

DNSSEC

Administration, teknik och lite juridik

Ilja Hallberg <iha@regexp.se>

Jakob Schlyter <jakob@crt.se>

<http://www.sigz.net>

Varför DNSSEC?

- DNSSEC gör infrastrukturen för DNS säkrare. Risken för manipulation av namnuppslagningar minskar.
- DNSSEC använder DNS för distribution av kryptografiska nycklar och signaturer
- DNSSEC möjliggör flexibel infrastruktur för distribution av nycklar och certifikat till t.ex. IPSec, TLS/SSL, SSH, VPN osv.

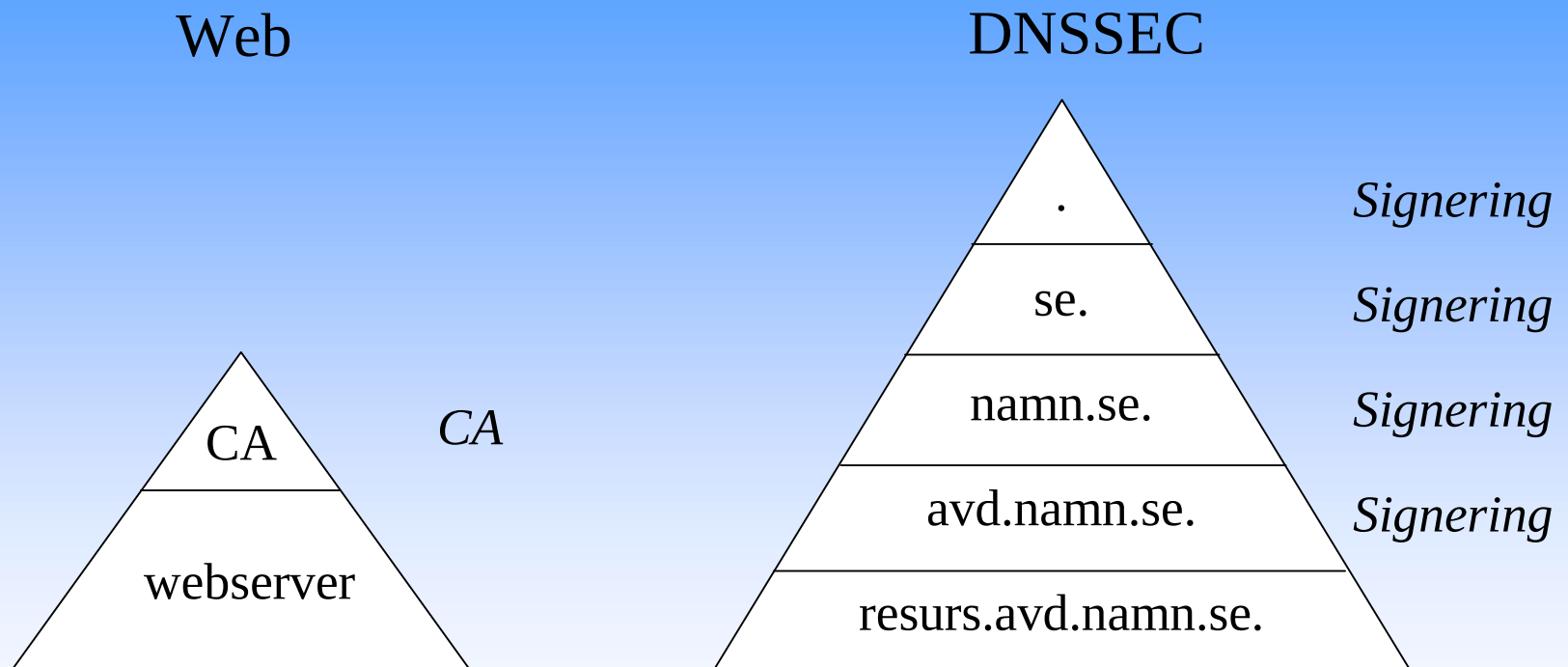
Varför DNSSEC?

- Andra säkerhetsarkitekturer behöver säkrare DNS
 - Både förfalskade certifikat och manipulerad DNS
 - Idap
 - SSL

HUR DNSSEC?

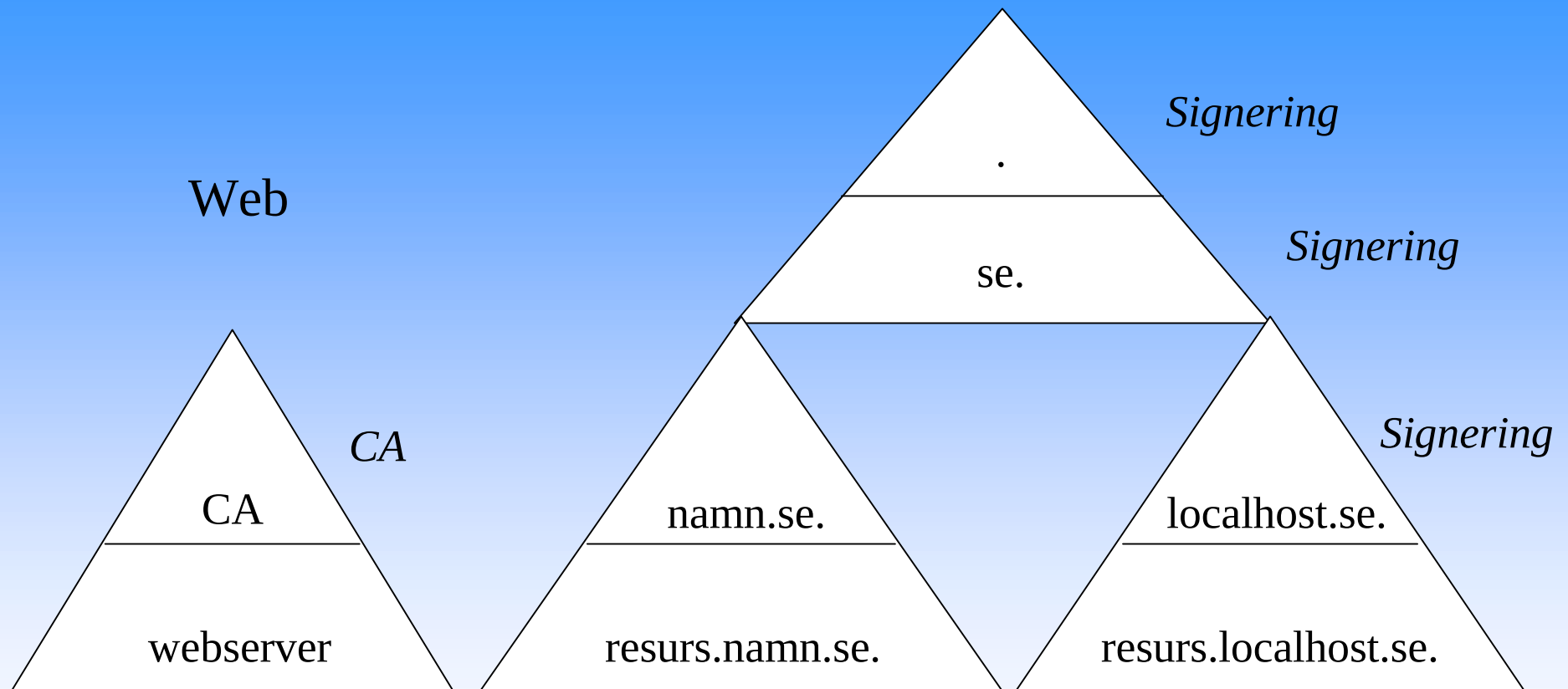
- Nyckelposter: KEY
- Signaturposter: SIG
- Icke-poster: NXT eller NO
- RSA, DSA, MD5, SHA

Flexibel hierarkisk struktur



Flexibel hierarkisk struktur

DNSSEC



DNSSEC nuvarande status

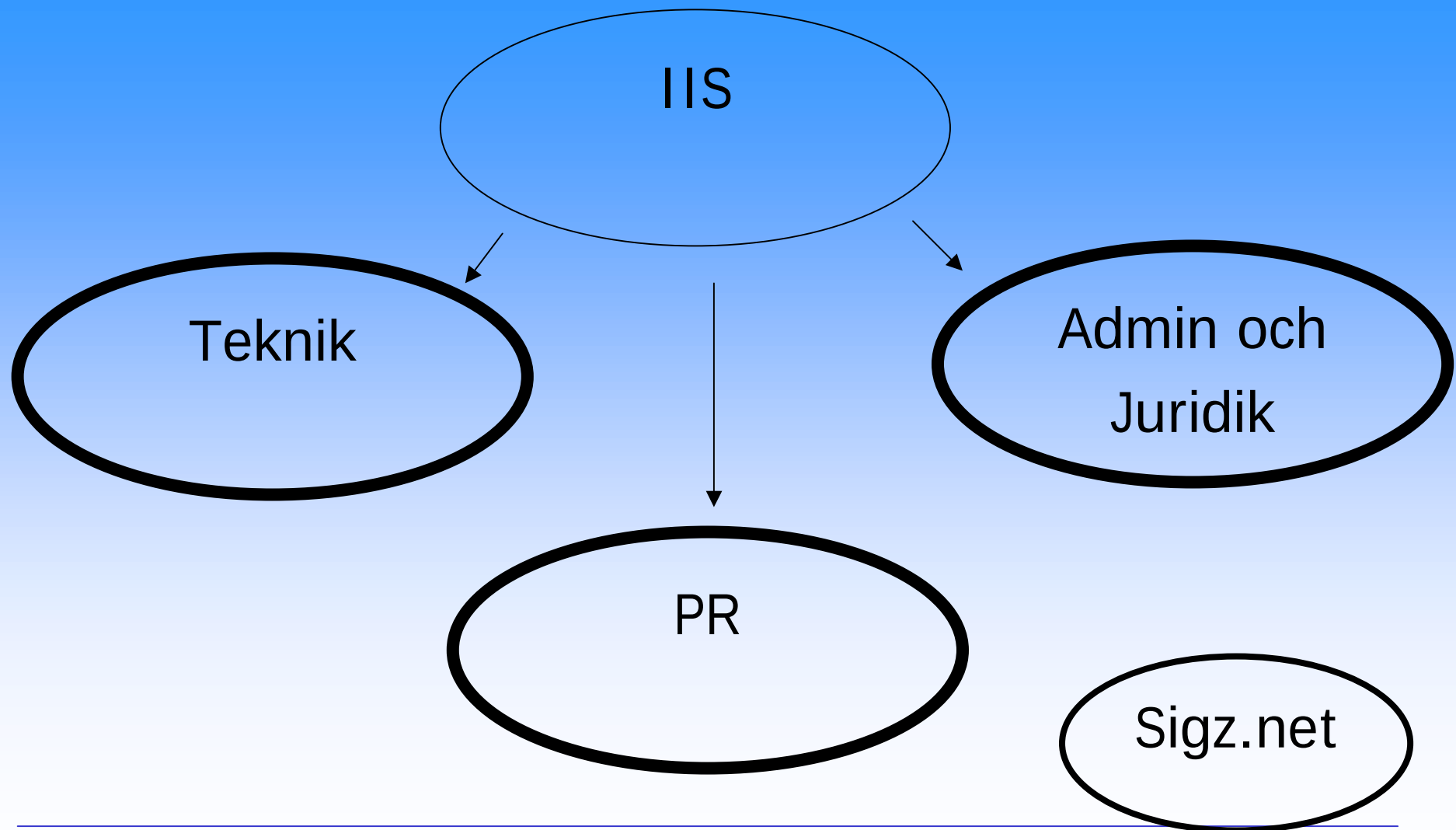
- The current collective wisdom is that DNSSEC is
 - 1) important
 - 2) a buzzword
 - 3) hard
 - 4) immature.

» Ed Lewis

Status i Sverige

- DNSSEC kommer att ta mer tid än vi tidigare trodde
- Vi tror fortfarande att DNSSEC är bra
- DNSSEC standardändringar: NXT och NO, nycklar och signaturer hos föräldrarn
- Insikt: envishet

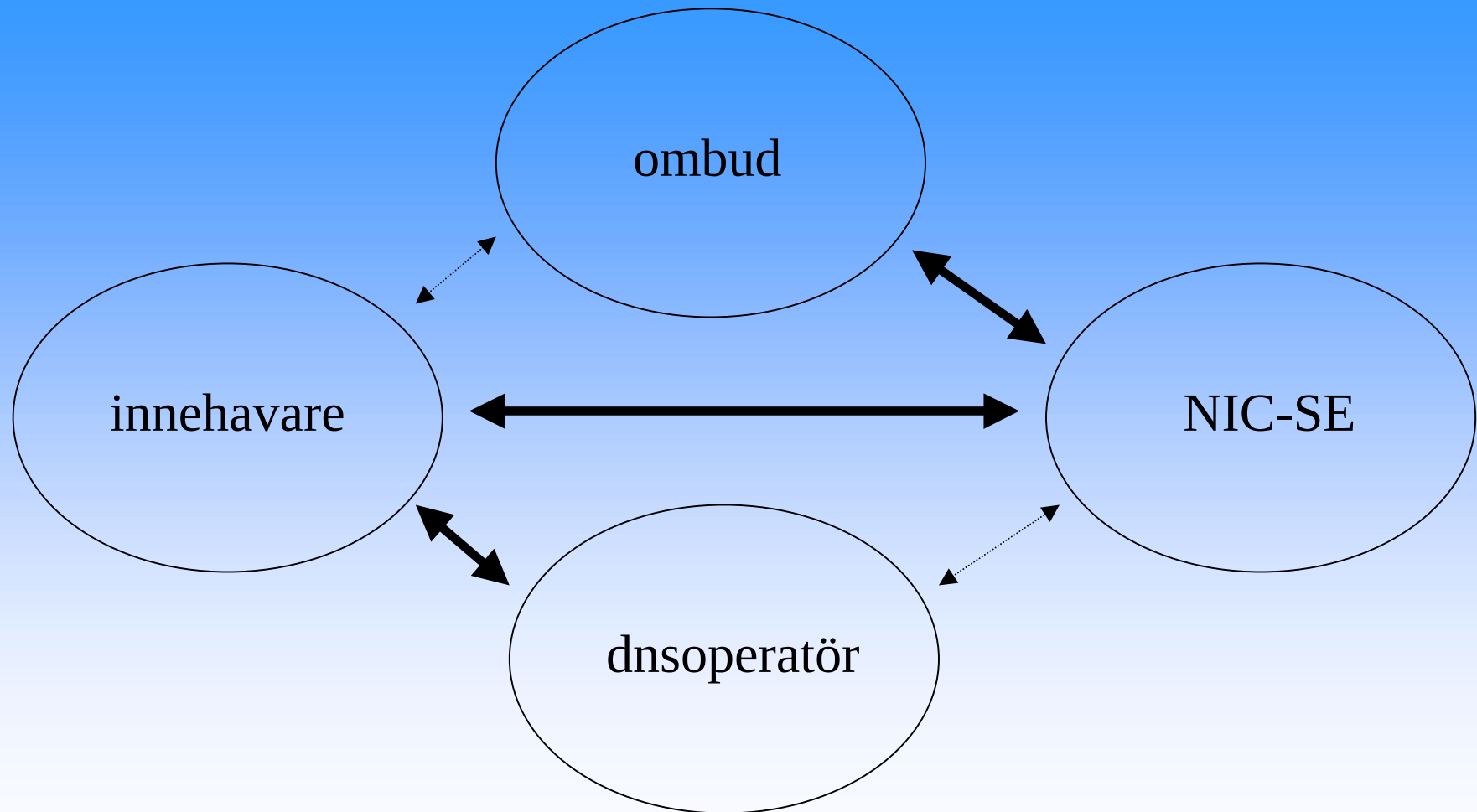
Hur arbetar vi i Sverige



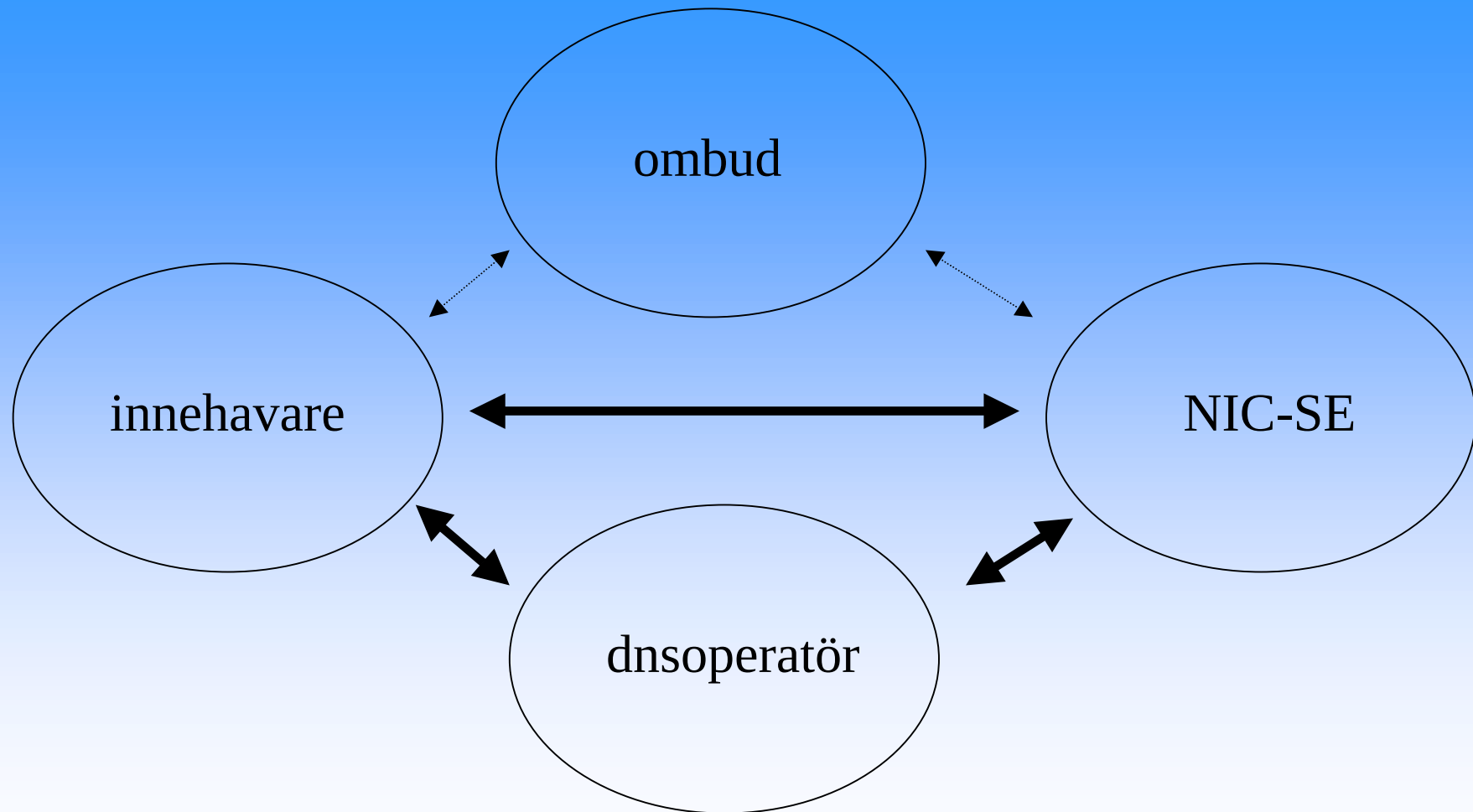
Problemlösning, abstraktionsnivåer

Administration, avtal, regler, juridik
DNSSEC, teknisk skötsel av zon
DNS och DNSSEC, protokoll och standard
Nätverk, datorer, backuper, etc.

Kontraktsförhållanden



Kommunikation



Juridik

- Konsumentlagstiftning
- Best effort och Non-performance
- Avtal: Rimligt skydd, rimliga förväntningar
 - Målgrupp och tillämplighet
 - Åtaganden
 - Ansvar
 - Finansiellt ansvar

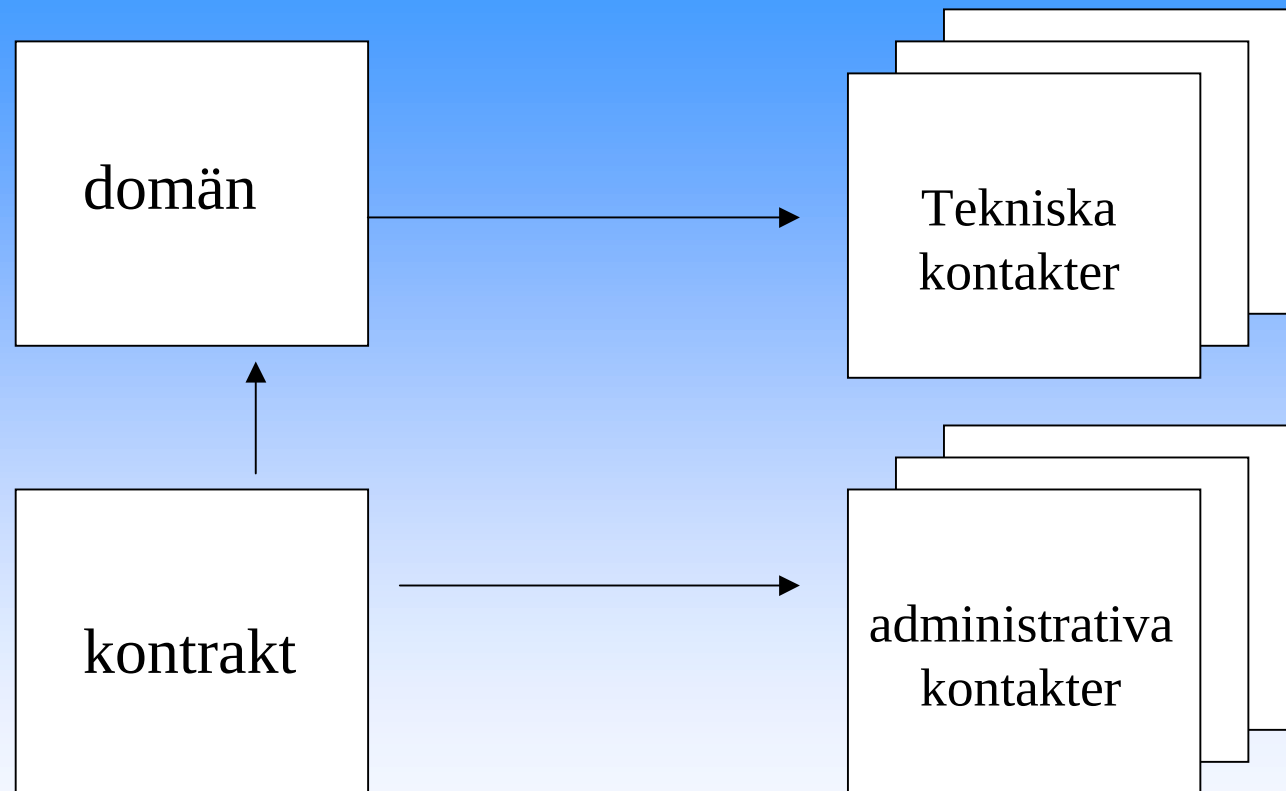
Administration

- Säkerhetsarkitektur, alla länkar i kedjan
- Automatisering
 - Autenticering
 - Roller: administrativa och tekniska kontakter
 - Ombud+ (superombud)
 - Dnsoperatörer
 - Webbgränssnitt och transaktionsgränssnitt

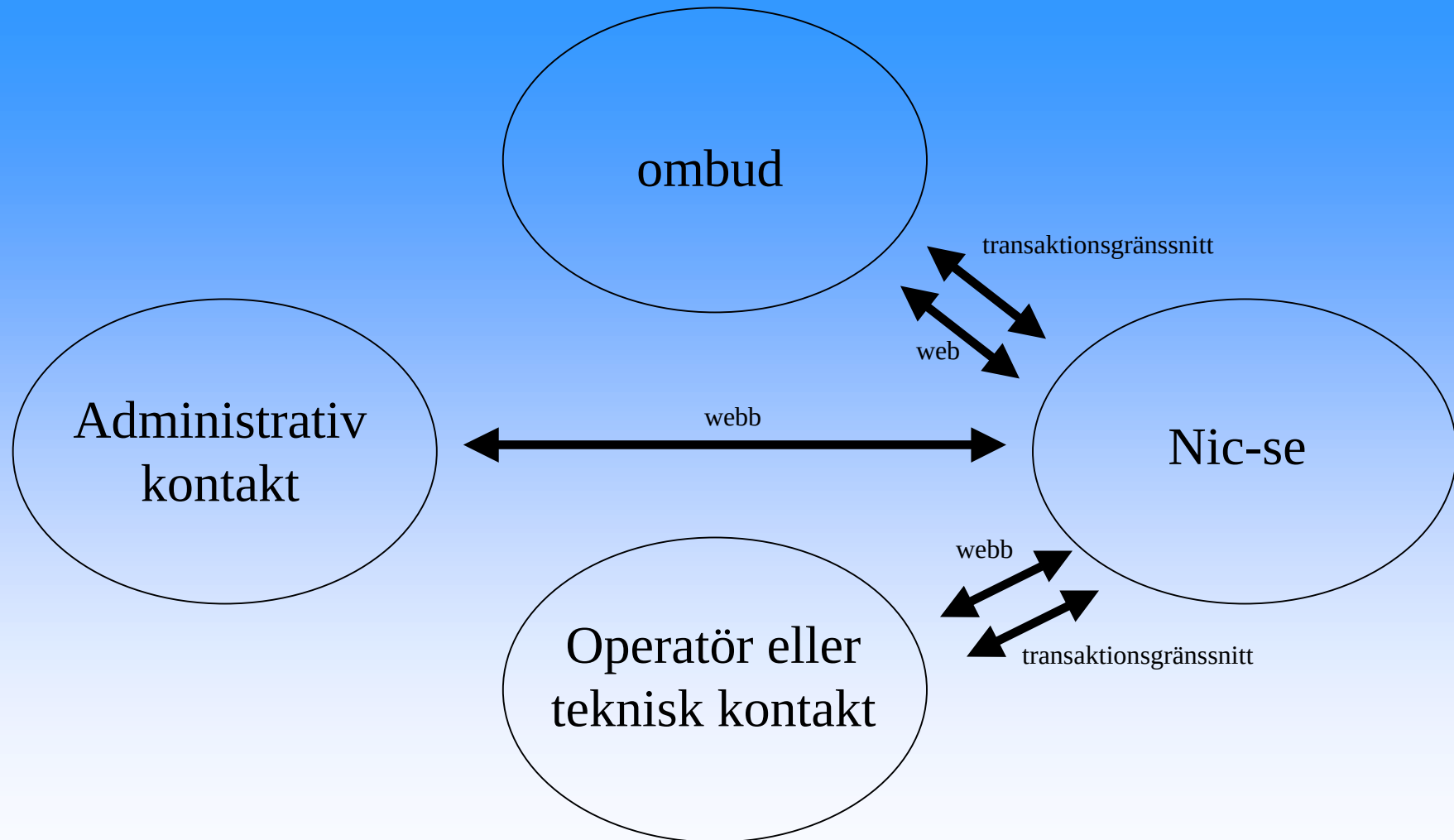
Autenticering

- Kontakter registrerar sig i NIC-SE:s databas
 - administrativ kontakt
 - teknisk kontakt
- Lösenord används i krypterade webbformulär eller transaktionsgränssnitt. Kanske pgp-krypterad epost. Självsignerade certifikat för kommunikation.

Roller



Förhållanden till databasen



Domäninnehavare

- Administrativ kontakt skapar sig i databas
- Välj ombud. Skriv kontrakt.
- Teknisk kontakt skapar sig i databasen
- Administrativ kontakt kontrollerar administrativa kontakter och tekniska kontakter i databasen
- Tekniska kontakter kontrollerar domänen

Ombud

- Tar hand om registrering, kontrakt
- Verifierar företags eller persons identitet
- Skapar domänen i databasen, lägger till administrativ kontakt
- Kan agera administrativ kontakt för innehavaren?
- Mer kontakt med innehavaren
- Transaktionsgränssnitt och ombudskontakt
- Omstart av säkerhetsrutinen för domän

Operatör

- Avtal med NIC-SE
- Registrerar tekniska kontakter
- Skriver driftavtal med domäninnehavare
- Får tillgång till transaktionsgränssnitt och operatörskontakt (dvs. grupper)
- Hanterar teknisk data för domänen

Svårigheter vid genomförande

- Förlorade lösenord
- Förlorade fysiska personer
- Separata verifieringskanaler för SSL-CERT och signaturer. Fax, telefon, brev
- Återkopplingsrutiner vid företagsverifiering. Registreringsbevis och adresser.
- Optimera på enkelhet. "Keep it simple, stupid"
- Genomförande: Flera steg, 2002-2003?
Påverkas av DNSSEC och IDN

Ytterligare noteringar

- Kostnad ~250 kr år. Så länge du inte gör fel.
- Samarbete med utlandet. IETF. Holland, Tyskland.
- Samarbete inom Sverige. T.ex. banker, högskolor och universitet?

Löser inte alla problem

- Revokering
- Kontroller av indata
 - <https://www.foreningssparbanken.se>
 - <https://www.sed.se>
 - <https://www.foreningssparbanken.se>
 - <https://www.seb.se>