The Day The Root Got Signed

VeriSign, Inc.

Root Zone Team
Outline

- VeriSign’s role in signing the root zone
  - Key management
  - Twice-daily signing operations
- A few photos from July 15th
- An obligatory graph
Zone Signing Keys

- VeriSign is responsible for the ZSK
- 1024-bit RSA with SHA-256
- New ZSK every 3 months
- Key material managed by VeriSign’s Cryptographic Business Operations unit
ZSK Ceremony

- 6 Trusted Persons
- 20 – 25 Minutes
- Past ceremonies were held in Mountain View, CA
  - these facilities went to Symantec in the recent sale
- New ceremony rooms in two geographically diverse locations on U.S. East Coast
- Output is a Key Signing Request ("KSR")
Key Signing Request

```xml
<RequestPolicy>
  <ZSK>
    <PublishSafety>P10D</PublishSafety>
    <RetireSafety>P10D</RetireSafety>
    <MaxSignatureValidity>P20D</MaxSignatureValidity>
    <MinSignatureValidity>P15D</MinSignatureValidity>
    <MaxValidityOverlap>P5D</MaxValidityOverlap>
    <MinValidityOverlap>P5D</MinValidityOverlap>
    <SignatureAlgorithm algorithm="8">
      <RSA size="1024" exponent="3"/>
    </SignatureAlgorithm>
  </ZSK>
</RequestPolicy>
```
ICANN holds the KSK and therefore must sign the root DNSKEY RRset

VeriSign sends Key Signing Request to ICANN every 3 months

ICANN holds a key ceremony and signs the DNSKEY RRset (all KSKs and ZSKs)

ICANN sends back a Signed Key Response ("SKR"), which contains RRSIGs

RRSIGs are added to the root zone data
- New root zone generated twice per day
- Many technical checks and validations
- Every difference between current zone and new zone must be correlated to an authorized root zone change
Signing and Publication

- Zone signed within secure facility
  - Signing system pulls zone in, signs it, and pushes it back out
  - Cannot push zone into signing system because of security policy

- All new signatures in each new zone

- Post-signing validation
  - Two validation tools written in different languages (Java, Perl) by different teams

- Manual approval required to publish new root zone

- Zone published to stealth master name servers and FTP site
Crypto Validation of root 2010071501

OK: 2 trusted KSKs found
OK: Apex DNSKEY RRset validated
OK: 0 expiring RRSIGs found
OK: 0 bad RRSIGs found
OK: 299 good RRSIGs found

Comparison to current zone

OK: Received 3655 RRs from 10.0.0.1
OK: Current serial 2010071500
DIFF: KSK 1 added, 1 removed, 0 unchanged
DIFF: ZSK 1 added, 1 removed, 0 unchanged
DIFF: RRSIG 1 added, 1 removed, 298 unchanged
DIFF: DS 0 added, 0 removed, 10 unchanged

Validation for root 2010071501 PASSED, 0 problems
Photos

From the Big Day
Piet Barber, Naming Resolution Operations
Brian Coppola (ResOps) and Ramesh Balasubramanian (Technical Support/Development)
Brad Verd (ResOps) and Mike Rader (Naming Product Operations)
Colleen Louw (Product Management), Tim Roe (Naming Product Operations), Greg Patrick (Resolution Operations)
Thomas Nguyen, Naming Resolution Operations
Matt Larson, VeriSign Labs, manually verifies the printed root zone!
Lots of photos snapped as the validatable root zone is published.
Graph

Sorry, must include at least one.
DNSKEY Queries
At A-root

Maintenance Window

Validatable Zone
Published at 20:50 UTC
R. I. P.
THE DURZ
Jan 27 - July 15
2010