DNSSEC Signing the Root & ICANN Update

RIPE NCC Regional Meeting

Moscow, Russia, 17 September 2009

Rick Lamb richard.lamb@icann.org

DNSSEC Timeline

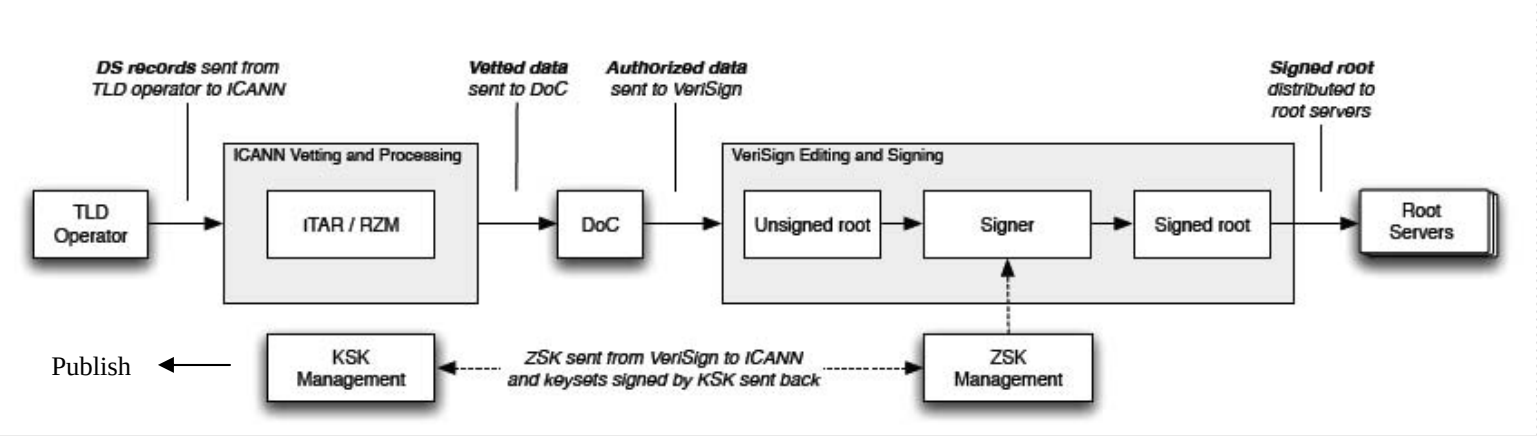
- Decades of development
- Trailblazing work by .se
- Continual and consistent Internet Community pressure to get the root signed – thank you RIPE
- Signed root testbeds
- pr, .br, .bg, .cz, .gov, .org, .th
- Experience over F.U.D.
- Kamninsky
- Proposals to sign the root
- NOI
- DoC Testing and Implementation Requirements for Interim signed root

Signing the Root

- Goal: Interim signed root by end of the year
- Following requirements from NTIA and NIST for interim signed root
- Intense cooperative effort between VeriSign and ICANN engineers

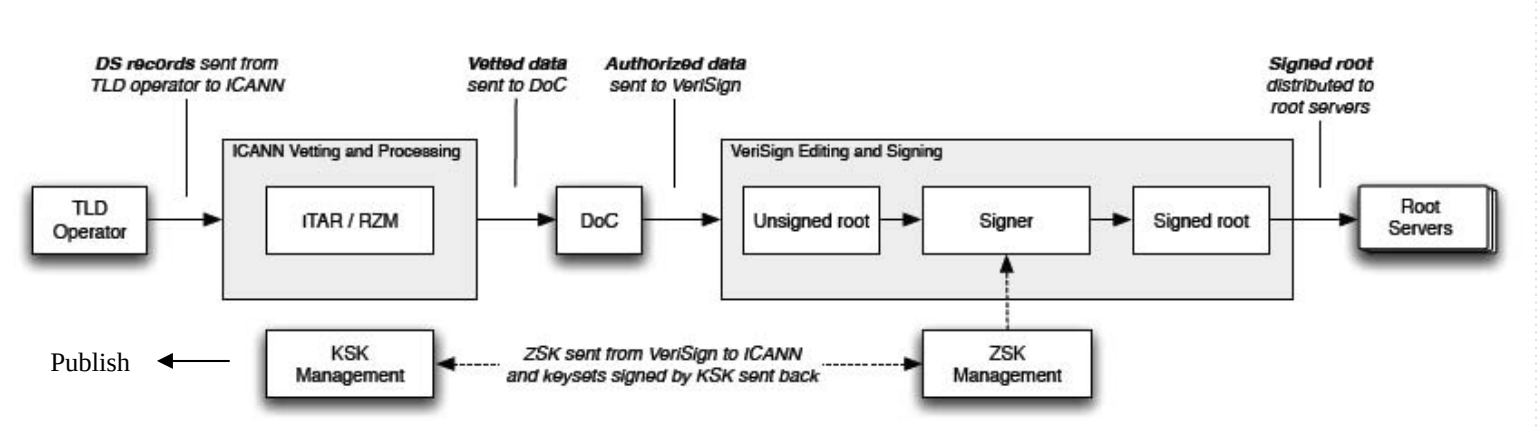
Technical Work in Progress - Flow

- TLD DS Flow



Technical Work in Progress - Flow

- KSK/ZSK Flow



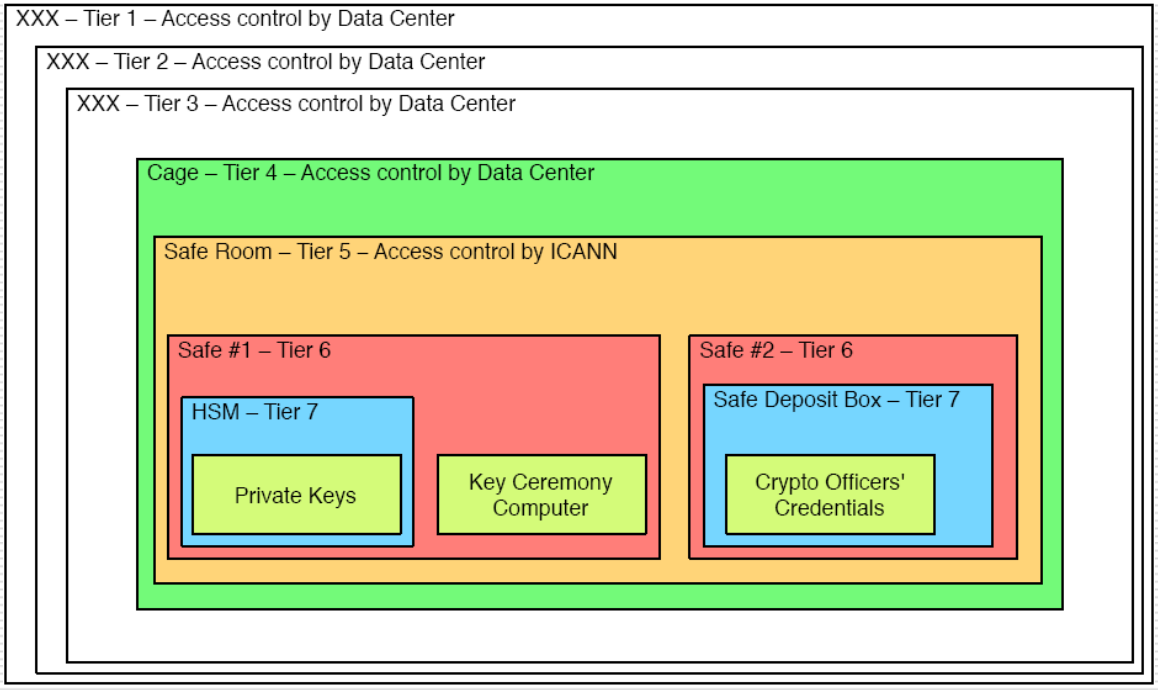
- Key Signing Request
  - XML
  - Proof of private key ownership
  - Signed

Technical Work in Progress - Key Management

- Initialization/Generation/Rollover/Backup
- Publication
- Signing
- Internet Community participation
- 3rd party Audit / DPS
- Parameters

Technical Work in Progress - Security

- Logical
  - Smartcards / m-of-n
- Physical
  - Facilities
  - Tiers
  - Safes
  - Boxes



ICANN Related Zones

- arpa - working with IAB, VeriSign, and NTIA
- in-addr.arpa – working with RIRs
- int – working with NTIA
- ip6.arpa, urn.arpa, uri.arpa, iris.arpa – just us
- iana.org, icann.org – just us

- Goal: Get them signed as quickly as possible

- Design: Generic Signing Infrastructure
  - Considering OpenDNSSEC

Questions?