TeliaSonera

Providing DNSsec resolving service for broadband customers – an ISP perspective

Mats Dufberg, TeliaSonera, Sweden

TeliaSonera

- TeliaSonera is a major telephony provider and ISP in the Nordic and Baltic region.
- TeliaSonera is the largest in that segment in Sweden.
- TeliaSoner offers many services in the telephony and IT market, e.g. fixed and mobile telephony, broadband for consumer market, leased line for corporation market, and server hosting.

2 roles in DNS

- Hosting – Publish DNS data for a domain name
  - E.g.: In the telia.se zone we will find the IP address of ”www.telia.se”. The zone telia.se **will be found on the DNS servers** that TeliaSonera has set up. To get the IP address we could send a DNS query to any of the servers. But how do we find the servers?
- Resolving – Find the DNS data for a DNS name
  - E.g.: When the web browser tries to contact www.telia.se, it sends a DNS query to **the local DNS server** (resolver), that will find the **DNS servers** (hosting) of telia.se, get the data and deliver it back to the web browser.
- IIS, as TLD registry of .SE, is responsible of the hosting of the .SE zone, and in that there are pointers to the DNS servers responsible of telia.se.
- Broadband subscribers normally use their Internet provider’s resolvers for DNS queries. TeliaSoneras role is to provide resolving service.

DNSsec

- DNSsec secured data requires DNS secured hosting of the domain.
  - The .SE zone is DNSsec secured.
  - In the next step, the domains under .SE must get DNSsec secured hosting.

- DNSsec secured hosting is wast of resources unless there is DNSsec secured resolving too!
  - It is through the resolving process that secured data provides information that can be used to verify that data has not been tampered with.
  - The ISP’s will be major players for broad introduction of DNSsec.

Field test with DNSsec resolving

- All changes of the TeliaSonera resolving service, i.e. introduction of DNSsec secured resolving, is a potential threat to stability and the service to the customers.
  - Changes in resolving must no be done without tests and validations where the customers will not be effected.
  - Tests in lab environment has its limitations.
  - Field tests in a real environment with real users is an important tool.
  - Lab tests and field tests **complement** each other.
- In the fall of 2006, we got the chance to conduct a field test of 8000 concurrent, active users. That gave us a chance to see how the DNS servers running as resolvers will handle DNSsec in this early stage of DNSsec.

Field test setting at Dreamhack

- Dreamhack is the larges LAN party of the world.
- It runs twice a year in Jönköping, Sweden.
- The field test was done during the event in Nov 30 — Dec 3, 2006.
- 8000 young people are sitting at their computers around the clock playing games, browsing the web and downloading. And indirectly using DNS.
- Information on Dreamhack <http://www.dreamhack.se>

DNSsec on Dreamhack

- TeliaSonera had 2 DNS servers at the event
  - Bind 9.3.2 was used.
  - DNSsec and resolving was turned on.
  - The public key of the .SE zone was set as the DNSsec trust anchor, i.e. only DNSsec data from .SE downwards was validated.
  - One server took the entire load, the other was a backup.
- How did it work?
  - No support issues.
  - The servers were acting well
  - Nothing strange happened.
  - No users noticed anyting.
- DNSsec resolving at the field test was no ”rocket science”!

Next step

- DNSsec is an upgrade of the DNS standards.
  - DNSsec resolving is a natural upgrade of plain resolving.
- The field test and lab tests show that there is a DNS server application that can be used in DNS production.
- TeliaSonera Sweden will in Q2, 2007, turn DNSsec on in the resolvers that all our broadband customers (and some leased line customers) use and are dependent on.
  - That will be no test, but an upgrade of production.

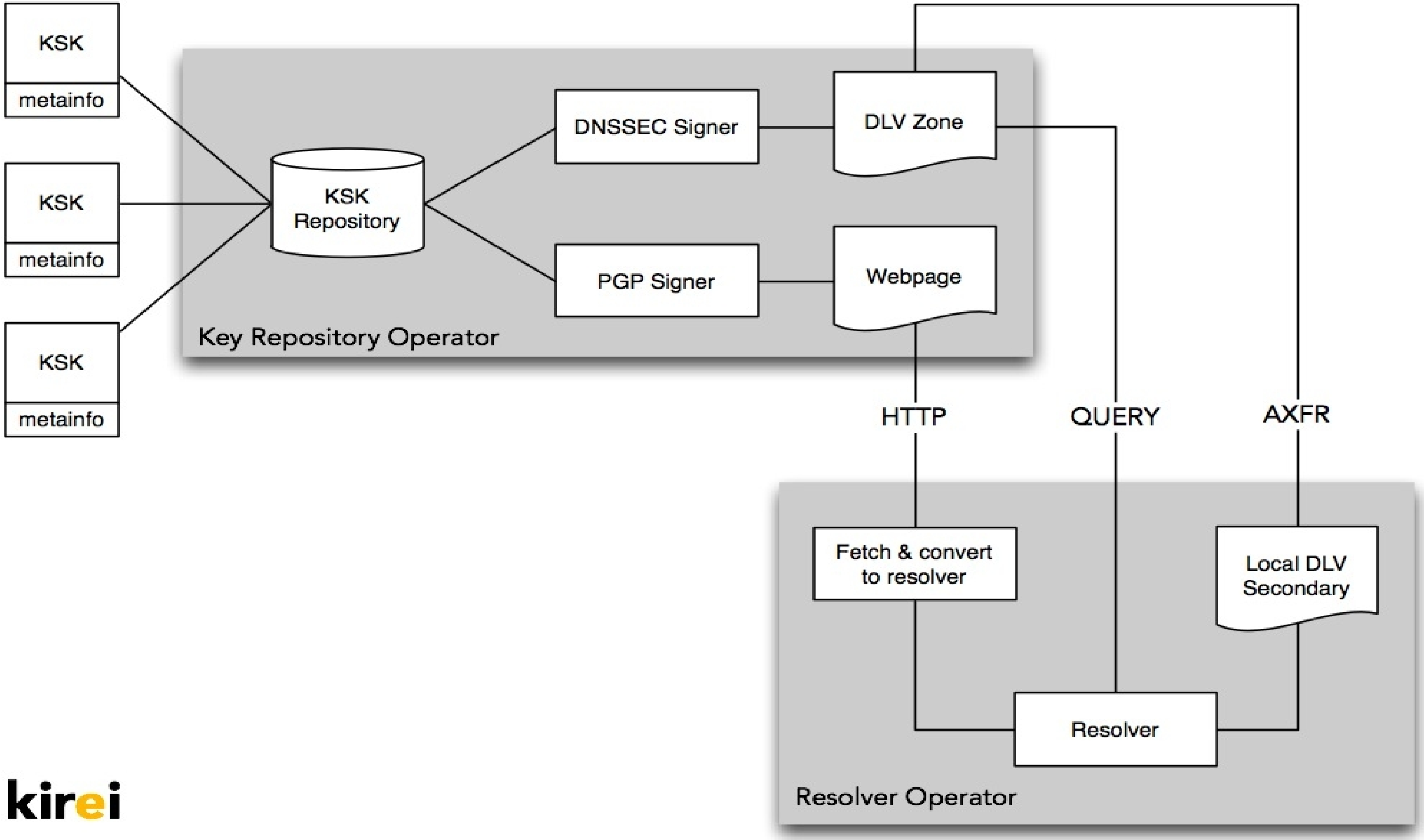
The limitations

- DNSsec resolvning requires a trust anchor to work. TeliaSonera Sweden will use the .SE public key as trust anchor.
  - Until the root zone is signed, the trust anchor must be one or several TLD public keys.
  - One, or a few trust anchors, is OK.
  - ISP:s will never accept to fetch multiple trust anchors at different sites.

The main alternative – signed root zone

- When the root zone is signed there will be one trust anchor to all DNSsec.
  - That would be a major step forward for DNSsec.
  - All ISP’s and all other parties running resolving servers really want that to happen.
- The lack of signed root zone may turn out to be a main obstacle for DNSsec.

Alternative 2: Create an separted DNSsec root



Picture by Jakob Schlyter [jakob@kirei.se], Kirei, Sweden.

Key repository operator

- Requirements
  - Must be internationally accepted.
  - Must be trustworthy.
  - Must have very good insight in the various TLD registries.
  - Must be an open organization.
- Candidates:
  - Centr, <http://www.centr.org/>, as administrative body and responsible for the repository.
  - RIPE, <http://www.ripe.net>, as the operating body for the repository.
- Centr is an organization of TLD’s, and meeting the requirements. But Centr’s strength is not operation. Ripe, on of the RIR’s, meet that requirement. They could create a strong trust anchor while waiting for ICANN and others to decide.

Questions?

- Any questions?

TeliaSonera