OpenDNSSEC at .SE

Rickard Bellgrim

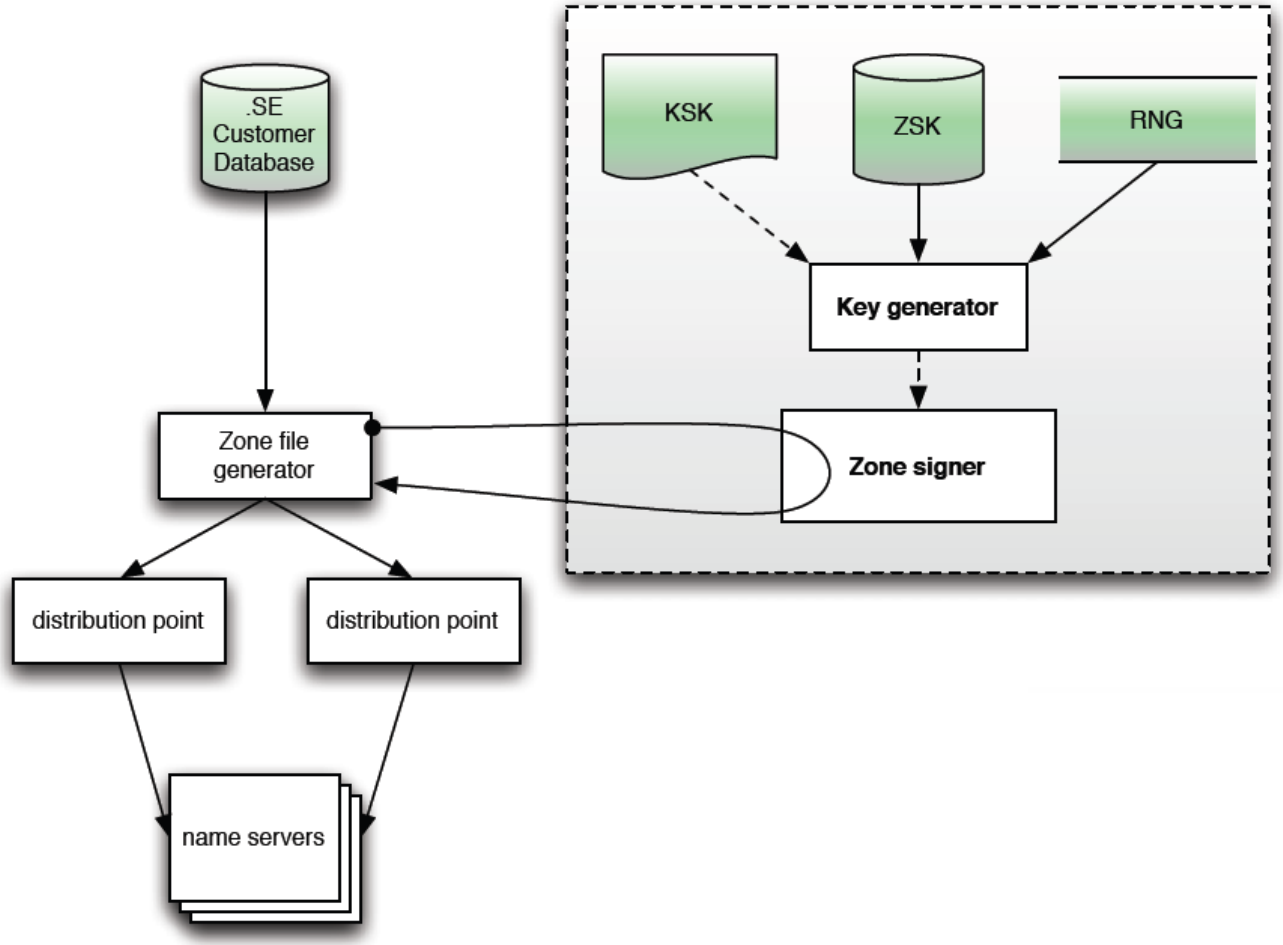
.se

Overview

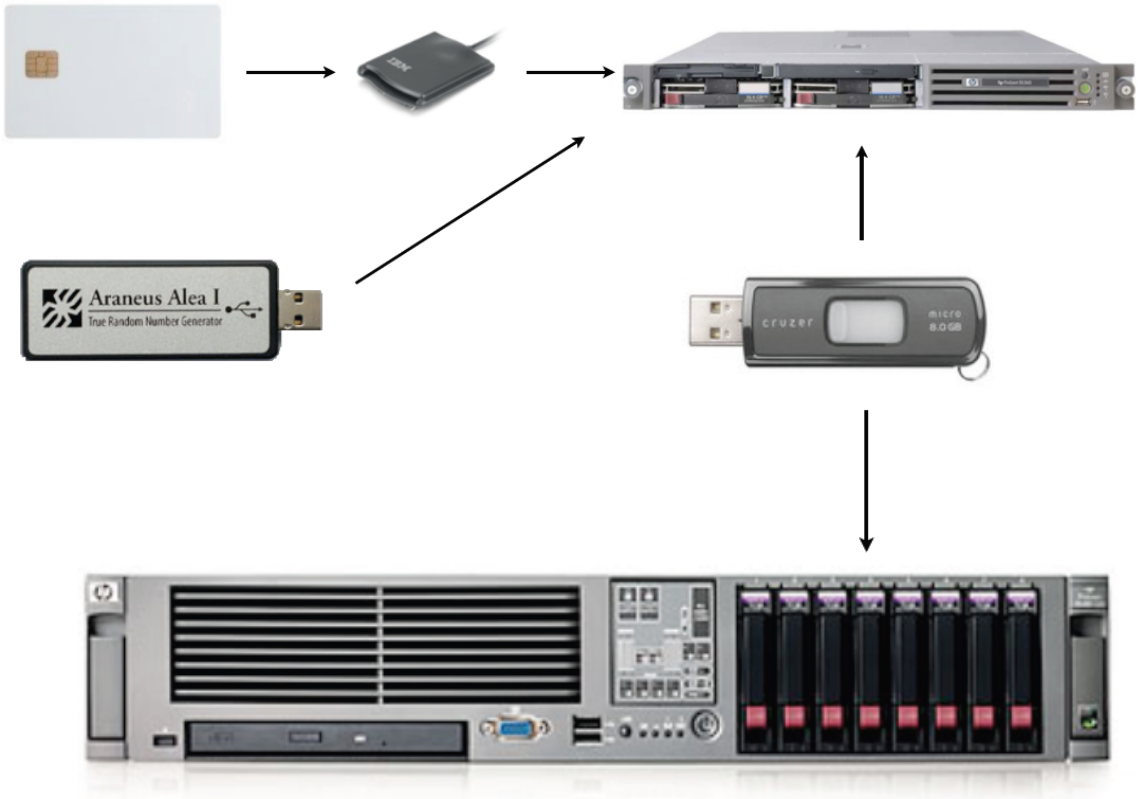
- Have been using DNSSEC since 2005
- Now replacing the system with OpenDNSSEC
- Will give us:
  - A faster system
  - Better documented
  - More knowledge about DNSSEC
  - Less administration

.se

The old system

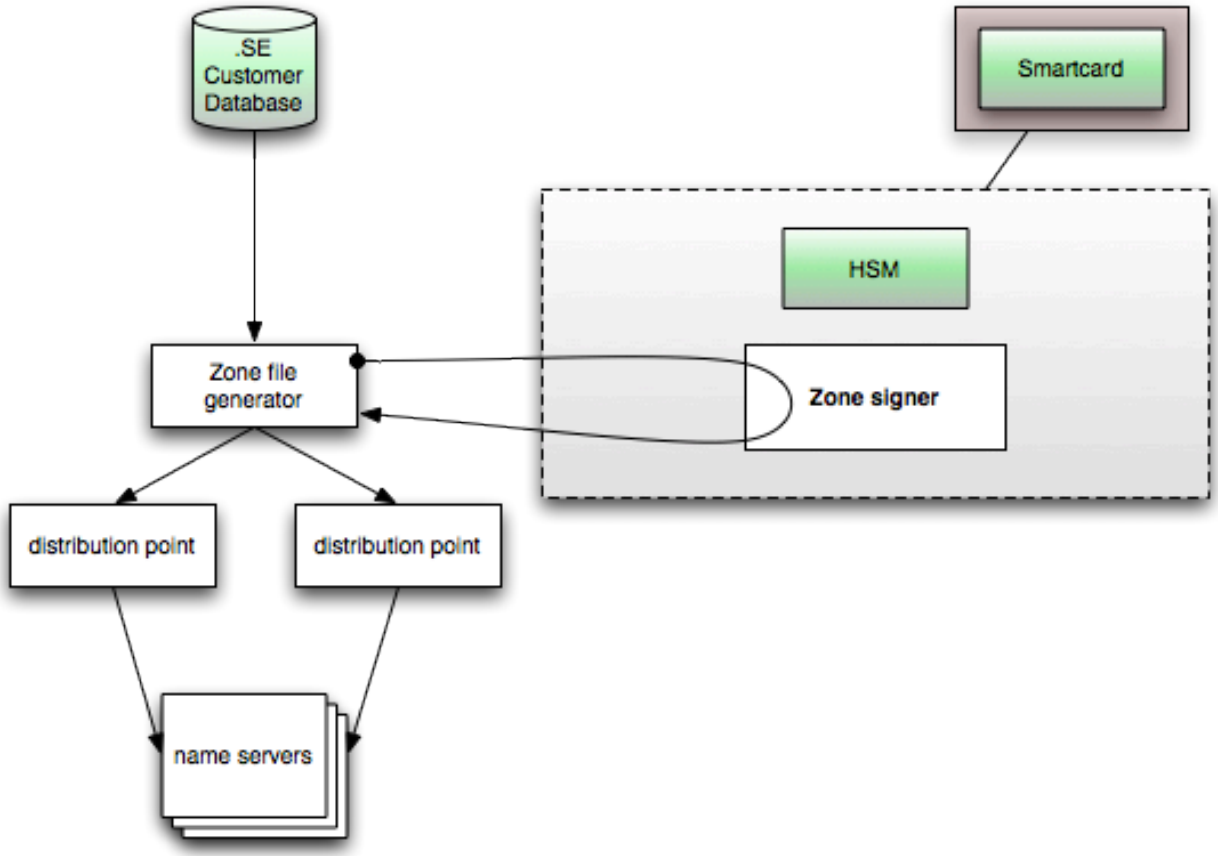


The old system



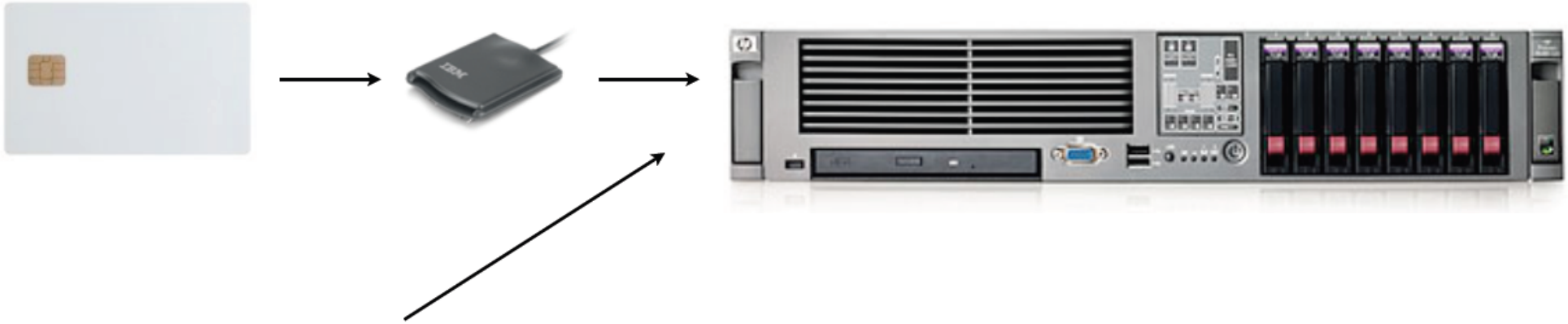
.se

The new system



.se

The new system



The new system

- Old KSK is on a smartcard, but will be replaced by the end of the year. Stored in a safe.
- New keys are stored in an HSM
  - SCA 6000
- The keys are now always online

.se

SCA 6000
Sun Crypto Accelerator 6000

Interface	PCI-Express x8
Certification	FIPS 140-2 level 3
Performance (RSA-1024)	13,000 sign/s
System support	Solaris, RHEL, SUSE
Price	$ 1,350

.se

Interface

- The server fetch and deliver the zone file using SCP
- Using cronjobs to trigger the events
- New overlapping KSK is introduced in the beginning of each year
- The key is manually extracted

Backup

- No need to continuously do backup of the keys
  - Pre-generated keys for 10 years
- We only need to synchronize the KASP database to the standby site

.se

Preparations

- September-November 2009
  - System testing
- December 2009
  - Create the acceptance tests
  - Educate the staff
- January 2010
  - Handling of the project risks
  - Tests of the deployment plan
  - Educate the staff

.se

Preparations

- February-March
  - Acceptance testing
  - Educate the staff
- 30 March
  - Is the system accepted?
- 9 April
  - Remind externally about the deployment

Deployment

- Step 1: Move the keys
- Step 2: Sign and publish the zone
- Step 3: Add new KSK to the zone
- Step 4: Announce new KSK

.se

Step 1 - Move the keys

- 13 April
- Move/copy old KSK+ZSK
- Pre-generate keys for 10 years
- Create the Security Officers

.se

Step 2 - Sign and publish the zone

- 19 April
- Run the zone generation and signing manually
- Test and verify on each step
- New signatures are created
- Publish the zone

Step 3 - Add new KSK to the zone

- 26 April
- Mark one of the pre-generated keys as the new KSK
- We use overlapping KSKs
- Included in the zone file

Step 4 - Announce new KSK

- 3 May
- First automatic ZSK rollover
- Send the public KSK to ITAR
- Recommend it as a Trust Anchor

.se

If something went wrong

- The old signer could be started again
- We have extra check before the zone is sent out
- Point of no return – when we added new KSK
  - It is the HSM and cannot be moved into a smartcard
  - Why can't it be thrown away? Someone might use it.

.se

Summery

- OpenDNSSEC has now successfully replace our old server
- First automatic ZSK rollover on Monday
- Announcing new TA on Monday

.se

Thank you

- Questions?

- rickard.bellgrim@iis.se