DNS root key management

TCRs and their role in DNS root signing procedures. First experience.

Dmitry Burkov
CO2 WCF

DNSSEC goals and deployment

- Attempt to correct some DNS design flaws known for years
- Root signing is necessary to improve confidence and acceptance in DNSSEC usage
- Hierarchical model of DNSSEC was chosen to deploy
- New technological and business process were added to DNS root management
- Why community involved – improve trust to procedure

New process and trusted community representatives

- First time community representatives began to participate in one of DNS root management processes which covered DNS root KSK generation, backup and key signing requests
- ICANN selected from members of DNS technical community:
  - 14 Crypto Officers (CO) – 7 for US East and 7 for US West key management facilities
  - 7 Recovery Key Share Holders(RKSH)
  - Backup COs and RKSHs

TCRs geographical distribution

From 5 RIR Regions

	Applied	Final		
		CO	RKSH	Backup
AfriNIC	4	2	1	1
APNIC	12	3	1	2
ARIN	20	3	2	4
LACNIC	5	2	1	3
RIPE	20	4	2	3

Crypto Officers

US East Coast Facility

- Alain Aina, BJ
- Anne-Marie Eklund Löwinder, SE
- Frederico Neves, BR
- Gaurab Upadhaya, NP
- Olaf Kolkman, NL
- Robert Seastrom, US
- Vinton Cerf, US

US West Coast Facility

- Andy Linton, NZ
- Carlos Martinez, UY
- Dmitry Burkov, RU
- Edward Lewis, US
- João Luis Silva Damas, PT
- Masato Minda, JP
- Subramanian Moonesamy, MU

Recovery Key Share Holders

- Bevil Wooding, TT
- Dan Kaminsky, US
- Jiankang Yao, CN
- Moussa Guebre, BF
- Norm Ritchie, CA
- Ondřej Surý, CZ
- Paul Kane, UK

Backup COs and RKSHs

Backup Crypto Officers

- Christopher Griffiths, US
- Fabian Arbogast, TZ
- John Curran, US
- Nicolas Antoniello, UY
- Rudolph Daniel, VC
- Sarmad Hussain, PK
- Ólafur Guðmundsson, IS

Backup Recovery Key Share Holders

- David Lawrence, US
- Dileepa Lathsara, LK
- Jorge Etges, BR
- Kristian Ørmen, DK
- Ralf Weber, DE
- Warren Kumari, US

ICANN DNS Operations team is responsible for KSK Operations of the DNSSEC Signing of ROOT zone.

- Joe Abley
- Mehmet Akcin
- David Conrad
- Dave Knight
- Dr. Richard Lamb
- Fredrik Ljunggren
- Jakob Schlyter

First KSK Ceremonies

- ICANN KSK Ceremony 1 – June 16-17, 2010 – Culpeper, VA
- ICANN KSK Ceremony 2 – July 12-13, 2010 – Los Angeles, CA
- ICANN KSK Ceremony 3 – November 1-2, 2010 – Culpeper, VA

Some experience

- Great job was done by the team to sign root in time
- Some process documents are still draft and can be improved (www.root-dnssec.org/documentation/)
- Some minor suggestions were made regarding some procedures (key for safes, signing tamper-evident bags, transportation application data between sites)
- Little surprise with change in process – KSK generation was combined with signing first KSR

TCRs role in new process

- We are not Key holders or keepers
- COs role – first of all – supervisors or witnesses of DNS root key management processes – imho
- Necessity in separate role of RKSHs is unclear as in catastrophe case COs can generate new KSK from scratch – now it is more psychological or political reverance

Conclusions and some ideas

- Key point – new process in DNS root management will now works in more open and transparent way
- No way back – as key issue is TRUST
- Looks possible to reevaluate other DNS root management processes
- AoC initiated process can give a chance not only to preserve, but to improve trust for DNS root
- Still one big challenge – need for scalability and automation of root management...

  ....

  can we believe Skynet©?

Links

Information about DNSSEC for the Root Zone
http://www.root-dnssec.org/

ICANN DNS Operations
http://dns.icann.org/


One World. One Internet. Everyone Connected.