Root Zone DNSSEC Deployment

ICANN 39, Cartagena, Colombia
8 December 2010
richard.lamb@icann.org
This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. Department of Commerce NTIA and National Institute of Standards and Technology (NIST)
High Level Design

• Trust / Integrity
  – Transparent operations
  – Direct public participation in key management
  – 3rd party Audit

• Security
  – Crypto
  – Physical
  – ID / ACS / multi-person access and control

• Availability
  – Sufficient time to perform operations
  – Mirror sites
  – Disaster recovery plan
Implementation and Roll-out

- Publish all material (film, scripts, s/w, results.. http://www.iana.org/dnssec)
- DNSSEC Practices Statement (DPS)
- 21 Trusted Community Representatives (TCR)
- SysTrust audit by PWC
- 2048 KSK, 1024 ZSK RSA keys; SHA256 hash
- FIPS 140-2 Level 4 HSM; 3-of-7 TCR to enable; Good RNG
- Multiple physical tiers /w multi-person anti-passback access control system
- 9 gauge stretched metal ceremony room construction; Safes certified to 20 hours surreptitious entry
- 24x7 monitoring: motion, seismic, video, guards
- ~60 day window to perform quarterly operation; 15 day signature validity periods
- Mirror sites in Los Angeles and Washington DC; 2 HSMs at each site
- Documented Disaster Recovery (DR) plans
- Incremental deployment with DURZ and extensive monitoring
Challenges

• Finding out what are “best practices”
• Embracing an audited IT security mindset
• Formalizing documentation of policy and procedures
• Contractors!!
• HSM/smartcards/PKCS11
Lessons Learned

• Identify your “customer” and then your risks first
• Develop and document policies and procedures, e.g., key management, DPS, scripts, DR plan – and institutionalize them
• Embrace PKCS11 and tamper evident bags
• Multiple compensating controls
• DNSSEC deployment does not have to be expensive; Learn from those on this panel and share our experiences.
• This is not static; annual review and incorporate improvements from community.
Root DNSSEC Design Team

Joe Abley
Mehmet Akcin
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
Dave Knight
Tomofumi Okubo
Jakob Schlyter
Duane Wessels

..and so many others!!

Links:
http://www.root-dnssec.org
http://www.iana.org/dnssec

richard.lamb@icann.org