Signing the Root

NANOG
Atlanta, GA
October 2010

Mehmet Akcin

ICANN

AS SEEN IN ROOT

```
. IN DS 19036 8 2
49AAC11D7B6F6446702E54A
1607371607A1A41855200FD
2CE1CDDE32F24E8FB5
```

Since July 15, 2010

Signing the Root

The Project

A cooperation between ICANN & VeriSign
with support from the U.S. DoC NTIA

ICANN

IANA Functions Operator

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

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

High Security

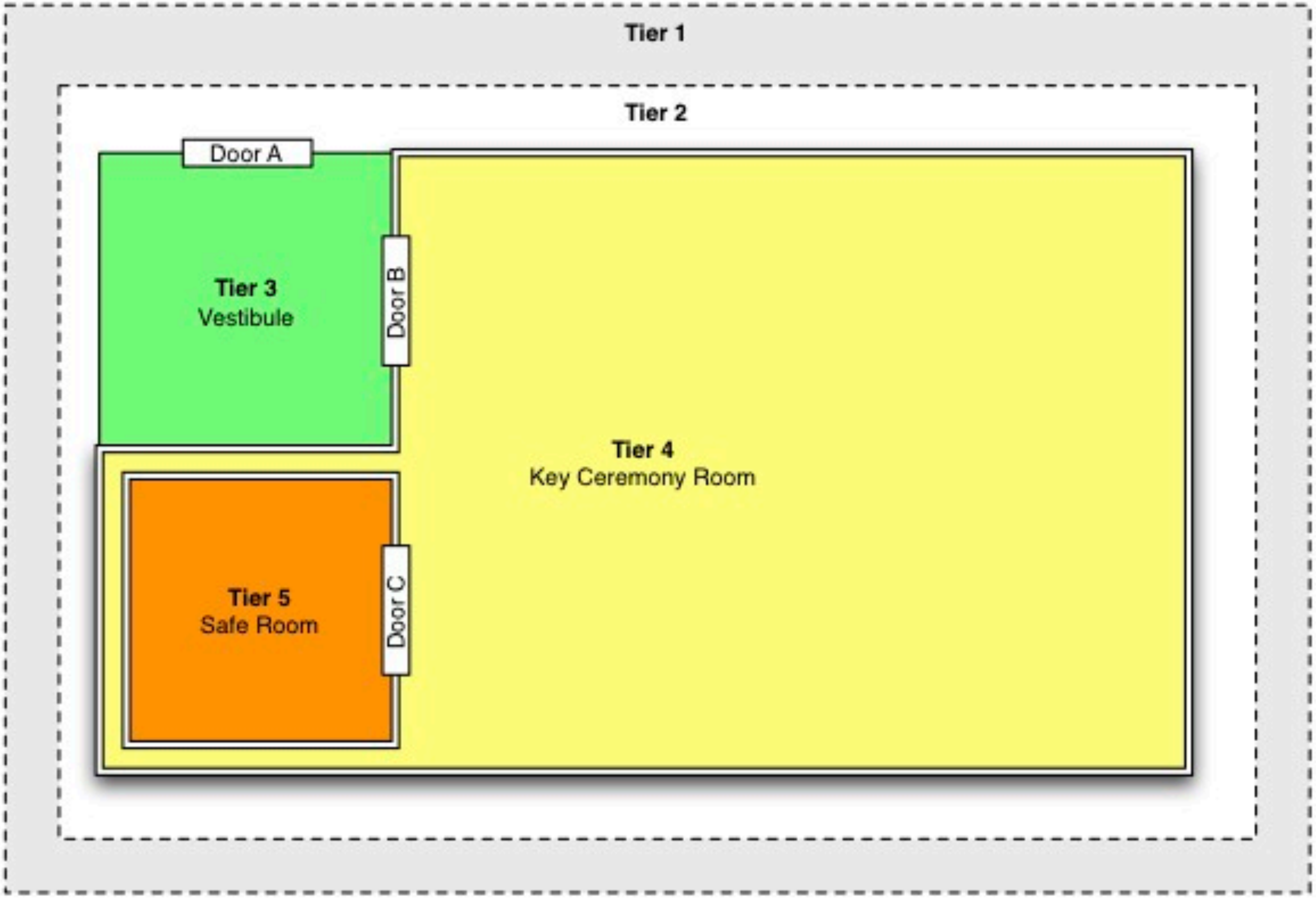
Root system should meet all NIST SP 800-53 technical security controls required by a HIGH IMPACT system

Community Involvement

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

Approach to Protecting the KSK

Physical Security



Physical Security

NOTICE
ALL EMPLOYEES AND VISITORS MUST WEAR IDENTIFICATION BADGES
NOTICE
UNAUTHORIZED PERSONS NOT PERMITTED BEYOND THIS POINT
NOTICE
NO FOOD OR DRINK BEYOND THIS POINT
NOTICE
TURN OFF CELLULAR PHONES, PAGERS AND OTHER WIRELESS DEVICES
NOTICE
NO FIREARMS OR WEAPONS ALLOWED ON THIS PROPERTY

Physical Security

More photos on http://dns.icann.org

Physical Security

Enforced Dual Occupancy

Separation of Duties

External Monitoring

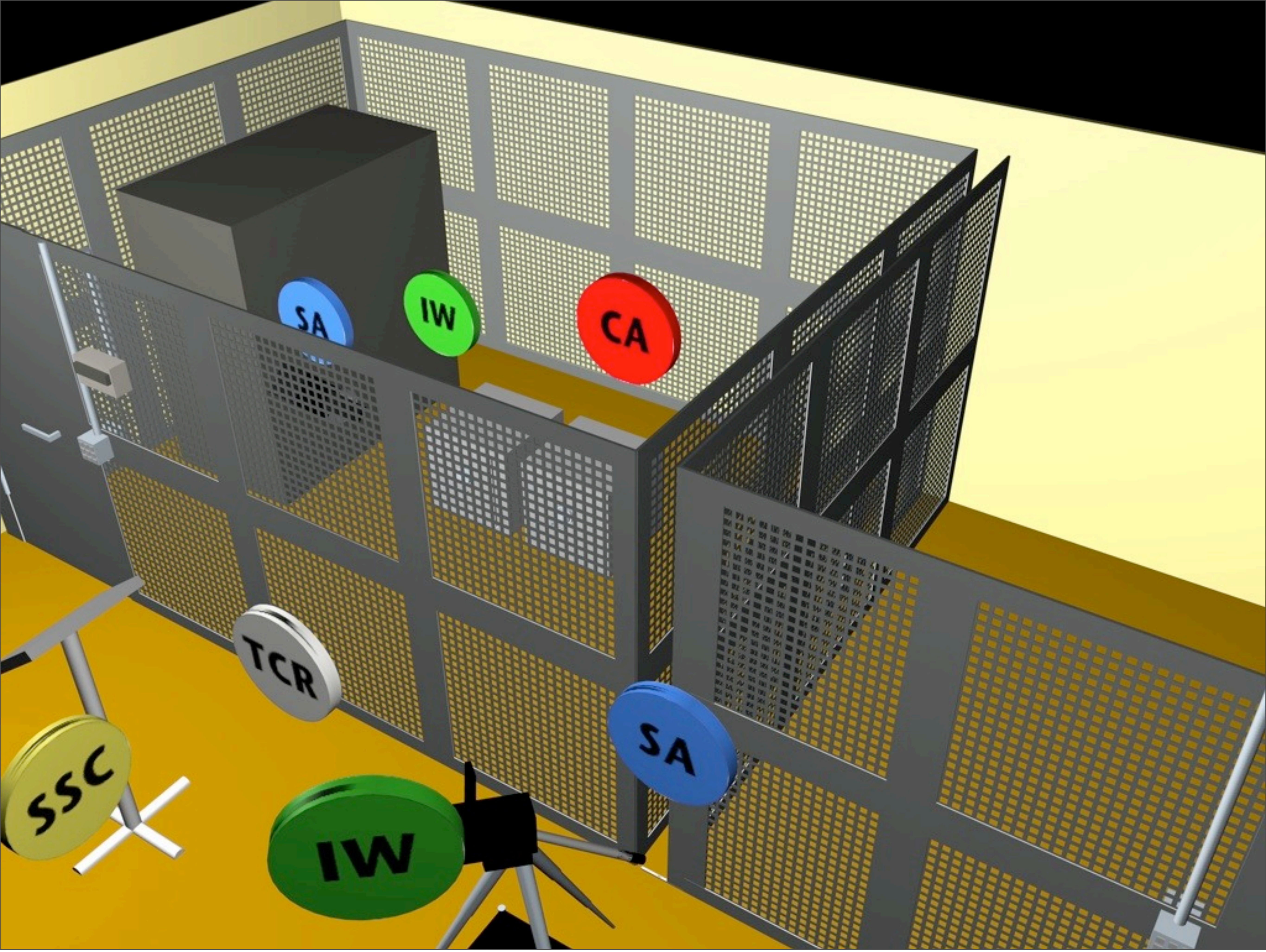
Video Surveillance

Motion, Seismic other Sensors

..and more

ICANN Staff Roles

Roles related KSK Ceremonies can be summarized as ;
Ceremony Administrator (CA) is the staff member who runs the ceremony.
Internal Witness (IW) is the ICANN staff witnessing and recording the ceremony and exceptions if any.
System Administrator (SA) is technical staff members responsible IT needs.
Safe Security Controllers (SSC) are the ICANN staff who operates the safe.


SA
IW
CA
TCR
SA
SSC
IW

DPS

DNSSEC Practice Statement

- 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
- Comparable to a certification practice statement (CPS) from an X.509 certification authority (CA)

Auditing & Transparency

- Third-party auditors check that ICANN operates as described in the DPS
- Other external witness may also attend the key ceremonies
- Working toward having a Systrust audit performed later this year

Trusted Community Representatives (TCRs)

- Have an active roll in the management of the KSK
    - as Crypto Officers needed to activate the KSK
    - as Recovery Key Share Holders protecting shares of the symmetric 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. Hopefully never.   Annual inventory.

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 Antoniello, 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

DNSSEC
Protocol Parameters

Split keys

- The Zone Signing Key (ZSK) is used to sign the zone
- The Key Signing Key (KSK) is used to sign the ZSK
- This split is not required by the protocol, but it enhances security by reducing access to the key which forms the trust anchor while reducing the importance of the key which must be exercised often to sign the zone.

Key Signing Key

- KSK is 2048-bit RSA
    - Rolled as required
    - RFC 5011 for automatic key rollovers
- Signatures made using SHA-256

Zone Signing Key

- ZSK is 1024-bit RSA
  - Rolled once a quarter (four times per year)
- Zone signed with NSEC
- Signatures made using SHA-256

Signature Validity

- DNSKEY-covering RRSIG (by KSK) validity 15 days
    - new signatures published every 10 days
- Other RRSIG (by ZSK) validity 7 days
    - zone generated and resigned twice per day

Key Ceremonies

- Key Generation
  - Generation of new KSK
- Processing of ZSK Signing Request (KSR)
  - Signing ZSK for the next upcoming quarter
  - Every quarter

Root Trust Anchor

- Published on a web site by ICANN as
  - XML-wrapped and plain DS record
    - to facilitate automatic processing
  - PKCS #10 certificate signing request (CSR)
    - as self-signed public key
    - Allows third-party CAs to sign the KSK
    - ICANN will sign the CSR producing a CERT

Milestones

2009

- August
  - Project to sign the root formally announced
- October
  - The plan receives first public airing at RIPE 59
- December
  - http://www.root-dnssec.org site launched
  - First signed root zone created internally at VeriSign

2010

- January through May
  - Incremental roll-out of the DURZ to the root servers
- June
  - First ceremony in Culpeper, Virginia
    - Created initial root zone KSK
    - Processed initial KSR for Q3/2010
  - First DS records added to the root zone

Key Ceremony I

2010

- July
  - 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
  - The root zone trust anchor is published by

Key Ceremony Participants and Attendees

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

The root is signed!

DNSSEC is now part of standard operations

ARPA

- ARPA is signed since March
  - Keys currently managed by Verisign, will change to a joint model like the root
- E164.ARPA signed by RIPE NCC since 2007
- Other ARPA children, with the exception of IN-ADDR.ARPA are signed by ICANN since April
  - Addition of DS records to ARPA in progress

DS Submission

- TLD operators can submit DS records to the IANA for inclusion in the root zone
- Instructions
  - http://www.iana.org/procedures/root-dnssec-records.html

Secured delegations

As of the start of this week the root zone contains 34 secured delegations

be bg biz br

cat ch cz dk

edu eu info lk

museum na org

pm se tf pr

tm uk us th

...and the 11 test IDN TLD zones

Start your validators!

- The trust anchor is available at
  - https://www.iana.org/dnssec/

Next KSK Ceremony

- The next ceremony will take place in Culpeper, VA on 2010 November 1-2
    - Detailed schedule can be found at
        - http://dns.icann.org/ksk/ceremony/ceremony-3/
        - Watch the HD Live Stream at
            - http://dns.icann.org/ksk/stream/

Questions?

mehmet@icann.org