DNSSEC for the Root Zone

NANOG 47, Dearborn, MI
October 2009

Joe Abley, ICANN

Matt Larson, VeriSign

This design is the result of a cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA

Design Requirements Keywords

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

Roles and Responsibilities

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

DoC NTIA

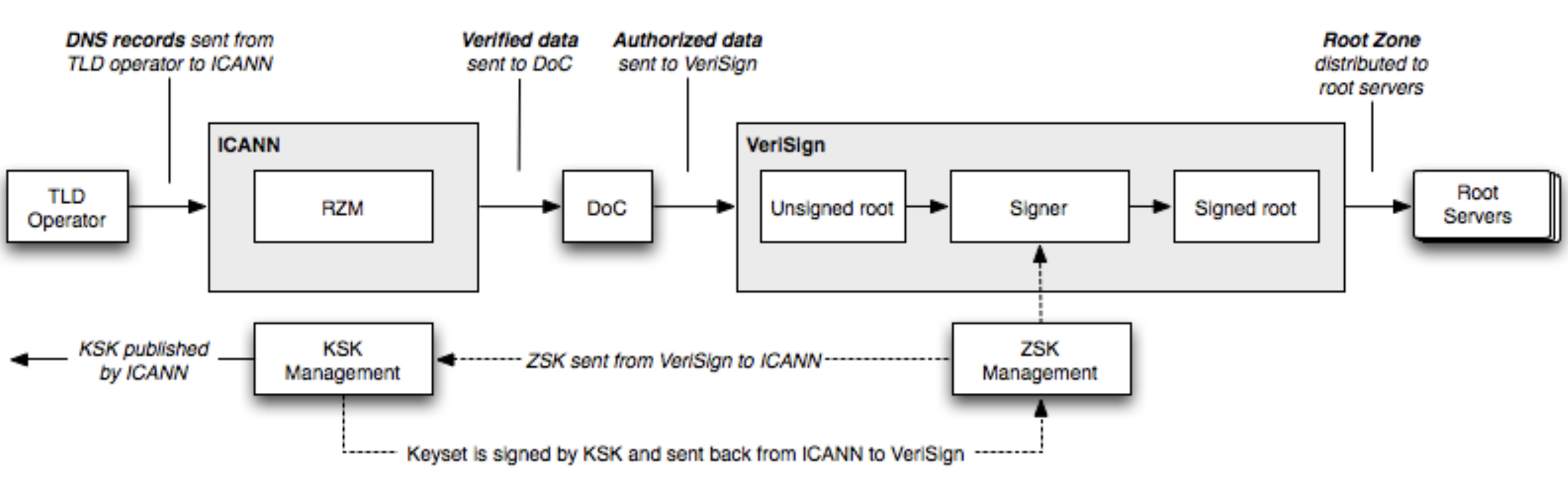
U.S. Department of Commerce
National Telecommunications and Information Administration

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

VeriSign

Root Zone Maintainer

- 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


DNS records sent from TLD operator to ICANN
Verified data sent to DoC
Authorized data sent to VeriSign
Root Zone distributed to root servers
TLD Operator
ICANN
RZM
DoC
VeriSign
Unsigned root
Signer
Signed root
Root Servers
KSK published by ICANN
KSK Management
ZSK sent from VeriSign to ICANN
ZSK Management
Keyset is signed by KSK and sent back from ICANN to VeriSign

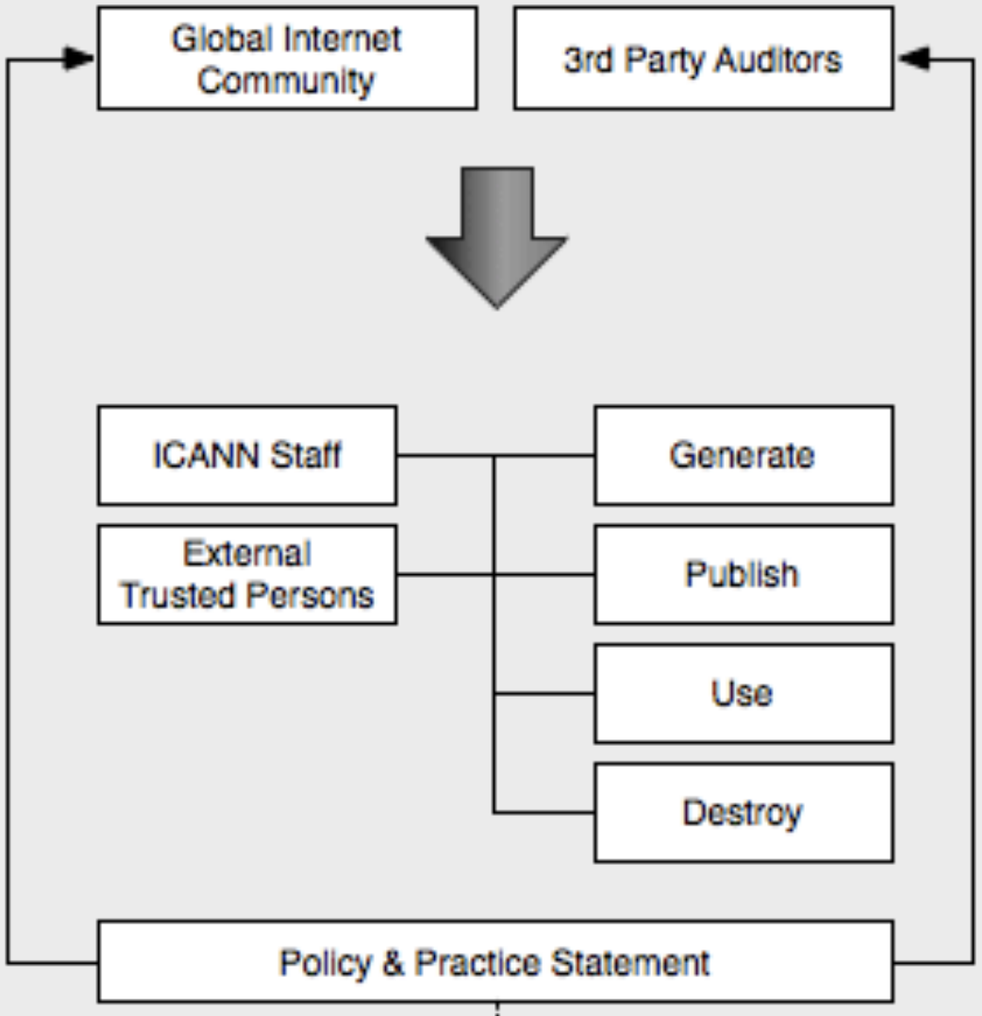
Proposed Approach to Protecting the KSK

DPS

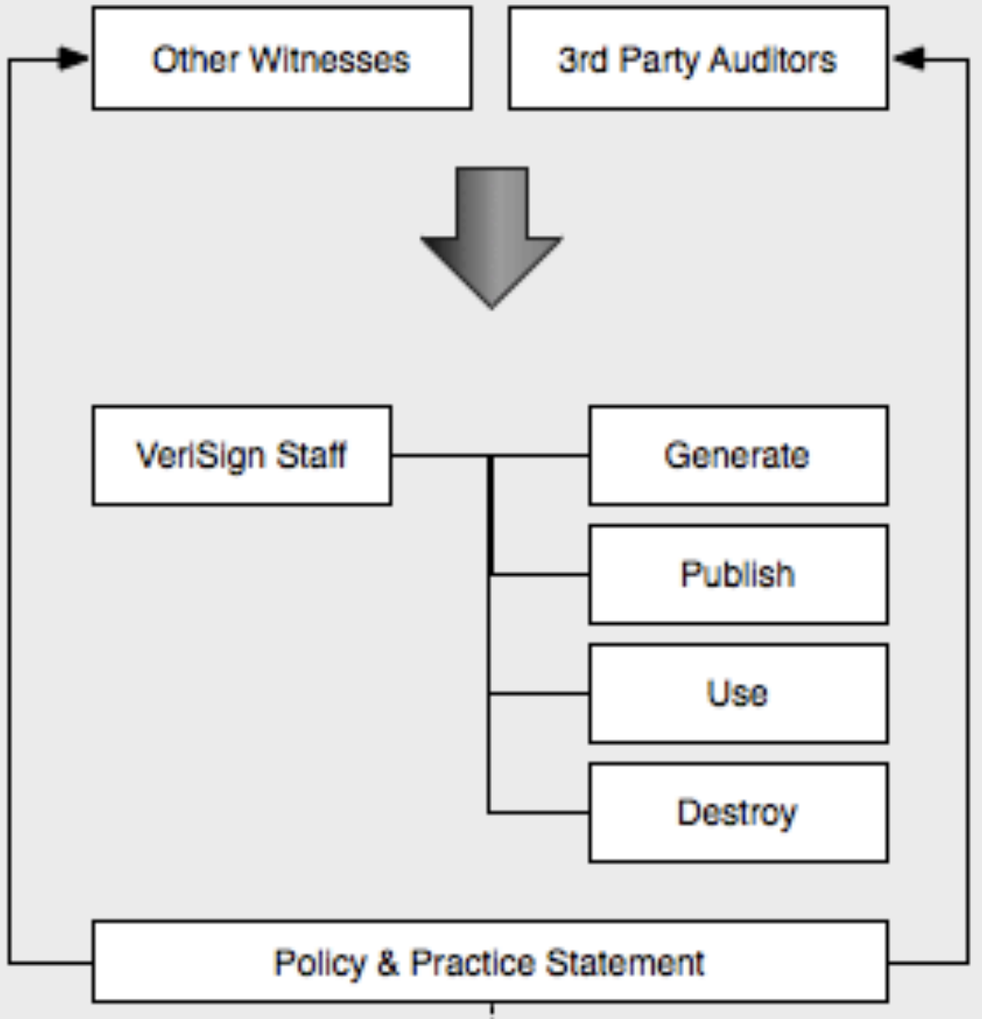
DNSSEC Policy & Practice Statement

- 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 certificate authority (CA)

Proposed Key Signing Key Management



Proposed Zone Signing Key Management



Community Trust

- Proposal that community representatives have an active roll in management of the KSK
  - as Crypto Officers needed to activate the KSK
  - as Backup Key Share Holders protecting shares of the symmetric key that encrypts the backup copy of the KSK

Auditing & Transparency

- Third-party auditors check that ICANN operates as described in the DPS
- Other external witness may also attend the key ceremonies

Proposed DNSSEC Protocol Parameters

Key Signing Key

- KSK is 2048-bit RSA
  - Rolled every 2-5 years
  - RFC 5011 for automatic key rollovers

- Propose using signatures based on SHA-256

Zone Signing Key

- ZSK is 1024-bit RSA
  - Rolled once a quarter (four times per year)
- Zone signed with NSEC
- Propose using signatures based on SHA-256

Signature Validity

- DNSKEY-covering RRSIG validity 15 days
  - re-sign every 10 days
- Other RRSIG validity 7 days
  - re-sign twice per day (with zone generation)

Key Ceremonies

- Key Generation
  - Generation of new KSK
  - Every 2-5 years
- 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

Proposed Deployment

Roll Out

- Incremental roll out of the signed root
  - Groups of root server "letters" at a time
- Watch the query profile to all root servers as roll out progresses
- Listen to community feedback for any problems

No validation

- Real keys will be replaced by dummy keys while rolling out the signed root
  - Signatures will not validate during roll out
  - Actual keys will be published at end of roll out

Timeline

Draft Timeline

- December 1, 2009
  - **Root zone signed**
    - Initially signed zone stays internal to ICANN and VeriSign
  - ICANN and VeriSign begin KSR processing
    - ZSK and KSK rolls
- January - July 2010
  - Incremental roll out of signed root
- July 1, 2010
  - KSK rolled and trust anchor published
  - **Signed root fully deployed**

ISP Security BOF

- Monday October 19, 1630

- Time set aside there for more technical discussion and Q&A

- Or find Joe