A provisional approach to DNSSEC Root Key Management: Trusted Community Representatives

RIPE 60

3 May 2010 Czech Republic

Richard Lamb

DNSSEC Program Manager / ICANN

Goal

- Improve confidence and acceptance in DNSSEC
- Direct participation by recognized members of the DNS technical community in root KSK generation, backup, and use (for signing)

TCR Positions

- 14 Crypto Officer (CO) – 7 for US East and 7 for US West key management facilities
- 7 Recovery Key Share Holder (RKSH)
- Backup COs and RKSHs will be sought
- If this approach proves successful during the first key generation and signing event, TCR term will be annual

How it works

COs and RKSHs participate in filmed, audited, Key Ceremony at ICANN key management facilities to:

- Generate root KSK as needed
- Sign root ZSK every quarter

How it works - CO

- CO – have physical keys to safe deposit boxes holding smartcards that activate the HSM
- ICANN cannot generate new key or sign ZSK without 3-of-7 COs

How it Works - RKSH

- RKSH – have smartcards holding pieces (M-of-N) of the key used to encrypt the KSK inside the HSM
- Backup KSK encrypted on smartcard held by ICANN
- If both key management facilities fall into the ocean, 5-of-7 RKSH smartcards and an encrypted KSK smartcard can reconstitute KSK in a new HSM

Requirements

- CO – Able to travel up to 4 times a year to US. Don’t lose key.
- RKSH – Able to travel on relatively short notice to US. Hopefully never. Annual inventory.
- Not from an organization affiliated with the root zone management process (ICANN, VeriSign, or the US Department of Commerce)

Selection Criteria

- Respected members of the DNS technical community
- Geographically Distributed

Candidates

- Sol period began 12 April 2010
- Sol period ended 23 April 2010

- 61 Candidates

Geographical Distribution

From 5 RIR Regions

- AfriNIC – 4
- APNIC – 12
- ARIN – 20
- LACNIC – 5
- RIPE – 20

Timeline

- Expect final selection and background checks complete by late May 2010
- Will publish selections and all candidate names and nationality
- Expecting Key Ceremony in mid-June 2010
- If Key Ceremony is successful – no longer provisional

Thank you to all those who volunteered!!

Questions?

http://www.root-dnssec.org/tcr/