VeriSign Root Improvements

January 31, 2007

VeriSign Root Improvements

+ IPv6
+ DNSSEC
+ Root Zone Management System

IPv6 Transport for Root Servers

- **February 4, 2008**: an important step forward for the IPv6 Internet!
- IPv6 addresses for VeriSign's two root name servers (and four others) added to the root zone
  - *a.root-servers.net:* 2001:503:BA3E::2:30
  - *j.root-servers.net:* 2001:503:C27::2:30
- These IPv6-enabled root servers:
  - Accept DNS queries received over IPv6
  - Send DNS replies back over IPv6
- Now possible for a recursive name server to resolve names using only IPv6 transport using:
  - IPv6 root name servers
  - IPv6 TLD name servers (including *.com* and *.net*)
  - IPv6 name servers for lower-level zones

DNSSEC for the Root Zone

+ Signing the root zone with DNSSEC would represent an important step forward in improving overall Internet security
+ A DNSSEC-signed root requires new activities, including:
  - Root key (key-signing key, or KSK) ownership, creation and maintenance
  - TLD key information (delegation signer, or DS record) provisioning in the root by IANA
  - Actual root zone signing (with zone-signing key, or ZSK) by VeriSign, which generates and publishes the root zone today
+ VeriSign can help advance DNSSEC signing the root by DNSSEC-enabling our root zone maintenance processes

DNSSEC Timeline and Phases

- VeriSign commits to making our root zone maintenance processes DNSSEC-capable by Q2 2008
- Plan two phases:
  - Phase 1: Initial signing (Q2 2008)
    - Obtain DS records for DNSSEC-enabled TLDs manually
    - Generate zone-signing keys (ZSK)
    - Sign the root zone
    - Make the signed zone available for test and pilot purposes
  - Phase 2: Add DNSSEC provisioning (Q3 2008)
    - Implement RFC 4310 DNSSEC extensions for EPP
    - Work with IANA to allow provisioning of DNSSEC info (DS records) for the root zone using EPP

DNSSEC Implementation Details

+ Root zone key-signing key (KSK)
  - Initial implementation allows for, but runs without, root zone KSK
  - Implementation assumes that in eventual production:
    - KSK will be generated by another party yet to be determined
    - VeriSign-generated ZSKs will be sent to this other party for signing
    - Signed KSK and ZSKs signed by KSK included in signed root zone
+ Signing environment
  - Key management and operating a secure signing environment is one of VeriSign's core strengths
  - Root zone DNSSEC signing will use the same procedures and environment that run VeriSign's certificate signing operations

Root Zone Management System

+ VeriSign has developed a new registry, the Root Zone Management System (RZMS), dedicated to the specific needs of the root zone:
  - Dedicated database to isolate root zone data
  - Workflow system to automate request processing and verification, and provide tracking and auditing
  - EPP interface with IANA to remove ambiguity inherent in legacy email template system
+ VeriSign's new system will interface with IANA's new Root Zone Management Workflow Automation system which:
  - Provides a web-based interface for TLD operators to submit changes
  - Has an EPP client to interface with VeriSign's new root registry system
+ VeriSign's and IANA's new systems will completely replace the legacy email templates with a modern, automated workflow system

Root Zone Management Improvements Timeline

- May 2007: VeriSign RZMS deployed in testing environment for IANA integration and testing
- August 2007: IANA integration testing begins (ongoing)
- Q2 2008 (projected): Parallel operations begin
  - During parallel operations, all root zone changes will be processed in both old and new systems (at both VeriSign and IANA)
  - Output of two systems will be compared: results must be identical
- Parallel operations will proceed for at least six months to ensure accuracy and stability of the new system