VeriSign's DNSSEC Plans for *.com*, *.net* and the root

Matt Larson

Vice President

Office of the CTO

Securing the DNS: Towards a more secure Internet

Internet Society panel

Stockholm, Sweden

28 July 2009

VeriSign’s DNSSEC History

- Long involvement with DNSSEC
  - Since early days of its development
  - Standards, research and development, prototypes and pilots
- DNSSEC standards development in the IETF
  - Core DNSSEC standard (RFCs 4033, 4034, 4035)
  - NSEC3 and Opt-Out (RFC 5155)
- Pilots
  - Projects open to public participation to test new concepts and protocols
  - Six DNSSEC-related pilots since 2000, including a signed root zone
- Unbound
  - Recursive name server and DNSSEC validator
  - Initial design and prototype work
  - Foundation for *www.unbound.net*

VeriSign's DNSSEC Plans

- Recognize demand for DNSSEC in *.com* and *.net*
- Largest change to DNS…ever
- Everything gets larger
  - Larger responses ➔ more bandwidth
  - Larger zones ➔ more memory, disks and bandwidth
- Major development effort
  - Every registry component affected
    - Registrar interface (EPP), database schema, business rules, new signing engine, DNS resolution (ATLAS), monitoring, and more
- Proceeding cautiously but deliberately

DNSSEC in *.net* and *.com*

- ***.net*** will be signed by the end of 2010
- ***.com*** will be signed in early 2011
- Details:
  - NSEC3 and Opt-Out
  - Registrars provision DS records with DNSSEC EPP extensions (RFC 4310)

DNSSEC in the Root Zone

- Root zone signing requirements developed by U.S. Department of Commerce
  - Invited expert technical review happening now
- Collaboration between VeriSign and ICANN
- VeriSign (as root zone maintainer):
  - Creates and manages zone-signing keys (ZSKs)
  - Creates, signs and publishes the root zone
- ICANN (as IANA functions operator):
  - Creates and manages key-signing keys (KSKs)
  - Signs root zone key sets
  - Publishes KSKs to the community
- Working toward implementation in 2009