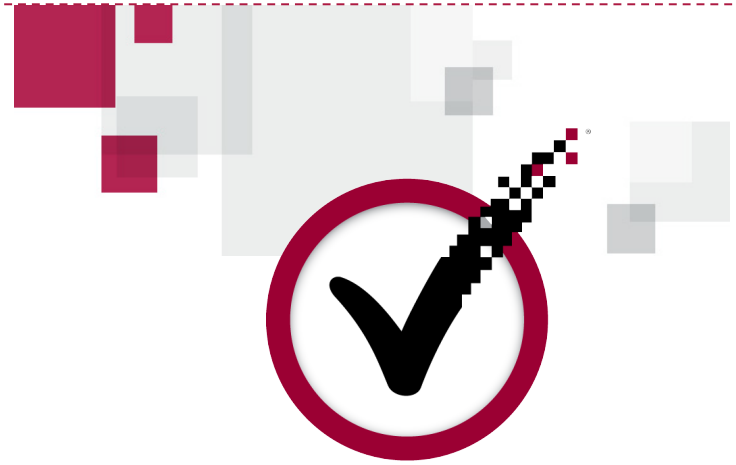
VeriSign®



DNSSEC Implementation Approach Panel

ICANN 39, Cartagena, Colombia

8 December 2010

Matt Larson

Vice President, DNS Research

VeriSign, Inc.

DNSSEC in *.com/.net*: High-level Design

- Tremendous scale of *.com/.net* requires entirely custom DNSSEC solution
- Registration system
  - Incremental signing
  - Signing server component abstracts multiple HSMs in multiple Tier 4 facilities
- Resolution
  - DNSSEC-enabled ATLAS, VeriSign's custom high-performance authoritative name server
- Key management
  - Cryptographic Business Operations (CBO) manages all key material
  - KSK offline

DNSSEC in *.com/.net*: Implementation

- Cautious and measured approach throughout
- Before deployment
  - EPP SDK with DNSSEC support
  - End-to-end operational Test & Evaluation (OT&E) environment, including both registration (EPP) and resolution (signed *.net* zone)
  - DNSSEC tool guide describing tools for DNSSEC implementation and corresponding tool kit (for registrars)
  - DNSSEC transfer white paper (for registrars)
  - Cloud signing service (for registrars)
  - DNSSEC interoperability lab (for hardware and software vendors)
  - Various tools, including DNSSEC debugging tool
    - *dnssec-debugger.verisignlabs.com*
- Deployment
  - *.net* before *.com*
  - Registration system DNSSEC-enabled first
  - Deliberately unvalidatable zone

DNSSEC in *.com/.net*: Challenges

- Scale
- Signing speed
  - Registration system SLAs
- Zone size
  - NSEC3 with Opt-out
- Scope
  - DNSSEC implementation affects every component
- Registrar adoption
  - DNSSEC needs registrar support to succeed
- Importance
  - *.com* and *.net* can't go down. Ever.

DNSSEC in *.com/.net*: Lessons Learned

- Incremental deployment possible
  - Deliberately unvalidatable zone concept
- RFC 4310 (EPP DNSSEC extensions) needed some changes
  - Now have revised specification, RFC 5910
- Minimal increase in TCP queries
  - Less than 1%
- DNSSEC does not break the Internet
  - Root signing uneventful
  - No issues with *.net* deployment thus far