Six Months Later

RIPE'51

Jakob Schlyter

Nexus

September 13th 2005, NIC-SE started to distribute the signed .se zone.

Six months later is now.

Nexus

Key Management

- Hardware Random Number Generator for key generation
- Smartcards for KSK protection
- Protected server for ZSK protection

Nexus

Signing

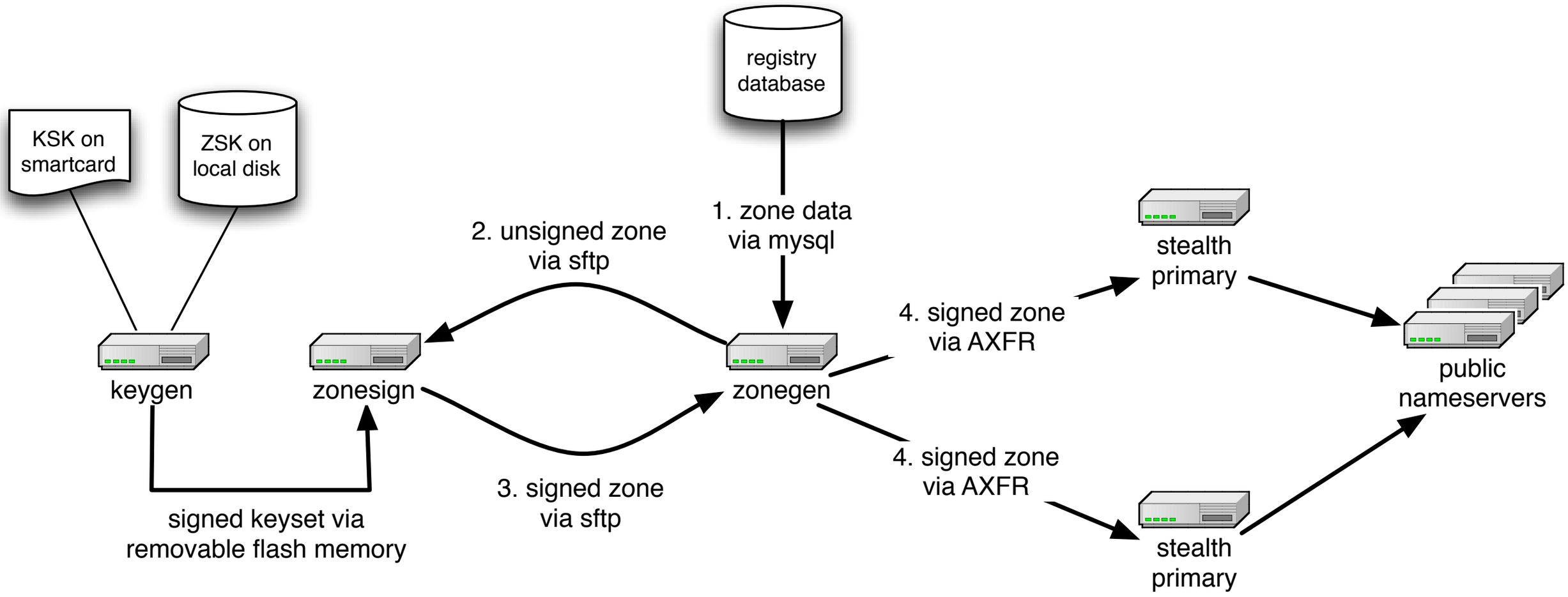
- The signer is placed between zone generator and distribution servers.
- Incremental signing using dnssec-signzone from ISC BIND.

Nexus

Distribution

- All .se name servers has been DNSSEC enabled since June 2005.
- Servers are running BIND or NSD on different platforms and operating systems.
- Initial distribution of the signed zone was carried out incrementally – one name server provider at a time was moved to the signed zone.

Dataflow Overview



Monitoring

- Nagios has been extended to perform basic DNSSEC checks
  - Warn for signatures soon to expire
  - Test for correct DNSSEC additional processing
  - Check the integrity of some signatures

Child DS Handling

- KEYMAN, presented at RIPE'48, will be introduced for early adopters Q4 2005.
- A future registry system will have more integrated DNSSEC support.

Documentation & Policy

- DNSSEC Policy and Practice Statement
- DNSSEC Limitation of Liability
- Deployment Information for other TLDs
- Internal technical and administrative documentation

Zone Walking

- The whois service for .se shows only registration status and delegation information.
- Extended information on domain names are only available via web and are protected by CAPTCHA.

Support Information

- Public mailing lists
- Basic configuration examples
- Public validating resolvers
  - ISC BIND
  - Nominum CNS

Lessons Learned

- Two issues came up just before deployment
  - Broken firewalls
  - Measuring deployment

Nexus

Firewalls & EDNS

- Some vendors ship firewalls that ignores the EDNS buffer size and drop packets longer than 512 bytes.
- Tests has shown that resolvers does timeout and turn EDNS off when this happens.
- DNSSEC users has to fix their firewalls or set the EDNS buffer size to 512 bytes.

Measuring Deployment

- The EDNS DO-bit is not very useful for measuring DNSSEC deployment:
  - BIND 9.0.0 - 9.2.1 always sets DO, but doesn't understand the response (and thus ignores it).
  - BIND 9.2.2 stopped setting DO.
  - BIND 9.3.x sets DO if configured to do DNSSEC.

Questions?

dnssec-info@nic.se

http://dnssec.nic.se/

Nexus