



Signering av .SE - lösningar och rutiner

Anne- Marie Eklund Löwinder
Kvalitets- och säkerhetschef

.se



Varför ville vi ha DNSSEC i .SE?

- Ökar integriteten i DNS.
- Ökar säkerheten för .SE:s domäninnehavare och deras användare.
 - En åtgärd mot pharming och andra DNS MITM attacker.
 - Förstärker infrastrukturen för Internet.
 - En tänkbar användning av DNSSEC är dessutom för säker distribution av attribut för andra säkerhetsprotokoll och lösningar.
- Efterfrågas av ansvarig myndighet, PTS.
- Behövs för att kunna lita på nya kritiska applikationer.

.se



Hi s t o r i k

- Första workshopen ägde rum i februari 1999.
- Tester har pågått sedan januari 2003.
- Öppna tester sedan januari 2004.
- RFC 4033, 4034 & 4035 (DNSSEC bis) publicerades i mars 2005.
- .SE började distribuera den signerade .se- zonen den 13 september 2005.
- .SE började ta emot signerade delegeringar från tidiga användare från mitten av november 2005.
- Mer omfattande testverksamhet inleddes februari 2006.
- Kommersiellt tillgängligt Q1 2007.

.se

Överväganden

- Införandet av DNSSEC nödvändiggör en juridisk analys. Frågan är dels vilken riskexponering införandet av DNSSEC innebär, dels i vilken mån avtalade begränsningar bör 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

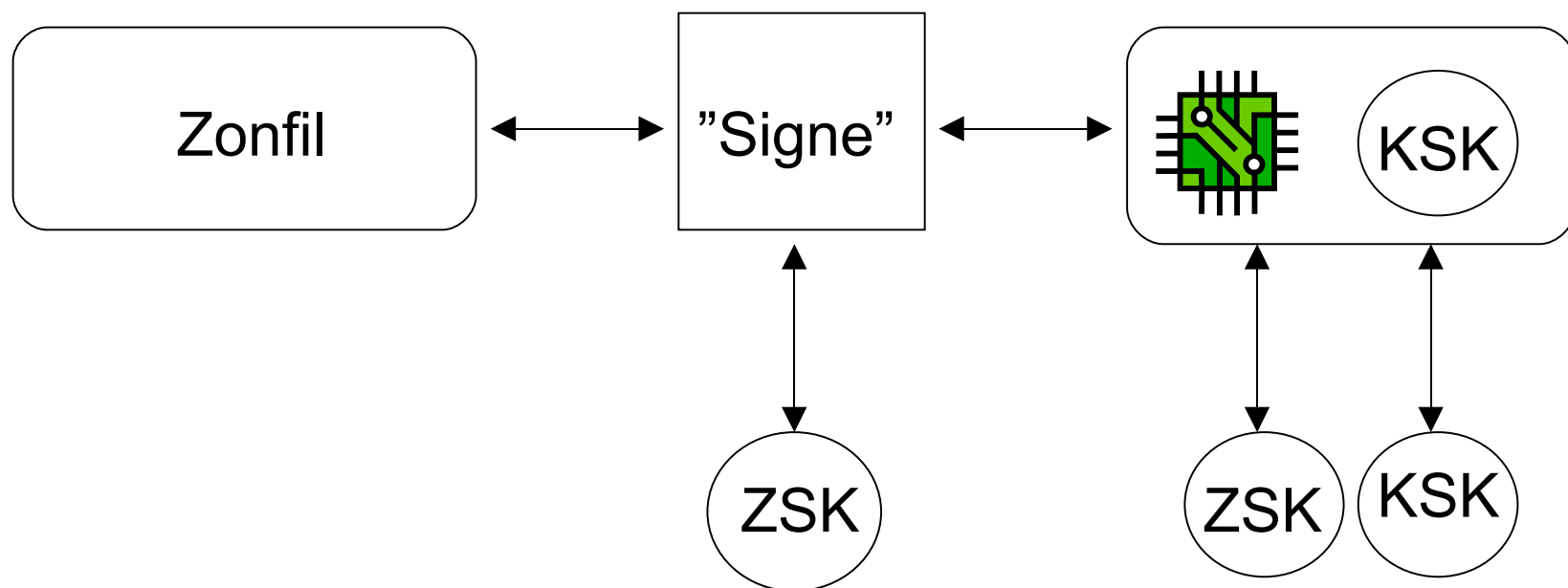


Vad har vi lärt oss?

En hel del!

.se

Nyckel administration är kritiskt!



.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



DPS - DNSSEC Policy and Practice Statement

- .SE verifierar kopplingen mellan en domän, en publik nyckel och innehavare av domänen, samt den tekniska kontaktpersonen.
- 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



Nyckel hantering 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 nyckelmateriel 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

Nyckel signeringsnyckel - 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 zonen.
- Generering av ZSK sker med frekvensen 1gång per månad.
- Nyckelparametrar:
 - RSA/SHA- 1
 - 1024 bitars nyckellängd.
- Lagringsmedia: flyttbart sekundärminne.
- Giltighetstid för ZSK är en månad.

.se

Akut nyckel byte

- 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 något i stil med draft- ietf- dnsext- trustupdate- timers- 05.txt.

.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



Frågor ?

.se