



DNSSEC in .com, .net and .edu

Matt Larson

Vice President, DNS Research

Office of the CTO



■ DNSSEC Program

- Methodical, incremental DNSSEC rollout to reduce implementation risk
- Implement DNSSEC in **.edu**, then **.net**, then **.com**
- Assist registrars
 - Tools and support to aid DNSSEC deployment
 - DNSSEC-capable Operational Test Environment (OTE)
- Interoperability lab for hardware vendors, ISPs, registries and registrars



■ DNSSEC in .edu

■ EDUCAUSE

- *“EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.”*
- Registry operator (business perspective) for .edu
- Cooperative agreement with U.S. DoC
- Sole registrar for .edu names

■ VeriSign

- Registry operator (technical perspective) for .edu
- Subcontractor to EDUCAUSE





■ DNSSEC in .edu

- DNSSEC deployment in .edu is a partnership between EDUCAUSE and VeriSign
- EDUCAUSE
 - DNSSEC-enable registrar systems
 - Accept key material from .edu registrants
 - Submit key material to VeriSign
 - Participate in test bed with selected institutional partners
- VeriSign
 - DNSSEC-enable registry system
 - Accept key material from .edu registrar
 - Publish signed .edu zone
 - Participate in test bed





Testbed Details

- Small number of institutions invited by EDUCAUSE to participate
- End-to-end testing:

Institution → EDUCAUSE → VeriSign → Test bed .edu zone file

- Test bed zone hosted on publicly accessible name servers
- Benefits:
 - EDUCAUSE and VeriSign can exercise new DNSSEC systems
 - Institutions gain experience, watch changes flow from UI to signed zone
- Test bed will not track production .edu contents
 - Production data copied to test bed once
 - Test bed contents will diverge over time





■ DNSSEC Parameters for .com, .net and .edu

- NSEC3 with Opt-Out
- RSA with SHA-1
- 2048-bit KSK
 - Rolled infrequently
- 1024-bit ZSK
 - Rolled quarterly
- DS changes provisioned over EPP
 - RFC 4310



DNSSEC Timeline

- Q1 2009: EPP SDK with DNSSEC released
- Q3 2009: .edu testbed opened
- Q3 2009: RSEP submission for .com and .net
- Q1 2010: .com/.net OTE available
- Q1 2010: **.edu signed**
 - Smaller zone, single registrar
- Q4 2010: **.net signed**
 - Larger zone, full registrar base
- Q1 2011: **.com signed**
 - Largest zone last after successful implementation in .net





Questions + Answers

Q + A

QUESTIONS + ANSWERS

