
TeliaSonera

Resolving DNSsec

Operational experiences from an ISP perspective

Mats Dufberg
TeliaSonera, mats.dufberg@teliasonera.com
2008-Oct-20

What I will present:

- I will present the experience that we have acheived since TeliaSonera started the prepartion for DNSsec enabled DNS resolving in the beginning of 2007.
- Our experience now include 16 months of DNSsec resolving in real production environment.
- I will also highlight the possible obstacles and problems that you might meet when turning DNSsec on.

What is TeliaSonera?

- TeliaSonera operates in multiple countries with IP backbones in Scandinavia, Europe and the US.
- TeliaSonera Sweden is the major telecommunication company in Sweden with fixed telephony, mobile telephony, leased line connections, broadband services and dial-up services.
- TeliaSonera Sweden has 1.5 to 2 million customers using IP connection through its backbone.

DNS resolving

- TeliaSonera Sweden has one dedicated, redundant and distributed DNS resolving system for all customers:
  - Dial-up
  - Broadband
  - Fiber to the home
  - Corporate leased line (optional)
  - Mobile broadband
  - 3G/GPRS
- In total 1.5-2 million users depend on our DNS resolving system.
- We have multiple Intel based servers with Linux OS.
  - Server program is ISC Bind 9 – currently ver. 9.4.2-P2 built with full DNSsec support.

The effect of the user of the DNSsec resolving

- DNSsec resolving is backward compatible with DNS resolving.
- The user will not discover that the resolvers are DNSsec enabled unless the query has set the DNSsec flag.
  - Plain DNS queries will get plain DNS answers even if DNSsec validation has been done.
- We do not expect the users to discover any new behavior of DNS.

- This is good news!

What is required for DNSsec resolving?

- DNSsec compatible server program, e.g. ISC Bind 9.3 or higher.
  - There are other alternatives such as
    - Nominum CNS
    - NLnet Labs Unbound
- DNSsec validation must be enabled (in Bind).
  - Check your application if validation is enabled by default.
- Select what zone (domain) or zones (domains) to trust, .SE in our case.
  - For each zone, add a trust anchor.
    - Trust anchor is equal to the public KSK of the zone. Every KSK in the zone can be added as trust anchor.
    - Check your application for the format of the trust anchor.
  - If you trust a zone, you will automatically trust sub-zones with correct DNSsec delegation (DS record included).

Trust anchors are needed

- No validation is done for a zone if there is no trust anchor for that zone or its ancestor.
- When the root zone is signed, we could use the root zone KSK's as trust anchors and trust the entire, contiguous DNSsec space.
  - Other trust anchors might be needed if there is a gap in the DNSsec space.
- DNSsec resolver without trust anchor is just a plain DNS resolver!

Turning DNSsec resolving on

- In February 2007 .SE launched DNSsec as a service in production (and not just pilot testing).
- During spring 2007 we prepared for DNSsec and tested DNSsec resolving in our lab.
- Our support organization got training on what DNSsec adds.
- In June 2007 we turned DNSsec on in the DNS resolvers in our production environment for almost all our Swedish customers.
  - Bind version was 9.4.1.
  - The update to DNSsec was done stepwise over a few days.
  - The only trust anchor that is configured is the .SE key.
- Since June 2007 we have upgraded Bind a few times to meet bugs and vulnerabilities.
- The resolvers have run DNSsec enabled since June 2007.

DNSsec traffic

- How much traffic is effected by the DNSsec update? – Bind does not provide us with any measures, so we can only guess.
  - We could dump the traffic, but we have not.

- .SE is the major TLD for the Swedish user community. Even though there are still few DNSsec delegations, the .SE zone itself is signed.
  - Every query for a new domain will start the validation process.

- Validation does not require that the query ask for validation. Validation is based the existence of trust anchor and DS record in delegation.

Instability, bugs...

- Problems with DNS resolving are know. What can we expect from DNSsec resolving?
  - Everything that can happen with DNS resolving can happen with DNSsec resolving. Plus more.

- Areas that we should look at are:
  - Stability
  - Performance
  - Resource requirement
  - Support calls from users (customers)
  - Troubleshooting
  - Key management (trust anchors)

Stability

- DNSsec resolving uses code in Bind not else used.
  - Fewer can discover and report the bugs.
- DNSsec validation adds a complex step to the resolver process – more things that can go wrong.

- Bind 9.4.1 was unstable with DNSsec enabled.
  - Bind crashed too often.
  - No service effect due to redundancy
    - No reported customer complaint.
  - A patch solved the problem.

- This has been the only real instability so far, but we should expect DNSsec resolving to be less stable than plain DNS resolving.

Performance and resource requirements

- We have seen no effect on performance.
  - Such as the time it takes for the resolver to reply.
- We have not yet seen any increase in CPU or memory usage.
  - Any increase has been hidden by variation in CPU load and memory usage and by increased load.
- We do not know what resource requirements to expect in the future.
  - We expect future DNSsec resolving to require faster CPU's and more memory than plain DNS resolving.
  - We monitor resource usage on servers.

- By adopting early, we can slowly increase capacity to meet increased load of DNS and increased use of DNSsec.

Support calls from users and troubleshooting

- We have not seen any support calls from customers that can be related to DNSsec as such.
  - Some errors in DNSsec configuration will cause the zone (domain) be unavailable with DNSsec resolving but still available with plain DNS resolving.
- Those errors will come!

- Bad news is that troubleshooting is more complex...

Bugs in Bind and home gateways 1 (2)

- In September 2007 (3 months after start of DNSsec resolving) some TeliaSonera customers could not reach DNSsec enabled domains.
- gavle.se (domain for Town of Gävle in Sweden) was severely effected by the problem.
  - The domain was the first domain with broad public usage to be DNSsec enabled.
  - Users could not reach their home town web site, www.gavle.se.
- On the surface, the symptomes were the same as if the DNS servers of gavle.se were unavailable.

- Luckily the gavle.se staff suspected some DNSsec related problem and called the .SE staff for help!

Bugs in Bind and home gateways 2 (2)

- The problem only appeared when the user sat behind DNSsec resolving built on Bind 9.4.1-P1 (which was a new update).
  - Bind 9.4.1-P1 incorrectly enabled the AD flag (authenticated data) in the answer for validated domains, even if the DNSsec flag was not set in query (the AD flag should not be set).
  - Some home GW's refused to pass answers with the AD flag set for no good reason (they should should just ignore it).
- A quick patch from ISC and a rebuilt Bind solved the problem. – We were close to turning DNSsec resolving off!

- We were all surprised that some cheap consumer hardware could risk stopping the DNSsec deployment!
- There are reports available on the behavior of home GW's in an DNSsec environment.

Key management – managing trust anchors

- DNSsec resolving requires one or more trust anchors.
  - The trust anchor in the resolver is the public KSK of the zone (domain) to trust.

- Managing of the trust anchor is done outside DNS.
  - Adding a trust anchor for a new zone (domain).
  - Renewing a trust anchor.
  - Removing a trusted zone (removing the trust anchors of the zone).

- Until the root zone is signed we might have multiple zones to consider as trusted zones.

Adding a trust anchor

- Select zone (domain) to trust.
- Determine how to fetch the KSK or KSK's.
- Securely fetch the KSK.
- Configure the DNSsec resolver with the trust anchor.

- Now the resolver will validate queries on that domain and its DNSsec enabled subdomains!

Renewing the trust anchor

- DNS resolving can be left running by itself.
- DNSsec resolving requires that the trust anchor or trust anchors are updated.
  - The trust anchor in the resolver is the public KSK of the domain (zone) to trust.
  - Contrary to SSL certificates there is no built in last date of validity.
  - It is an administrative decision of the domain owner when to do a key roll-over.
    - We depend on announced roll-over dates.
  - When the KSK has been rolled over, the trust anchor must be updated.

Missing to renew a trust anchor

- If the trust anchors do not match the KSK's of the zone, the DNSsec resolver will refuse to return any data for that domain.
- Missed update will make that domain, and all its subdomains, unavailable!
  - We know, because we have been there!

- Make sure to have a process for renewals.

- Make sure to have tools for renewals.

Remove a trusted zone

- Removing a zone as trusted is simple: remove the trust anchors.
- If the renewal process for the zone does not work, removal could be the answer.

What the TLD's can do for key management

- Until root is signed we need the TLD KSK as trust anchor in the DNSsec resolver.
  - When root is signed you might still want trust anchors to some TLD's.
- The TLD can help make key management easier:
  - Have 2 KSK's with overlapping lifetime. .SE has a two-year lifetime of the two KSK's, and one of KSK's is renewed each year.
  - Publish its KSK key roll-over policy and procedures and follow them.
  - Do not invent the wheel again – reuse the same procedures as other TLD's if possible.
  - Be RFC 5011 compliant in the KSK roll-over.
    - RFC 5011: "Automated Updates of DNS Security (DNSSEC) Trust Anchors"

RFC 5011 – automatic renewal of trust anchors

- RFC 5011: ”Automated Updates of DNS Security (DNSSEC) Trust Anchors” Set by the IETF (proposed standard).
- Defines how to make trust anchor renewal automatic in a DNSsec resolver – if the TLD is compliant in its KSK roll-over.
  - Does not help how to insert initial trust anchor.
- It has not yet been implemented by any TLD (as far as I know).

Emergency KSK key roll-over

- Do not expect unplanned renewal of trust anchors due to emergency roll-over of KSK to be handle automatically.
- With many trust anchors the risk is higher that a needed emergency renewal is missed.
- This is an area that requires some additional planning and thoughts.
- If different TLD’s have similar procedure and cooperate we will probably see fewer missed emergency roll-over.

Signed root zone

- The DNSsec model assumes that the root zone is signed.
- When the root zone is signed we could concentrate on other issues instead of trying to find work arounds.

- A signed root zone will make life much easier for all DNSsec resolver operators.
  - We could be able to validate the entire, contiguous DNSsec space with one trust anchor.

…thanks


TeliaSonera