Implementing DNSSEC at the Root

NTIA – ICANN – VeriSign

ICANN DNSSEC Workshop
June 24, 2009
Notice of Inquiry

• NTIA issued a Notice of Inquiry (NOI) on the implementation of DNSSEC at the root zone level on October 9, 2008.

• Fifty five (55) comments from industry, non-profit organizations, academia, and individuals were submitted by the November 24, 2008 deadline.

• http://www.ntia.doc.gov/DNS/dnssec.html
NOI Results

• The NOI process revealed almost unanimous consensus among the 55 respondents that DNSSEC should be implemented at the root zone level.

• Other important points raised through the process:
  – Implement DNSSEC as soon as practically possible,
  – Implement in a manner that maintains the security and stability of the DNS,
  – DNSSEC implementation should be aligned with functions of the root zone management process,
  – DNSSEC is about data, integrity, and authenticity – not control.
Post NOI – Moving Forward

• DNSSEC to be implemented with a goal of a signed root by the end of 2009.

• An interim approach closely aligned with the existing root zone management process will be utilized to ensure rapid implementation while maintaining the security and stability of the DNS.

• Once implemented, interim approach will be reviewed taking into consideration any advancement in technology, process and/or procedure related to DNSSEC, to determine whether the approach needs to be adjusted.

• This is an iterative process that will include ongoing consultation with the DNS technical community.
Basic Architecture

- IANA Functions Operator (ICANN) Responsibilities
  - Root Key Signing Key (KSK) management process, in consultation with VeriSign.
  - Publication/Distribution of the Root Key
  - Receive and process TLD public key information
Basic Architecture

• Root Zone Maintainer (VeriSign) Responsibilities
  
  – Sign Root Zone as a part of existing root zone generation and distribution responsibilities
  
  – Management of the Zone Signing Key (ZSK) process, in consultation with ICANN
Current Root Zone Management

TLD Operator
  Change Request

IANA Functions Operator
  ICANN
  Per the IANA functions contract
  Process Change Request

Root Zone Maintainer
  VeriSign
  Per the Cooperative Agreement
  Edit Database/Generate Zone File
  Distribute Zone File

Root Server Operators
  A, B, C, M

Administrator
  NTIA
  Verify/Authorize Change Request
Root Zone Management + DNSSEC

KSK management process to be led by the IANA Functions Operator (ICANN) in consultation with the Root Zone Maintainer (VeriSign). Further details to be developed taking into account baseline technical requirements from the Department and subject to Department approval.

IANA Processing
- TLD Change Request + TLD Public Key Update
  - Change Request + Public Key Updates
  - Generate KSK
  - Sign Root Keyset

IANA Functions Operator

Root Zone Maintainer
- Generate ZSK
- Edit Database/Generate Zone File
- Sign Zone
- Distribute Zone File

Root Server Operators
A, B, C, M

Administrator
- Verify/Authorize Change Request

TLD Operator
- Change Request + Public Key Updates

Distribute Root Public Key to DNS Community
Next Steps

- Seek input on draft technical requirements from technical community
- ICANN and VeriSign to draft testing and implementation plans
- Consult with technical community on draft testing and implementation plans
- Initiate testing