Swedbank

DNSSEC from a bank perspektive

Swedbank's experience

2008-10-20

Kjell Rydjer
Senior Security Architect
Swedbank / CIO Strategy and Architecture
kjell.rydjer@swedbank.se

About Swedbank

Employees	22 215
Private customers	9,3 M
Corporate customers	531 600
Branches	913
ATM’s	2323
Cards	7.5 M

Geographical reach June 2008

Sweden	
Population	9.2 M
Employees	8,635
Private customers	4.1 M
Of which Internet customers	*2.4 M*
Corporate customers	282000
Of which Internet customers	*223 000*
Branches	436
ATM´s	863
Cards	3.6 M

Estonia	
Population	1.3 M
Employees	3,346
Private customers	1.2 M
Of which Internet customers	*0.9 M*
Corporate customers	91,000
Branches	87
ATM´s	560
Cards	1.2 M

Latvia	
Population	2.3 M
Employees	2,659
Private customers	0.9 M
Of which Internet customers	*0.7 M*
Corporate customers	57,000
Branches	74
ATM´s	332
Cards	0.9 M

Russia	
Population	142,1 M
Employees	475
Private customers	2 800
Corporate customers	600
Branches*	3
ATM's	9

*St Petersburg, Moscow and Kaliningrad

Lithuania	
Population	3.4 M
Employees	3 237
Private customers	3.0 M
Of which Internet customers	*1.0 M*
Corporate customers	80,000
Branches	123
ATM´s	395
Cards	1.4 M

Ukraine	
Population	46.2 M
Employees	3 481
Private customers	0.2 M
Corporate customers	21,000
Branches	190
ATM´s	164
Cards	0.4 M

Background

- Swedbank have tested DNSSEC since January 2006
- DNSSEC collaboration with other Swedish banks since May 2007
  - Handelsbanken, SEB and Nordea
- Postponed early plan to use DNSSEC in production Q4 2007
  - SOHO router bug

Test of DNSSEC at Swedbank (Jan 2006)

- Two new DNS-servers
  - To prevent production disturbance when testing DNSSEC, two new logical name servers was installed - one primary and one secondary.
- dnssec-fsb.se
  - The domain dnssec-fsb.se was registered and delegated to the new name servers.
- Easy installation
  - 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
  - TSIG encryption was installed between the primary and secondary name server to secure zone transfers (Server Security)
- Singning the zone
  - 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.

Swedbank

Observations after the technical installation

- Attend a DNSSEC course before the test
- It’s a advantage to have experience of PKI before start testing
  - 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)
- Lack of DNS administration tools
- Total calendar time for test installation = 2-3 weeks (for one person)

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

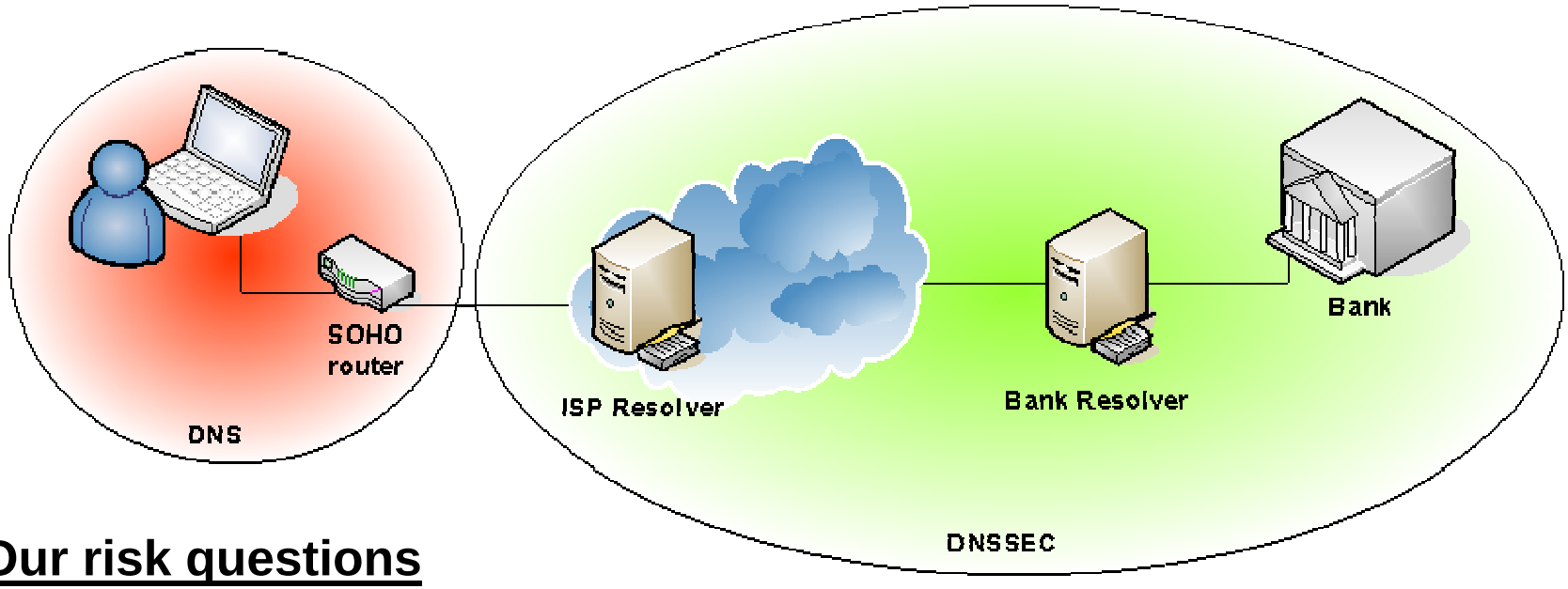
…some apprehensions

- Tools
  - Historically, DNS operation has been an small cost for the bank.
    With increasing administrations as a consequence of DNSSEC (key management, zone signing, handling revolvers etc.) the cost will increase if not good assistance tools or/and products are available.
- Different zones
  - Just now we only talking about .SE.
    What will happened when several top domains will be signed?
    How will administration be effected by different routines for different zones?
    - different rules and regulations in different countries?
    - different administrations tools
    - different identification demands for PKI Management etc.?
- Will the root domain ”.” ever be signed?

DNSSEC collaboration with other Swedish banks

- Vision = BIG4
  - Four biggest banks and four biggest ISP supporting DNSSEC
- Started in May 2007
- Attendes
  - Swedbank, Handelsbanken, SEB, Nordea and .SE
  - Together we four banks have 6 million internet bank customers
- Sharing experiences
- Discussed risks
- Technical workshops with DNS administrators
  - Project leader from .SE
  - Written white paper about how to set up DNSSEC
- Develop management tool
- Early plan: All four banks using DNSSEC in production Q2 2008

The DNSSEC bugg in SOHO routers



Our risk questions

- What will happen if the client start using DNSSEC?
- Do we think that the end user can upgrade firmware in SOHO routers?
- Must we wait for new SOHO routers?
- What is our risk to be exposure of the Kaminskys DNS flaw
- Will we take a chance?

How to implement DNSSEC

1. The country top domain must sign their zone (e.g. .SE)
2. Encourage the biggest ISP:s to sign their zones
3. Then the companies and public authorities
   - protection against fraud attacks
   - high demands of availability
4. In the end the clients

Potentials obstacles:

SW and HW not supporting DNSSEC

Swedbank

What's next?

1. Must handle the SOHO router bug
2. Stressed by Kaminskys findings about DNS flaw (DNSSEC seems to be the answer)
3. Sign Root "." for DNSSEC
4. Sign .COM for DNSSEC

Swedbank

Questions ?

Kjell Rydjer
Swedbank AB (publ)
Senior Security Architect
Mobile: +46 70 2196770
E-mail: kjell.rydjer@swedbank.se