

Contents

- Small DNS introduction.
- MIM attack.
- What is DNSSEC?
- Why DNSSEC helps.

Anatomy of a DNS Packet

**Header
ID (16 bits)**

Question

Answer

Authority

Which server is authoritative for this info

Additional

Extra info that may be handy

ID was never meant as anti spoof mechanism.

Optimization.

Players in the DNS World



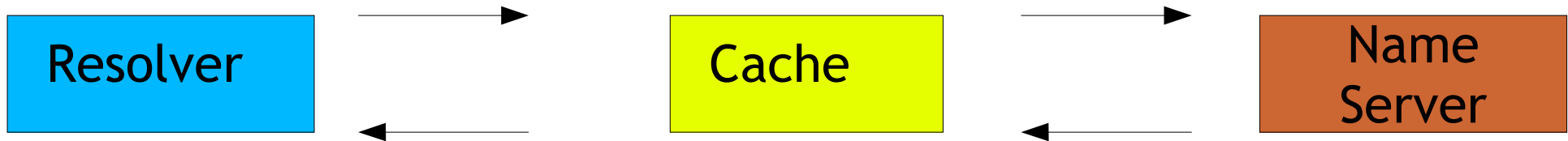
Sits on your local PC.
Converts from and to
DNS format.

Cache answers.
(Optimization)

Gives back the
final answer.

A Query in Action

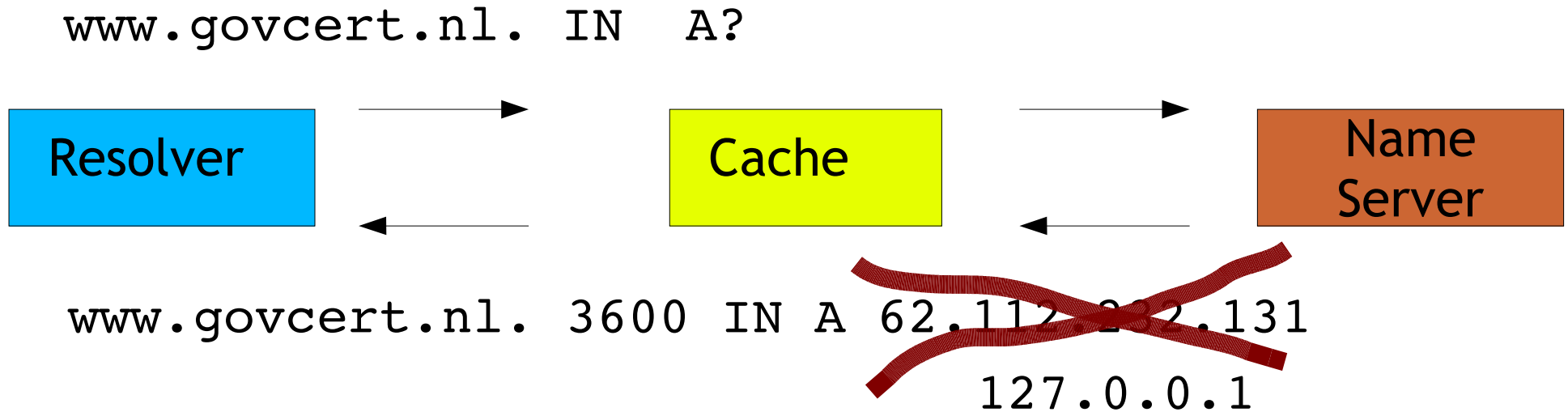
`www.govcert.nl. IN A?`



`www.govcert.nl. 3600 IN A 62.112.232.131`

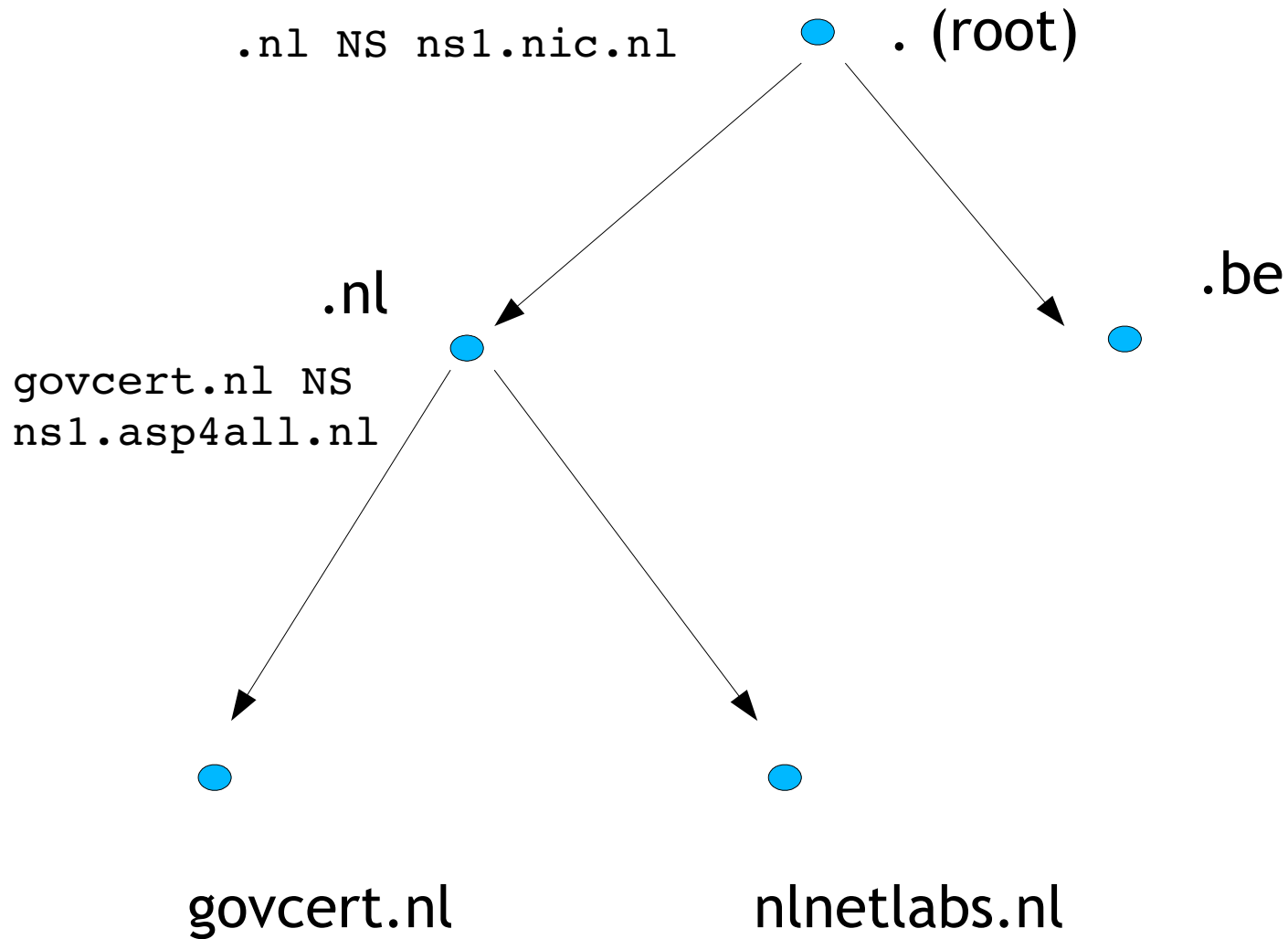
This is the hard part of DNS. Its called: recursive resolving.

A Spoof in Action



- If the cache accepts it, *all* resolvers will get the wrong answers for 3600 sec.
- If the resolver accepts it, it will mess up this query.
- Simple to do on a wireless LAN.
- *Much* harder on the Internet.

Resolving: Following Delegations



DNSSEC to the Rescue - Basics

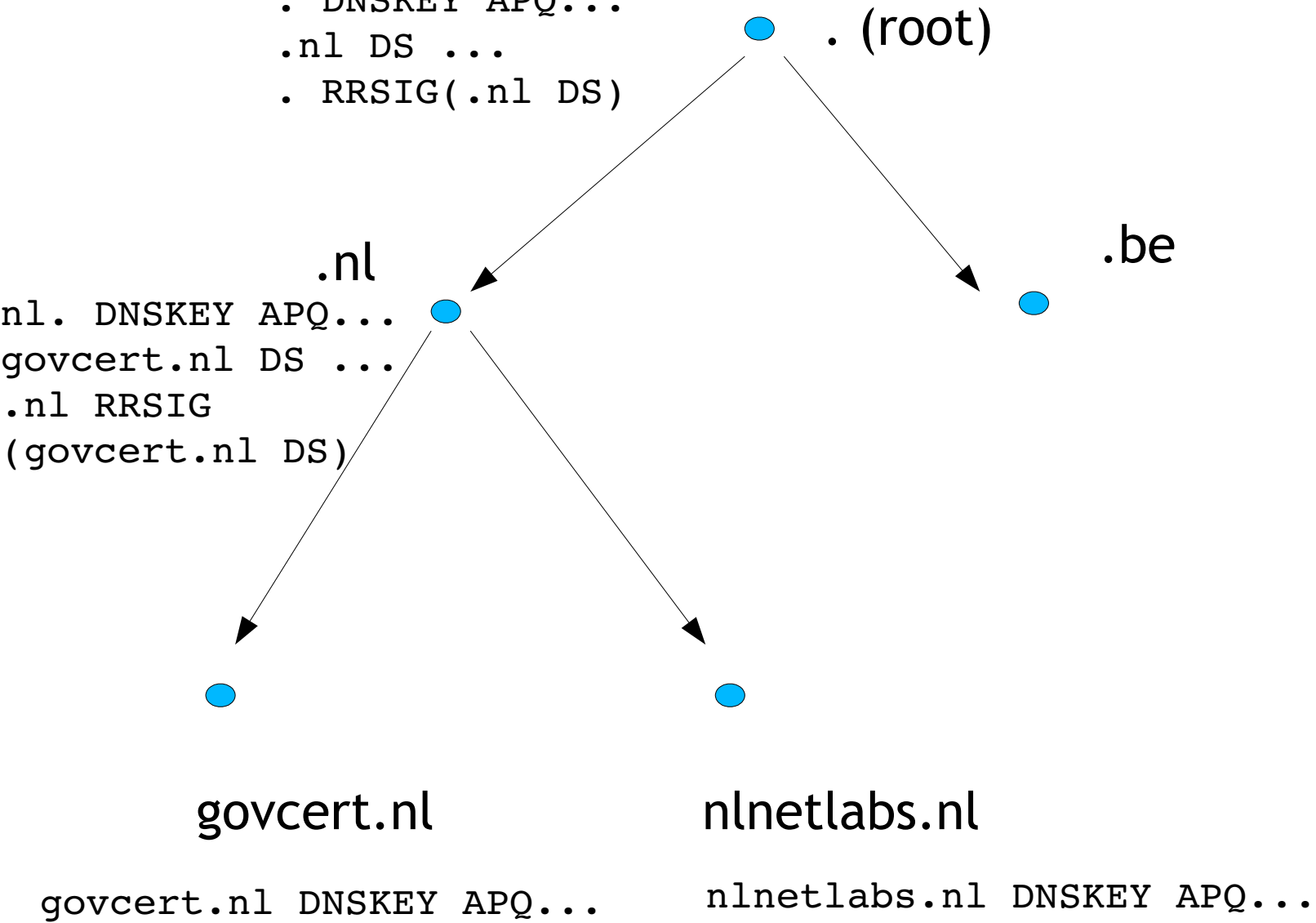
- DNSSEC adds public key cryptography to the DNS.
- Public keys are published in the DNS.
- Public keys chained via “Chain of Trust”.
- Each “answer” is signed.
- Documented in RFCs: 4033, 4034 and 4035 (just released).
- Private key(s) used to sign DNS data offline.

DNSSEC - Chain of Trust

```

. DNSKEY APQ...
.nl DS ...
. RRSIG(.nl DS)

```



DNSSEC - Example Packet

```
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id 15280
;; flags: qr aa rd ; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; nlnetlabs.nl.          IN          SOA

;; ANSWER SECTION:
nlnetlabs.nl.  86400    IN          SOA          open.nlnetlabs.nl.
hostmaster.nlnetlabs.nl. 2005041500 28800 7200 604800 18000
nlnetlabs.nl.  86400    IN          RRSIG       SOA RSASHA1 2 86400 (
    20050514235004 20050414235004 43791 nlnetlabs.nl.
    AT1AQdbbHuIF6wGQwUvOIUlzXS/NjdaqW+AYI6sYp5A
    aXbzbUubVYjKMA9zHktIzmTyzl6vx2v9oxamWpMwalq2
    0Mq1/EVjWtR+asKQ/hQwXNNC9Ci2YsKoWk0Qrgx4Pkt
    J+z8qtDxppUDEpxd6V+DiMXMA0ytnY9fZNUQLnlqM=
)
```

A Spoof in Action, DNSSEC Enabled

www.govcert.nl. IN A?



www.govcert.nl. 3600 IN A ~~62.112.232.131~~
127.0.0.1

www.govcert.nl. 3600 IN RRSIG "A 62.112.232.131"

- Resolver/Cache already knows DNSKEY of govcert.nl.*
- RRSIG does not validate.

DNSSEC - Ponder and Discuss

- Roll out on the Internet is hard (look at IPv6).
- Root should be signed first (or a big TLD).
- Globally updating anchored root key(s) is difficult.
- No real incentive for roll out, unless something “major” happens.
- .SE has advanced plannes for DNSSEC deployment.

Documentation

RFC 4033 (Introduction, quite readable).

NSD/BIND9 DNSSEC enabled.

<http://www.dnssec.net>

<http://www.dnssec-deployment.org>