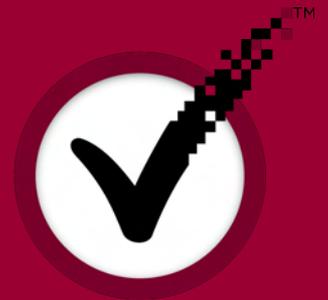


DNSSEC Root Zone Signing Proposal

Pat Kane



Proposal Attributes

- + Preserves the existing roles and responsibilities
- + Shares responsibility of the root zone key-signing key (KSK)
- + Calls for root zone maintainer to sign the root zone
- + Uses existing and proven resources and processes
- + Calls for significant testing before production deployment

Preserve Existing Roles and Responsibilities

- + No changes to established roles that have been in place for many years and have proven reliable
- + IANA function: accepts and checks change requests from TLD community and vets them
 - A procedural role
- + DoC NTIA: authorizes changes for inclusion in the root zone
 - An oversight role
- + VeriSign: generates root zone and distributes to root servers
 - A technical role
- + Each role appropriate to the particular organization's capabilities and expertise

Shared Responsibility for Root Zone KSK

- + KSK should have multiple organizations to share responsibility
 - Risks of organizational failure or capture
- + Control can be split with M-of-N authorization technique
- + If key is split, which N organizations control it?
- + Proposal: existing 12 root operators
 - Already trusted to publish the root zone
 - Established track record of technical operations
 - Varied organizations (multiple countries and organization types)
 - Neutral, with no stake in contents of the root zone
- + Need a qualified third party as KSK custodian
 - Custodian ensures safety of the KSK but cannot use it

VeriSign to Sign the Root Zone

- + Appropriate for organization that generates and distributes the zone to sign it
 - Would be complicated, require extra protections and potentially introduce delay to sign zone elsewhere
- + Signing organization should generate and manage zone-signing keys (ZSKs)
 - Shorter-term, lower-value keys
 - Hardware Security Module (HSM) issues
- + VeriSign is the current root zone maintainer and should therefore sign the root zone

Existing and Proven Resources and Processes

- + Root zone signing is an important function and must be treated accordingly:
 - **Appropriate facilities for key storage and signing**
 - Secure, multi-tier access, biometric authentication
 - FIPS 140-2-compliant HSMs
 - Key ceremony room for secure, transparent and auditable key generation
 - **Mature and documented processes**
 - Clear roles and responsibilities
 - **Experienced personnel**
 - Familiar with industry-standard processes
- + Certificate Authority business makes VeriSign uniquely qualified for:
 - **Creating ZSKs and signing the root zone**
 - **Acting as KSK custodian to securely facilitate KSK creation and use**

Significant Testing

- + Signing the root would be the biggest change to the DNS since its creation
- + Cannot just sign the root and hope for the best!
- + Need a widely used test bed to discover problems before production deployment
 - Cannot knock entire cities off the Internet
- + Proposal: Advanced Root Services Testbed
 - Existing root operators (all or a subset) run additional root servers
 - These testbed servers load a signed root zone
 - Recursive name server operators opt-in by installing the testbed's "root hints file"
 - Test bed would be widely publicized but time-bounded to not live forever

Proposed Architecture

