



# **Hot mot nyckelhantering i DNSSEC – och lite om hur man undviker dem**

Anne-Marie Eklund Löwinder  
Kvalitets- och säkerhetschef

**.se**



# Överväganden

- Införandet av DNSSEC nödvändiggör en juridisk analys.
  - Vilken riskexponering innebär införandet av DNSSEC.
  - i vilken mån bör avtalade begränsningar göras i detta ansvar.
- En naturlig målsättning är att ansvarsnivån skall upplevas som rimlig och skälig av samtliga parter.
- .SE tar t.ex. inget ansvar för underliggande zoners nycklar eller hanteringen av dessa.

.se

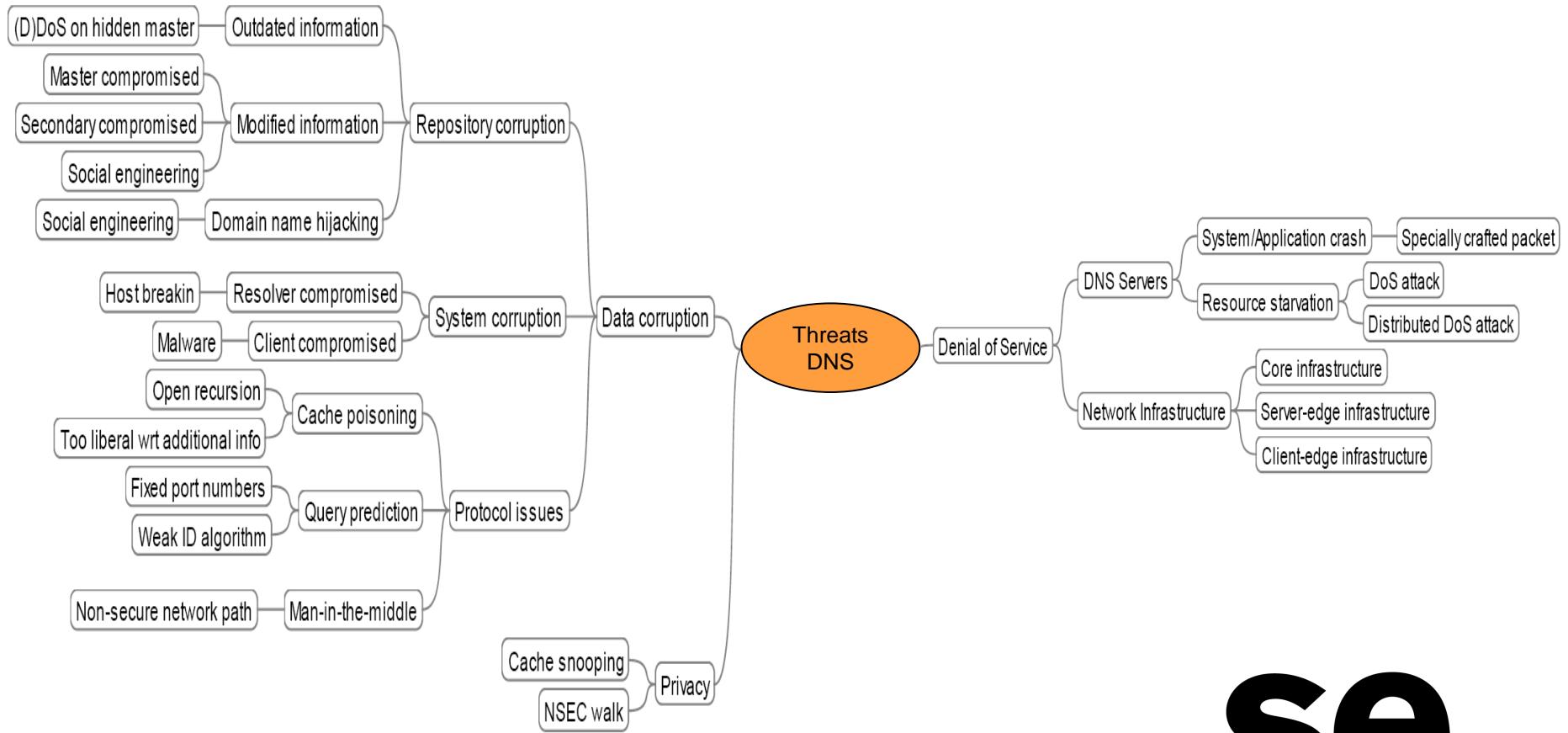


**Vi har hållit på sedan 1999...  
Vad har vi lärt oss?**

**En hel del!**

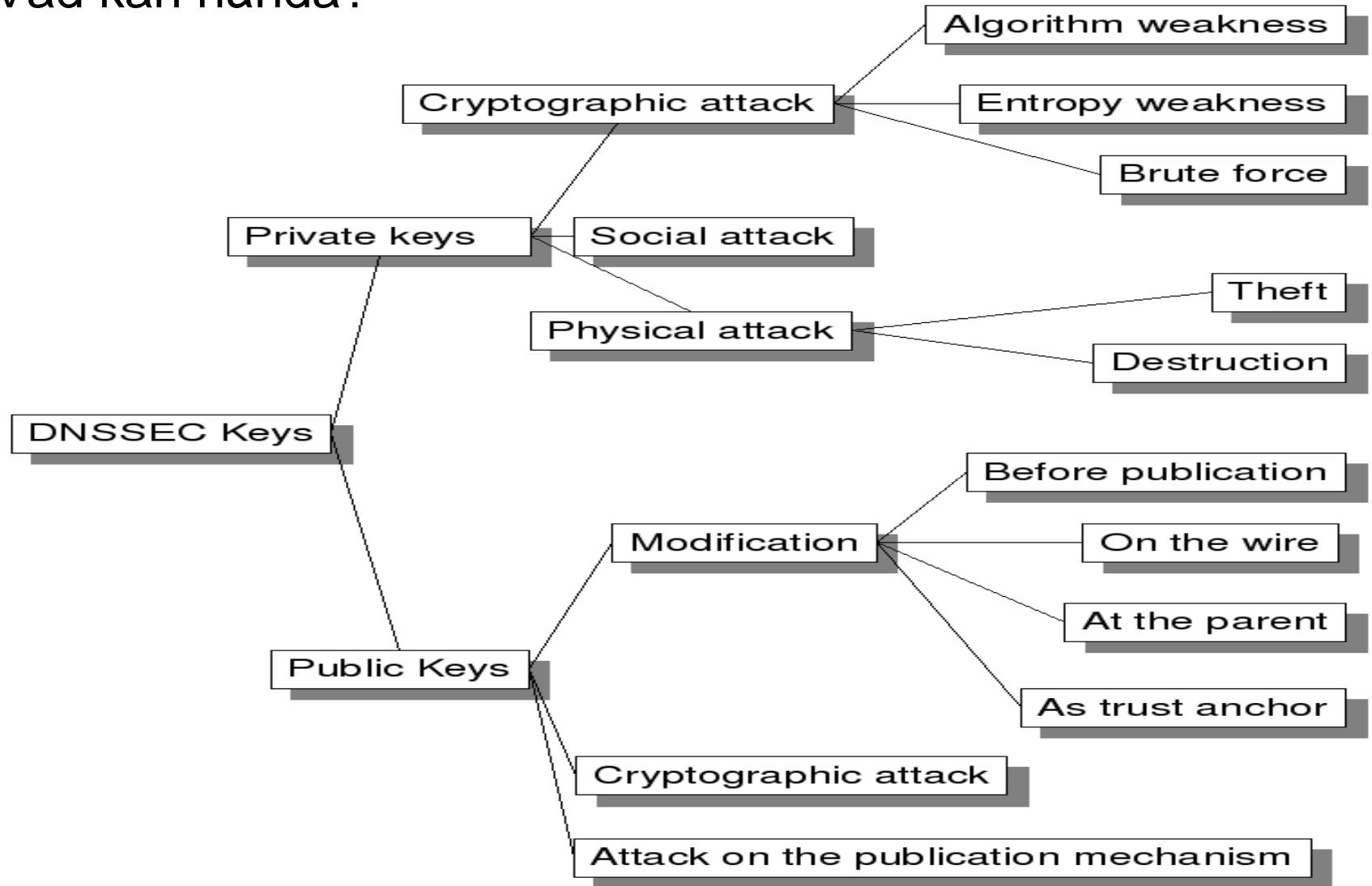
**.se**

# Hot mot DNS

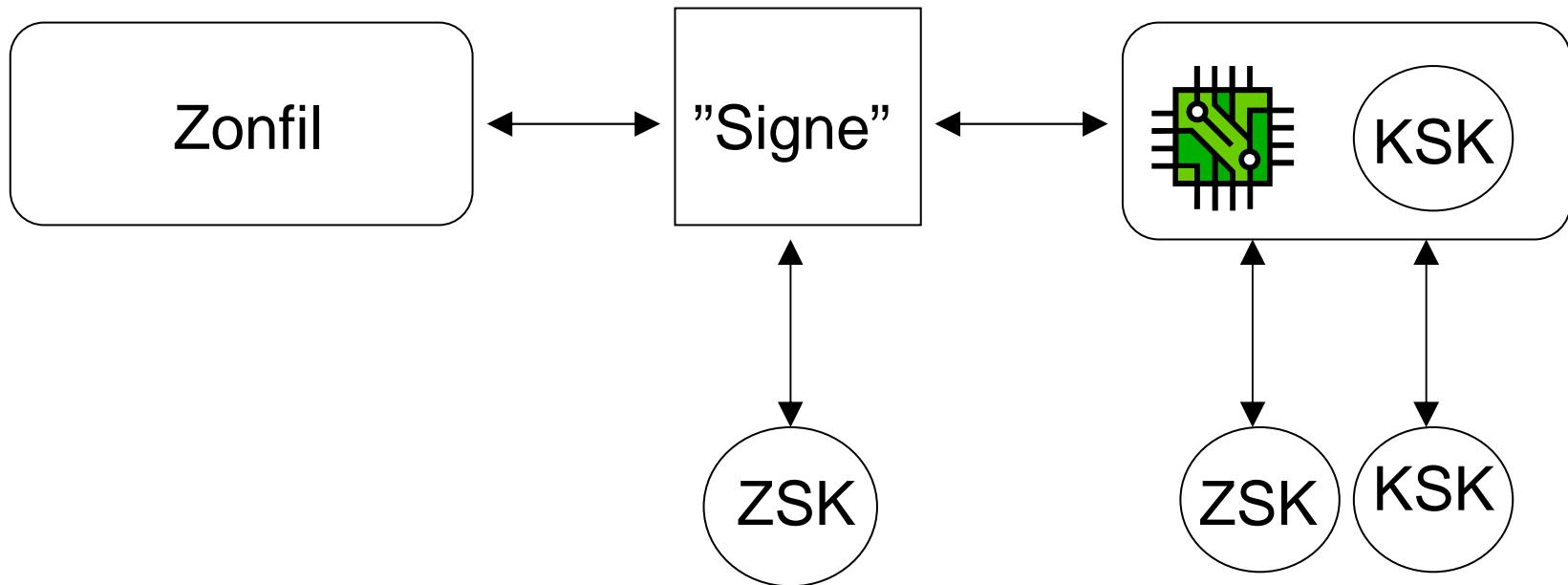


.se

# Vad kan hända?



# Nyckeladministration är kritiskt!



.se



# Privata nycklar

- Kryptografiska attacker
  - Svagheter i valda algoritmer
  - Svagheter i slumptalsgenerering
  - Uttömmande sökning (Brute force)
- Sociala attacker
- Fysiska attacker
  - Stöld
  - Destruktion

.se



# Publika nycklar

- Modifieringsattacker
  - Före publicering
  - På sladden
  - Hos föräldern
  - Hos trust anchor
- Kryptografiska attacker
- Attack på publiceringsmetoden

.se



# **Införande – att tänka på**

- Policy, policy, policy
- Personal och kompetens
- Algoritm/-er
- Nyckellivslängd
- Nyckelbyten
- Automatisering

**.se**



# Byte av olika parametrar

- Regelbundna planerade nyckelbyten.
- Akuta nyckelbyten.
- Byte av algoritm.

.se



# Lagringsalternativ – Privat nyckel

- Beroende på "värde".
- Online eller offline.
  - Direktåtkomst.
  - Manuell hantering krävs.
  - Online/offline.
- Hardware Security Module, HSM.
- Åtkomstkontroll till lagringsplats.
- Olika val är möjliga för KSK respektive ZSK.
- Genererings- och signeringrutiner.

.se



# Publicering av publika nycklar

- Hur?
  - Genom föräldern (DS/DNSKEY).
  - DNSSEC Lookaside Validation, DLV.
  - Separat kanal, OOB (Out of band).
    - Webbsida.
    - Dagstidning.
    - E-postlista.
  - Egen kanal (In band).
    - Endast uppdateringar enligt RFC 5011.

.se



# **Policy för nyckelpublicering**

- Var?
- Hur?
- När, hur ofta?
- Policy för publicering av policy....

**.se**



# **DPS – DNSSEC Policy and Practice Statement**

- DPS beskriver rutinerna för hur verifieringen sker, vilka rutiner .SE har och hur .SE hanterar sina nycklar.
- DPS syftar till att göra det möjligt för omvärlden att avgöra vilken tillit de vill ha till .SE:s DNSSEC-hantering.
- <http://www.iis.se/pdf/se-dnssecps-a.pdf>

**.se**



# Nyckelhantering för .se-zonen

- Teknisk miljö för nyckelgenerering
- Rutiner för:
  - Generering av nycklar
  - Förvaring av nycklar
  - Användning av nycklar
  - Byte av nycklar
  - Publicering av nycklar

.se



# Tillvägagångssätt

- Inga operationer får genomföras av någon person ensam eller med obehöriga personer närvarande.
- Generering av nyckelmaterial måste alltid göras av minst två personer. Båda ska vara närvarande under hela operationen.
- De olika personalkategorierna ansvarar för var sin hemlighet.
- Signering sker automatiskt och i samband med zongenerering (varannan timme).

.se



# **Frekvens Nyckelsigneringsnyckel - KSK**

- KSK används enbart för att signera ZSK.
- Generering av KSK sker med frekvensen 1 gång per år.
- Nyckelparametrar:
  - RSA
  - 2048 bitars nyckellängd
- Lagringsmedia: aktivt kort ("smart card")
- Giltighetstid två år. Detta medför att vi har nycklar som har en giltighetstid som överlappar varandra med 1 år.
- Publika KSK är de nycklar som kommuniceras till Internetanvändare.

**.se**



# **Frekvens Zonsigneringsnyckel - ZSK**

- ZSK används enbart för att signera data i se-zonen.
- Generering av ZSK sker med frekvensen 1 gång per månad.
- Nyckelparametrar:
  - RSA/SHA-1
  - 1024 bitars nyckellängd.
- Lagringsmedia: flyttbart sekundärminne.
- Giltighetstid för ZSK är en månad.

**.se**



# Akut nyckelbyte

- Viktigt att ha rutiner för akut nyckelbyte!
- ZSK har ett osäkerhetsfönster på 5 dagar.
- KSK har ett osäkerhetsfönster på 6 veckor, dvs. lika länge som vi signerar med KSK.
- För att byta KSK på ett effektivt sätt behövs signerad rot, DLV eller RFC 5011 – Automated updates of DNS Security (DNSSEC) Trust Anchors.

.se



# **Signering av .SE:s egna zoner**

- Utse ansvarig administratör.
- Kartlägg samtliga domäner.
- Kontrollera namnservrar – DNS baskonfiguration.
- Välj ut domäner att signera.
- Kravspecifikation – tidplan.
- Sträva efter automatisering.

**.se**



# Övervakning är viktigt

- Övervakningssystemet har kompletterats för att utföra basala DNSSEC-kontroller:
  - Varnar för signaturer som är på väg att gå ut.
  - Testar den extra DNSSEC-hanteringen i produktionen så att den görs korrekt.
  - Kontrollerar äktheten hos vissa signaturer.

.se



# Summering

- Vi är fortfarande i början av utvecklingen.
- Det är mycket att tänka på och många ställningstaganden att göra.
- Skriv ner och dokumentera allt.
- Publicera allt som går att publicera.
- Automatisera allt ni kan, särskilt nyckelbyten.

.se



# Frågor?

.se