DNSSEC – Why Not?

APTLD Meeting, April 8, 2011
Noumea, New Caledonia
richard.lamb@icann.org ICANN
What are you trying to do?
  ◦ Reliability – Cant Set and Forget, Key Management
  ◦ Be Trusted – Transparency and Security

Risk Analysis
  ◦ What are you trying to protect against
Common Threads from Successful Deployments

- Reliability
  - Automation, Monitoring

- Complexity
  - Documented Step-by-Step Processes

- Trust
  - Secure
  - Public Documentation and Notifications
  - Witnesses / Audited
Automation

- Pre-generate key material
  - Every 6 months, or even very year.
  - Signer automatically incorporates material.
  - Trust tied to key management.

- Check before commit
- Monitoring tools for impending expiration
Trust

• Say what you do
  – Set Expectations
  – Make public (e.g., DNSSEC Practices Statement – DPS)

• Do what you say

• Prove it
  – Auditor$
  – External Witness

• Secure IT
  – Physical
  – Crypto
Documentation – Root

Root DPS

91 Pages and tree of other documents!
Security

@ root

FIPS 140-2 Level 4

Class 5 Safes
Security – Crypto

@ Some TLDs

- But FIPS 140-2 Level 3 is also common
- Many TLDs using Level 3 .com, .uk, etc...
- $9K–$40K
Security – Physical

@ Some TLDs
But this is also “level 3”
Conclusions

- DNSSEC deployment does not have to be costly nor complicated
- Successful deployments have shown automation and clearly defined procedures are key
- Various solutions and options exist