

Signering av roten

Lars-Johan Liman

Netnod/Autonomica

DNS-roten signeras

- Mål:
 - ▶ Alla rootservrar skall bekvämt leverera svar som är signerade med en nyckel med vars hjälp man kan verifiera att svaret inte förvanskats under transporten.
 - ▶ "Alla" (relevanta) spelare skall kunna observera och dra slutsatser.
 - ▶ "Alla" skall ha kunnat yttra sig och hörts.
 - ▶ Ingen "väsentlig" grupp skall vara förvånad över händelsen.

Stegvis utrullning

Vecka m. start	Server-ID
27 jan	L
8 feb	A
1 mar	M, I*
22 mar	D, K, E
12 apr	B, H, C, G, F
3 maj	J

* Drivs av Netnod/Autonomica

DURZ

- Deliberately Unvalidatable Root Zone.
- Signerad med riktiga nycklar
- Nycklarna publiceras ***inte!***
 - ▶ I stället publiceras en dummy-nyckel.
- Denna zon innehåller alla sorters legobitar, men går (avsiktligen) alltså inte att validera.

Roller

- ICANN/IANA
 - ▶ Genererar och hanterar nyckelsigneringsnyckel (KSK).
 - ▶ Signerar zonsigneringsnycklar (ZSK) buntvis med jämna mellanrum och i förväg.
 - Föreslagen process med observatörer.
 - ▶ Bereder och skickar uppdateringar till DoC/NTIA och Verisign för godkännande resp. implementering (som tidigare).

Roller

- Verisign
 - ▶ Genererar och hanterar zonsigneringsnyckel (ZSK).
 - ▶ Implementerar ändringar från IANA som auktoriserats av NTIA (som tidigare).
 - ▶ Signerar rotzonen med ZSK.
 - ▶ Genererar zoner.
 - DURZ (nu).
 - Skarpt signerad zon (senare).
 - Osignerad zon (hela tiden).
 - ▶ Publicerar zonen till rotserver-operatörer (som tidigare).

Roller

- US DoC/NTIA
 - ▶ Auktoriserar ändringar i rotzonen (som tidigare).
 - ▶ Verifierar att ICANN/IANA och Verisign följer sina processer (som tidigare).

Roller

- Rotserveroperatörer
 - ▶ Publicerar rotzonen globalt (som tidigare).
 - ▶ Stegvis ändring från osignerad zon till DURZ, och sedan till skarp zon.

Utvärdering

- Extensiv och koordinerad statistikinsamling.
 - ▶ DNS OARC (Operations and Analysis Research Center).
 - ▶ Analysera ev. flytt av trafikströmmar från signerade till osignerade servrar under utrullning.

1 juli 2010

- (Alla rotservrar kör redan signerat data, DURZ.)
- Byter från dummy-nyckel till skarp nyckel och publicerar denna.
- **Roten är därmed signerad!**
- ... men när börjar de koppla in toppdomänerna så att kedjan sluts ned till .SE (m.fl.)?