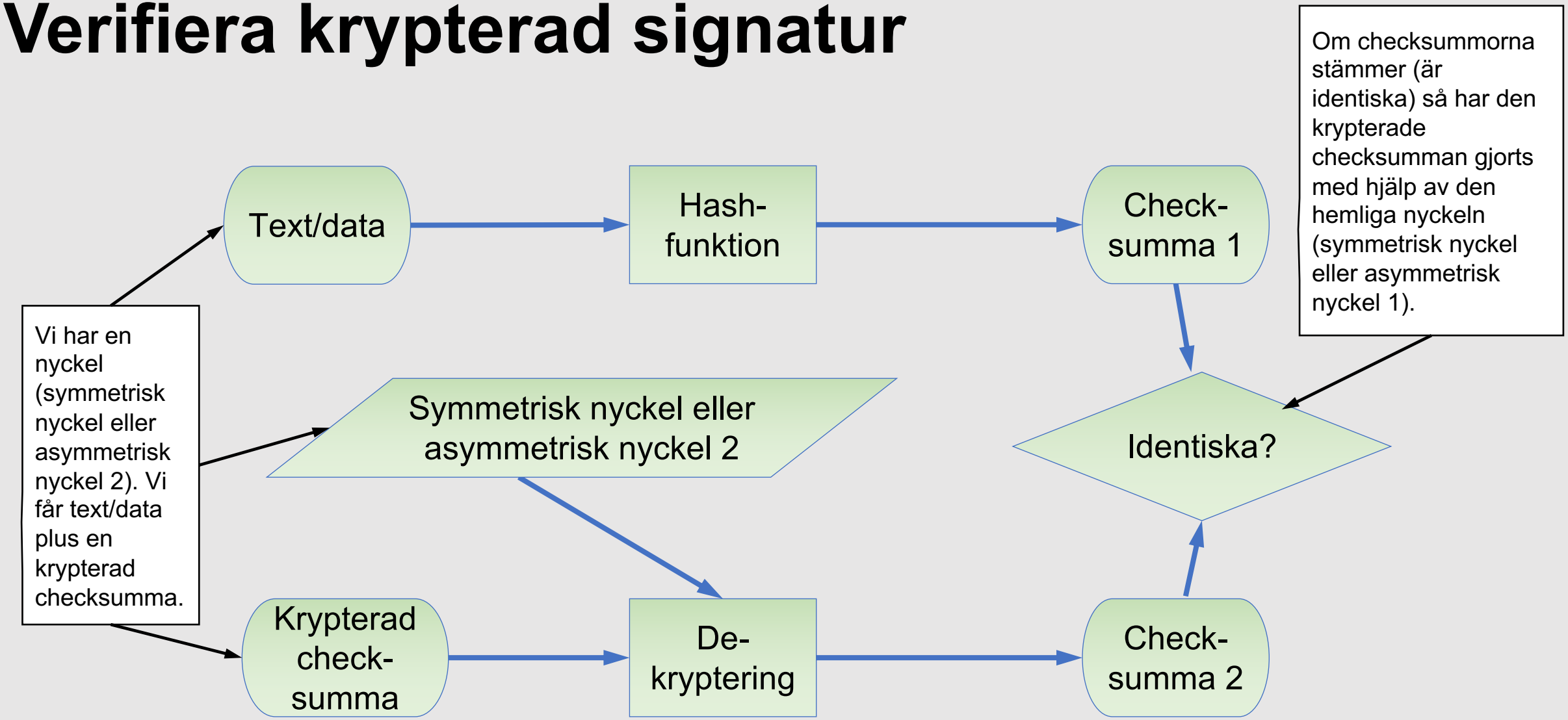
▶Signaturer

[Till Innehåll]

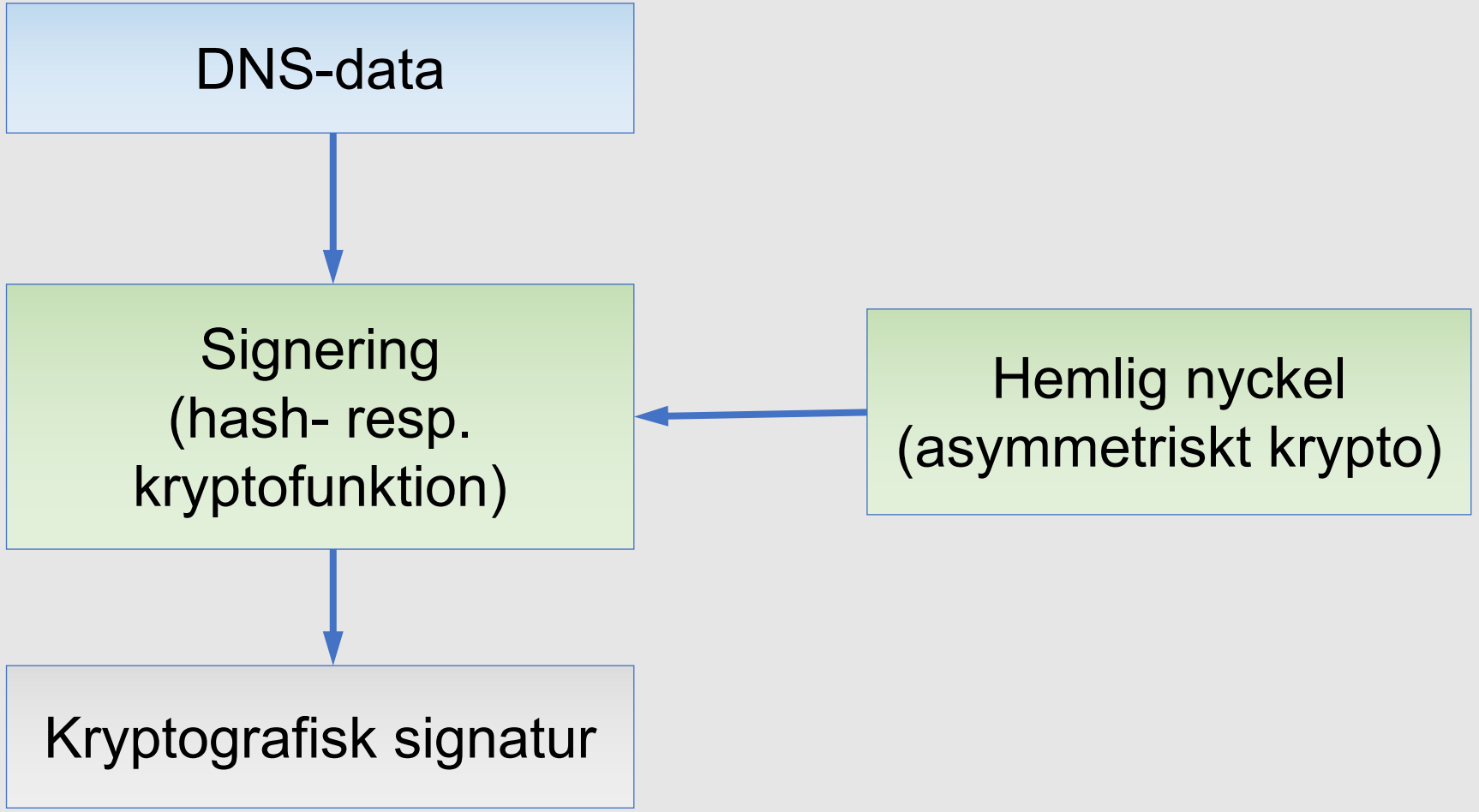
Skapa krypterad signatur



Verifiera krypterad signatur



DNSSEC-signerad zon



DNSSEC-signerad zon

De kryptografiska signaturerna lagras i zonen för att vara tillgängliga via DNS-uppslagningar.

Om klienten signalerade stöd för DNSSEC så följer signaturerna med, annars inte.

▶"dig" med +dnssec

[Till Innehåll]

```
; <<>> DiG 9.10.6 <<>> www.kth.se a +dnssec +mult
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12890
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
;; QUESTION SECTION:
;www.kth.se.            IN A

;; ANSWER SECTION:
www.kth.se.            600 IN A 130.237.28.40
www.kth.se.            600 IN RRSIG A 8 3 600 (
                       20220222004834 20220122235846 35811 kth.se.
                       u45znydGc2H8lChbockeANSmIpLQRR35YT+fFoZA867C
                       lsTc52BJdLbYTDe8N76407aE60cUzHP28D/iLRB3pAgY
                       fVESSUdURrG8b3rFeKwuLCiRtb0tu2OCmVtZ8SokJnxs
                       2PuzEx3jD6rTn8n1cVCSf990Q/Lpip1Jfs6YkyCiSFsD
                       8I/9ZWEyIo0mgVwOSE7ZDs1YRCbd4Bg36h0rU6Ilu1y4
                       BlslG9hdDTPvOiuJsFGf9wDS1hzGZW+oxNBZU6SNrhnF
                       uvDMAEO6FDkd3GuXAj5LnPmKiYrIO72qMrpXQEtdDQH0
                       fFB17qXdI0KTbl9yhHuz9L7k0ecNB/6lRQ== )

(...)
```

Säger åt ”dig” att fråga efter DNSSEC-poster och DNSSEC-validering.

2 poster i svarssektionen:
- Den efterfrågade dataposten
- En DNSSEC-signatur

Klienten skickade DO-flaggan och frågade efter DNSSEC-poster och DNSSEC-validering. Servern stödjer DNSSEC

DO-flaggan finns i svaret om
1. om den fanns i frågan och
2. om servern stödjer DNSSEC.

```
; <<>> DiG 9.10.6 <<>> www.telia.se a +dnssec +mult
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21136
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
;; QUESTION SECTION:
;www.telia.se.          IN A

;; ANSWER SECTION:
www.telia.se.          3600 IN   A 81.236.63.162

(...)
```

Säger åt ”dig” att fråga efter DNSSEC-poster.

1 post i svarssektionen:
- Den efterfrågade dataposten

Zonen är inte DNSSEC-signerad.

Fråga efter DNSSEC-poster.

När zonen inte är signerad så blir svaret som vanligt även om vi frågar efter DNSSEC.

```
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> @localhost www.dnssec-failed.org a +mult +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23977
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 34e06dd504a02e2d585ac1aa5e3bf5e1e2d6b8d024e5a7f7 (good)
;; QUESTION SECTION:
;www.dnssec-failed.org.   IN A

;; ANSWER SECTION:
www.dnssec-failed.org.    7187 IN  A 68.87.109.242
www.dnssec-failed.org.    7187 IN  A 69.252.193.191

(...)
```

Säger åt ”dig” att fråga efter DNSSEC-poster.

Här ställs frågan till en DNS-resolver som inte hanterar DNSSEC.

- Ingen DO-flagga satt i svaret även om den var satt i frågan.
- Inga DNSSEC-poster.

```
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> @localhost www.dnssec-failed.org a +mult +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 40005
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: a65cdb476166147249fdb4985e3c02096692aefdf2db7b02 (good)
;; QUESTION SECTION:
;www.dnssec-failed.org.   IN A

;; Query time: 4768 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Feb 06 12:09:45 UTC 2020
;; MSG SIZE  rcvd: 78
```

Säger åt ”dig” att fråga efter DNSSEC-poster.

Här ställs frågan till en DNS-resolver som hanterar DNSSEC, och som dessutom validerar. Uppenbarligen något problem som upptäcks med DNSSEC.

En resolver som validerar enligt DNSSEC kommer att göra det oavsett om klienten (t.ex. ”dig”) signalerar stöd för DNSSEC eller inte.

▶Verktyg för DNSSEC

[Till Innehåll]

Verktyg för att testa för DNSSEC-fel

Använd gärna ett verktyg för att testa efter fel i DNSSEC. Det skarpaste verktyget är **DNSViz** när det gäller DNSSEC-kontroll.

1. Gå till https://dnsviz.net/
2. Välj ett domännamn att testa, t.ex. www.kth.se och www. dnssec-failed.org. Domännamnet behöver inte motsvara en zon.

Zonemaster testar också DNSSEC (plus en massa annat).

1. Gå till https://zonemaster.iis.se/ eller kör zonemaster-cli på kommandoraden.
2. Välj en zon att testa, t.ex. kth.se och dnssec-failed.org. Det måste var en zon, inte vilket domännamn som helst.

▶Posttyper för DNSSEC

[Till Innehåll]

Nya posttyper för DNSSEC

Följande posttyper har lagts till för hanteringen av DNSSEC:

- DNSKEY
- RRSIG
- NSEC
- DS
- CDS
- CDNSKEY
- NSEC3
- NSEC3PARAM

Nya posttyper för DNSSEC

DNSKEY, RRSIG, NSEC, NSEC3 och DS måste man veta vad de gör och hur de fungerar för att man ska kunna ”läsa” ett DNS-svar med DNSSEC på rätt sätt.

CDS, CDNSKEY och NSEC3PARAM kommer visserligen inte i normala DNS-frågor, men man måste ändå veta vad de betyder.

Nya posttyper för DNSSEC

De nya posttyperna används bara för DNSSEC och har ingen betydelse utanför DNS och DNSSEC.

Nya posttyper för DNSSEC

DS, CDS, CDNSKEY, NSEC3 och NSEC3PARAM kommer att behandlas i kommande föreläsningar.

▶DNSKEY

[Till Innehåll]

DNSKEY

Den publika nyckel för DNSSEC för en specifik zon (asymmetriskt krypto).

```
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
```

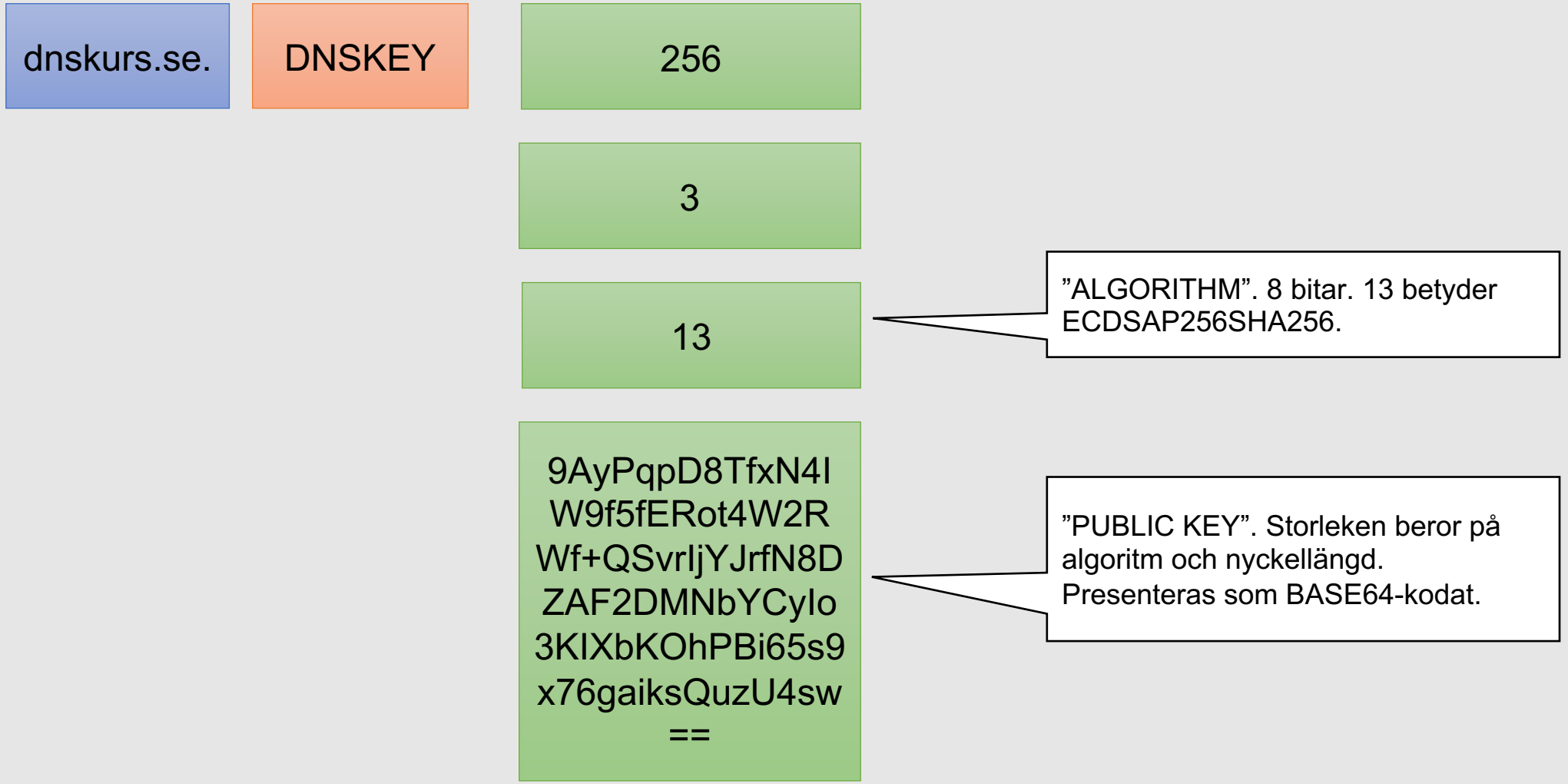
”dig +multiline” ger hjälpsam information som kommentar efter ";" -- inte del av datat.

"Owner name"	Posttyp	RDATA
dnskurs.se.	DNSKEY	256
		3
		13
		9AyPqpD8TfxN4lW9f5fERot4W2RWf+QSvrljYJrfN8DZAF2DMNbYCylo3KIXbKOhPBi65s9x76gaiksQuzU4sw==

”Owner name” är alltid samma som namnet på zonen. DNSKEY ligger alltid i apex för DNSSEC.

”FLAGS”. 16 bitar (flaggor). För DNSSEC så är bit 7 alltid satt och bit 15 kan vara satt. Värde 256 eller 257.

”PROTOCOL”. 8 bitar. Alltid värdet 3.


dnskurs.se.
DNSKEY
256
3
13
”ALGORITHM”. 8 bitar. 13 betyder ECDSAP256SHA256.
9AyPqpD8TfxN4IW9f5fERot4W2RWf+QSvrljYJrfN8DZAF2DMNbYCyIo3KIXbKOhPBi65s9x76gaiksQuzU4sw==
”PUBLIC KEY”. Storleken beror på algoritm och nyckellängd. Presenteras som BASE64-kodat.

DNSSEC-algoritmer

Lista över DNSSEC-algoritmer:

- https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

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

- https://www.rfc-editor.org/rfc/rfc8624.html#section-3.1

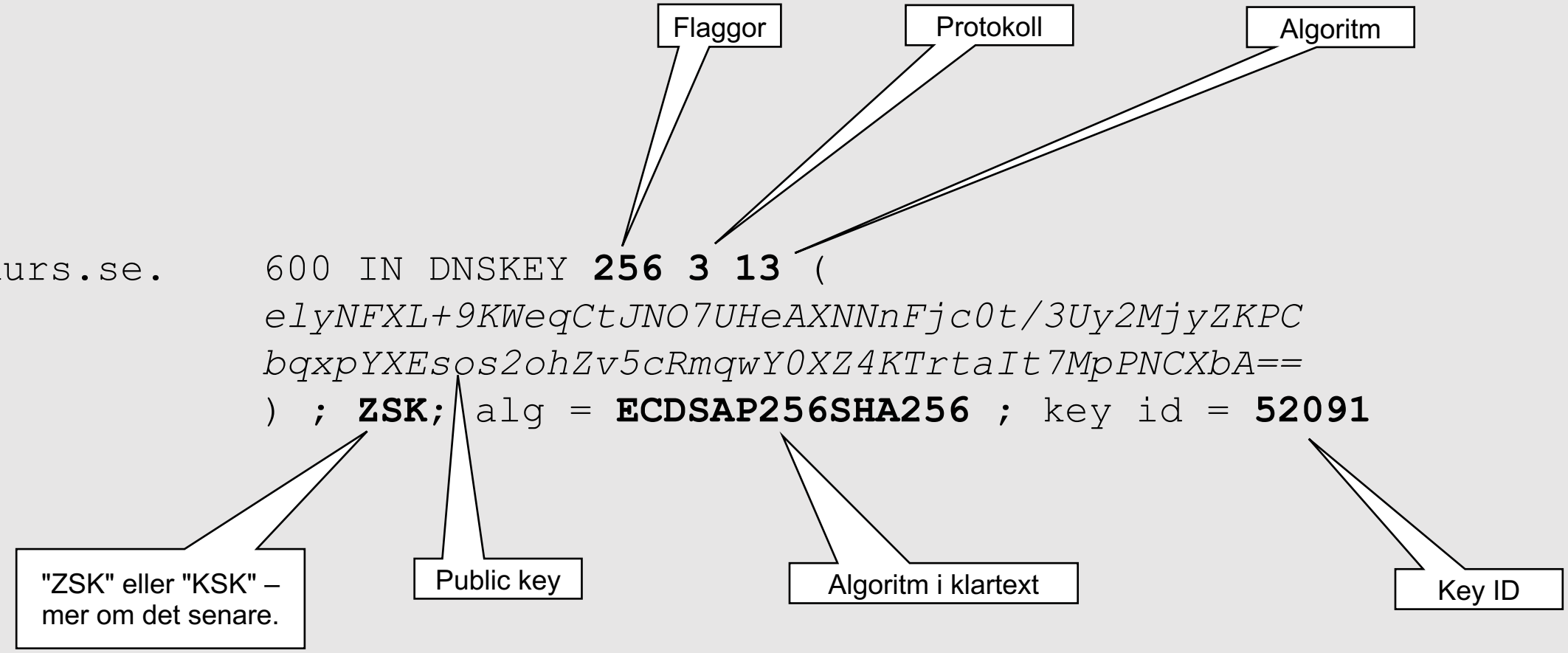
DNSKEY – ”key tag” (key id)

Andra DNS-poster refererar till ”key tag” (key id) på DNSKEY. Den räknas ut från RDATA. Det är ett 16-bitars heltal (65.536 olika värden). Det är inte en unik identifierare för DNSKEY. Det finns fler än 65.536 möjliga värden på DNSKEY.

Information efter ";" är en kommentar – inte en del av datat.

```
dnskurs.se.     600 IN DNSKEY 256 3 13 (
                9AyPqpD8TfxN4IW9f5fERot4W2RWf+QSvrIjYJrfN8DZ
                AF2DMNbYCyIo3KIXbKOhPBi65s9x76gaiksQuzU4sw==
                ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 23863
```

DNSKEY


Flaggor
Protokoll
Algoritm
dnskurs.se. 600 IN DNSKEY 256 3 13 (
elyNFXL+9KWeqCtJNO7UHeAXNNnFjc0t/3Uy2MjyZKPC
bqxpYXEsos2ohZv5cRmqwY0XZ4KTrtaIt7MpPNCXbA==
) ; ZSK; alg = ECDSAP256SHA256 ; key id = 52091
"ZSK" eller "KSK" – mer om det senare.
Public key
Algoritm i klartext
Key ID

DNSKEY

Med ”dig +multiline +nocrypto” så döljs detaljerna i den publika nyckeln i visningen och ersätts med ”[key id = xxxx]”

```
$ dig se dnskey +multiline +nocrypto
(...)
;; ANSWER SECTION:
se.         2785 IN DNSKEY 257 3 8 (
                 [key id = 59407]
                 ) ; KSK; alg = RSASHA256 ; key id = 59407
se.         2785 IN DNSKEY 256 3 8 (
                 [key id = 12175]
                 ) ; ZSK; alg = RSASHA256 ; key id = 12175
se.         2785 IN DNSKEY 256 3 8 (
                 [key id = 24984]
                 ) ; ZSK; alg = RSASHA256 ; key id = 24984
(...)
```

Bra när det är flera nycklar i DNSKEY RRset och man inte behöver detaljerna i själva nyckeln.

Nyckeln för DNSSEC

DNSSEC bygger på asymmetrisk kryptering, vilket betyder att det finns ett nyckelpar, två nycklar:

- Ena nyckeln hålls privat (hemlig) och används för är hemlig nyckel för att utföra signeringen av data.
- Andra nyckeln görs publik för att möjliggöra validering.

Den ***publika nyckeln*** ligger i ***DNSKEY***. Den privata nyckeln hålls utanför DNS och zonen men måste finnas tillgänglig när man signerar.

DNSKEY RRset

I varje signerad zon så finns det ett DNSKEY RRset med en eller flera DNSKEY-poster. Klassiskt modell så är det två med olika roller, ibland bara en kombinerad nyckel.

DNSKEY RRset ligger alltid i apex tillsammans med SOA-posten och NS-posterna för zonen.

DNSKEY och signering

DNSKEY används för signering av DNS-datat (mer om detta senare).

Men, för att vara stringent:

- DNSKEY innehåller den publika nyckeln som kan användas för validering, inte signering.
- DNSKEY innehåller även annan information.
- Det är den privata nyckeln som hör ihop med en specifik DNSKEY, som används för signering. Den finns utanför DNS.

DNSKEY och giltighetstid

DNSKEY har, i princip, evig livslängd. Det finns inget start- eller slutdatum i den.

- DNSKEY bör bytas ut när snabbare datorer kan knäcka nyckellängden eller algoritmen.
- Om algoritmen inte längre accepteras av resolvrar så måste DNSKEY ersättas med ny.
- Om den privata nyckeln kommer på avvägar så bör DNSKEY bytas ut.
- Om zonen byter DNS-operatör så byts DNSKEY normalt ut.

Giltighetstid för certifikat och SSH-nycklar

Som jämförelse, certifikat för TLS (SSL) som har en definierad giltighetstid. Både start- och slutdatum.

SSH-nycklar har liksom DNSKEY i princip evig giltighetstid. Dessa byts ut av liknande skäl som DNSKEY.

▶RRSIG

[Till Innehåll]

RRSIG

Checksumma (hash) av ett helt RRset. Hashen är krypterad med en specifik DNSKEY (eller mera korrekt, dess privata nyckel).

```
www.kth.se.      600 IN RRSIG A 8 3 600 (
                20200304174736 20200203171423 25833 kth.se.
                fVI02ZPGzNHHEEO0Nzcfbc1SQud4umndvLZxG9ksA0X/
                aW5TcbQtfMiSMzCJdjUILRqiic0/3cU8TdQANnMKg3gP
                BVpvH5FxYD/mqFnajWzZjl4pE3dV4l/n5PSnmA7ZG36Y
                U3MQJ6NPGNdiDnoNC4Ma8gU2VRkBx/FAO6GM+wBfrMoz
                L9Rwkc8VxQRIutm1iNcw8qVzd3qY+uu2suyHg39/dHnM
                GXhrsHGsiVa8+OLwO1ygksBxxjQaEQPUXd0wD2kmk2up
                ktM4U9FAhOfvco8oHBT7jse7ucpZOUsK3LybULRh33EF
                7G+HcgF50uombCzTifafYSnZeMx4d7pVQQ== )
```

Se tidigare föreläsning för definition av RRset.

dnskurs.se.

RRSIG

”Owner name” är samma som det RRset det gäller.

RRSIG signerar RRset av ***alla*** posttyper, t.ex. A, AAAA, NS, SOA, MX o.s.v. Inklusive DNSEC-posttyper som DNSKEY, NSEC, DS o.s.v.

Undantag, ***RRSIG signeras aldrig*** av RRSIG.

UTC = "Koordinerad universell tid", se https://sv.wikipedia.org/wiki/Koordinerad_universell_tid

A

”TYPE COVERED”. Posttyp på det RRset som denna RRSIG gäller. A i detta fall.

13

2

600

20190214090448

Signaturen slutar gälla, datum och tid i UTC

20190131090448

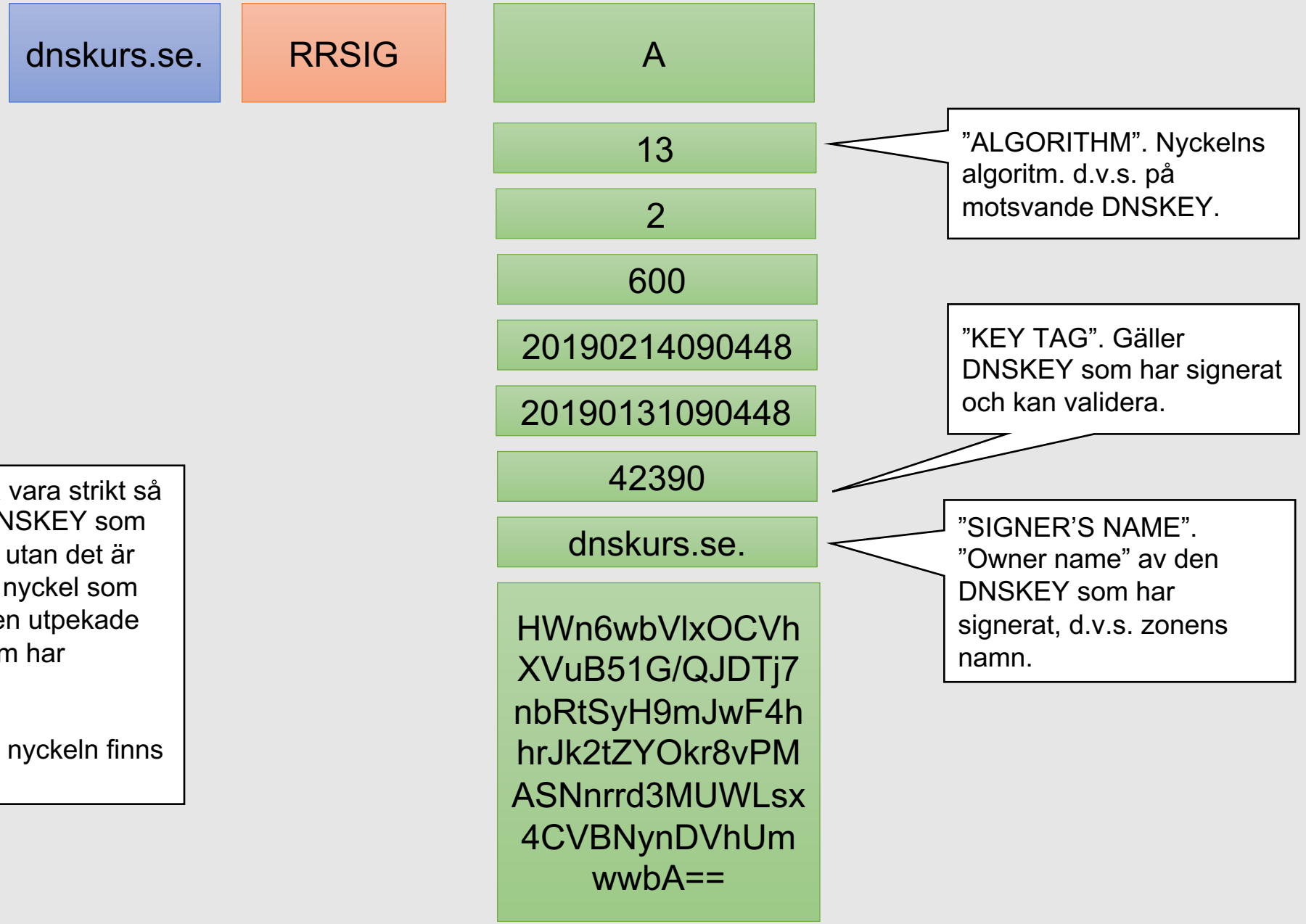
Signaturen börja gälla, datum och tid i UTC.

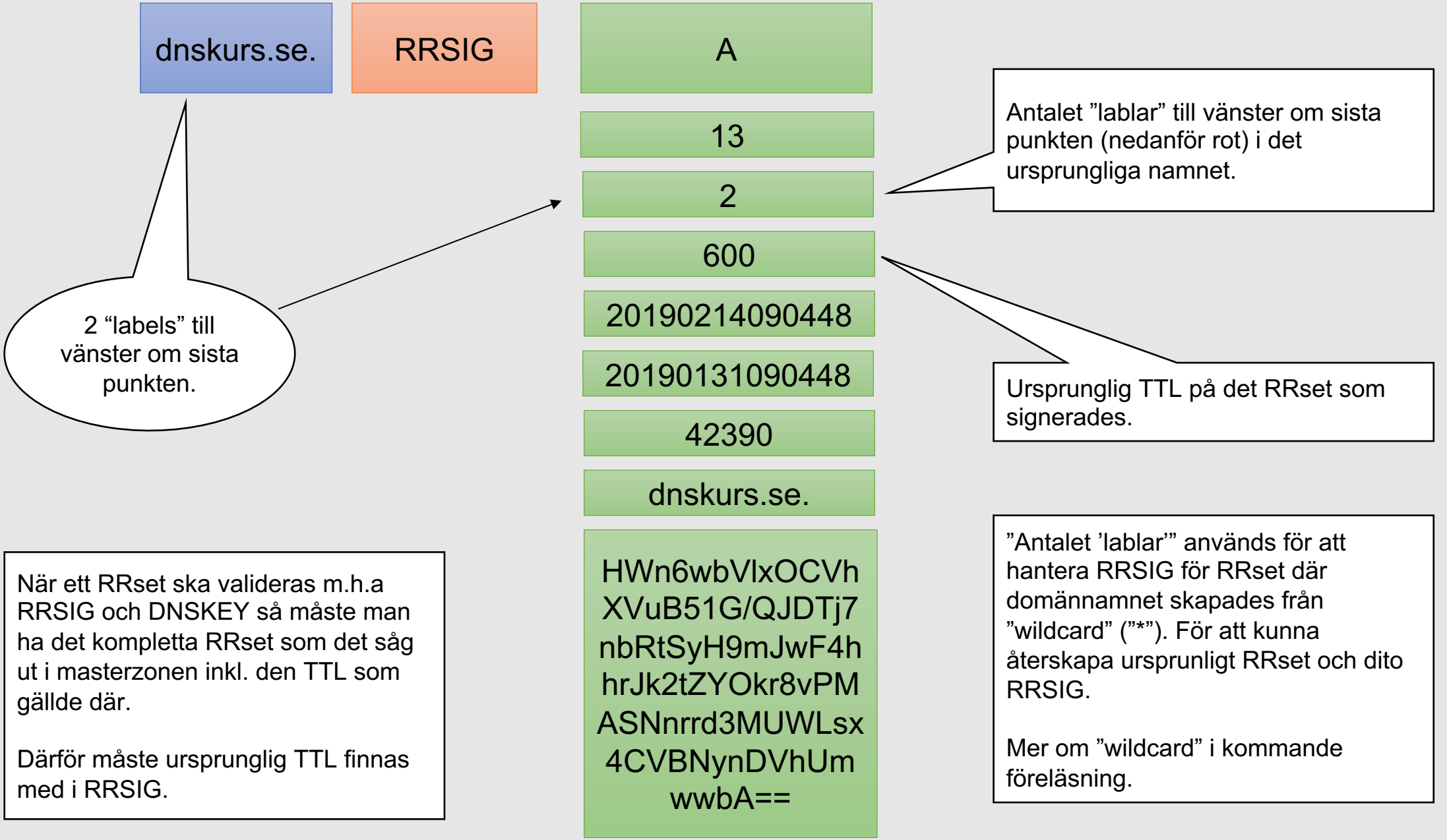
42390

dnskurs.se.

HWn6wbVlxOCVhXVuB51G/QJDTj7nbRtSyH9mJwF4hhrJk2tZYOkr8vPMASNnrrd3MUWLsx4CVBNynDVhUmwwbA==

Signatur (krypterad hash) i BASE64.


dnskurs.se.
RRSIG
A
13
2
600
20190214090448
20190131090448
42390
dnskurs.se.
HWn6wbVIxOCVhXVuB51G/QJDTj7nbRtSyH9mJwF4hhrJk2tZYOkr8vPMASNnrrd3MUWLsx4CVBNynDVhUmwwbA==
”ALGORITHM”. Nyckelns algoritm. d.v.s. på motsvande DNSKEY.
”KEY TAG”. Gäller DNSKEY som har signerat och kan validera.
”SIGNER’S NAME”. ”Owner name” av den DNSKEY som har signerat, d.v.s. zonens namn.
Om man ska vara strikt så är det inte DNSKEY som har signerat, utan det är den hemliga nyckel som motsvarar den utpekade DNSKEY som har signerat.
Den hemliga nyckeln finns inte i DNS.


dnskurs.se.
RRSIG
A
13
2
600
20190214090448
20190131090448
42390
dnskurs.se.
HWn6wbVlxOCVhXVuB51G/QJDTj7nbRtSyH9mJwF4hhrJk2tZYOkr8vPMASNnrrd3MUWLsx4CVBNynDVhUmwwbA==
2 “labels” till vänster om sista punkten.
Antalet ”lablar” till vänster om sista punkten (nedanför rot) i det ursprungliga namnet.
Ursprunglig TTL på det RRset som signerades.
När ett RRset ska valideras m.h.a RRSIG och DNSKEY så måste man ha det kompletta RRset som det såg ut i masterzonen inkl. den TTL som gällde där.
Därför måste ursprunglig TTL finnas med i RRSIG.
”Antalet ’lablar’” används för att hantera RRSIG för RRset där domännamnet skapades från ”wildcard” (”*”). För att kunna återskapa ursprunligt RRset och dito RRSIG.
Mer om ”wildcard” i kommande föreläsning.

Antalet ”lablar” nedanför rot enligt RRSIG

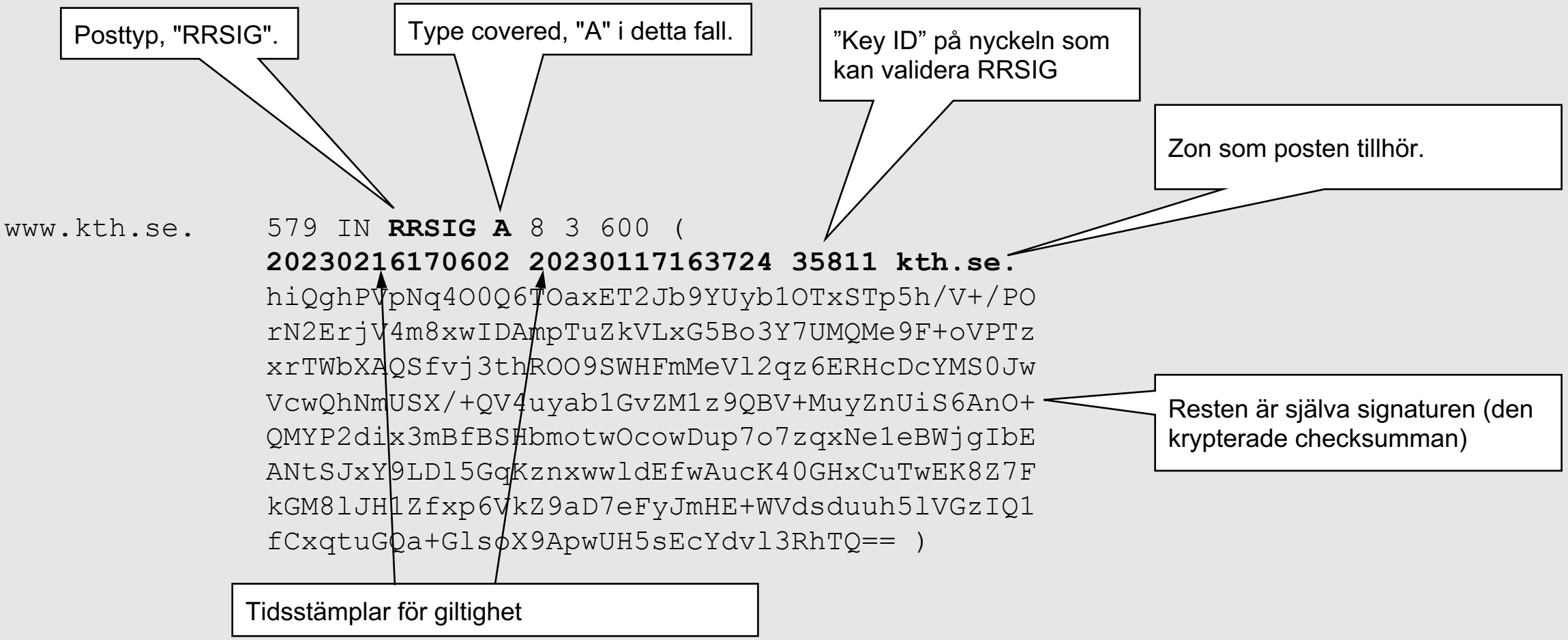
Domännamn (exempel)	Antal ”lablar”	Antal ”lablar” nedanför rot	Antal ”lablar” nedanför rot enligt RRSIG
www.kth.se.	4	3	3
kth.se.	3	2	2
se.	2	1	1
. (rot-noden)	1	0	0
*.kth.se.	3	3	**2**

Wildcard-namn.

Mer om ”wildcard” i kommande föreläsning.

Wildcard-label räknas bort (kan bara finnas en och är alltid den första, längst ner).

RRSIG


Posttyp, "RRSIG".
Type covered, "A" i detta fall.
”Key ID” på nyckeln som kan validera RRSIG
Zon som posten tillhör.
www.kth.se. 579 IN RRSIG A 8 3 600 (
20230216170602 20230117163724 35811 kth.se.
hiQghPVpNq4O0Q6TOaxET2Jb9YUyb1OTxSTp5h/V+/PO
rN2ErjV4m8xwIDAmpTuZkVLxG5Bo3Y7UMQMe9F+oVPTz
xrTWbXAQSfvj3thROO9SWHFmMeVl2qz6ERHcDcYMS0Jw
VcwQhNmUSX/+QV4uyab1GvZM1z9QBV+MuyZnUiS6AnO+
QMYP2dix3mBfBSHbmotwOcowDup7o7zqxNe1eBWjgIbE
ANtSJxY9LDl5GqKznxwwldEfwAucK40GHxCuTwEK8Z7F
kGM8lJH1Zfxp6VkZ9aD7eFyJmHE+WVdsduuh5lVGzIQ1
fCxqtuGQa+GlsoX9ApwUH5sEcYdvl3RhTQ==)
Resten är själva signaturen (den krypterade checksumman)
Tidsstämplar för giltighet

RRSIG

Med ”dig +multiline +nocrypto” så döljs detaljerna i signaturen i visningen och ersätts med ”[omitted]”

```
dig www.kth.se a +dnssec +multiline +nocrypto

(...)
;; ANSWER SECTION:
www.kth.se.     571 IN A 130.237.28.40
www.kth.se.     571 IN RRSIG A 8 3 600 (
                20230216170602 20230117163724 35811 kth.se.
                [omitted] )
```

Bra när man inte behöver detaljerna i själva signaturen.

RRSIG och signering

1. Skapa en checksumma (hash) av en kombination av
   - det RRset som ska signeras, och
   - fälten i RRSIG:s RDATA förutom signaturen.
2. Kryptera checksumman med en DNSKEY – med dess privata nyckel utanför DNS.
3. Den krypterade checksumman är en signatur som läggs i RRSIG för det RRset det gäller.
4. Signeringen kan verifieras med samma DNSKEY – med dess publika nyckel som ligger i DNSKEY.

RRSIG och giltighetstid

En DNS-zon utan DNSSEC kan sättas upp och sedan lämnas utan att ändras i åratal.

En signerad zon har RRSIG med begränsad livslängd. Den signerade zonen måste signeras om innan RRSIG löper ut.

Första och sista giltighet sitter i RRSIG-posten.

Dessutom så måste alla ha (någorlunda) korrekt tid.

RRSIG, RRset och TTL

Samma ”owner name” kan hysa flera olika RRset. Exempel på kommande bilder.

Varje RRset kan ha sin TTL.

RRset: samma "owner name", klass och posttyp.

RRSIG, RRset och TTL

```
;; ANSWER SECTION:
kth.se.          7200 IN   A 130.237.28.40

;; ANSWER SECTION:
kth.se.          1800 IN   SOA a.ns.kth.se. hostmaster.kth.se. (
                 (...)
                 )

;; ANSWER SECTION:
kth.se.          1800 IN   NS b.ns.kth.se.
kth.se.          1800 IN   NS nic2.lth.se.
(...)

;; ANSWER SECTION:
kth.se.          3600 IN   TXT "KTH Royal Institute of Technology, SWEDEN"
kth.se.          3600 IN   TXT "MS=ms86914267"
(...)
```

TTL sätts per RRset, även när flera RRset har samma ”owner name”.

RRSIG, RRset och TTL

Med DNSSEC så har varje RRset sin RRSIG, minst en RRSIG för varje RRset.

RRSIG har alltid samma TTL som det RRset som den är RRSIG för.

RRSIG, RRset och TTL

```
;; ANSWER SECTION:
kth.se.         7200 IN A 130.237.28.40
kth.se.         7200 IN RRSIG A 8 2 7200 (
                20200227012630 20200128004109 25833 kth.se.
                [omitted] )
```

TTL sätts per RRset och RRSIG får samma TTL som ”sitt” RRset.

```
;; ANSWER SECTION:
kth.se.         1800 IN NS b.ns.kth.se.
kth.se.         1800 IN NS a.ns.kth.se.
kth.se.         1800 IN NS ns2.chalmers.se.
kth.se.         1800 IN NS nic2.lth.se.
kth.se.         1800 IN RRSIG NS 8 2 1800 (
                20200215055135 20200116045414 25833 kth.se.
                [omitted] )
```

Med ”dig +multiline +nocrypto” så döljs detaljerna i signaturen i visningen och ersätts med ”[omitted]”

RRSIG, RRset och TTL

Normalt:

DNS-poster med samma ”owner name” och ”posttyp” är ett RRset med *samma* TTL.

RRSIG:

RRSIG med samma ”owner name” kan ha *olika* TTL. Istället är ”covered” RRset som styr.

Flera RRSIG med samma owner namn är ***inte*** ett RRset (undantag).

▶NSEC

[Till Innehåll]

Existerar eller inte

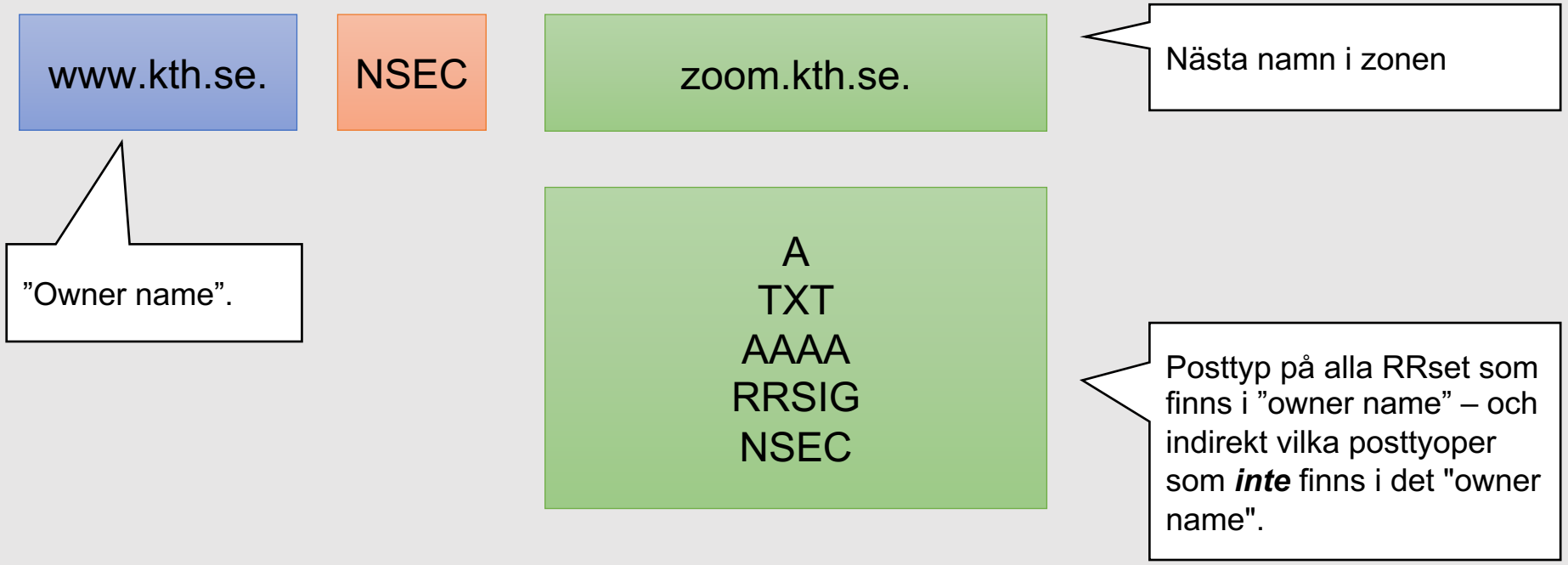
RRSIG kan bara signera RRset. RRset representerar existerande data för existerande domännamn.

Icke-existens kommer i form av NXDOMAIN eller NODATA. Det behövs ett RRset som anger att namnet eller posttypen inte finns för att kunna ha RRSIG.

NSEC

Sökta namnet finns inte eller posttypen finns inte för det namnet.

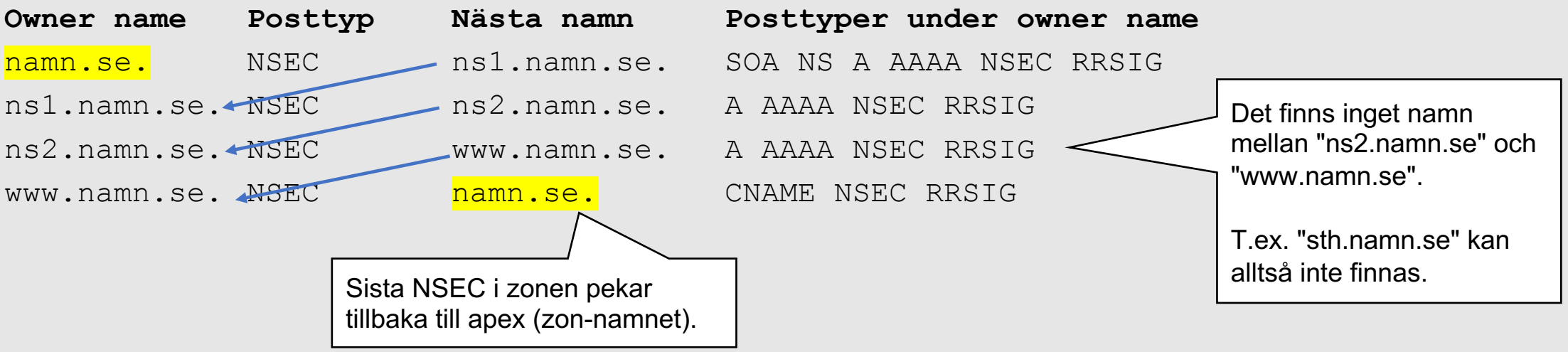
```
www.kth.se.   86400 NSEC     zoom.kth.se. A TXT AAAA RRSIG NSEC
```



Verifieras av RRSIG som andra DNS-poster.

NSEC

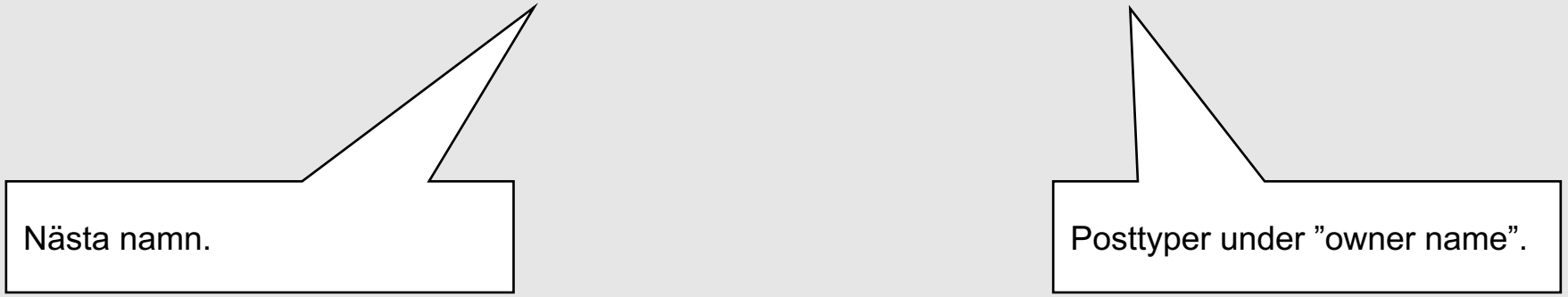
När DNSSEC är aktiverat för zonen så läggs det till en NSEC-post för varje namn i zonen. Den pekar på nästa namn i zonen och signalerar att det inte finns något namn mellan dessa. Den berättar också vilka posttyper som finns för varje namn.



NSEC

NSEC-posten är två funktioner i en DNS-post. När vi validerar icke-existens så använder vi den ena av de två funktionerna, inte båda samtidigt.

```
www.kth.se.NSEC        zoom.kth.se.        A TXT AAAA RRSIG NSEC
```



Se uppdatering av denna bild nedan.

NSEC

```
www.kth.se.   NSEC   zoom.kth.se.        A TXT AAAA RRSIG NSEC
```

Namnet i ”owner name” finns. Första delen av RDATA pekar ut nästa domännamn i zonen. Namn däremellan kan inte finnas.

Används vid NXDOMAIN.

Andra delen av RDATA används inte vid NXDOMAIN.

Se uppdatering av denna bild nedan.

NSEC

```
www.kth.se.   NSEC     zoom.kth.se.      A TXT AAAA RRSIG NSEC
```

Namnet i ”owner name” finns. Andra delen av RDATA berättar vilka posttyper som finns i ”owner name”. Andra posttyper finns inte.

Används vid NODATA.

Första delen används inte vid NODATA.

Se uppdatering av denna bild nedan.

NSEC – exempel NODATA

```
;; QUESTION SECTION:
;www.kth.se.        IN MX

;; AUTHORITY SECTION:
kth.se.         1800 SOA a.ns.kth.se. hostmaster.kth.se. (
                2020020521 ; serial
                14400      ; refresh (4 hours)
                900        ; retry (15 minutes)
                604800     ; expire (1 week)
                86400      ; minimum (1 day)
                )
kth.se.         1800 RRSIG SOA 8 2 1800 (
                20200307134001 20200206124001 25833 kth.se.
                ufXX2M3fyjqgk/E0KADSEIulID8k2uZ9YfetzZ7Dqg4e
                (...)
                ViHrM8XvVlth+G5w9i/8XOQ74H+OK/G4/A== )
www.kth.se.     86400 NSEC zoom.kth.se. A TXT AAAA RRSIG NSEC
www.kth.se.     86400 RRSIG NSEC 8 3 86400 (
                20200227172652 20200128164931 25833 kth.se.
                nXSsGzTYcYqf3Gbs9YCDb9McBu9GtSxssQxOaL3pTW49
                (...)
                oD++PpjSu4nW0JfXsg76BnobNo1BvXZuTg== )
```

Frågar efter MX under www.kth.se.

I ett NODATA-svar så har vi alltid en SOA-post i "authority section".

RRSIG för SOA-posten.

Det finns ingen MX under www.kth.se.

RRSIG signerar NSEC RRset (NSEC-posten).

NSEC – exempel NXDOMAIN

```
;; QUESTION SECTION:
;za.kth.se.      IN A

;; AUTHORITY SECTION:
kth.se.              1743 IN SOA a.ns.kth.se. hostmaster.kth.se. (
                          2023092574 ; serial
                          14400      ; refresh (4 hours)
                          900        ; retry (15 minutes)
                          604800     ; expire (1 week)
                          86400      ; minimum (1 day)
                         )
kth.se.              1743 IN RRSIG SOA 8 2 1800 (
                          20231101130907 20231002120907 35811 kth.se.
                          [omitted] )
kth.se.              1743 IN NSEC _672f5810f0e3cef9228ccc19c17fc991.kth.se. A (...)CAA
kth.se.              1743 IN RRSIG NSEC 8 2 86400 (
                          20231013084018 20230913075621 35811 kth.se.
                          [omitted] )
www.xpres.kth.se.    1743 IN NSEC zoom.kth.se. CNAME RRSIG NSEC
www.xpres.kth.se.    1743 IN RRSIG NSEC 8 4 86400 (
                          20231026032245 20230926024208 35811 kth.se.
                          [omitted] )
```

"*" kan användas som ”wildcard” i zonen för att representera en hel label eller flera. Mer i kommande föreläsning.

Det finns ingen "*.kth.se".

Det finns ingen "za.kth.se".

NSEC

För NSEC så krävs en entydig ordning mellan namnen i en zon.

- A-Z sorteras som a-z.
- Sorteringen görs som strängar av oktetter.
- Sortering på labelnivå där tom kommer först, d.v.s. ”nada.kth.se” kommer före ”www.nada.kth.se”, som kommer före ”www.kth.se”.

Exempel på sortering (från RFC 4034, avsnitt 6.1, sidan 19):

```
example
a.example
yljkjljk.a.example
Z.a.example
zABC.a.EXAMPLE
z.example
\001.z.example
*.z.example
\200.z.example
```

NSEC

Det kan inte finnas två eller fler NSEC med samma "owner name".

▶Domännamn utan data

[Till Innehåll]

Domännamn utan data

I .se-zonen så finns det data direkt under .se, t.ex. SOA-posten. Det finns även data under t.ex. a.ns.se:

```
a.ns.se. A 192.36.144.107
```

Men det finns ingen data under ns.se. men ns.se finns. Den kallas för en ***empty non-terminals***.

När vi frågar med vanlig DNS så blir det som en vanliga NODATA oavsett ***query type***.

```
; <<>> DiG 9.10.6 <<>> se any @b.ns.se +mult +noedns +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22069
;; flags: qr aa; QUERY: 1, ANSWER: 20, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;se.                    IN ANY

;; ANSWER SECTION:
se.                172800 IN RRSIG  SOA 8 1 172800 (
                        20231020112336 20231006191103 7906 se.
                        n5jhKfLyg9W8+PZz84kanAmmMSOvS6etydvIg/DoUe3F
                        VwfMlDudmaMJKi7js6aq9vBhEhR20Oww5DbDN8BbfZdh
                        5iV7oBK681kztsIyspnNfFvnC7+yWU0JTT0y2aFakTWX
                        ZBiqpUjAexUA0A3AXgB1llQM8+VABDxSKM6S1zJPeiB1
                        ws32QFzV4YxEs3KnzgeuDmp5zVrFhIYg+rdZ3P2/87L4
                        s23kykFI5OXnN5sGR/x8G2u8lNIO8NK+VMH7sACyWC5j
                        6L4PEBzozD8z7EspNlXirOapRGNAwMwz4bPAJjqiiYjd
                        /W+cOmL2mhgH9zdMSbFOX6fTgsVAoJ48fA== )
(...)
```

Om vi frågar en se-server efter ”se any” så får vi svar på alla DNS-poster som finns där.

```
; <<>> DiG 9.10.6 <<>> a.ns.se any @b.ns.se +mult +noedns +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12941
;; flags: qr aa; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;a.ns.se.                IN ANY

;; ANSWER SECTION:
a.ns.se.        172800 IN A 192.36.144.107
(...)
```

Om vi frågar efter ”a.ns.se any” så får vi svar på alla DNS-poster som finns där.

```
; <<>> DiG 9.10.6 <<>> ns.se any @b.ns.se +mult +noedns +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28120
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;ns.se.                  IN ANY

;; AUTHORITY SECTION:
se.             7200 IN  SOA catcher-in-the-rye.nic.se. registry-default.nic.se. (
                         2023100622 ; serial
                         1800       ; refresh (30 minutes)
                         1800       ; retry (30 minutes)
                         864000     ; expire (1 week 3 days)
                         7200       ; minimum (2 hours)
                         )
(...)
```

Om vi frågar efter ”ns.se any” så får vi ett normalt NODATA-svar.

Det är en tom nod, inga DNS-poster.

Namnet (noden) finns.

Empty non-terminals

Följande gäller för empty non-terminals:

- Det finns inga poster i noden (namnet).
- Under noden, ett eller flera steg ner, så finns det en nod med en eller flera DNS-poster.
- Det blir ett NODATA-svar för alla frågor om namnet.

Empty terminals?

Nej, en nod som varken har DNS-post i sig eller någon underliggande nod existerar inte.

Noderna i DNS-trädet uppstår genom att det finns DNS-posters vars ***owner name*** har namnet i sig. Ev. tomma noder “på vägen” kommer då att skapas.

Inga noder kan skapas nedanför den nedersta noden med data.

NXDOMAIN

NXDOMAIN betyder att det efterfrågade namnet inte finns.

Det betyder också att det inte finns någon subdomän till det efterfrågade namnet, det finns inga noder under namnet.

- Om det blir NXDOMAIN på "a.b.c" så betyder det att "x.a.b.c" inte existerar.

Konsekvensen är att resolvrar kan använda en cachad NXDOMAIN för att avgöra att en subdomän också blir NXDOMAIN.

▶NSEC och empty non-terminals

[Till Innehåll]

Domännamn utan data

När vi frågar efter ett ”empty non-terminal” med DNSSEC så blir det ingen NSEC för namnet, utan ett NSEC som omger namnet och som visar att namnet inte finns med data.

NSEC pekar på nästa namn med data (DNS-post).

Namnet finns fortfarande, så det blir inte NXDOMAIN, utan NODATA.

```
; <<>> DiG 9.10.6 <<>> ns.se any @b.ns.se +mult +dnss +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51601
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;ns.se.                 IN ANY

;; AUTHORITY SECTION:
se.             7200 IN  SOA catcher-in-the-rye.nic.se. registry-default.nic.se. (...)
se.             7200 IN  RRSIG SOA 8 1 172800 (...)
nrz.se.         7200 IN  NSEC a.ns.se. NS RRSIG NSEC
nrz.se.         7200 IN  RRSIG NSEC 8 2 7200 (
```

NODATA

Närmast före namn med data.

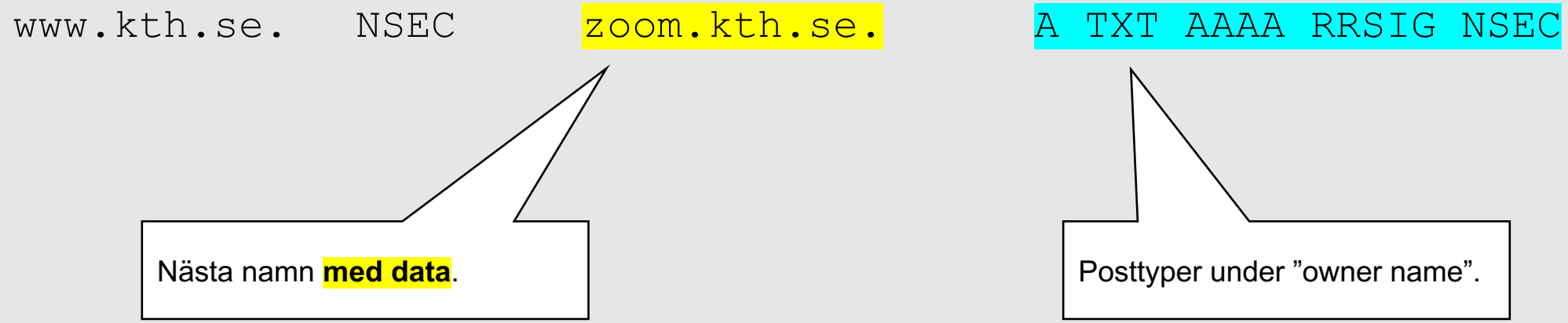
Nästa namn med data. Om ”a.ns.se” finns i zonen, så finns också ”ns.se” med automatik.

Sorteringsordning:

nrz.se < ns.se < a.ns.se

NSEC (uppdaterad)

NSEC-posten är två funktioner i en DNS-post. När vi validerar icke-existens så använder vi den ena av de två funktionerna, inte båda samtidigt.



NSEC (uppdaterad)

```
www.kth.se.   NSEC  zoom.kth.se.      A TXT AAAA RRSIG NSEC
```

Namnet i ”owner name” finns. Första delen av RDATA pekar ut nästa domännamn i zonen **med data**. Namn däremellan kan inte finnas **med data** (men ev. utan data).

Används vid NXDOMAIN.

Används vid NODATA om ”query name” är ”empty non-terminal”.

Andra delen av RDATA används inte vid dessa fall.

NSEC (uppdaterad)

```
www.kth.se.   NSEC     zoom.kth.se.      A TXT AAAA RRSIG NSEC
```

Namnet i ”owner name” finns. Andra delen av RDATA berättar vilka posttyper som finns i ”owner name”. Andra posttyper finns inte.

Används vid NODATA där ”query name” har någon DNS-post.

I dessa fall används inte första delen.

NSEC aldrig ensam

NSEC-poster skapas inte i noder där det inte finns någon annan data.

I noden ”se” finns bl.a. SOA och där finns det en NSEC-post.

```
se.   NSEC    0.se.   NS SOA TXT RRSIG NSEC DNSKEY
se.   SOA     catcher-in-the-rye.nic.se. (...)
```

I noden ”a.ns.se” finns bl.a. A och AAAA, och där finns en NSEC-post.

```
a.ns.se. NSEC    b.ns.se.    A TXT AAAA RRSIG NSEC
a.ns.se. A       192.36.144.107
a.ns.se. AAAA    2a01:3f0:0:301::53
```

I noden ”ns.se” finns inga andra DNS-poster, och där finns ingen NSEC.

NSEC pekar på nästa namn med data

Om det finns ett namn utan data så skapar vi inget NSEC. Listan över posttyper kan aldrig vara bara en NSEC-post.

Owner name	Posttyp	Nästa namn med data	Posttyper under owner name
namn.xa.	NSEC	www.sth.namn.xa.	SOA NS NSEC RRSIG
www.sth.namn.xa.	NSEC	namn.xa.	CNAME NSEC RRSIG

Sista NSEC i zonen pekar tillbaka till apex (zon-namnet).

Nästa namn i zonen är ”sth.namn.xa”, men den är tom, inga DNS-poster, ingen data. Nästa namn i zonen **med** data är ”www.sth.namn.xa”. NSEC-posten kommer att peka på det namnet istället.

▶CNAME, RRSIG och NSEC

[Till Innehåll]

RRSIG och NSEC i zonen

För varje RRset så finns det en RRSIG. För varje namn med minst ett RRset så finns det en NSEC. Det gäller även tillsammans med CNAME.

CNAME får normalt inte kombineras med annan data, men:

- CNAME måste kombineras med RRSIG
- CNAME måste kombineras med NSEC

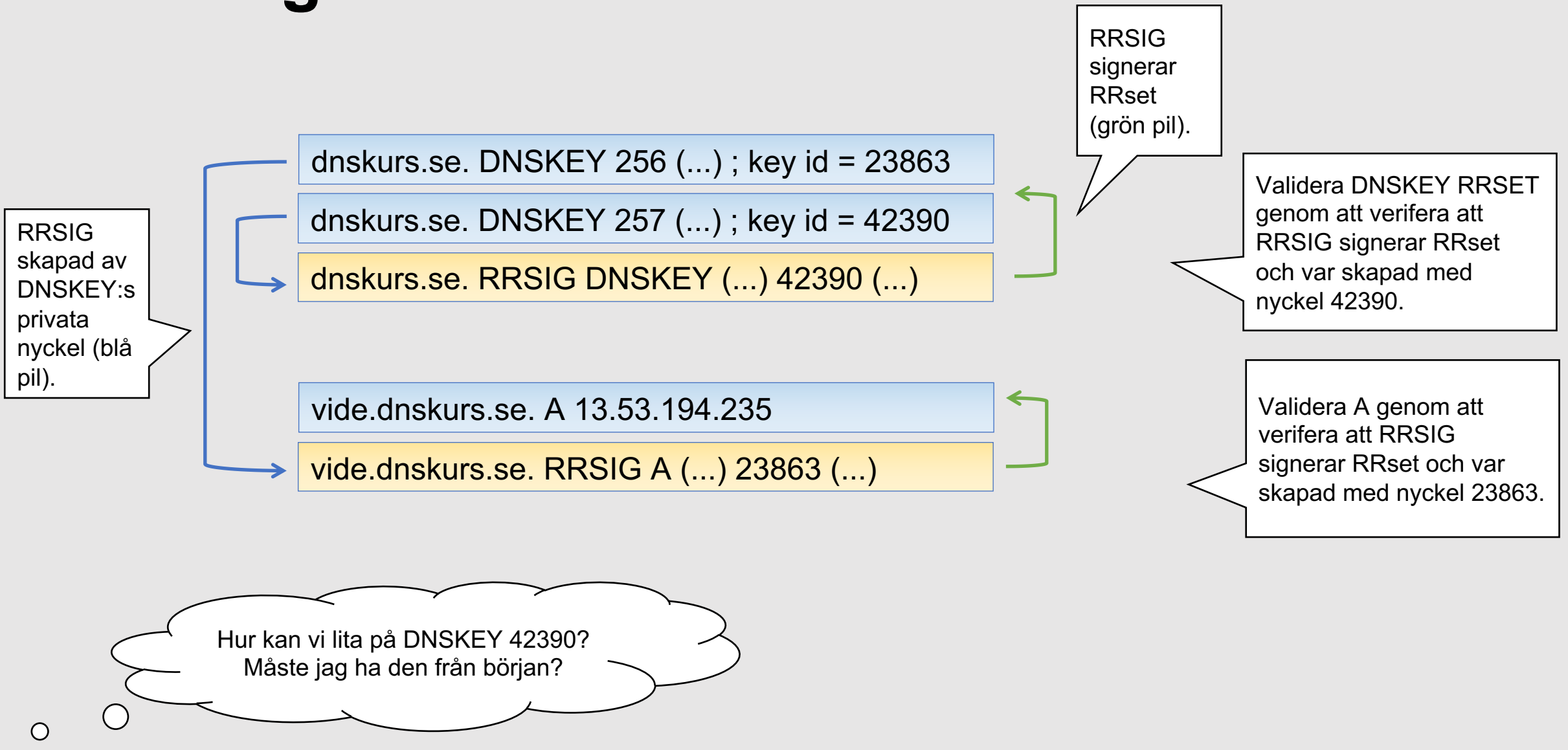
RRSIG och CNAME

```
; <<>> DiG 9.10.6 <<>> www.sunet.se cname +dns +mult
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65313
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;www.sunet.se.          IN CNAME

;; ANSWER SECTION:
www.sunet.se.    293 IN CNAME webc.sunet.se.
www.sunet.se.    293 IN RRSIG CNAME 8 3 300 (
                20190216094347 20190206084347 7636 sunet.se.
                CsQ2UKABmZg1s0sMiOsE1Gac3HfQN6mK7rjfkJfVVMa6
                PMFfcww4idMAHMPBW9ROI6tdXd74aZRfA6Z91HEYzeXb
                AG0DZAGh3S8JaHH4NsCuxRrRn5K2TGSqLXkpqzGXFdpJ
                DrJ8B3xDNcMTJUtEsotw/ZYPi386rRoVmaU1rMo= )
(...)
```

▶Validering

[Till Innehåll]

Validering


RRSIG signerar RRset (grön pil).
Validera DNSKEY RRSET genom att verifera att RRSIG signerar RRset och var skapad med nyckel 42390.
RRSIG skapad av DNSKEY:s privata nyckel (blå pil).
dnskurs.se. DNSKEY 256 (...) ; key id = 23863
dnskurs.se. DNSKEY 257 (...) ; key id = 42390
dnskurs.se. RRSIG DNSKEY (...) 42390 (...)
vide.dnskurs.se. A 13.53.194.235
vide.dnskurs.se. RRSIG A (...) 23863 (...)
Validera A genom att verifera att RRSIG signerar RRset och var skapad med nyckel 23863.
Hur kan vi lita på DNSKEY 42390?
Måste jag ha den från början?

Validering

Mer om validering i nästa föreläsning. Och mer om DNSSEC.

▶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.