

Why DNSSEC?

Swedbank's experience

2007-03-28

Agenda

- Background
- Experiences from the implementation
- Apprehensions
- Roadmap

Background

Reasons and motivation of introduction of DNSSEC at Swedbank

- Necessary for Swedbank to be at the front edge when it comes to secure communication over Internet
- DNSSEC is one way to prevent Pharming and Phishing
- Increase the security when establishing sessions
- Makes it more difficult to manipulate DNS information/record
- We can see an increased threatening picture of targeting attacks to bank customers and their home computer environment

Test of DNSSEC at Swedbank

- To prevent production disturbance when testing DNSSEC, two new logical name servers was installed - one primary and one secondary.
- The domain dnssec-fsb.se was registered and delegated to the new name servers.
- The installation and configuration of the new servers was easy, because Swedbank already had a well-designed infrastructure of our Internet services. We have run our own DNS production for a long time..
- TSIG encryption was installed between the primry and secondary name server to secure zone transfers (Server Security)
- A pair of keys was created (ZSK and KSK). We used them to sign the zone dnssec-fsb.se. The public key KSK were after that distributed to .SE, to establish the chain between the domains .se and dnssec-fsb.se.

Observations after the technical installation

- The hardest part of the test implementation was understanding the key handling in DNSSEC
- It was easy to set up the DNSSEC test environment (when we understood the key handling)
- We are positive to DNSSEC!

Apprehensions

Estimated cost for technical DNS administrations

(cost for domain name administration are not included)

- DNS cost today: about 50 hour/year
- Estimated DNSSEC cost: half-time job/year
- DNSSEC demand more active service and management
- DNSSEC demand education of administrative personnel

Apprehensions

1. Historically, DNS operation has been an small cost for the bank.
With increasing administrations as a consequence of DNSSEC (key management, zone signing, handling resolvers etc.) the cost will increase if not good assistance tools or/and products are available.
2. Just now we only talking about .SE. How will we be effected when several top domains will be signed?
How will administration be effected from a higher perspective for a organisation?
Differents rules and regulations, differents administrations tools, differents identification demands for PKI Management etc.
3. Will the root domain "." ever be signed?
4. How will the increased securiness be presented in the browser for our customer?
For example: Customer visiting www.swedbank.se = safe
Customer visitng www.swedbank.com = unsafe

Will Microsoft and Mozilla implement a DNSSEC indicator in their browsers?

5. What happens when an observant customer visiting www.swedbank.com and notice that it doesn't use DNSSEC as www.swedbank.se and contact Customer Service Desk and ask how that come?
How do Swedbank inform our customer in the best way to avoid insecureness for the customer?
How do we explain that we continue to show information under .com when .se is more "secure"?

We also consider...?

- Will BankID (public Smartcard service in Sweden) be an identification method to use for logon to KEYMAN (.SE's interface for Key Management)
- It will be lots of identification methods signing serveral international zones

Roadmap

1. We are running DNSSEC test at the moment!
2. The ISP's must start.
We know that TeliaSonera will sign their zone in summer 2007
3. But it's not enough with one operator.
We hope that all the "Big 4" ISP in Sweden. .SE are working on it.
4. Roadmap for Swedbank and DNSSEC
 - April-07: Synchronizing meeting with three major Swedish banks about DNSSEC
 - April-07: Starting up DNSSEC project in Swedbank
 - Enable our two resolvers to DNSSEC
 - Set up a roll-out plan from DNS to DNSSEC
 - Educate and reorganize the production organisation for DNSSEC
 - Roll-Out starts Q1 2008

Questions?

Kjell Rydjer

Senior Security Architect

Swedbank / CIO Strategy and Architecture

kjell.rydjer@swedbank.se