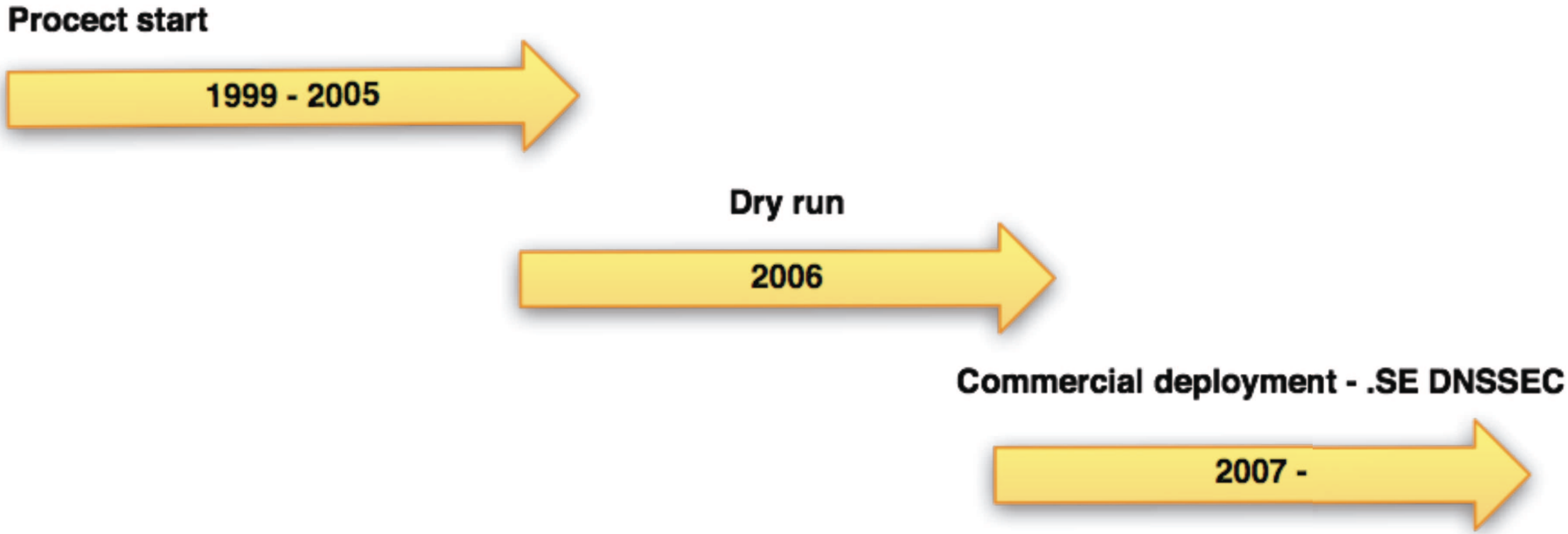
OpenDNSSEC

Patrik Wallström

Projektledare, FoU

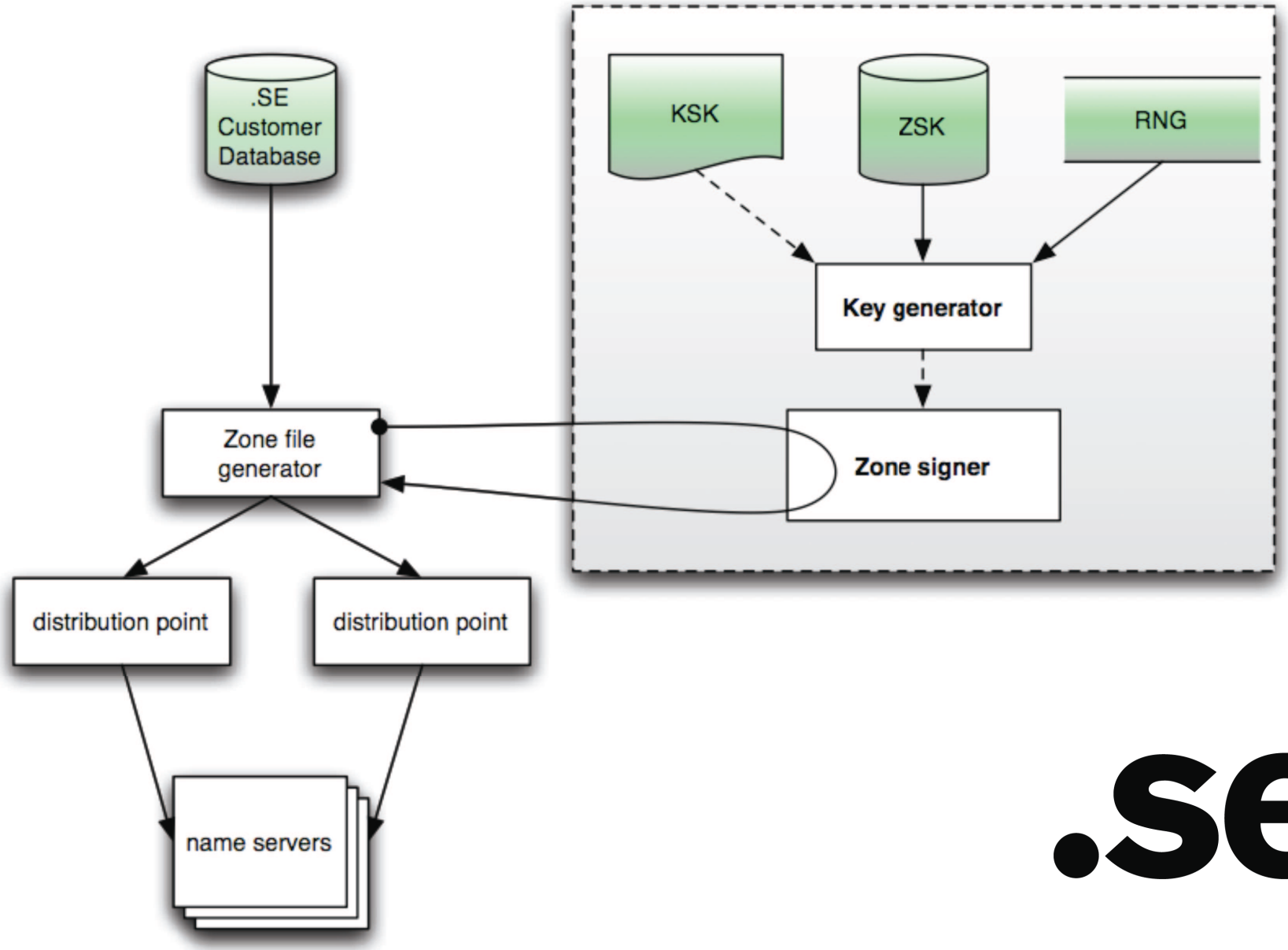
.se

.SE DNSSEC History

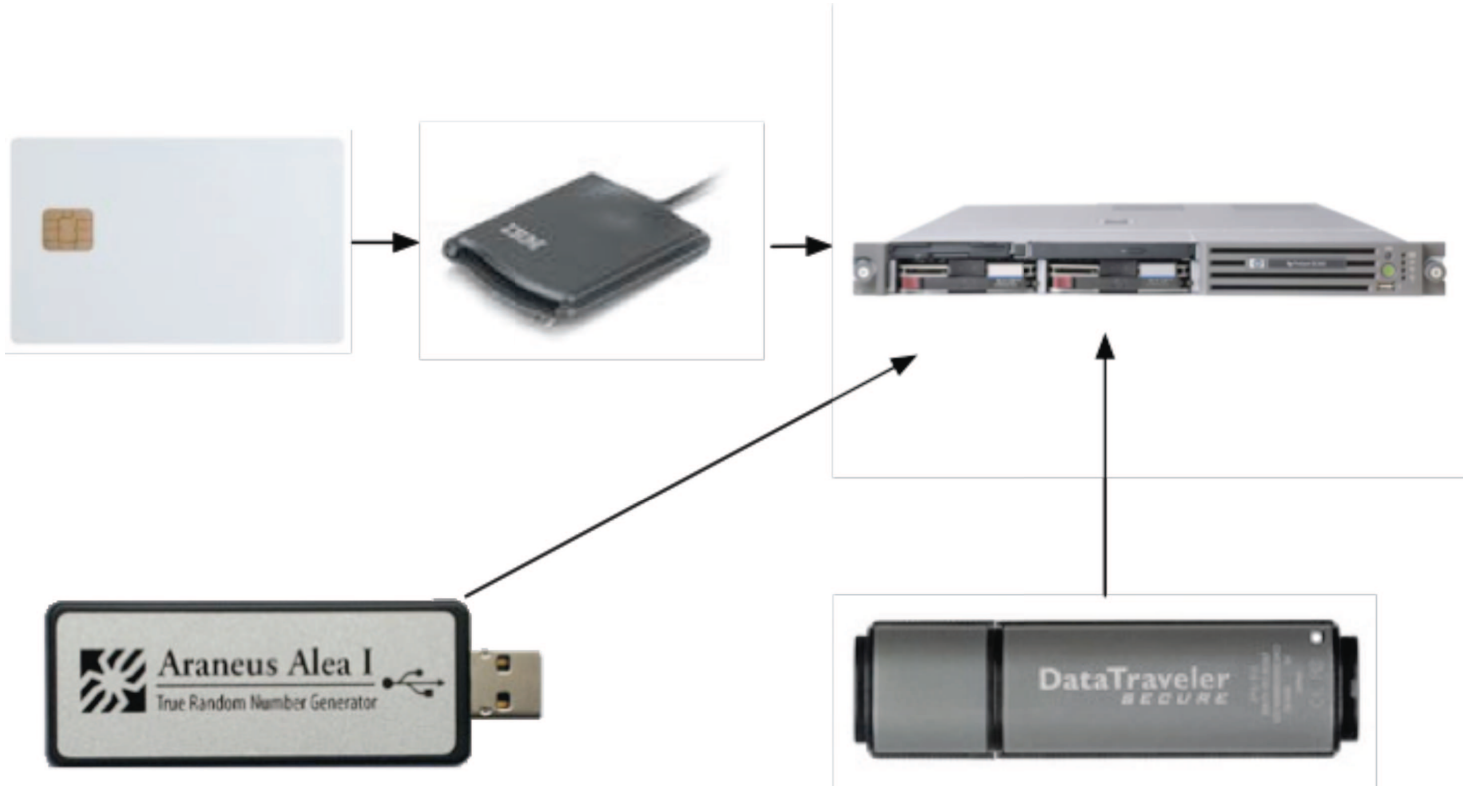


.se

The Current .SE System



DNSSEC Key Generator



.se

Some Considerations

All key operations are **manual**

- dependencies on people
- people are more prone to errors

Signing is done in software using ISC BIND

- no hardware crypto accelerators supported
- ... so signing is slow

Built for **one** zone only

- .SE have approximately 100 zones

.se

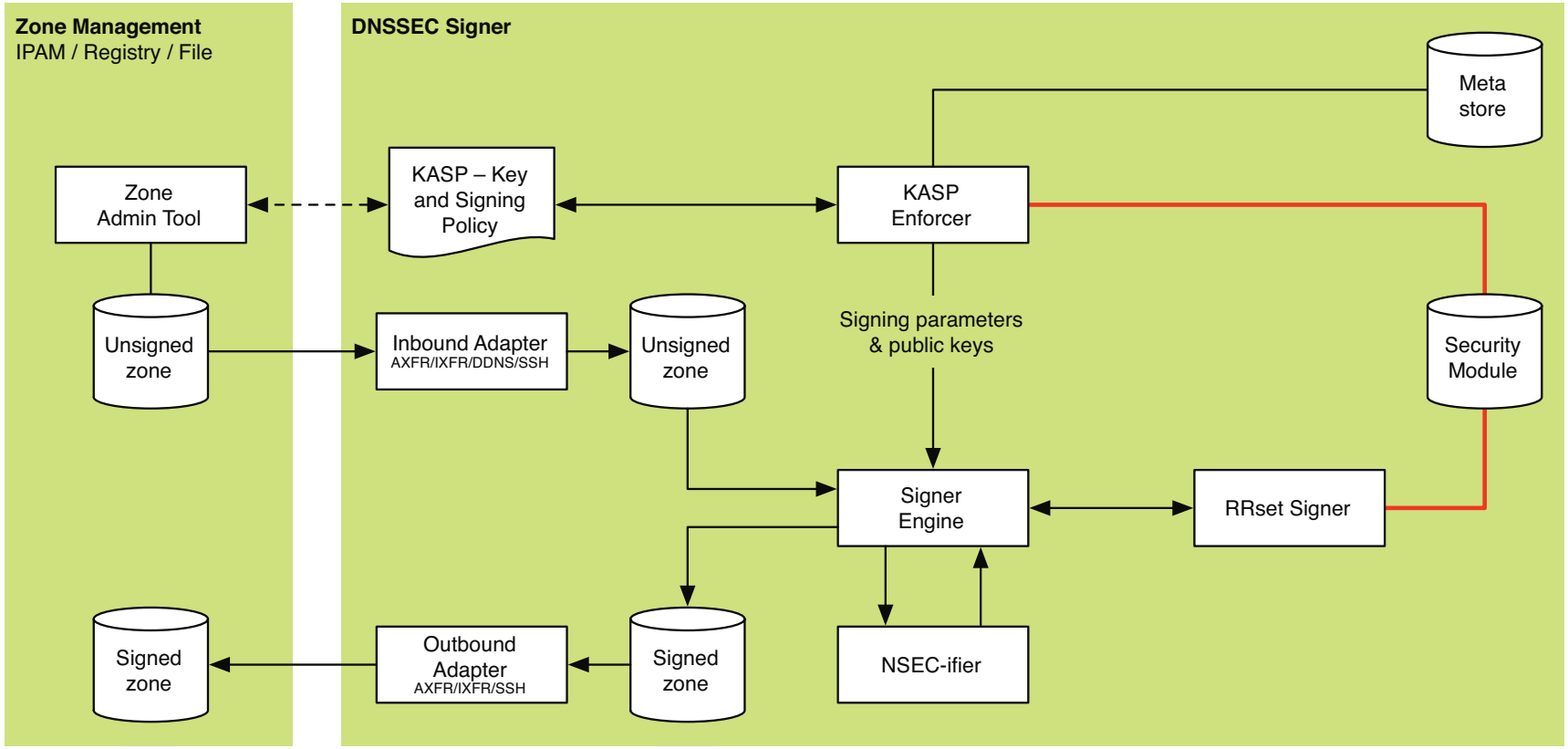
OpenDNSSEC

Is a collaboration between

- .SE
- Kirei AB
- John Dickinson
- NLNet Labs
- Nominet

.se

OpenDNSSEC architecture



.se

Using HSM

What is a HSM?

- Stores keys (master keys) in hardware
- Performs operations with those keys

Why use one?

- Security (FIPS)
  - Private key never allowed outside the HSM
  - You know where your keys are
- Performance
  1 – 14,000 signatures per second.

Are they expensive?

- $50 - $50,000

.se

KASP - Key and Signing Policy

Zone Signing Parameters

- Zone resigning interval (i.e. how often should we sign the zone)
- Signature refresh interval (i.e. how old are signatures before resigning them)
- Signature validity (i.e. for how long is the signatures valid)
  - Default validity
  - Signature for NSEC/NSEC3 validity (if not default)
- Signature jitter (Use jitter +/- for signature validity)
- Use RFC 5011 mechanism (yes/no)
- Clockskew (Maximum time discrepancy expected between resolvers and nameservers)
- TTL for RRSIG records
- TTL for DNSKEY records

- Also parameters for NSEC / NSEC3

.se

KASP - Key and Signing Policy

Key parameters for the zone

- KSK Algorithm
- KSK Length
- KSK Lifetime
- KSK Repository (e.g. what HSM/softtoken/...)
- KSK Overlap (number of simultaneus keys in use)

- ZSK Algorithm
- ZSK Length
- ZSK Lifetime
- ZSK Repository (e.g. what HSM/softtoken/...)

.se

KASP - Key and Signing Policy

The policy is stored as XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<signer-policy>
      <zone>
      <name>opendnssec.se</name>
        <signatures>
          <resign unit="hours">2</resign>
          <refresh unit="days">3</refresh>
...
```

API for r/w through SFTP over SSH or WebDAV over HTTP/HTTPS.

.se

Key Metastore

- Internal Key Identifier
- Zone
- Algorithm (RSA-SHA1, DSA, ECC, ...)
- Key Length
- Key Usage (KSK/ZSK)
- Key Flags
- Original Key Tag
- Revoke Key Tag (if revoked)
- Key Location Reference
  - Key Filename
  - OpenSSL EVP Key Reference
  - PKCS#11 URI
- Key State
- Timestamps
  - Key Generation
  - Key Published
  - Key Ready for use
  - Key Active
  - Key Retired
  - Removed
  - Revoked

.se

The KASP Enforcer

- Enforces the policy described by KASP
- Runs as daemon
- Ensures enough keys exist
- Removes old keys
- Ensures the signer is run as needed

.se

The Signer Engine

The signer engine is the core of this system. It drives the whole signing process by reading the KASP database and enforcing the policy KASP defines.

The Signer Engine is responsible for:
- resigning before signatures expires
- resigning when the keys have changed
- creating a new NSEC3 chain, update NSEC3PARAM, wait for distribution, remove old chain
- updating the SOA serial when changing keys

.se

The Signer Engine

- Logically separated
  - Signer
  - NSEC-ifier
  - RR-set signer
- NSECifier
  - Adds NSEC(3) RR's
- RRSet signer
  - Signs an RRSet
  - Talks to the keystore

.se

Inbound and Outbound adapters

Handles inbound and outbound zone data:

- Variety of mechanisms
- AXFR / IXFR
- svn
- files
- ssh
- database
- DDNS

.se

Openness

http://www.opendnssec.se/

.se

Thank you

patrik.wallstrom@iis.se