



# DNSSEC Update

*Mehmet Ackin  
Critical Infrastructure Engineer  
ICANN*



*Presented by:  
Baher Esmat  
Manager, Regional Relations - Middle East*

*APTLD Meeting  
Amman, Jordan  
1 Nov, 2010*

# Signing the Root

*The project has been  
coordinated by ICANN and  
VeriSign with support from  
DoC/NTIA*

# ROLES AND RESPONSIBILITIES

# ICANN: IANA Function's Operator

- Manages the Key Signing Key (KSK)
- Accepts DS records from TLD operators
- Verifies and processes request
- Sends update requests to DoC/NTIA for authorization and to VeriSign for implementation

# DoC/NTIA

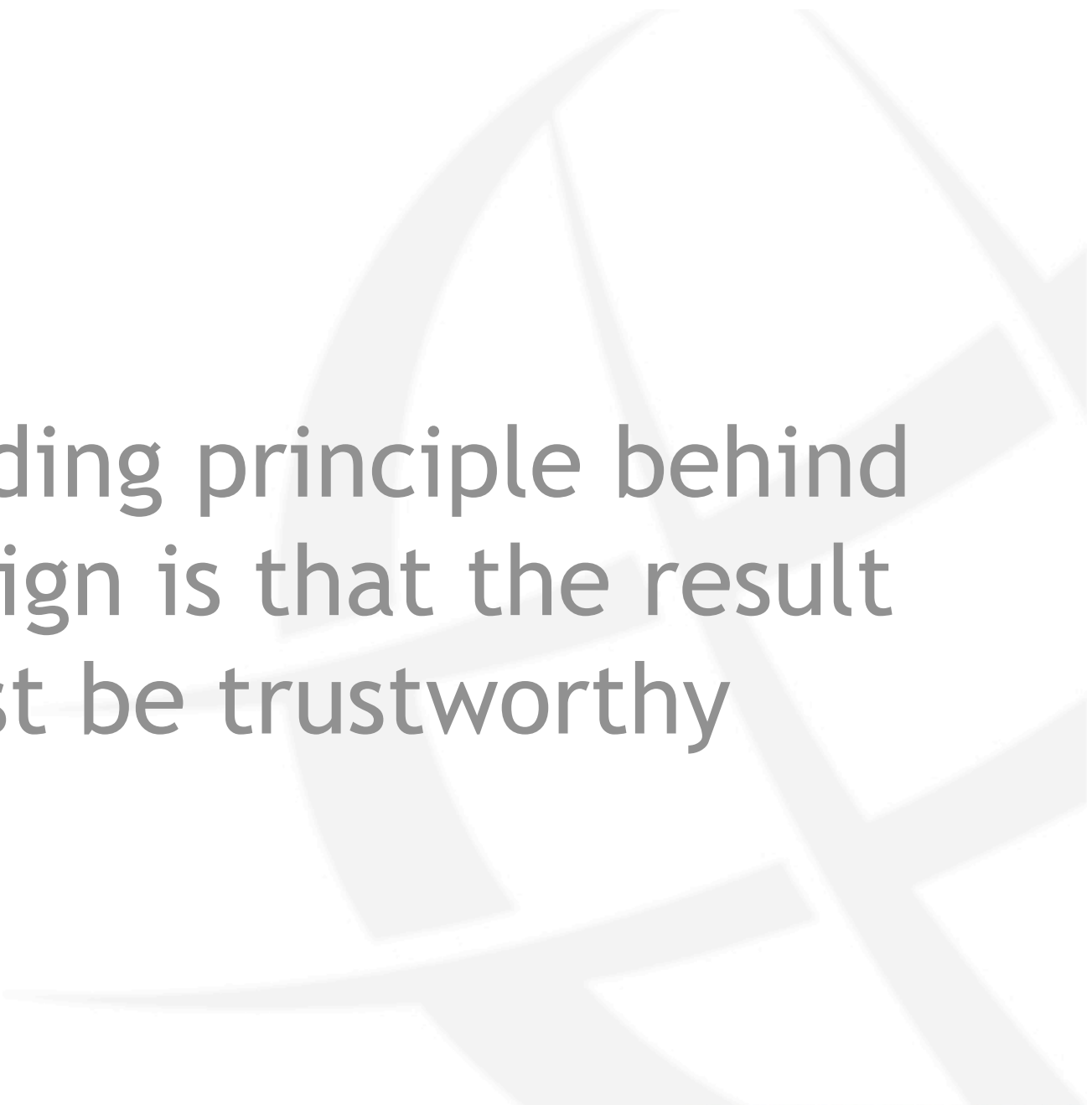
- Checks that ICANN has followed their agreed upon verification/processing policies and procedures
- Authorizes changes to the root zone
  - DS records
  - Key Signing Keys
  - DNSSEC update requests follow the same process as other changes

# VeriSign

- Manages the Zone Signing Key (ZSK)
- Incorporates NTIA-authorized changes
- Signs the root zone with the ZSK
- Distributes the signed zone to the root server operators

# DESIGN





The guiding principle behind  
the design is that the result  
must be trustworthy

# Transparency

*Processes and procedures should  
be as open as possible for the  
Internet  
community to trust the signed root*

# Audited

*Processes and procedures should  
be audited against industry  
standards,  
e.g. ISO/IEC 27002:2005*

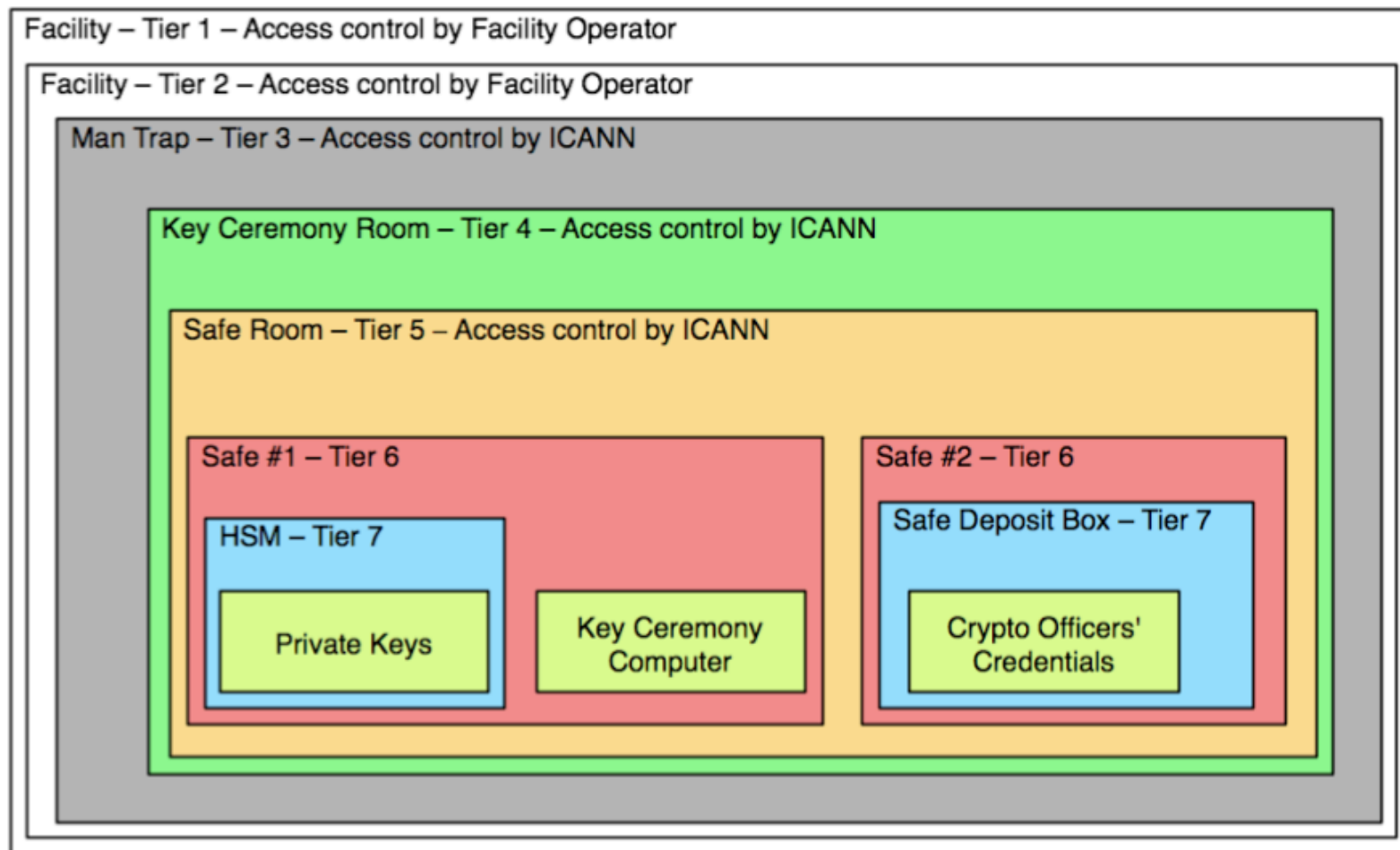
# DNSSEC Practice Statement (DPS)

- States the practices and provisions that are employed in root zone signing and zone distribution services
  - Issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. DoC NTIA
- Third-party auditors check that ICANN operates as described in the DPS

# High Security

*Root system should meet all NIST  
SP 800-53 technical security controls  
required by a HIGH IMPACT system*

# Physical Security



# Physical Security



# Community Involvement

*Trusted representatives from the community are invited to take an active role in the key management process*

# Trusted Community Representatives (TCRs)

- Have an active role in the management of the KSK
  - as Crypto Officers needed to activate the KSK
  - as Recovery Key Shareholders have pieces of the key that encrypts the backup copy of the KSK

# Crypto Officer (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
- Able to travel up to 4 times a year to US

# Recovery Key Shareholder (RKSH)

- Have smartcards holding pieces (M-of-N) of the key used to encrypt the KSK inside the HSM
- If both key management facilities fall into the ocean, 5-of-7 RKSH smartcards and an encrypted KSK smartcard can reconstituted KSK in a new HSM
- Backup KSK encrypted on smartcard held by ICANN
- Able to travel on relatively short notice to US

## CO

---

- Alain Aina, BJ
- Anne-Marie
- Eklund Löwinder, SE
- Frederico Neves, BR
- Gaurab Upadhaya, NP
- Olaf Kolkman, NL
- Robert Seastrom, US
- Vinton Cerf, US
  
- Andy Linton, NZ
- Carlos Martinez, UY
- Dmitry Burkov, RU
- Edward Lewis, US
- João Luis Silva Damas, PT
- Masato Minda, JP
- Subramanian Moonesamy, MU

## CO Backup

---

Christopher Griffiths, US  
Fabian Arbogast, TZ  
John Curran, US  
Nicolas Antonello, UY  
Rudolph Daniel, UK  
Sarmad Hussain, PK  
Ólafur Guðmundsson, IS

## RKSH

---

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

## BCK

---

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

# DEPLOYMENT

# Deliberately Unvalidatable Root Zone (DURZ)

- A method to allow conservative and controlled deployment of DNSSEC to the root
- Main purpose is to measure effect on normal DNS resolutions
- Deploy incrementally in the root (Jan-10 to May-10)

# Root Signing

- June 2010
  - First ceremony in Culpeper, Virginia
    - Created initial root zone KSK
    - Q3/2010 ZSK signing request (KSR) processed
  - First DS records added to the root zone
- July 2010
  - Second ceremony in Los Angeles, California
    - Key material from the first ceremony replicated and stored
    - Q4/2010 KSR processed
    - Live streamed to the world
  - The fully validatable signed root zone is published to the root servers by VeriSign

# Key Ceremony



# Key Ceremony



# COMMUNICATIONS

# Communications

- Mailing lists
  - IETF DNS lists (e.g. DNSOP)
  - non-IETF DNS lists (e.g. DNS-OARC)
  - General operator lists (e.g. NNNOG)
- Project website
  - <http://www.root-dnssec.org>

# The root is signed!

*TLD operators can submit DS records to the IANA for inclusion in the root zone*

<http://www.iana.org/procedures/root-dnssec-records.html>



Questions?