TeliaSonera

Finding a singel trust anchor for DNSsec resolving service

Mats Dufberg, TeliaSonera, Sweden
Eva Örnberg, TeliaSonera, Sweden

TeliaSonera

- TeliaSonera is a major Telephony and Internet Broadband provider in the Nordic and in the Baltic region.
- TeliaSonera is the largest company in that segment in Sweden and Finland.
- TeliaSonera offers many services in the Internet, Telephony and IT market, e.g. fixed and Mobile Telephony, Broadband, IP-Tv for Consumer market and Internet, IP VPN and Managed services for the Business market
- TeliaSonera is also a leading Global IP-Carrier

- Read more on http://www.telia.se/ and http://www.teliasonera.com/

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.
- The .SE TLD 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 for its customers.

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 waste 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.

Next step

- DNSsec is an upgrade of the DNS standards.
  - DNSsec resolving is a natural upgrade of plain resolving.
- TeliaSonera Sweden will in Q2, 2007, turn DNSsec on in the resolvers that all our broadband customers (and some business customers) use and are dependent on.

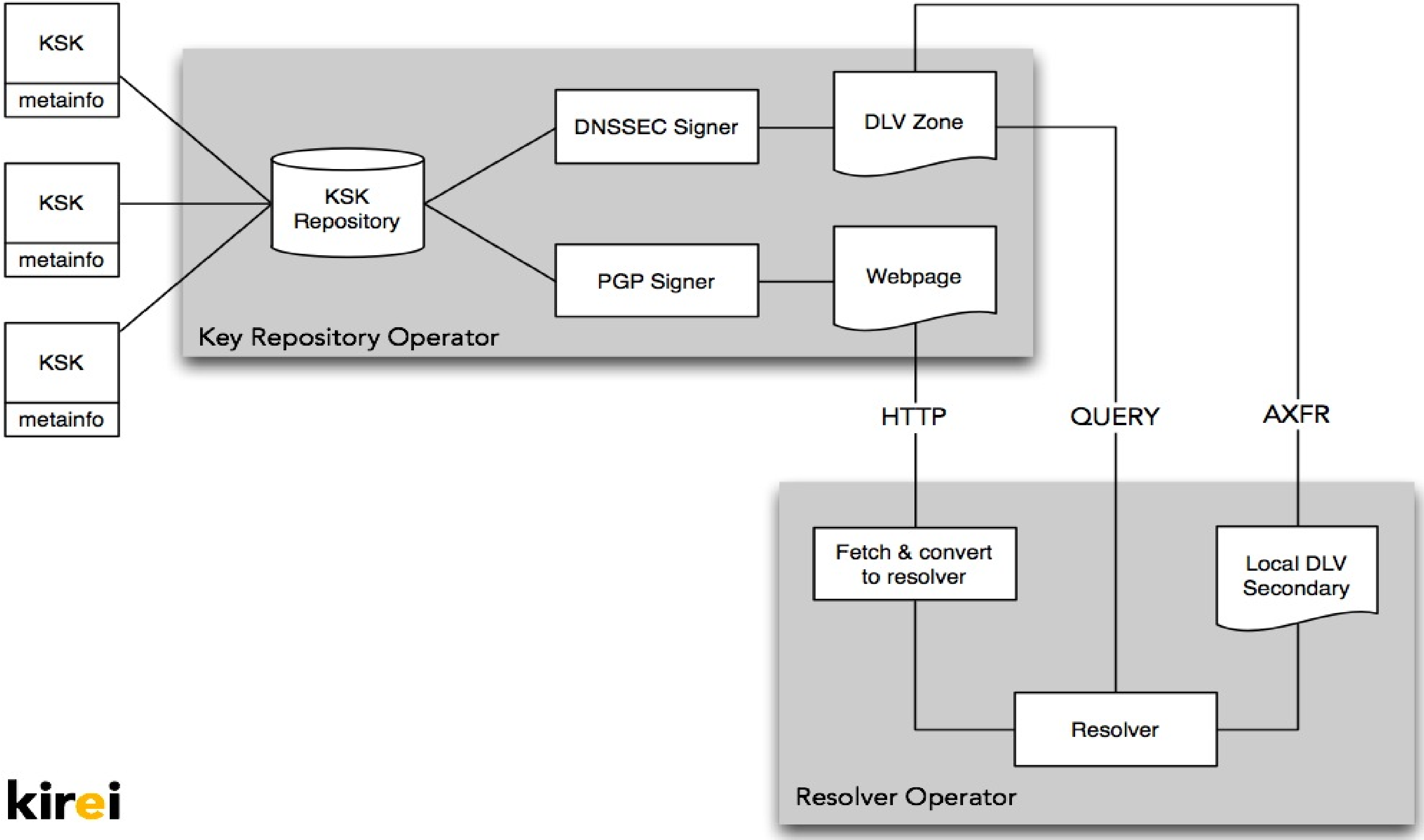
The limitations and the catch

- DNSsec resolvning requires a trust anchor to work. TeliaSonera Sweden will use the .SE public key as a 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, e.g. web sites and ftp archives.

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 a separated DNSsec trust anchor



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

What should the trust anchor contain?

- The trust anchor should be a replacement for the root zone until it has been signed.
  - It should contain what the root zone could contain, i.e. the keys of the TLD zones.
  - It could also contain DNSsec keys for highest level reverse zones
- The trust anchor should not be a commercial service to the public or to the industry.
  - It should not contain keys that naturally belong to other TLD’s.
- The trust anchor must only contain keys to TLD’s where the TLD Registry has signed an agreement to keep the trust anchor updated with new keys etc.

Key repository operator requirements

- The key repository operator
  - Must be internationally accepted.
  - Must be trustworthy.
  - Must have very good insight in the various TLD registries.
  - Must be an open organization.
  - Must not have commercial interests that conflicts with the role.

Key repository operator candidate

- RIPE NCC meets the requirements for being a repository operator of a single trust anchor. Together with the TLD registries that have signed their TLD zone, RIPE could create a strong trust anchor while waiting for ICANN and others to come to decision.

Why should RIPE take the role?

- RIPE’s members are ISP’s that will run into the problem of handling multiple trust anchors or stick to a few. I.e. it is in the interest of RIPE members that RIPE runs the service.
- RIPE will contribute to the development of a more secure Internet.
- RIPE will strengthen its reputation as an important player on the public Internet.
- RIPE already has good contact with several TLD’s.
- The reverse zones that RIPE already has signed will be used ”in production”.

Proposal

- TeliaSonera proposes that RIPE NCC investigates the possibilities of hosting a DNSsec trust anchor.
- We also propose that RIPE invites the registries of the signed TLD’s for a discussion.

Contact information

- Postal: Mats Dufberg, TeliaSonera Sverige AB, SE-123 86 Farsta, Sweden

- Email: mats.dufberg@teliasonera.com

- Mobile: +46-70-2582588

TeliaSonera