DNSSEC @ RIPE NCC

Anand Buddhdev
DNS Services

K-root

Legend
- K (red) Global node
- K (blue) Local node
- K (red with star) IPv6 enabled node

RIPE NCC

K-root in Espoo
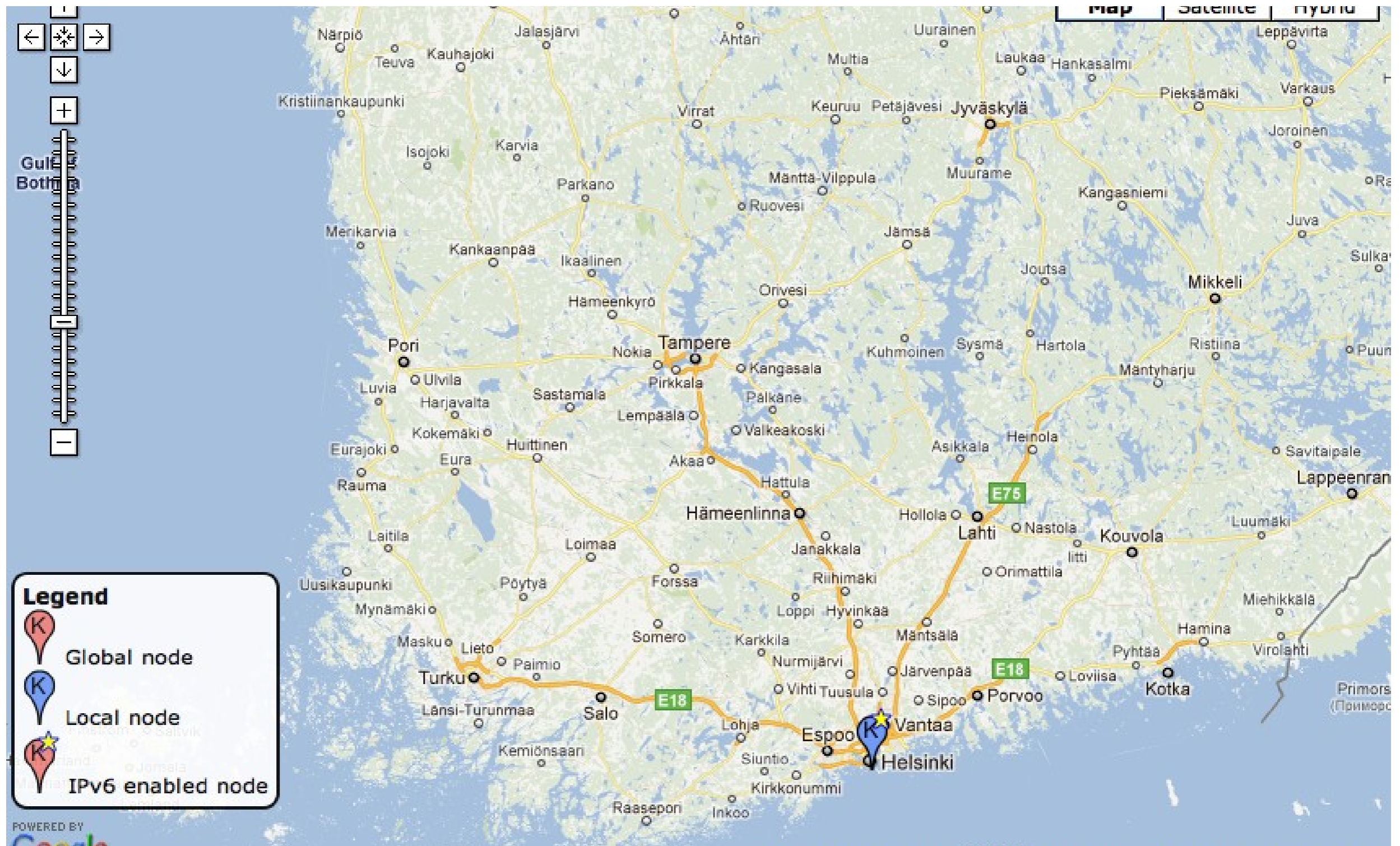
Reverse DNS

185/8

↓

185.in-addr.arpa

Infrastructure

- Anycasted clusters in Amsterdam and London

- AS 197000

- in-addr.arpa, ip6.arpa and RIPE NCC zones

Secondary DNS

```
;; ANSWER SECTION:
sy.      86400     IN  NS     ns2.tld.sy.
sy.      86400     IN  NS     ns-sy.ripe.net.
sy.      86400     IN  NS     ns1.tld.sy.
```

Other DNS Services

- ENUM delegations
- AS112 node in Amsterdam
  - 3,000 q/s
- RIPE NCC internal services

RIPE
NCC

DNSSEC History

- Signed zones in 2005

- Olaf Kolkman's perl tools

- Trust anchors on RIPE NCC website

- ZSKs rolled monthly

- KSKs rolled every 6 months

- Many manual steps – human error

Current DNSSEC Setup

- Secure64 signers in production since June 2010
  - FIPS 140-2 level 2 certified
- Updated DNSSEC policy and practice statement
  - http://www.ripe.net/rs/reverse/dnssec/dps.html
- 116 signed zones
  - 10 islands of trust
- 1024-bit ZSK, 2048-bit KSK

DNSSEC Provisioning

```
domain:     14.0.193.in-addr.arpa
descr:      RIPE NCC K-ROOT
admin-c:    RNDS-RIPE
tech-c:     OPS4-RIPE
zone-c:     OPS4-RIPE
mnt-by:     RIPE-DNS-MNT

…

…
ds-rdata:  17218 5 1 05e7398…
ds-rdata:  17218 5 2 2445412…
changed:    dns-services@ripe.net 20110412
```

Secure Delegations

KSK Roll-over Issues

- Missing signatures over DNSKEY RRset
- Timing issues
  - Outgoing KSK withdrawn too soon
- Signatures made using wrong key
- Wrong parent checked for DS record
- Lots of parent zones to update, each with its own procedures

Walled-garden Roll-overs

- During KSK roll-over, stop publishing zones
- Verify all zones against all keys
- Check if published DS records match new keys
- Update DS records of one or two zones
- If it looks good, then update all the rest

RIPE
NCC

To Roll-over or Not?

- Roll-overs necessary
  - Practice
  - Catch bugs in software

- How frequent?
  - Yearly roll-overs

Why Sign Reverse Zones?

- Practice
  - Reverse zones usually less important
  - Breakage is bearable
- Possible use of reverse DNS for secure routing
  - "Watch this space"

Questions?