Signing the Root

a comparison between the two root signing proposals from ICANN and Verisign

Jakob Schlyter – jakob@kirei.se
RIPE'57, Dubai, United Arab Emirates

Executive Summary

ICANN vs Verisign

Similarities

- Root zone maintainer signs the zone.
- Root zone maintainer creates the ZSK.

Differences

- Who should be the root zone maintainer?
- Who should control the KSK?

Background

Definitions

- TLD Manager
- Zone Autenticator
- Zone Editor and Compiler
- Zone Signer
- Zone Auditor
- Zone Distributor

Definitions

- TLD Manager – the one managing a TLD
- Zone Autenticator – ICANN
- Zone Editor and Compiler – Verisign
- Zone Signer – doesn't exist (yet)
- Zone Auditor – U.S. Department of Commerce
- Zone Distributor – Verisign

Today

1. TLD Manager submits request to ICANN.
2. ICANN processes the change request.
3. ICANN sends change request to both US DoC and Verisign.
4. US DoC authorizes the change request.
5. Verisign updates the zone file.
6. Verisign distributes the zone to the root server operators.

KSK Control and Use

ICANN

- Parties, to be defined by the community, participates in the KSK generation and publication through a *Key Ceremony*.
- The KSK is generated by and stored in a HSM located at ICANN (but might be controlled by other organisations).
- Exact usage of the KSK to be defined by the community.

Verisign

- The root server operators participates in the KSK generation and publication through a *Key Ceremony*.
- The KSK is generated by and stored in a HSM at Verisign.
- Only M-of-N root server operators can authorise usage of the key.
- Root server operators gather once a year to sign the DNSKEY RRsets for the next 12 months.

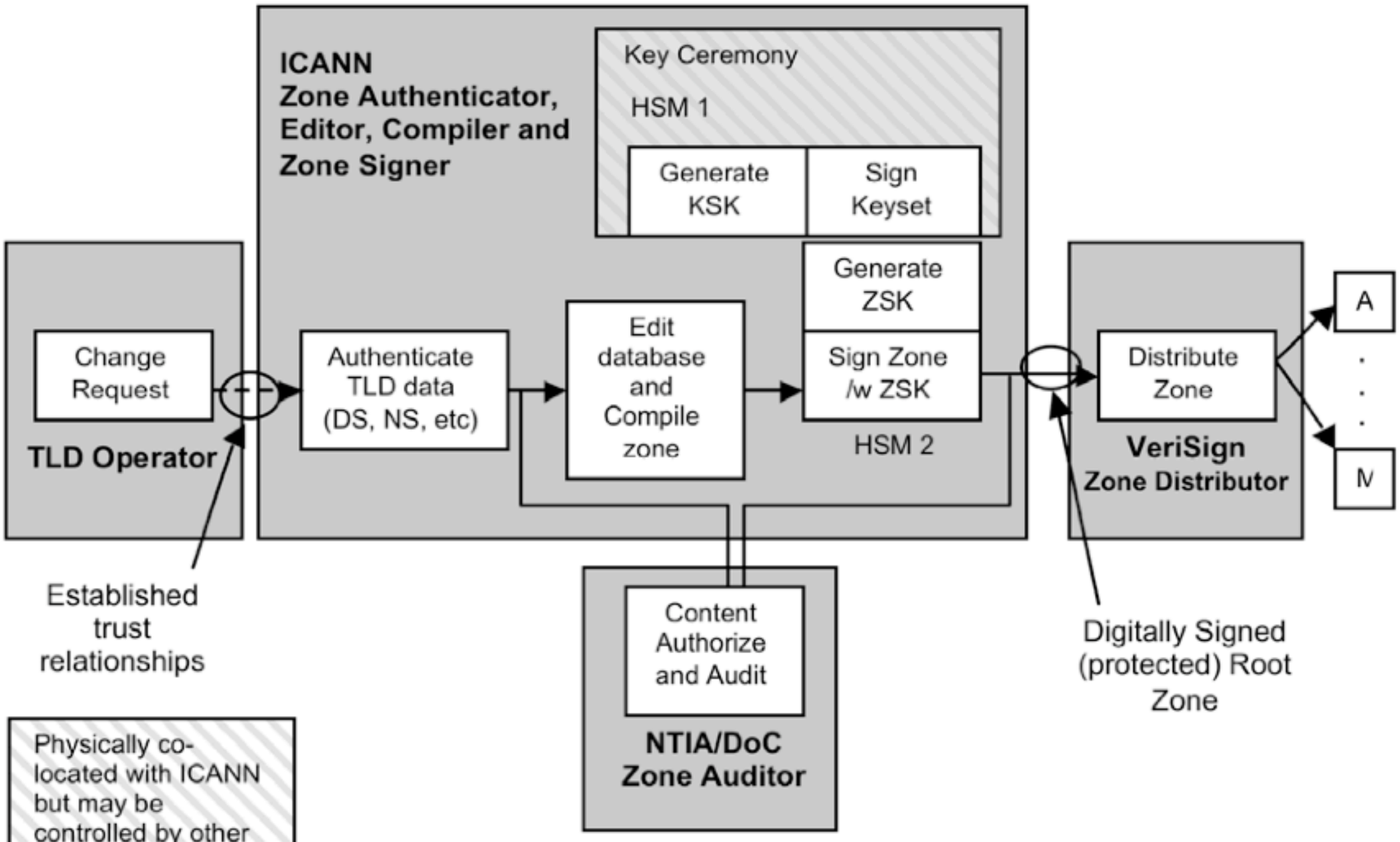
Root Zone Generation & Signing

At first...

1. TLD Manager submits request to ICANN.
2. ICANN processes the change request.
3. US DoC authorizes the change request.

ICANN

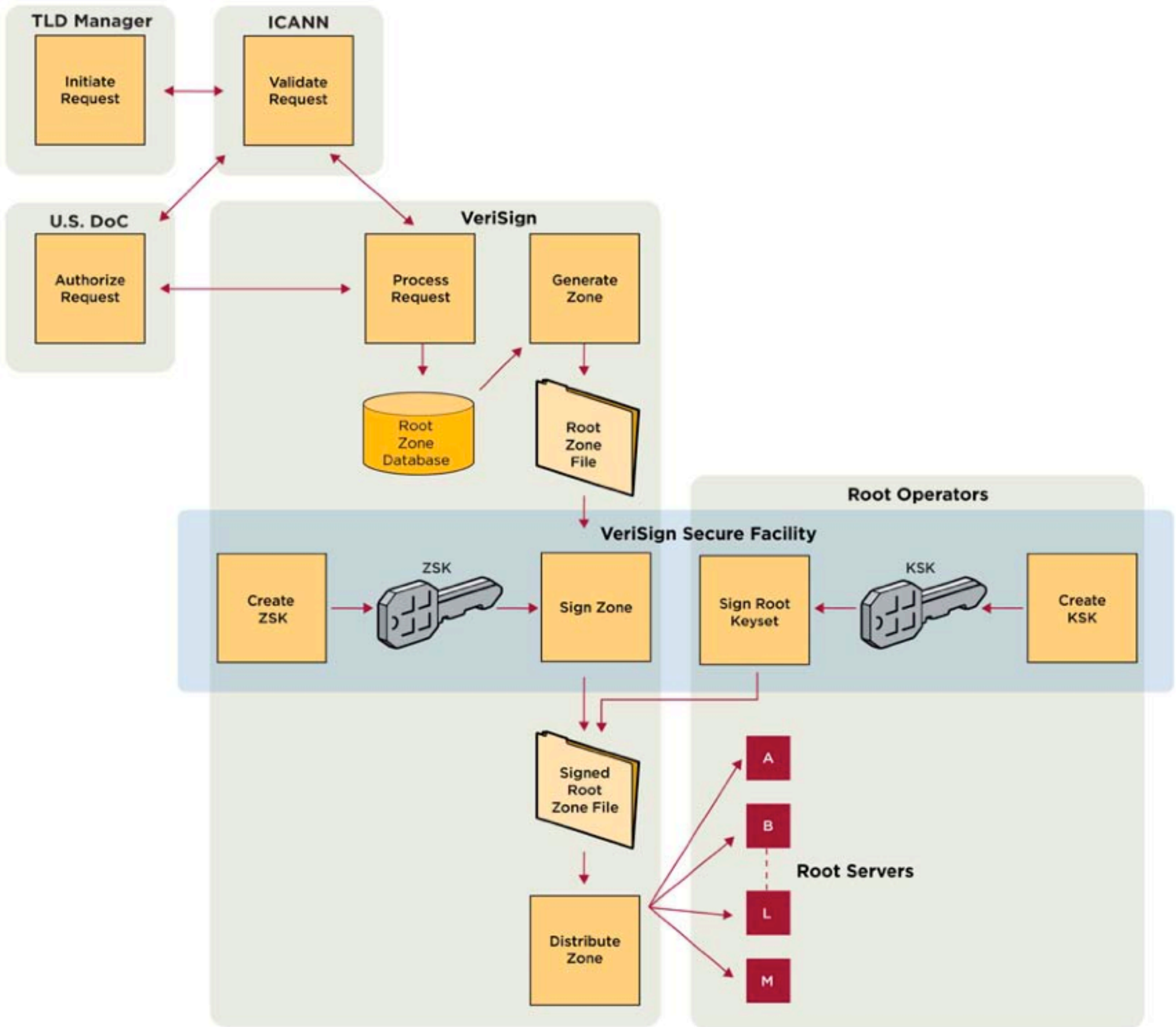
4. ICANN edits the root zone.
5. ICANN signs the root zone.
6. ICANN transfers the signed root zone to Verisign.
7. Verisign distributes the signed zone to the root server operators.



Simplified diagram showing ICANN as the single signing entity

Verisign

4. ICANN sends the authorised request to Verisign.
5. Verisign edits the root zone.
6. Verisign signs the root zone.
7. Verisign distributes the signed zone to the root server operators.


TLD Manager
Initiate Request
ICANN
Validate Request
U.S. DoC
Authorize Request
VeriSign
Process Request
Generate Zone
Root Zone Database
Root Zone File
Root Operators
VeriSign Secure Facility
Create ZSK
ZSK
Sign Zone
Sign Root Keyset
KSK
Create KSK
Signed Root Zone File
Distribute Zone
A
B
L
M
Root Servers

The Next Step

Notice of Inquiry

U.S. Department of Commerce

National Telecommunications and Information Administration

Enhancing the Security and Stability of the Internet's Domain Name and Addressing System

The Notice of Inquiry

The Department of Commerce (Department) notes the increase in interest among government, technology experts and industry representatives regarding the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. The Department remains committed to preserving the security and stability of the DNS and is exploring the implementation of DNSSEC in the DNS hierarchy, including at the authoritative root zone level. Accordingly, the Department is issuing this notice to invite comments regarding DNSSEC implementation at the root zone.

Comments to

dnssec@ntia.doc.gov

Comments are due on

November 24, 2008

Comments will be posted at

http://www.ntia.doc.gov/DNS/DNSSEC.html

Do send comments!

It's not for U.S. Citizens only…

The End