www.netnod.se

DNSSEC – DET NÄRMAR SIG ...

Lars-Johan Liman, M.Sc.

Netnod Internet Exchange
Stockholm, Sweden

DNSSEC – den eviga historien ...

- T-shirt “It’s done!” 1995 ...
- TREFpunkt 1999 ...
- Kurser i 10+ år ...

- ... men vad ska det vara bra för?

DNS är en viktig del av infrastrukturen!

- Alla ställen du surfar till.
- Alla ställen du skickar mail till.
- Många gånger när du ringer med VoIP.
- Sociala funktioner.
- Tillgång till databaser.
  - T.ex. genom appar i nallen.
- Betalningar.
  - Kreditkortssystem
- Marknadsföring
- ...

DNS är en viktig del av infrastrukturen!

- Spamutskick.
- Distribution av malware (trojaner, virus, ...)
  - Skapande av botnets
- Döljande av illegal verksamhet (barnporr, ...)
  - ”Fast flux” ...
- Marknadsmässiga attacker ...
  - Namnförväxlingar, varumärkesutpressning, ...
- DDoS attacker ...
  - DNS-reflexion

- Infrastruktur används av alla och för allt möjligt ...
  ... bra som dåligt!

Vissa saker *kan* man skydda sig emot!

1. **Transaktionssignaturer (TSIG)**
2. **Secure DNS (DNSSEC)**

Olika ändamål!

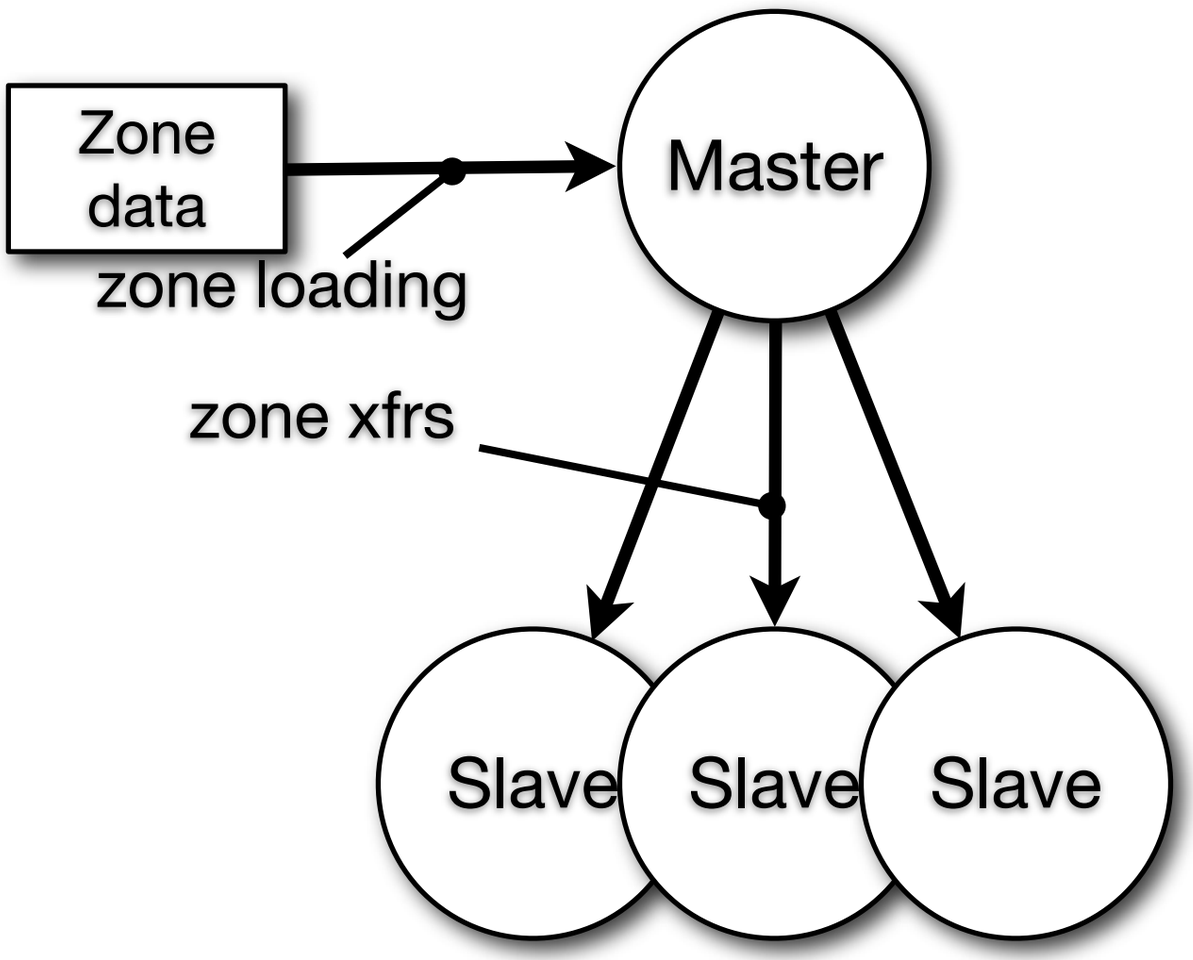
För bägge gäller: “It takes two to tango.”

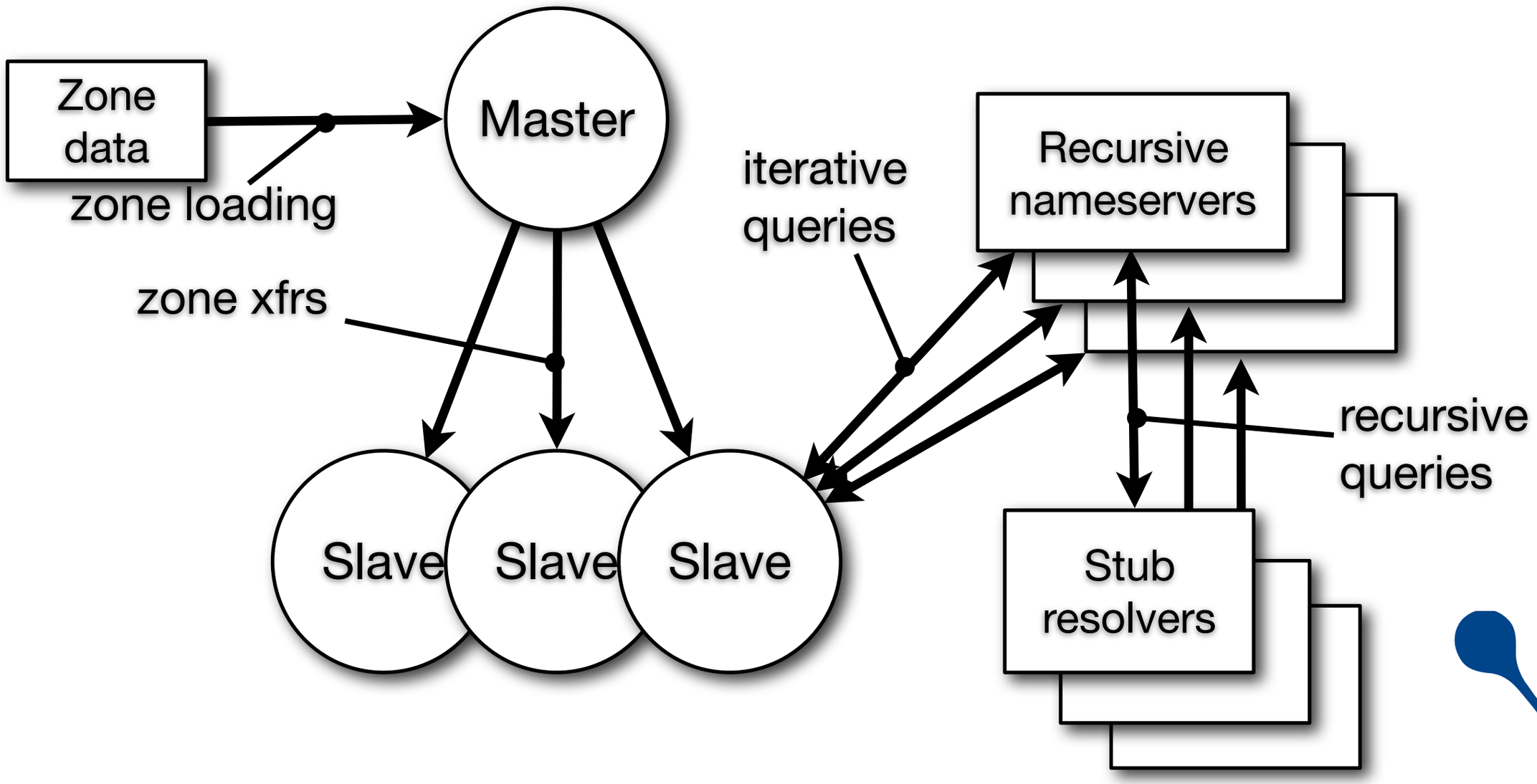
… men man måste börja någonstans med att …

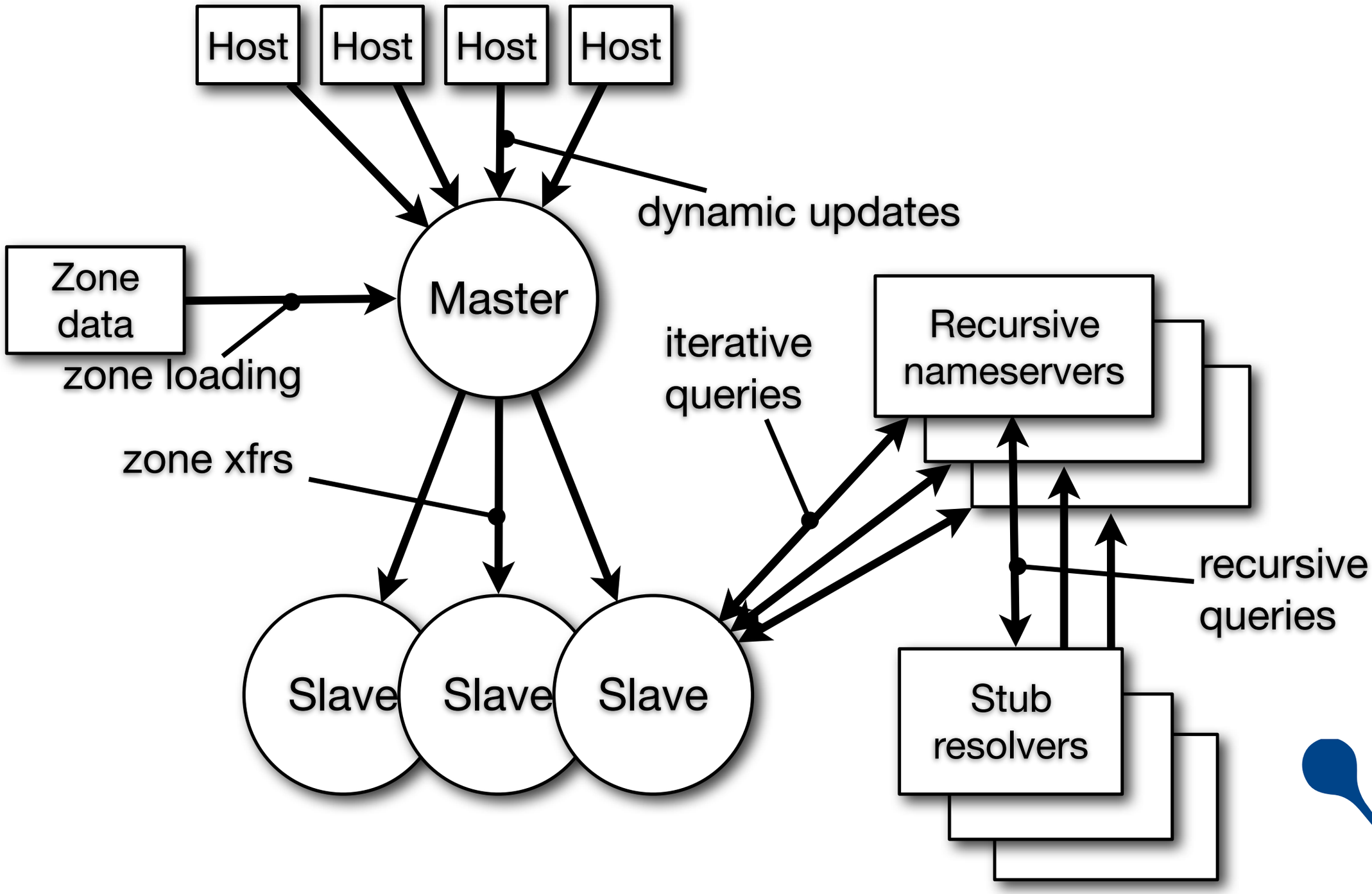
- **… att utnyttja skyddsmekanismer (ENKELT!)**
- **… att tillhandahålla skyddsmekanismer. (Tyvärr inte lika enkelt …)**

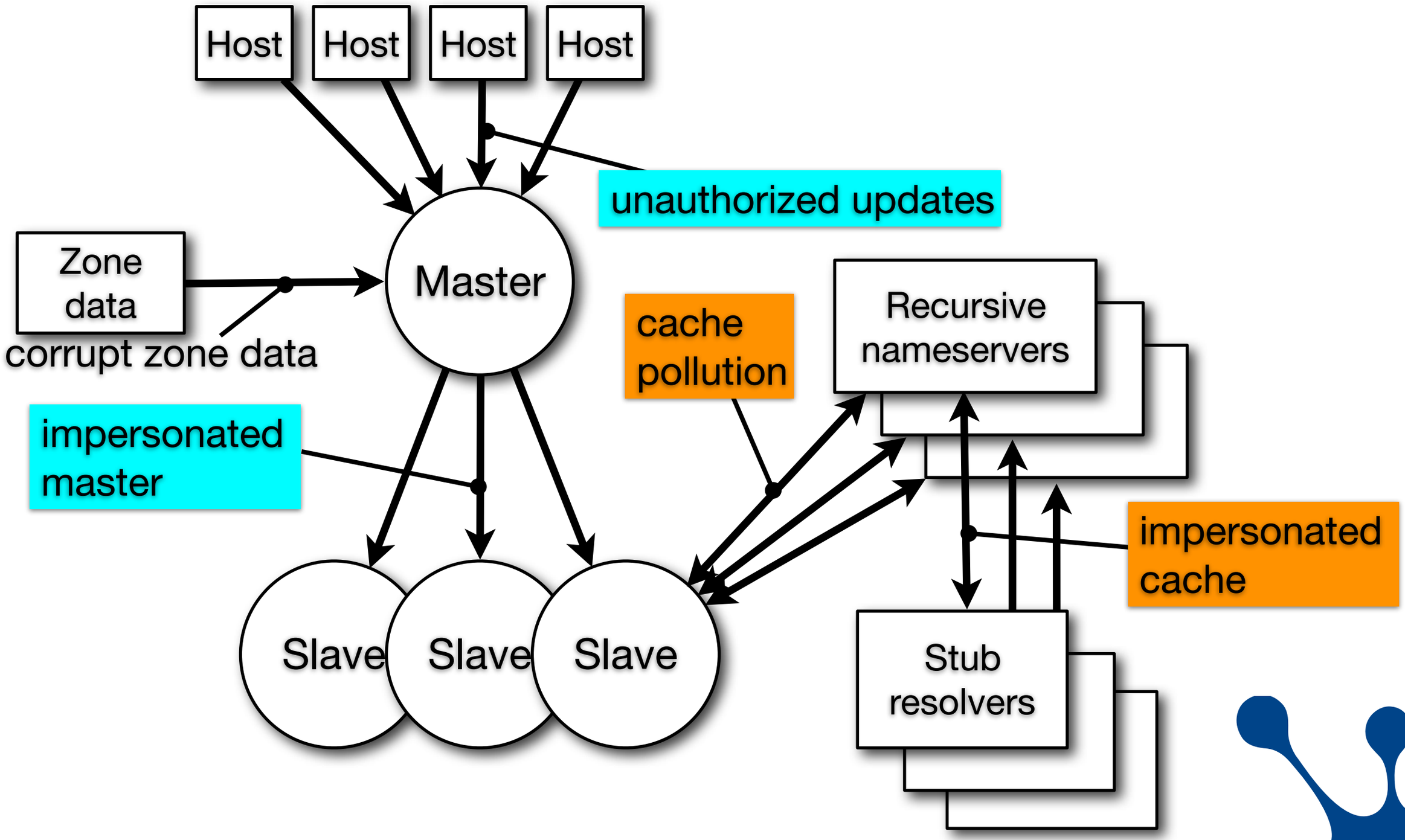
DNS OCH SÄKERHET

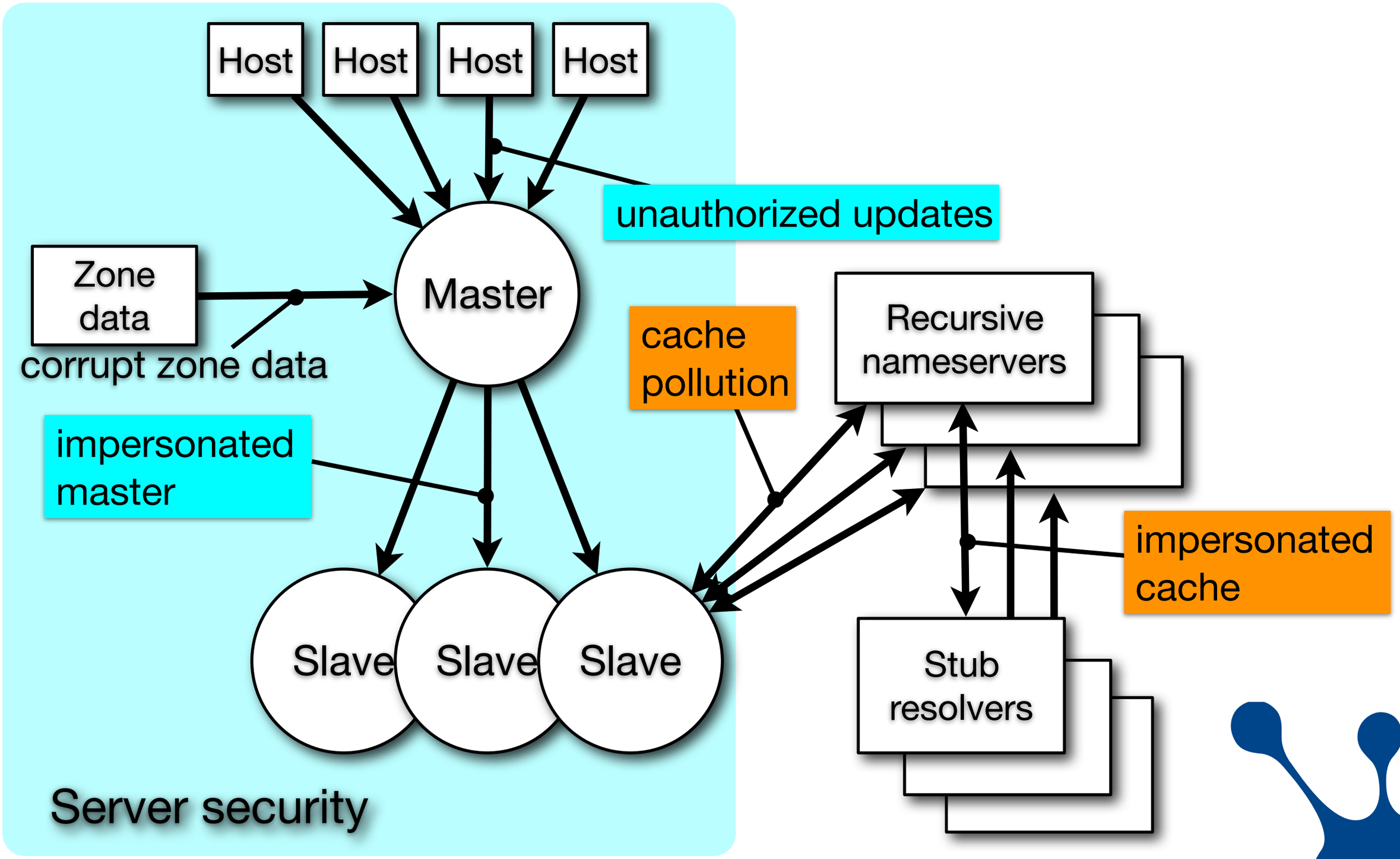
DNS-transaktioner

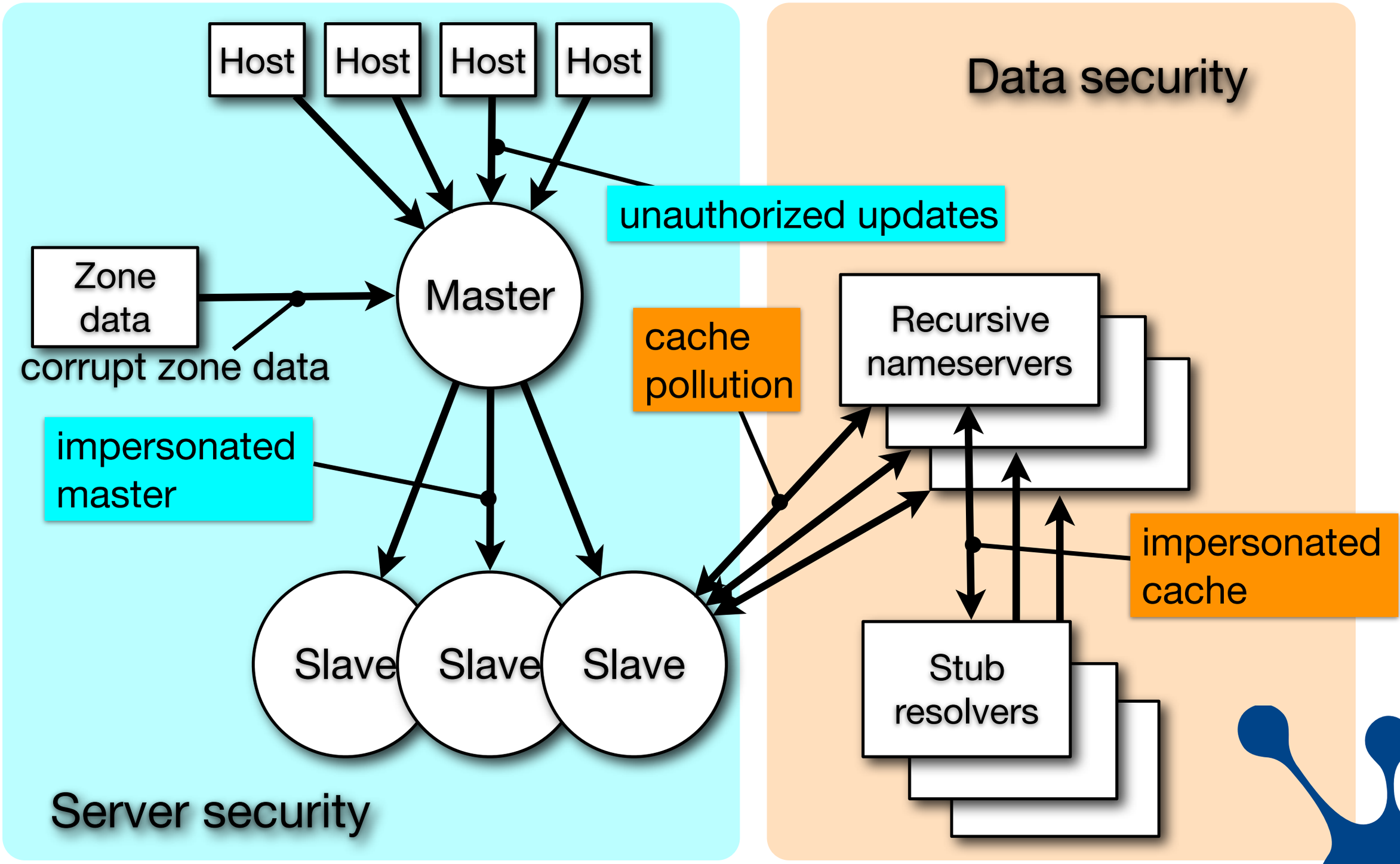



Zone
data
zone loading
Master
zone xfrs
Slave
Slave
Slave
iterative
queries
Recursive
nameservers
recursive
queries
Stub
resolvers


Host
Host
Host
Host
dynamic updates
Zone data
zone loading
Master
zone xfrs
iterative queries
Recursive nameservers
recursive queries
Slave
Slave
Slave
Stub resolvers


Host
Host
Host
Host
unauthorized updates
Zone data
corrupt zone data
Master
cache pollution
Recursive nameservers
impersonated master
impersonated cache
Slave
Slave
Slave
Stub resolvers

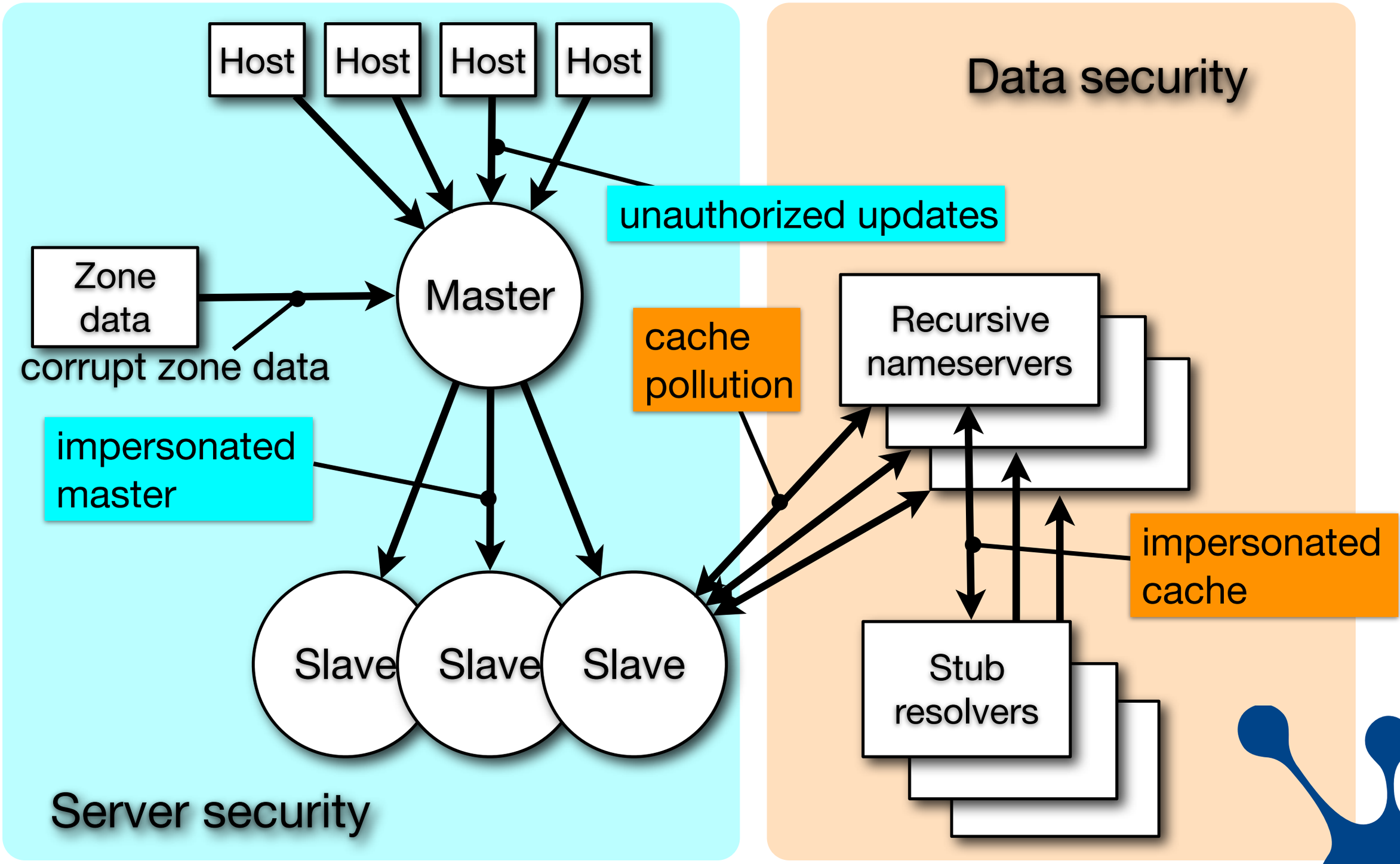

Host
Host
Host
Host
unauthorized updates
Zone data
corrupt zone data
Master
cache pollution
Recursive nameservers
impersonated master
impersonated cache
Slave
Slave
Slave
Stub resolvers
Server security


Host
Host
Host
Host
Data security
unauthorized updates
Zone data
corrupt zone data
Master
cache pollution
Recursive nameservers
impersonated master
impersonated cache
Slave
Slave
Slave
Stub resolvers
Server security

Serversäkerhet – datasäkerhet

- Våra egna datorer kan vi konfigurera säkert.
- Andras datorer kan vi inte lita på.

- Ute på nätet måste data klara sig självt!

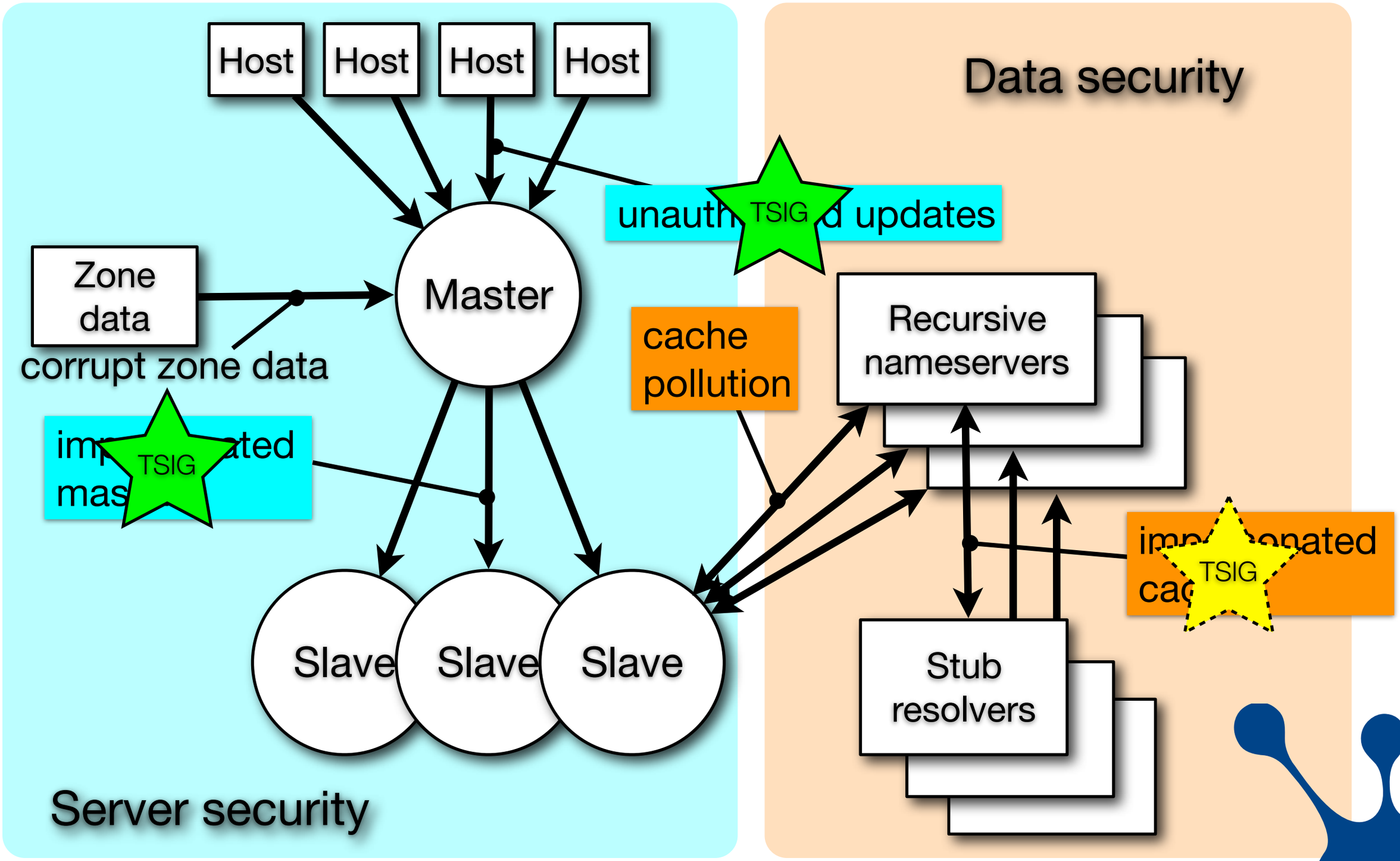

Host
Host
Host
Host
Data security
unauthorized updates
Zone data
corrupt zone data
Master
cache pollution
Recursive nameservers
impersonated master
impersonated cache
Slave
Slave
Slave
Stub resolvers
Server security

Serversäkerhet – TSIG

- Transaktionssignaturer (TSIG)
- Signaturer med symmetrisk kryptering.
- IDENTISK kryptonyckel på bägge sidor.
- IDENTISKA nycklar används för att skapa respektive för att verifiera signaturer.
- Bägge parter kan skapa och verifiera signaturer.

TSIG – problem?

- Nyckeldistribution, nyckeldistribution, nyckeldistribution, ...
- En viss nyckel bör endast användas av ett visst par av datorer.
- Jobbig administration om många parter.
- Tidsberoende!
  - NTP is your friend ...


Host
Host
Host
Host
Data security
unauth TSIG d updates
Zone data
Master
corrupt zone data
cache pollution
Recursive nameservers
imp ated mas
TSIG
imp onated ca
TSIG
Slave
Slave
Slave
Stub resolvers
Server security

Datasäkerhet – DNSSEC

- Secure DNS (DNSSEC)
- Signaturer med ASYMMETRISK kryptering.
- OLIKA kryptonycklar på bägge sidor.
- OLIKA nycklar används för att skapa respektive för att verifiera signaturer.
- Bara ena parten kan skapa signaturer
- Bara andra parten kan verifiera signaturer.

- Data ”bär med sig” sin egen säkerhet i form av signaturer.

netnod

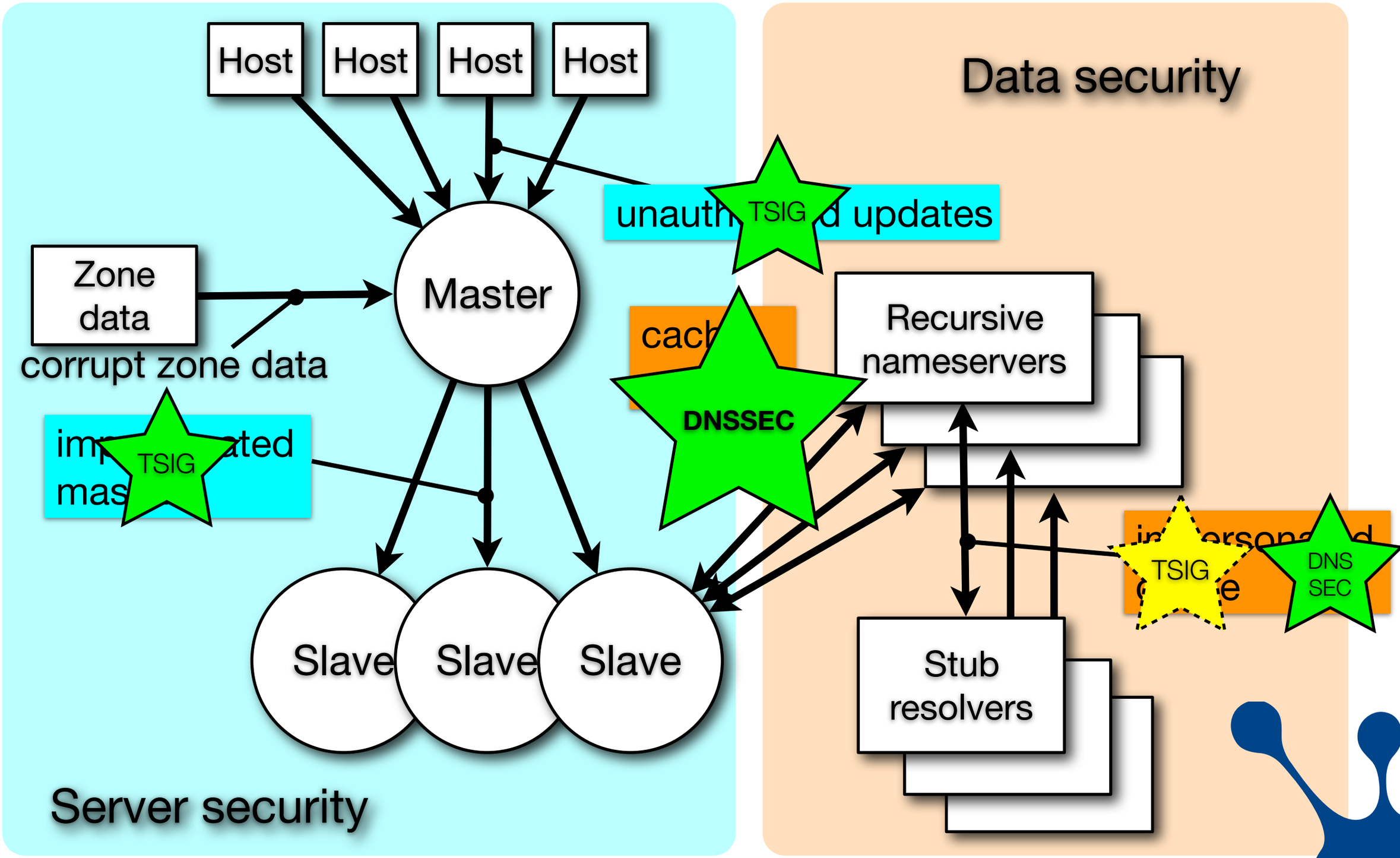
www.netnod.se

Foto: Gomér & Andersson AB, använt med tillstånd.

DNSSEC – problem?

- ~~Nyckeldistribution, nyckeldistribution, nyckeldistribution, …~~
- ~~En viss nyckel bör endast användas av ett visst par av datorer.~~
- ~~Jobbig administration om många parter.~~
- Tidsberoende!
  - NTP is your friend …
- Kräver konstant underhåll!
  - Automatisera!
- Fler felkällor och fler felmoder.

- REFLEXIONSATTACKER!
  - Har eg. inte med DNSSEC att göra.


Host
Host
Host
Host
Data security
Zone data
corrupt zone data
Master
unauth TSIG d updates
cach
Recursive nameservers
DNSSEC
TSIG
Slave
Slave
Slave
TSIG
DNS SEC
Stub resolvers
Server security

Cache pollution

- Utnyttjar det faktum att mellanliggande servrar mellanlagrar DNS-data.
- Lurar dem att lagra falska poster.
- Sätter långt ”bäst-före-datum” på posterna, så de ligger kvar länge och förstör.
-

klient

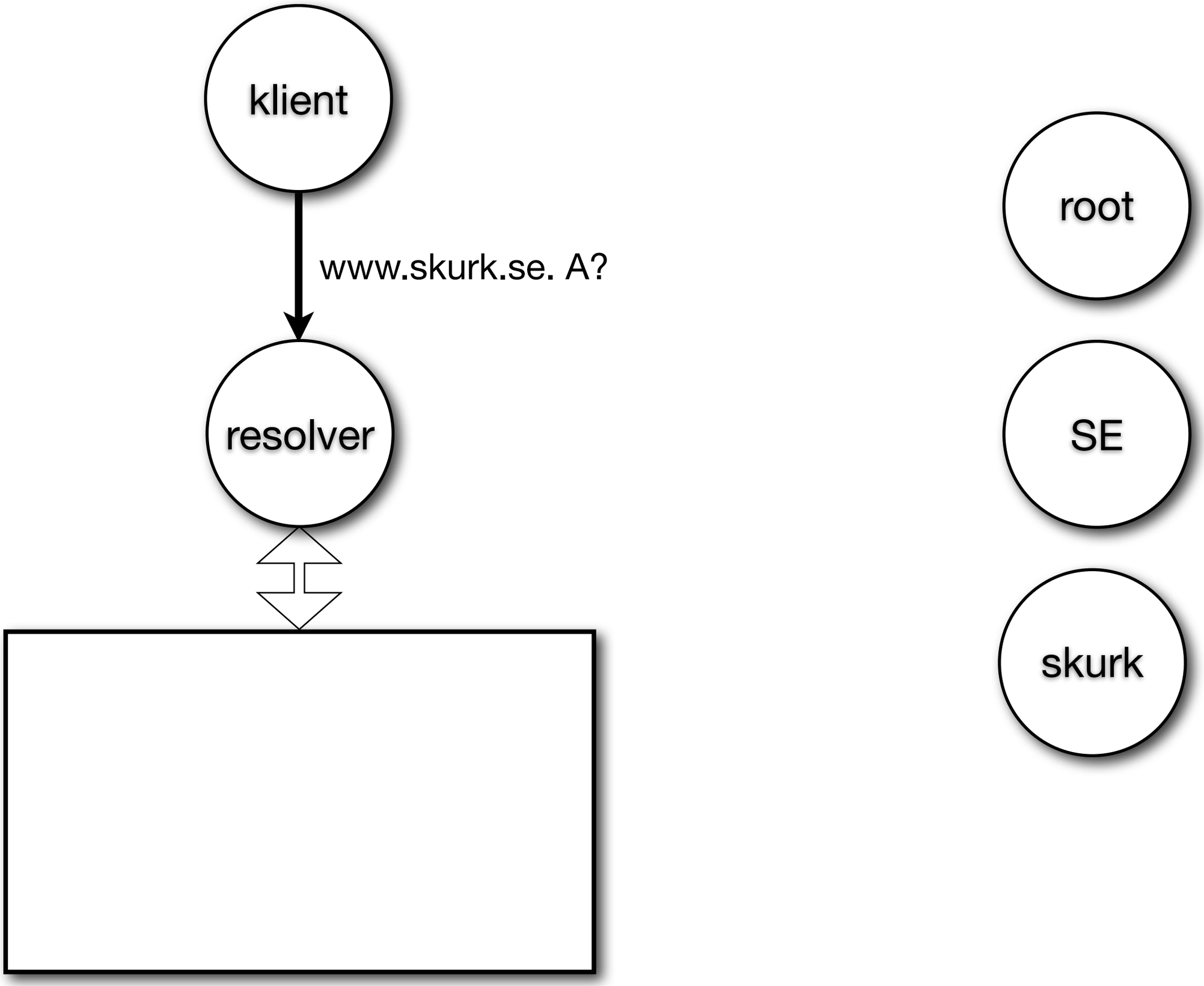
resolver

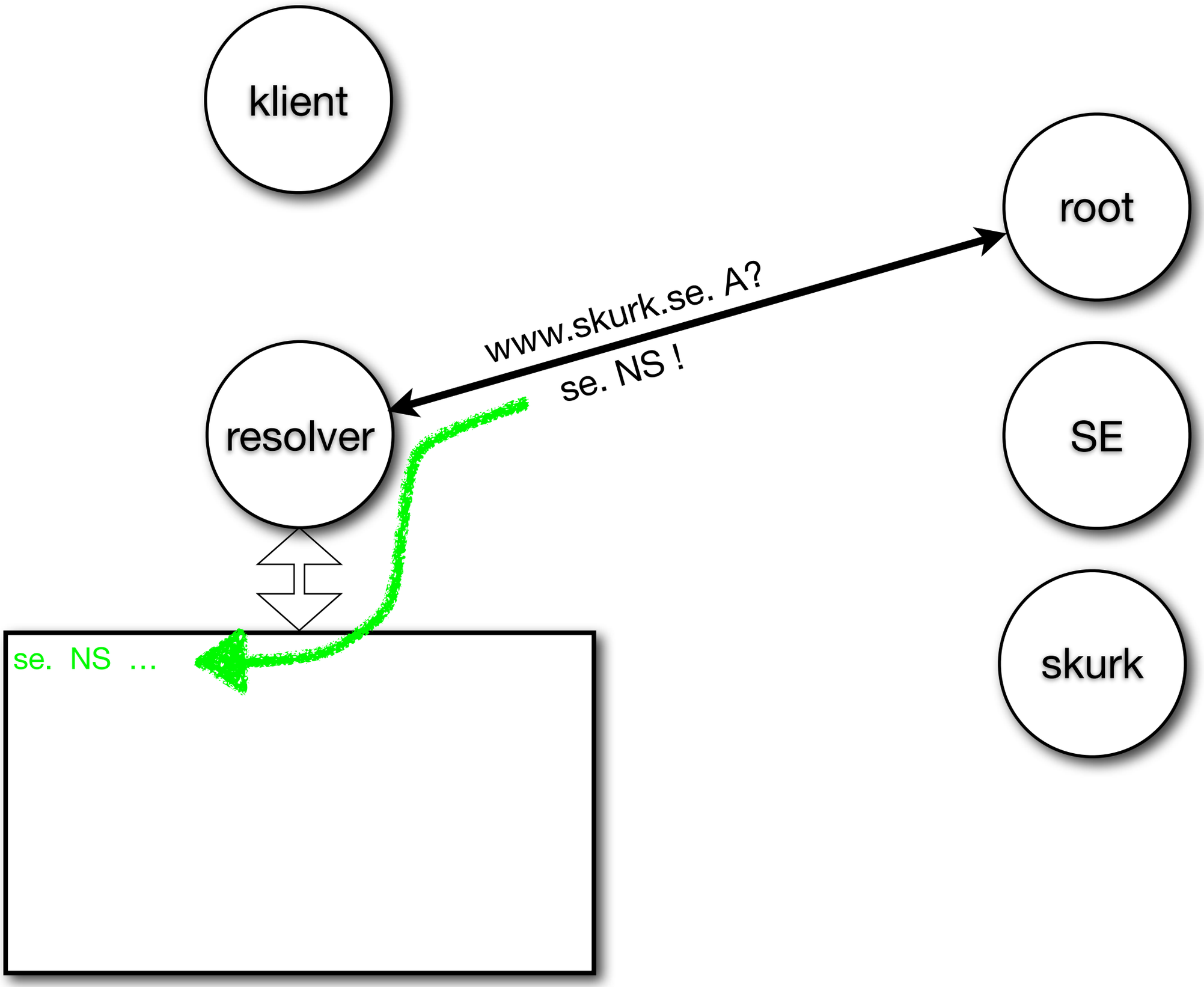
root

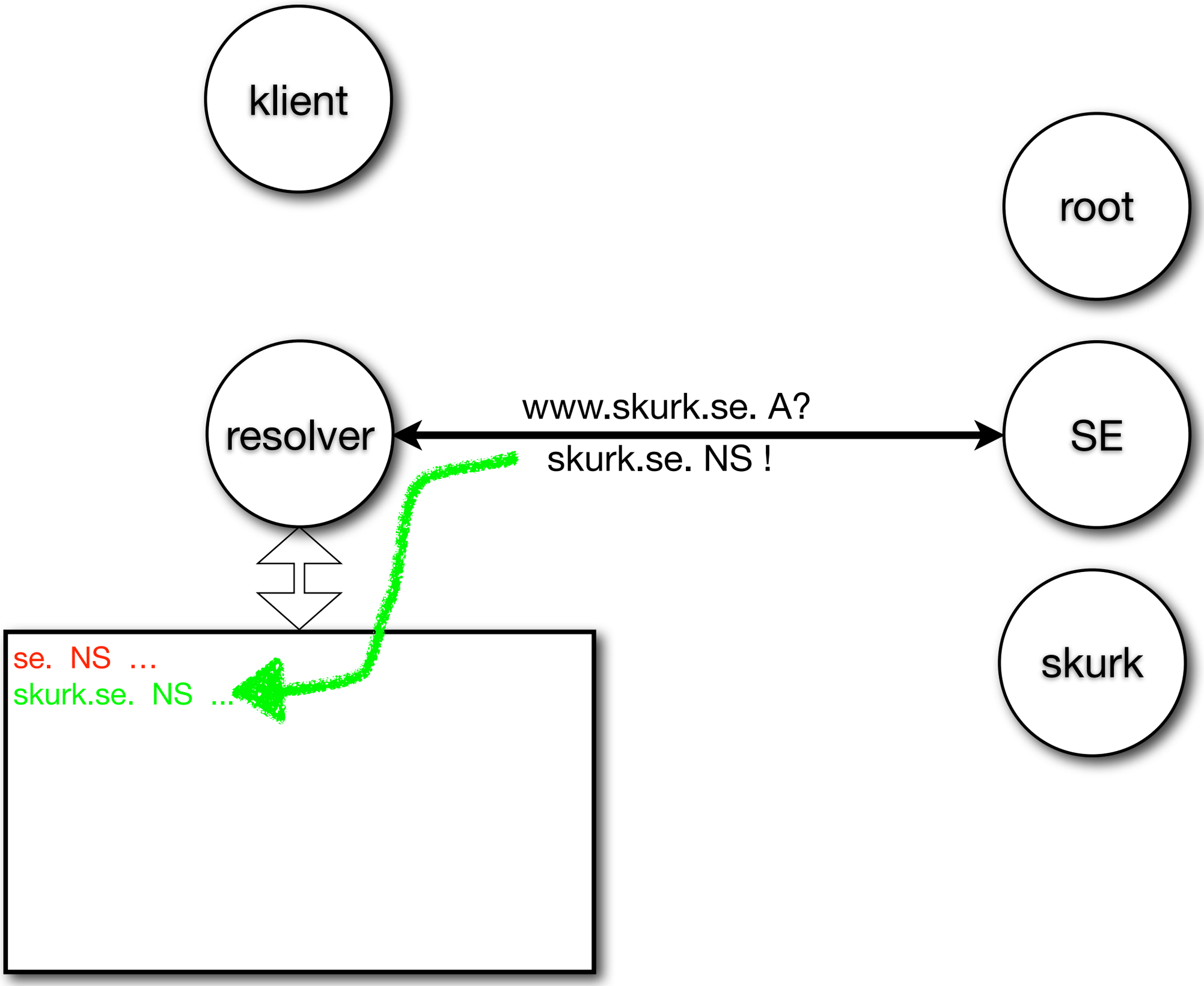
SE

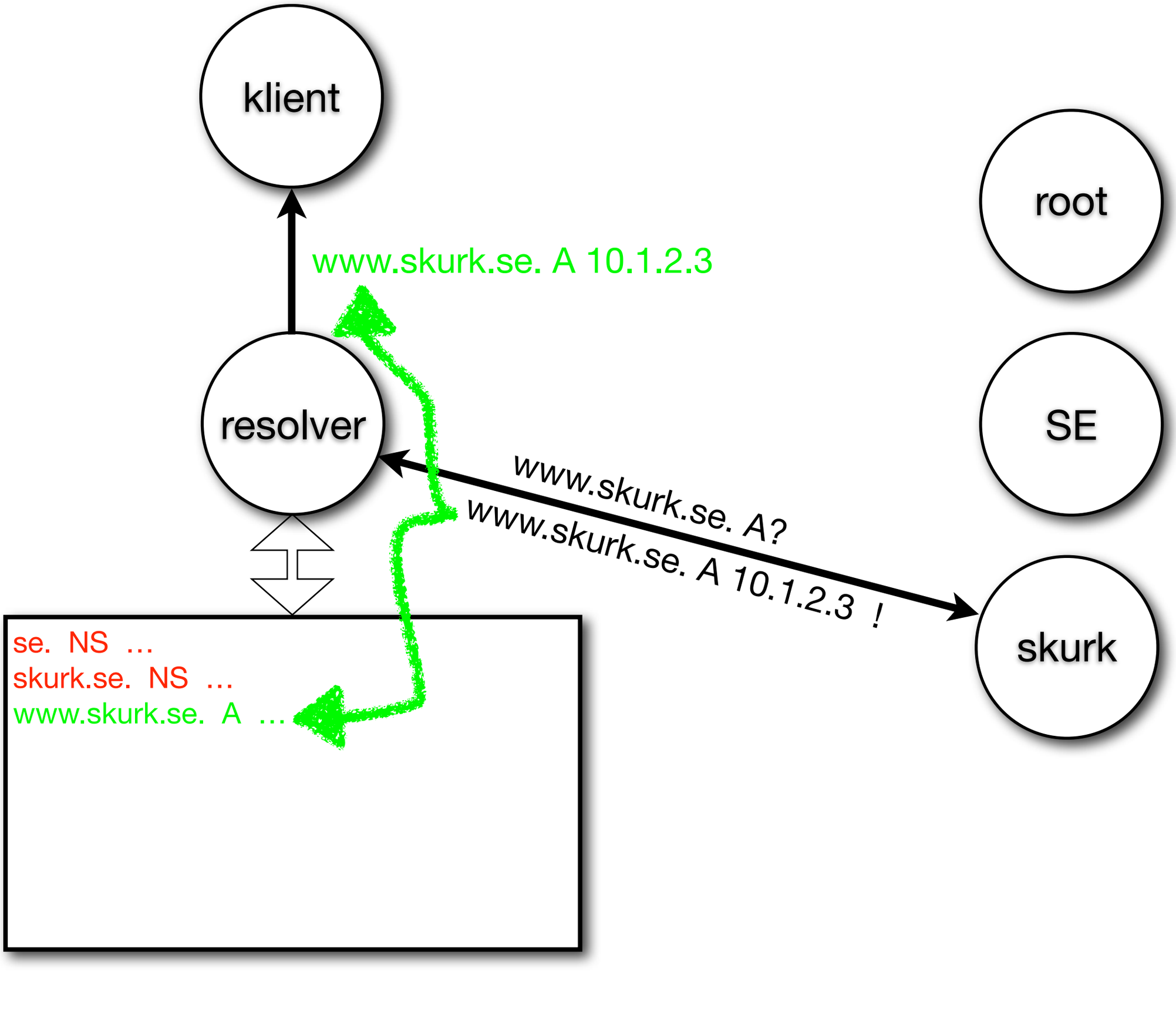
skurk

cache


klient
www.skurk.se. A?
resolver
root
SE
skurk

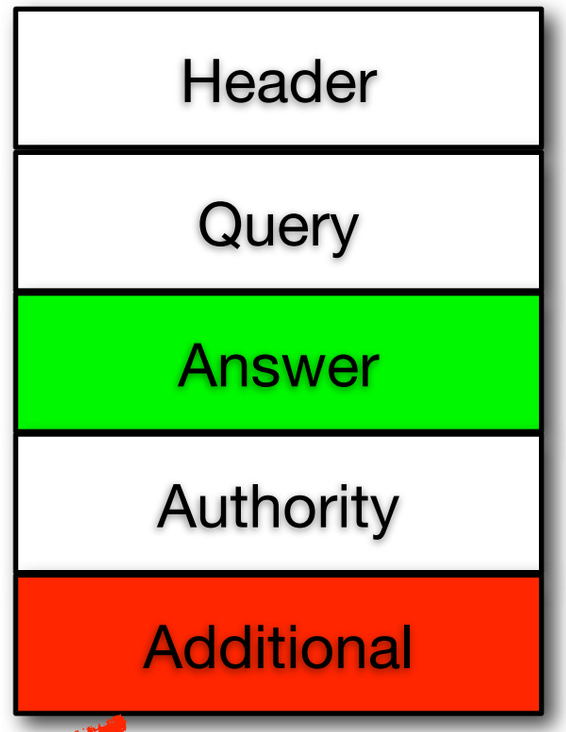

klient
root
www.skurk.se. A?
se. NS !
resolver
SE
skurk
se. NS ...

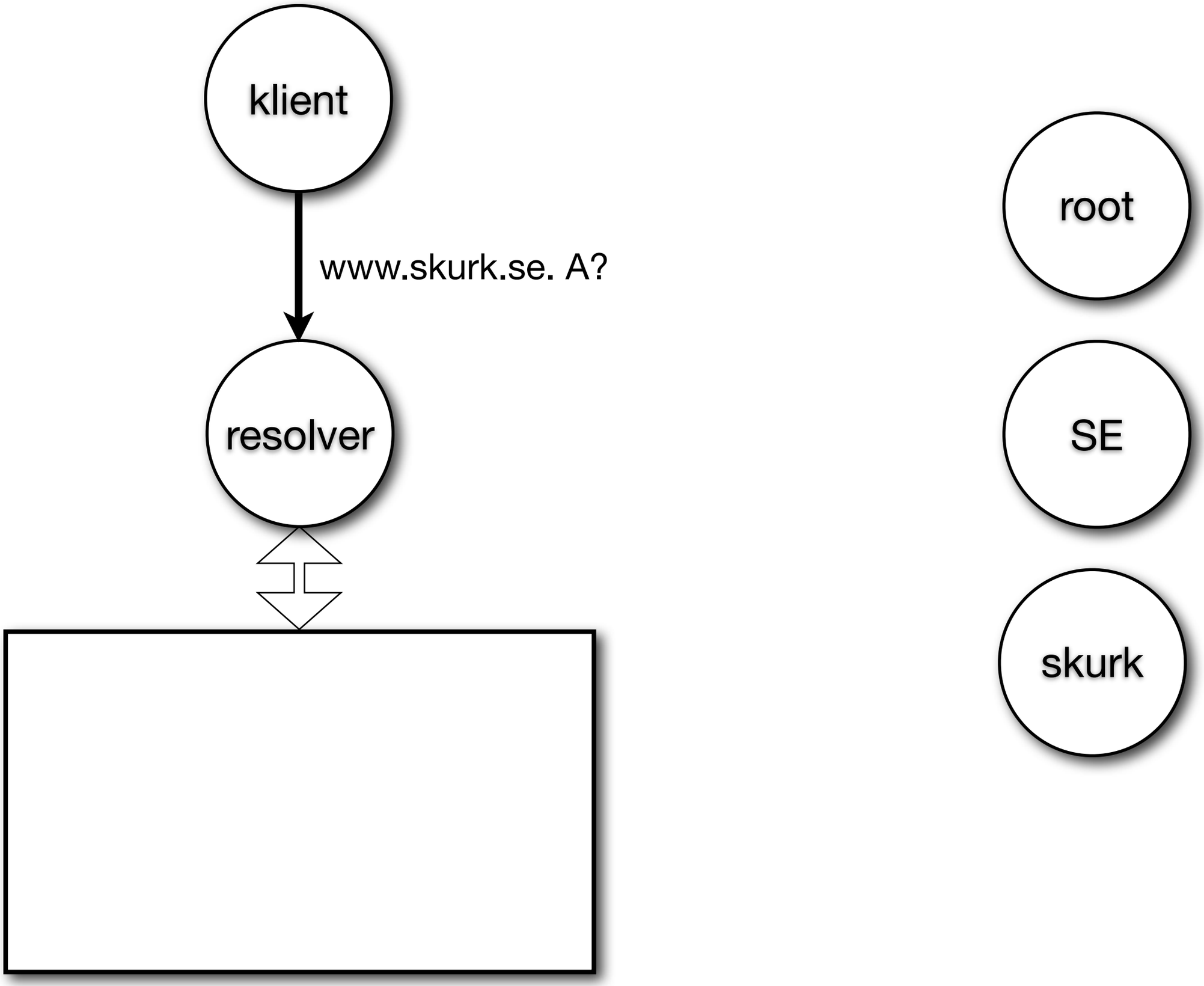

klient
root
resolver
www.skurk.se. A?
skurk.se. NS !
SE
skurk
se. NS ...
skurk.se. NS ...

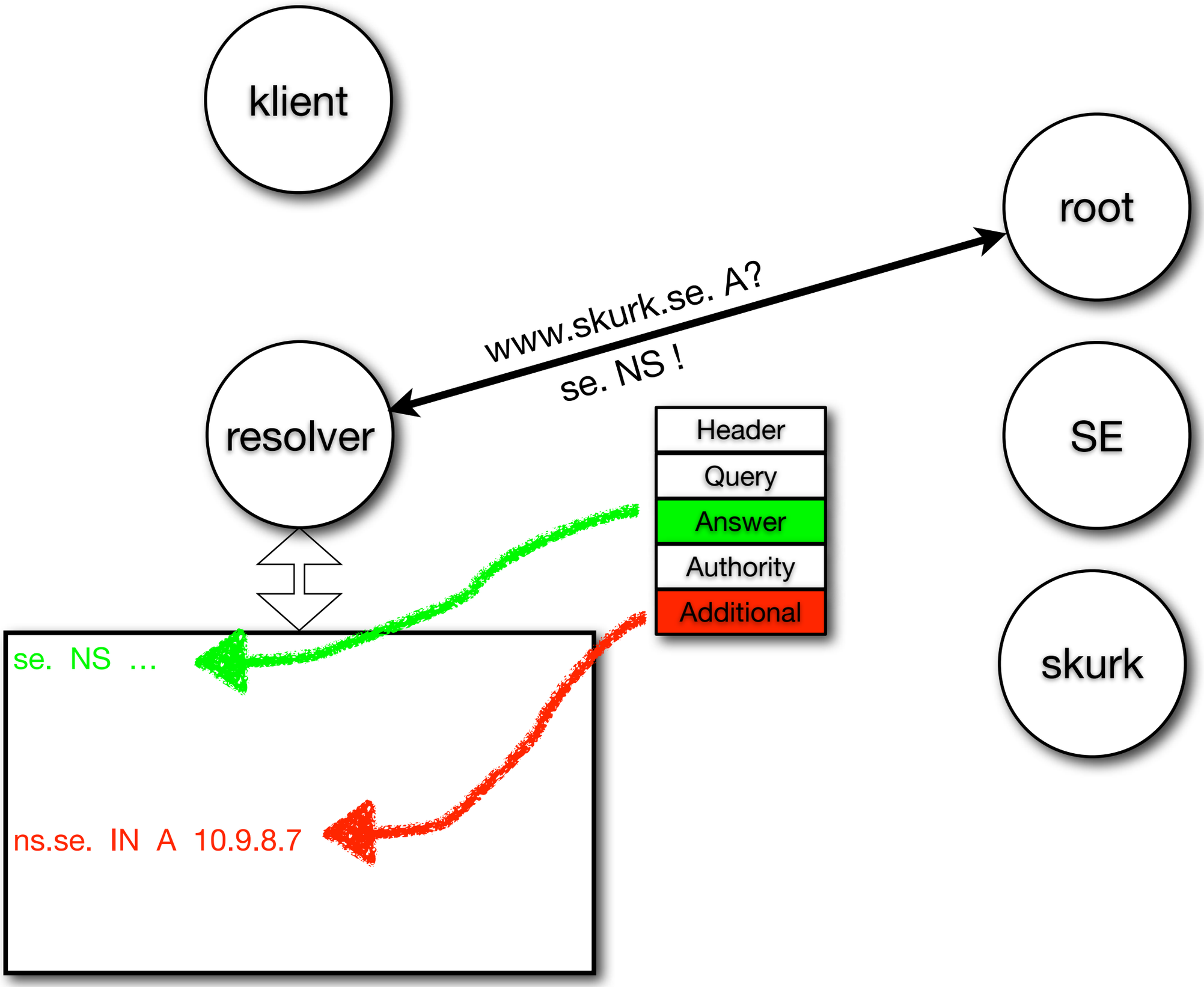

klient
www.skurk.se. A 10.1.2.3
resolver
root
SE
www.skurk.se. A?
www.skurk.se. A 10.1.2.3 !
skurk
se. NS …
skurk.se. NS …
www.skurk.se. A …

Teknisk djupdykning – ”additional data”

- Oftast behöver man skicka ”extra data” för att resolvern skall kunna jobba vidare.
- Vanligast: IP-adreserna till nameservrarna för domänen man hänvisar till.
  - ”glue records”
- DNS-paket har en särskild avledning för sådan information: ”ADDITIONAL DATA”.




klient
www.skurk.se. A?
resolver
root
SE
skurk


klient
root
www.skurk.se. A?
se. NS !
resolver
SE
Header
Query
Answer
Authority
Additional
skurk
se. NS ...
ns.se. IN A 10.9.8.7

klient

root

resolver

www.skurk.se. A?

skurk.se. NS !

SE

Header

Query

Answer

Authority

Additional

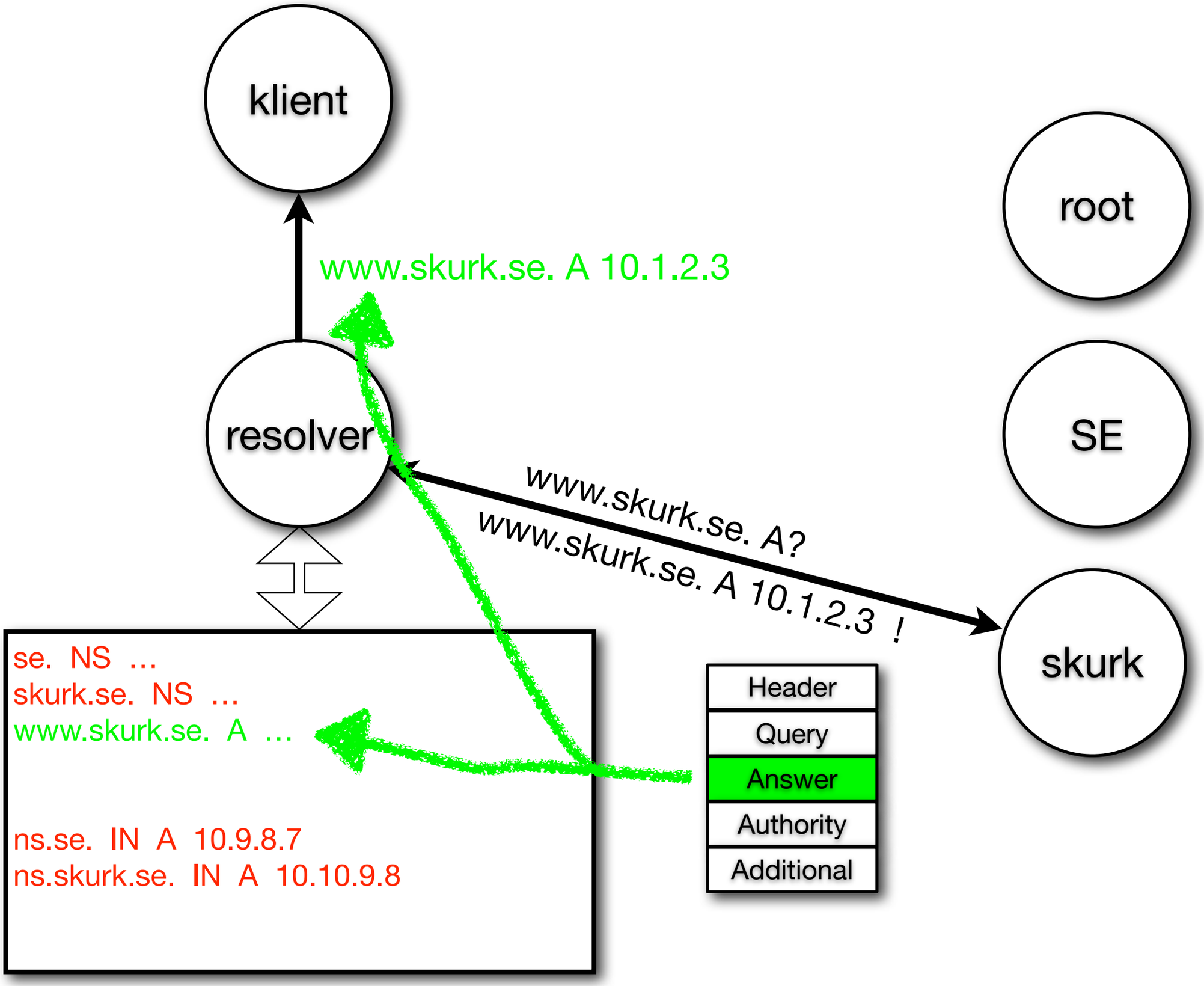
skurk

se. NS ...

skurk.se. NS ...

ns.se. IN A 10.9.8.7

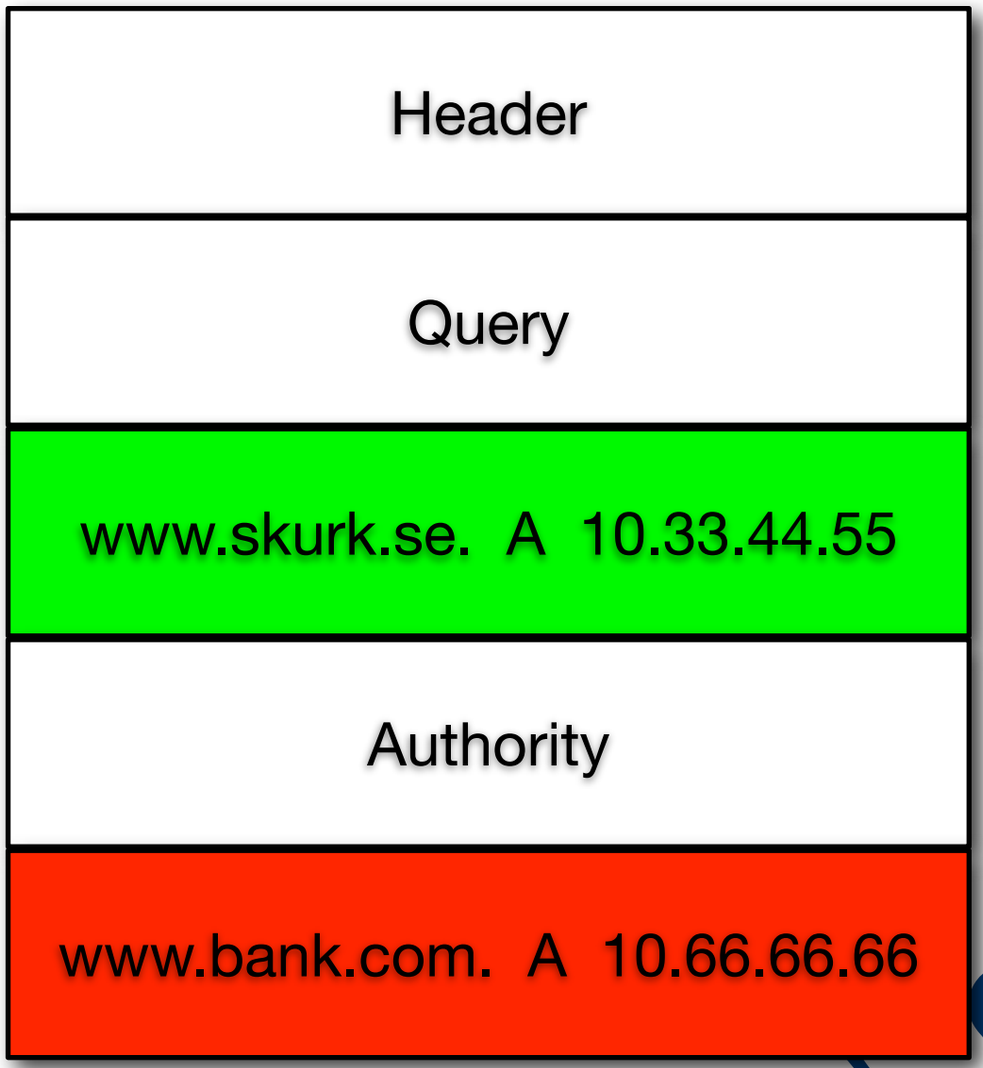
ns.skurk.se. IN A 10.10.9.8

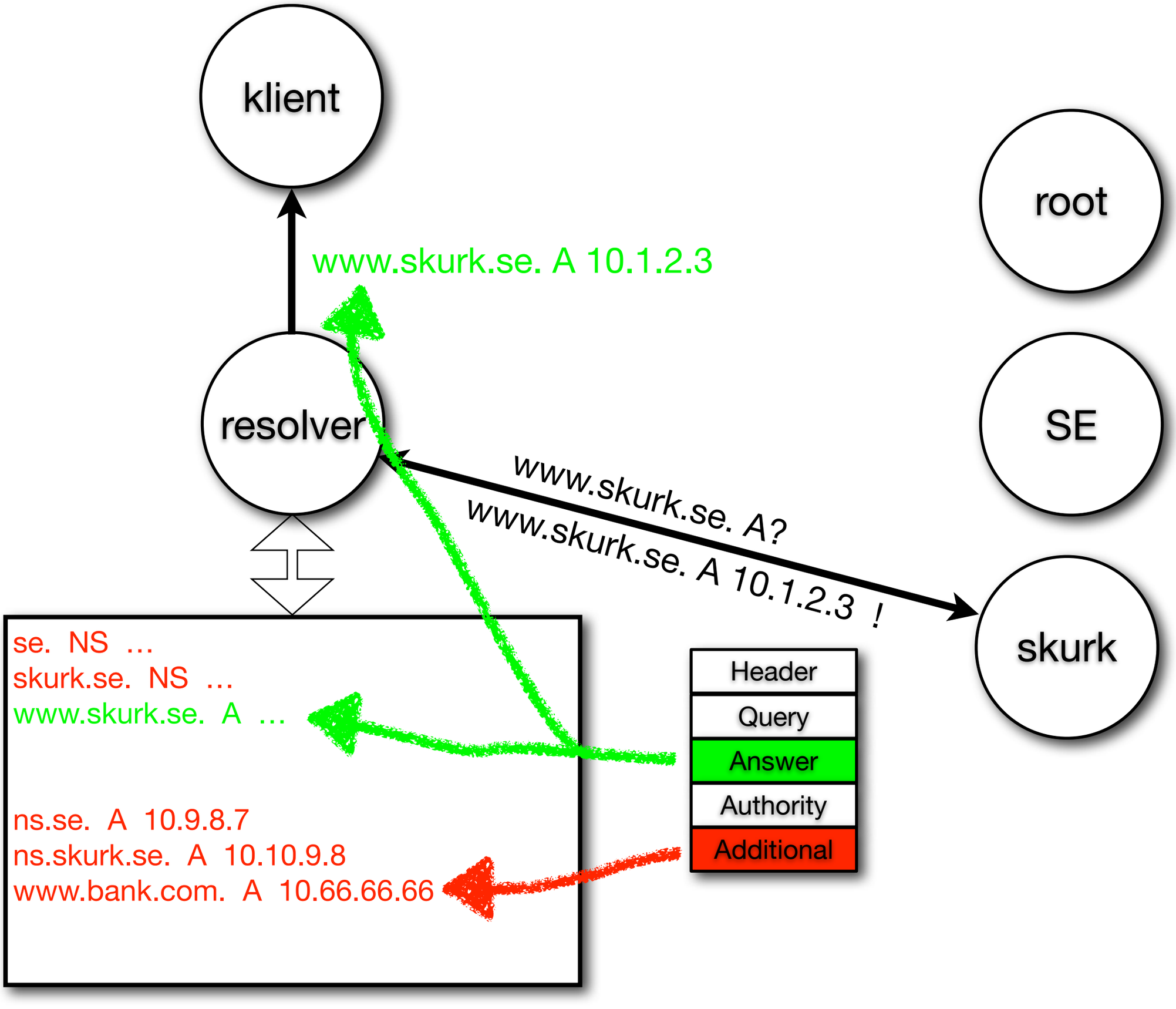

klient
www.skurk.se. A 10.1.2.3
resolver
www.skurk.se. A?
www.skurk.se. A 10.1.2.3 !
root
SE
skurk
se. NS …
skurk.se. NS …
www.skurk.se. A …
ns.se. IN A 10.9.8.7
ns.skurk.se. IN A 10.10.9.8
Header
Query
Answer
Authority
Additional

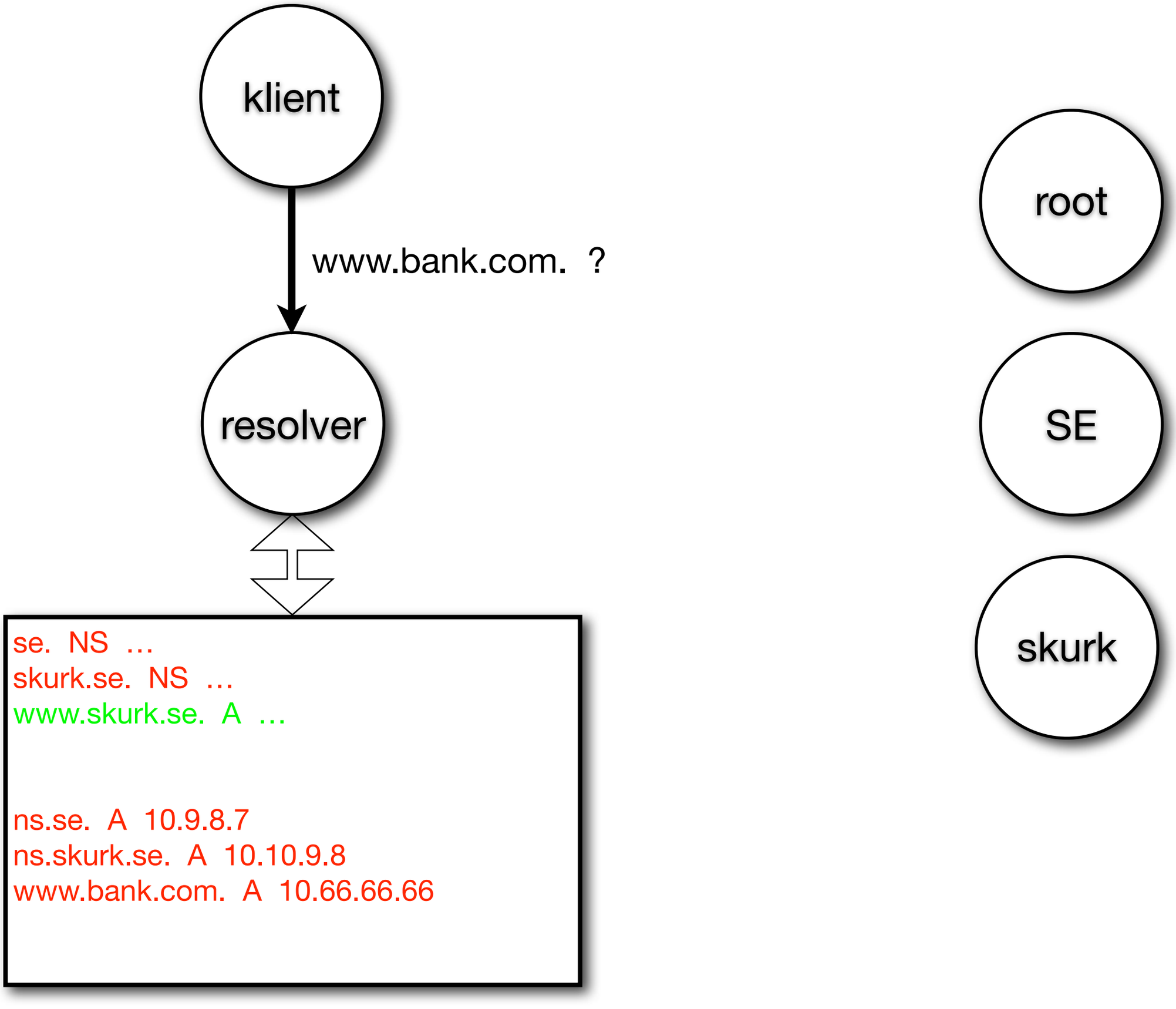
Det elaka tricket ...

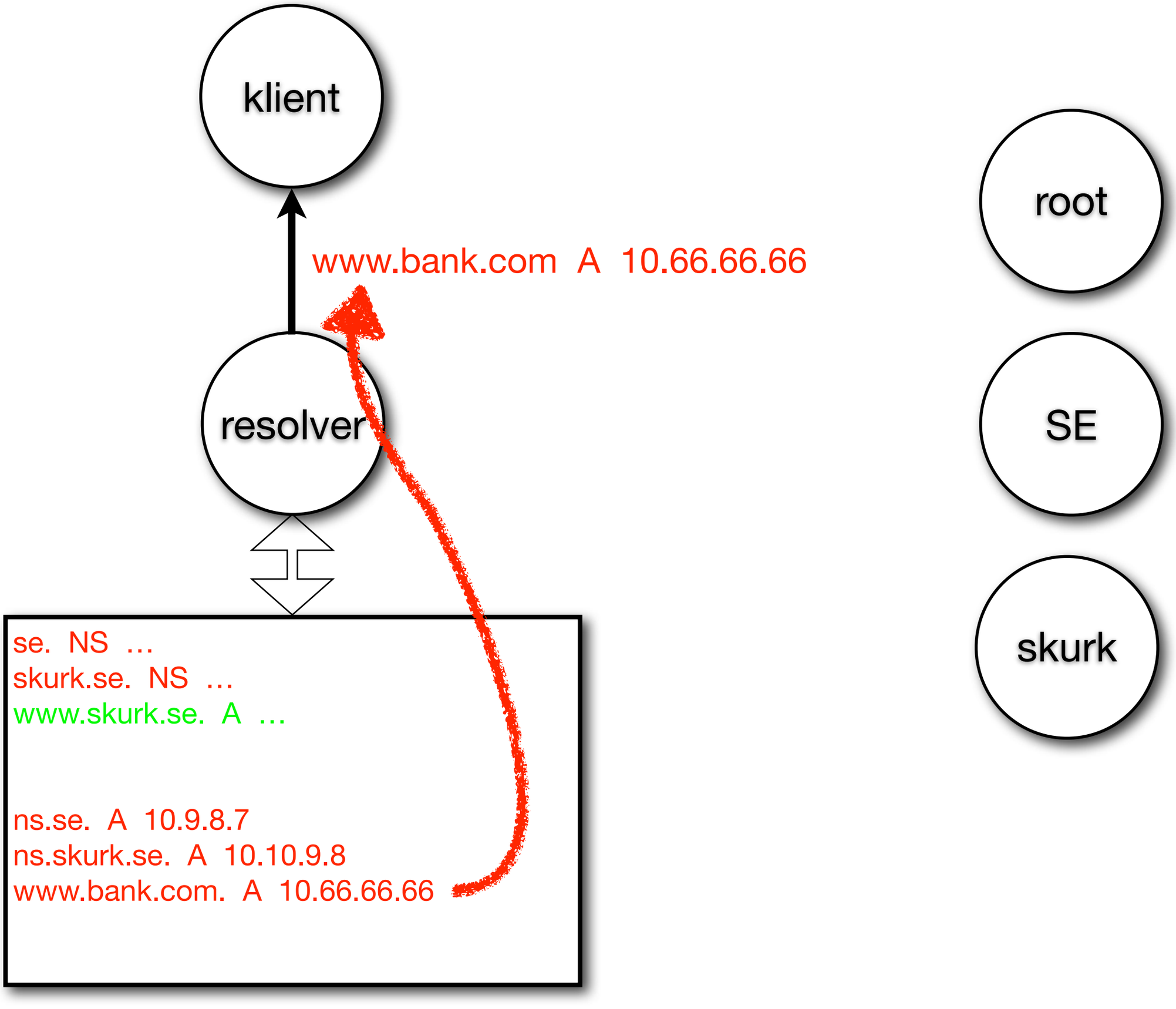
- **Vad händer om man stoppar in *NÅGOT ANNAT* än det som faktiskt är nödvändigt ... ?!**

OBS!



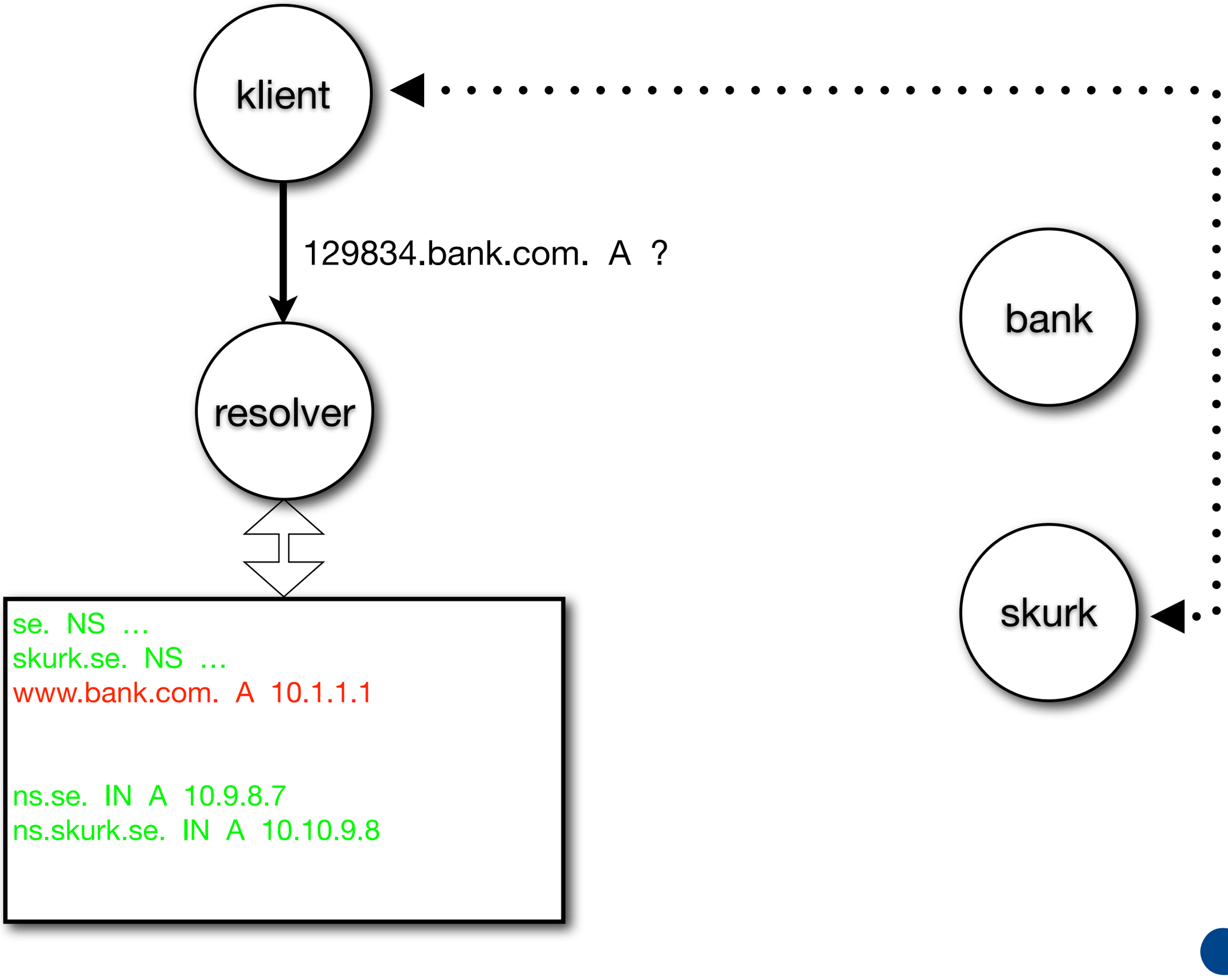

klient
www.skurk.se. A 10.1.2.3
resolver
www.skurk.se. A?
www.skurk.se. A 10.1.2.3 !
root
SE
skurk
se. NS …
skurk.se. NS …
www.skurk.se. A …
ns.se. A 10.9.8.7
ns.skurk.se. A 10.10.9.8
www.bank.com. A 10.66.66.66
Header
Query
Answer
Authority
Additional


klient
www.bank.com. ?
resolver
root
SE
skurk
se. NS …
skurk.se. NS …
www.skurk.se. A …
ns.se. A 10.9.8.7
ns.skurk.se. A 10.10.9.8
www.bank.com. A 10.66.66.66


klient
www.bank.com A 10.66.66.66
resolver
root
SE
skurk
se. NS …
skurk.se. NS …
www.skurk.se. A …
ns.se. A 10.9.8.7
ns.skurk.se. A 10.10.9.8
www.bank.com. A 10.66.66.66

”Kaminskybuggen”

- Sätt att snabbt åstadkomma cache poisoning.
- Många parametrar i DNS-paketen lätt förutsägbara – dåligt säkerhetstänk vid programmering.
- Parametrar i DNS-protokollet lätt gissade – gammal protokolldesign (= inte programmerarnas fel!).
- Kan förgifta en cache på enstaka minuter.


klient
129834.bank.com. A ?
bank
resolver
skurk
se. NS …
skurk.se. NS …
www.bank.com. A 10.1.1.1
ns.se. IN A 10.9.8.7
ns.skurk.se. IN A 10.10.9.8

klient

resolver

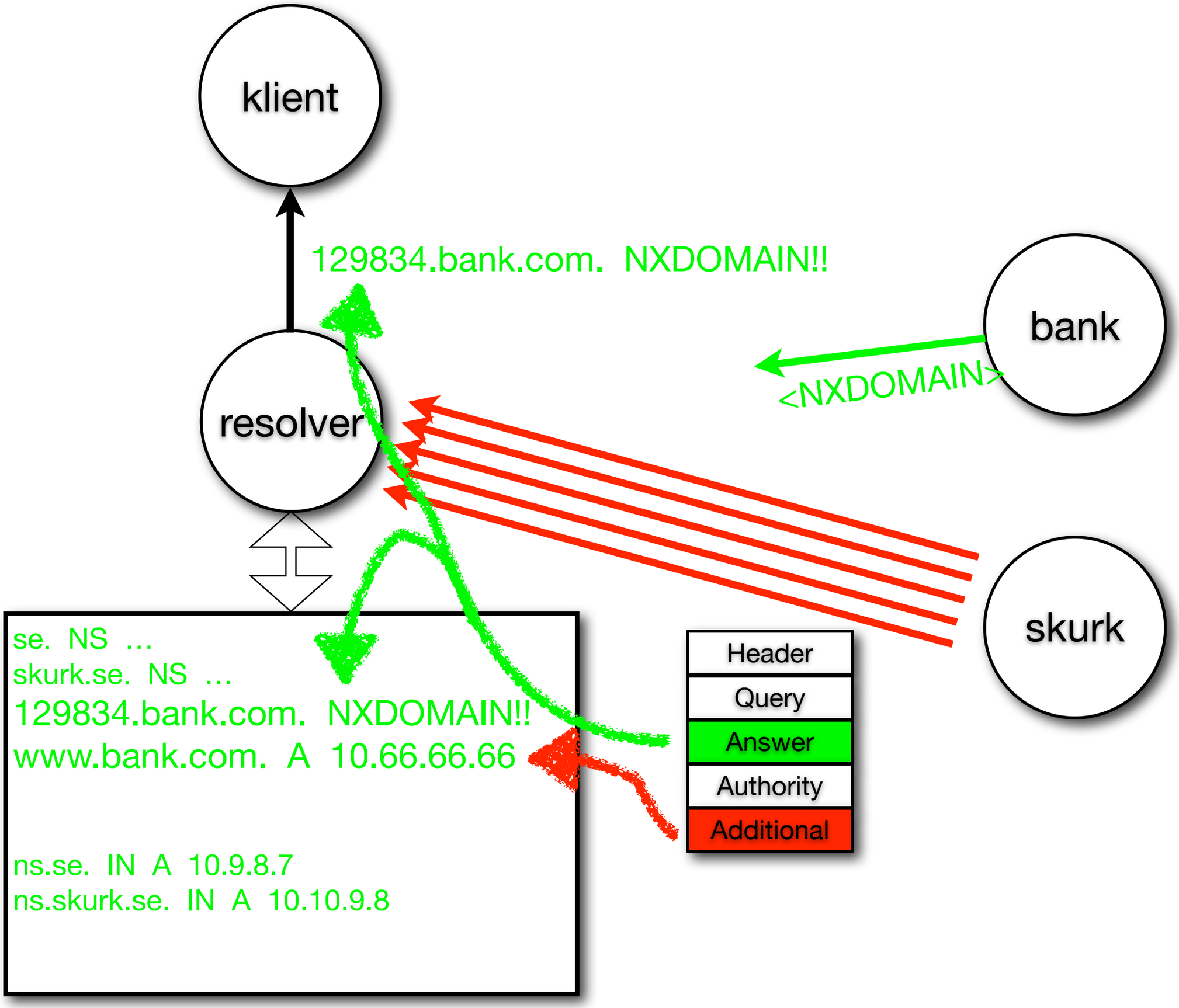
129834.bank.com. A ?

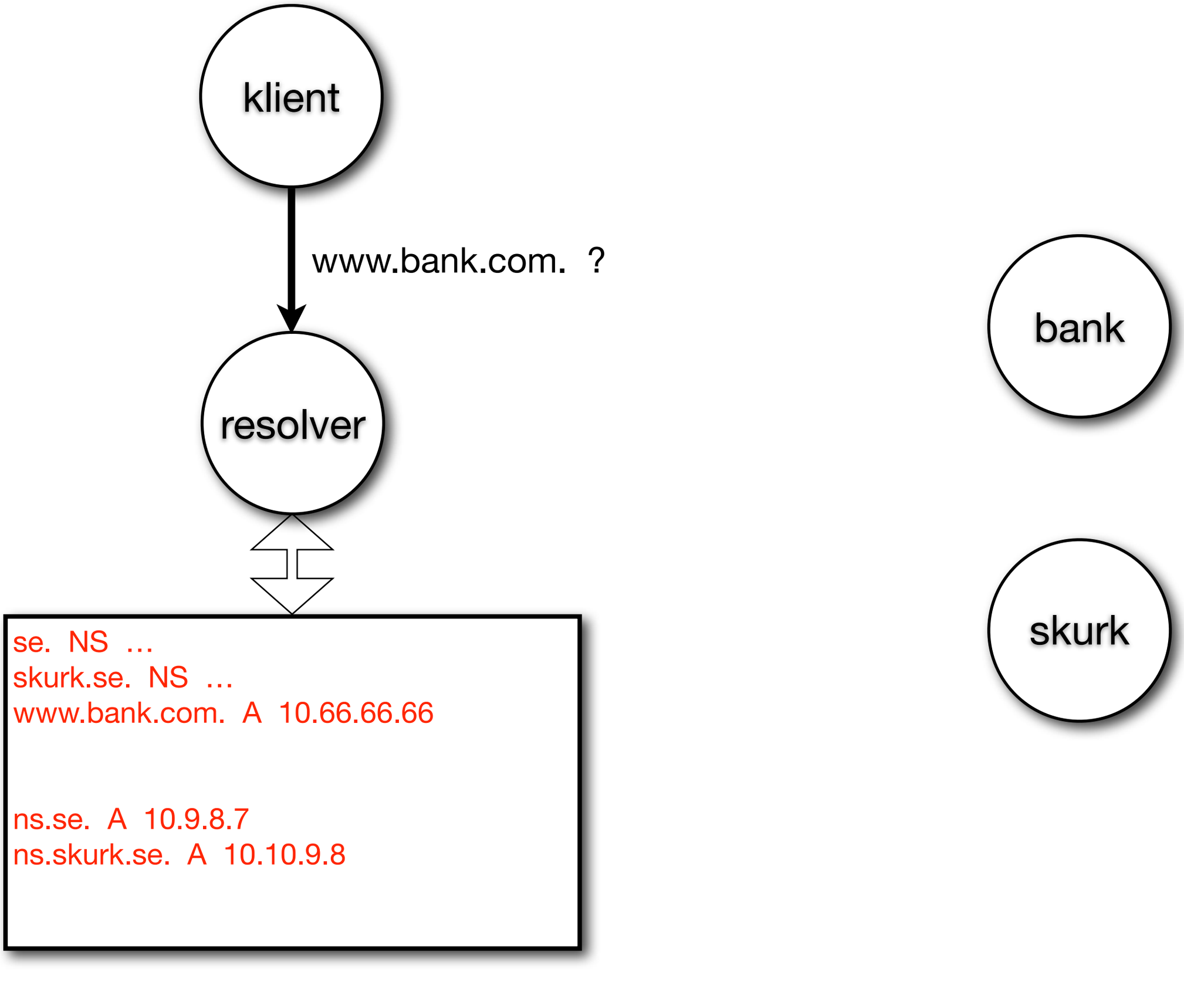
bank

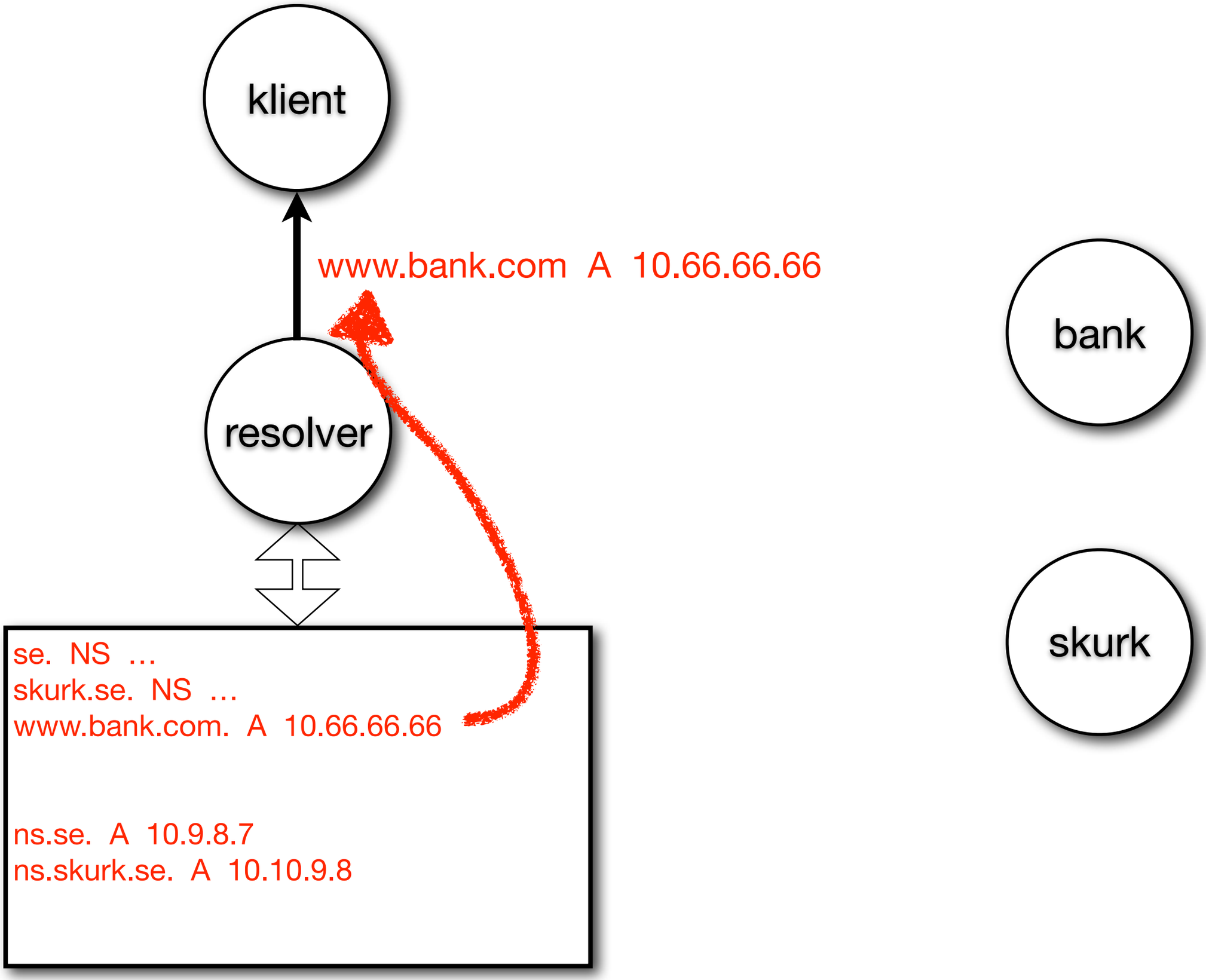
skurk

se. NS …
skurk.se. NS …
www.bank.com. A 10.1.1.1

ns.se. IN A 10.9.8.7
ns.skurk.se. IN A 10.10.9.8


klient
129834.bank.com. NXDOMAIN!!
bank
<NXDOMAIN>
resolver
skurk
se. NS ...
skurk.se. NS ...
129834.bank.com. NXDOMAIN!!
www.bank.com. A 10.66.66.66
ns.se. IN A 10.9.8.7
ns.skurk.se. IN A 10.10.9.8
Header
Query
Answer
Authority
Additional


klient
www.bank.com. ?
resolver
se. NS …
skurk.se. NS …
www.bank.com. A 10.66.66.66
ns.se. A 10.9.8.7
ns.skurk.se. A 10.10.9.8
bank
skurk


klient
www.bank.com A 10.66.66.66
bank
resolver
skurk
se. NS …
skurk.se. NS …
www.bank.com. A 10.66.66.66
ns.se. A 10.9.8.7
ns.skurk.se. A 10.10.9.8

Skydd – DNSSEC

- Programmakarna har höjt ribban en aning genom att införa ”mer slump” i protokollets parametrar.
- Detta gör det svårare, men inte omöjligt. Det tar bara lite längre tid eller fler botar.
- Det enda riktiga skyddet heter DNSSEC.

DNSSEC som PKI

- DNSSEC kan användas för att distribuera kryptonycklar och certifikat på ett autentiserat sätt.
- SSHFP (secure finger print) för SSH identifierar datorer när man loggar in med SSH så att man vet att man har kommit till rätt dator.
- TLSA är en mer generell (nyare) posttyp för användning med TLS (POP, IMAP, LMTP, SMTP) men kan även transportera nyckelinformation och hela certifikat för andra ändamål (t.ex. S/MIME).
- SPF identifierar vilka datorer en domän skickar mail från, så att man kan identifiera spam som kommer från ”fel” server.
- Många fler potentiella användningsområden.
- Ex: Autentisering vid domänregistreringsärenden.

EFTERMIDDAG

www.netnod.se

BIND OCH AUTOSIGNERING

SUNET-dagarna, Malmö, 2012-10-24, Lars-Johan Liman

BIND och validering

- I BIND 9.9.2 är det mycket enkelt:
- DNSSEC är påslaget per default.
- Rotnyckeln installeras i en egen liten fil vid ”make install”.
  - Tänk till runt DLV-nyckeln som också kommer med!
- Allt som behövs är att slå på validering med automagisk nyckeluppdatering.
- ... och att ta emot frågor.

Exempel på named.conf för validerande BIND 9.9.2

```
options {
    directory "/etc/domain";
    dnssec-validate auto;
    allow-query { 10.0.0.0/8; };
};
```

- Katalogen pekar ut var filen bind.keys finns och var filen managed-keys.bind (och .jnl) får läggas.
- Släpp inte in frågor från vem som helst. Extra viktigt när man kör DNSSEC, så att man inte bidrar till DDoS-attacker.

```
zone "test.liman.se" {
    type master;
    file "test.liman.se.zone";
    update-policy local;
    auto-dnssec maintain;
};
```

Auktoritativ server

```
zone "test.liman.se" {
     type master;
     file "test.liman.se.zone";
     update-policy local;
     auto-dnssec maintain;
};
```

- update-policy behövs, eftersom named använder dynDNS för att rotera nycklar i zonen.
- auto-dnssec säger åt named att sköta hela nyckelruljansen.