DNSSEC

Internetdagarna 2005

Jakob Schlyter

NIC-SE

Nexus

Vad har hänt sedan sist?

NIC-SE

Nexus

Nytt från IETF

- RFC 4033-4035 publicerades i mars 2005
- Utveckling av metoder för nyckelbyte
- Diskussioner kring driftrekommendationer
- Utveckling av NSEC3

Nytt från RIPE

- RIPE-359 (RIPE NCC DNSSEC Policy) publicerades i oktober 2005
- ripe.net signerad
- RIPE's zoner under in-addr.arpa signeras under hösten

Nyckelhantering

- Med hjälp av KEYMAN kan en DNS-operatör enkelt hantera sina nycklar hos NIC-SE.
- NIC-SE kommer att börja testa KEYMAN under november och december.

DNSSEC(.se) - Select Domain - Mozilla {Build ID: 2004042110}

https://dnssec.nic-se.se/keyman/auth/domains.html

Search

DNSSEC(.se)
Select Domain

Authenticated as jakob2.

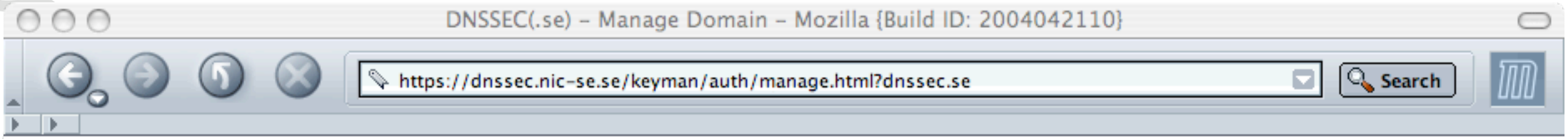
Please select domain to manage:

Domain	Secure	Last updated
dnssec.se	Yes	2004-04-27 10:10:28
xn--rksmrgs-5wao1o.se (räksmörgås.se)	No	

---

subjectName: /C=SE/CN=Jakob Schlyter/emailAddress=jakob@schlyter.se
issuerName: /C=SE/O=Schlyter/CN=Schlyter Root CA

Done



DNSSEC(.se)
Manage Domain

Authenticated as jakob2.

Help

Select active keys for **dnssec.se**:

Active	Algorithm	Fingerprint	Key Tag	Parent Status	Child Status
☐	RSA/SHA1	bad85b2fafee265c7fb24ac6aa2ec15e990df6cd	47940	Active since 2004-04-14 17:16:37	OK
☑	RSA/SHA1	5242b348e36954eca4c381e9078d17d74927d97c	38577	New	OK
☐	RSA/MD5	eda8e8cb20f58d7e774de0f424bed98d0044aa9b	38554	New	Unused
☐	RSA/DSA	24ad595dea4ec86c4fb3ccc53154da369a7a7048	57551	New	Unused

Submit New Active Keys Reset

Cancel Update

---

subjectName: /C=SE/CN=Jakob Schlyter/emailAddress=jakob@schlyter.se
issuerName: /C=SE/O=Schlyter/CN=Schlyter Root CA

DNSSEC(.se) - Confirm Update - Mozilla {Build ID: 2004042110}

https://dnssec.nic-se.se/keyman/auth/confirm.html

Search

DNSSEC(.se)
Confirm Update

Authenticated as jakob2.

Help

Confirm new active keys for **dnssec.se**:

Algorithm	Fingerprint	Key Tag	Parent Status	Child Status
RSA/SHA1	bad85b2fafee265c7fb24ac6aa2ec15e990df6cd	47940	Active since 2004-04-14 17:16:37	OK
RSA/SHA1	5242b348e36954eca4c381e9078d17d74927d97c	38577	New	OK

Notice:
Removed keys should be kept in child zone for at least (TTL of key + zone refresh time) seconds.

Confirm New Active Keys

Cancel Update

---

subjectName: /C=SE/CN=Jakob Schlyter/emailAddress=jakob@schlyter.se
issuerName: /C=SE/O=Schlyter/CN=Schlyter Root CA

Done

Nexus

Verifiering

- För att kunna verifiera posterna i .se behöver varje resolver känna till aktuell nyckel för .se.
- Nyckeln publiceras på webbplatsen http://dnssec.nic.se/ samt på sändlistan dnssec-announce@lists.nic.se.

Nexus

Hur gör man?

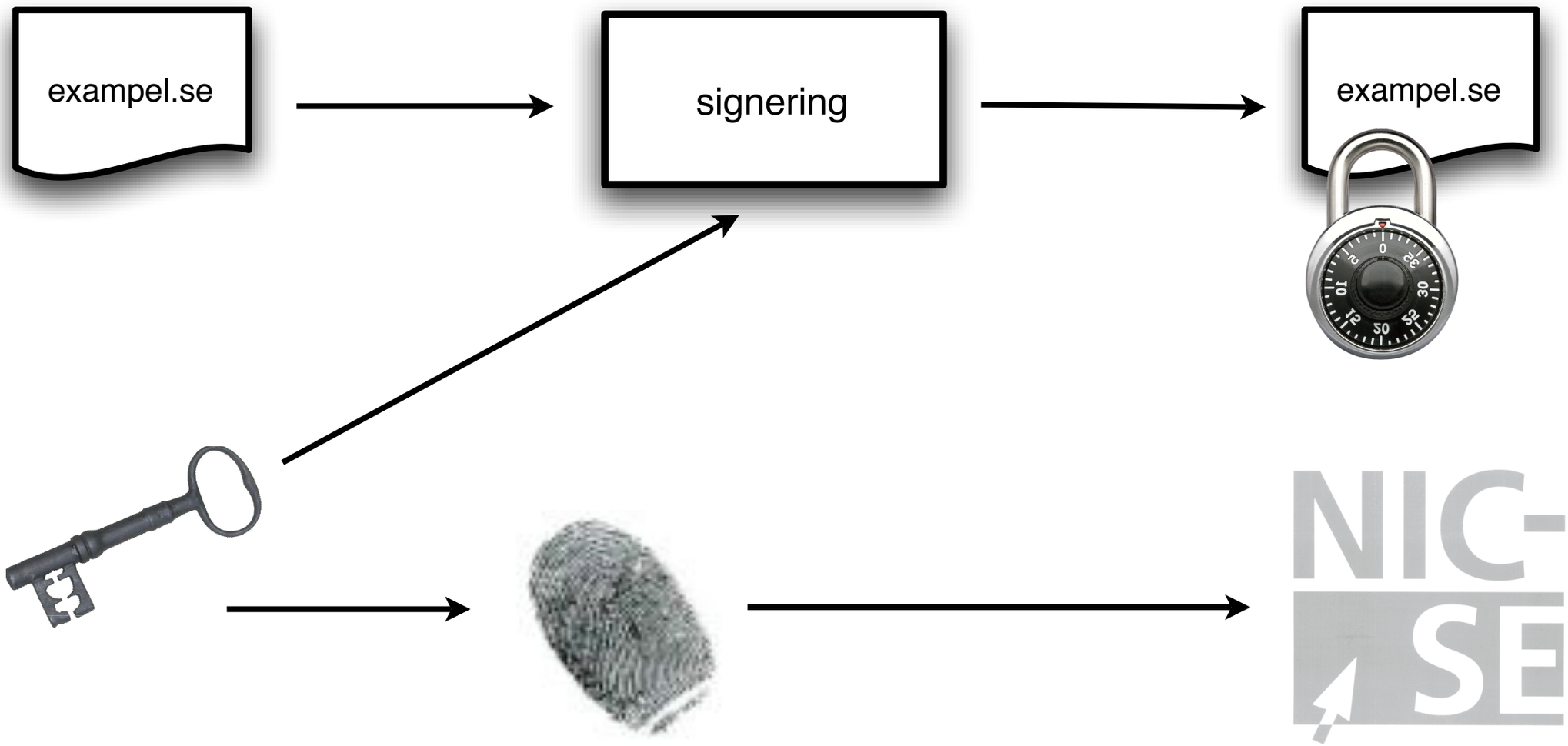
Nexus

Steg för steg

- Kontrollera att alla namnservrar för domänen hanterar DNSSEC.
- Signera zonen – glöm inte att detta är en återkommande process.
- Registrera nyckeln hos NIC-SE.

Nexus

Signering



Nexus

Programvara

Auktoritär	**Rekursiv**
ISC BIND	ISC BIND
Nominum ANS	Nominum CNS
NSD	

Nexus

Att tänka på ...

NIC-SE

Nexus

Kör inte BIND 8

Nexus

Kontrollera att eventuell brandvägg hanterar EDNS

Nexus

Skilj på auktoritära och rekursiva namnservrar

Nexus

Publika Namnservrar

- NIC-SE driver ett antal publika namn-servrar för dem som vill testa säkra namnuppslag:
  - bind.dnssec.se
  - cns.dnssec.se
- http://dnssec.nic.se/recursive/

Information

Meddelanden om viktiga förändringar

➡ **dnssec-announce@lists.nic.se**

Diskussionslista för användare

➡ **dnssec-users@lists.nic.se**

Prenumerera via http://lists.nic.se/

dnssec-info@nic.se

http://dnssec.nic.se/

Nexus