Final Report on DNSSEC Deployment Testing and Evaluation in the Root Zone

Executive Summary

This document summarizes the results and observed effects of testing deployment of DNSSEC in the root zone of the DNS. It is our finding that testing was successful and that no harmful effects of the implementation have been observed despite extensive measurement and observation.

Supported by the summary of the design, documentation, implementation and testing work already completed and described here, ICANN and VeriSign request authorization to proceed with full deployment of DNSSEC in the root zone.

Contact Information

This document was jointly prepared by ICANN and VeriSign. For more information, please contact:

Joe Abley
Director, DNS Operations, ICANN
joe.abley@icann.org
+1 310 578 8673

Matt Larson
VP DNS Research, VeriSign Labs
mlarson@verisign.com
+1 703 887 3690

Table of Contents

Introduction

The US Department of Commerce (DoC) issued a draft set of high-level requirements in August 2009 for the deployment of DNSSEC in the root zone. The requirements anticipated a collaboration between the Internet Corporation for Assigned Names and Numbers (ICANN) acting as IANA Functions Operator per the IANA functions contract, VeriSign, Inc. (VeriSign) acting as Root Zone Maintainer per the Cooperative Agreement, and DoC acting as Root Zone Administrator. Together, the three organisations would design, document and implement processes and systems to meet the DoC requirements.

These high-level requirements were subsequently finalized in a document[1] issued by DoC to its root zone management partners ICANN and VeriSign in October 2009. Although this document identified a "goal of an operationally signed root by year-end 2009" it was agreed between the parties that responsible deployment would take longer. It was initially estimated that an operationally-signed root zone would be available in July 2010, and the implementation continues to support that target launch window. The target deployment date is 2010-07-15[2].

[1] "Testing and Implementation Requirements for the Initial Deployment of DNSSEC in the Authoritative Root Zone", DOC, 2009-10-26

[2] Technical Status Update issued 2010-05-18, http://www.root-dnssec.org/2010/05/18/status-update-2010-05-18/

Design

ICANN and VeriSign (the Design Team) developed an implementation approach[3] which is prudent and conservative with respect to the stability and security of the global Domain Name System (DNS), and which also meets the technical requirements of DoC.

The responsibilities for various aspects of deploying DNSSEC in the root zone have been divided between ICANN and VeriSign in such a way that existing roles for root zone management are preserved and minimally extended.

ICANN will provide the interface to Top-Level Domain (TLD) managers for submission of DNSSEC public key data, consistent with its role as IANA Functions Operator. In this role, ICANN is also responsible for the management and operation of the root zone Key Signing Key (KSK), including key initialisation, exercising the key and publishing trust anchors. ICANN also undertakes to involve the Internet technical community in the execution of various aspects of key management to provide a high level of transparency and engender trust in the key management and, by extension, in the trust anchor. ICANN is solely responsible for the KSK.

DoC is responsible for authorizing changes to the root zone. With the deployment of DNSSEC, this role is expanded to include authorization of TLD DNSSEC public key material (DS RRSets[4]) and KSK-signed key material (the root zone DNSKEY RRSet[5]) for inclusion in the root zone.

VeriSign, in its role as Root Zone Maintainer is responsible for incorporating DoC-authorized DNSEC-related changes into the root zone, signing the root zone with the Zone Signing Key (ZSK), and distributing the resulting signed root zone to root servers. VeriSign is solely responsible for the ZSK.

Details of the implementation approach have been presented[6] by the Design Team to technical audiences at various operational and engineering venues. The technical, engineering expertise within the Design Team together with the combined experience of the audiences of these briefings supports the finding that the approach is technically sound and operationally prudent.

---

[3] The design approach is documented in "DNSSEC Root Zone High Level Technical Architecture", "DNSSEC Practice Statement for the Root Zone KSK Operator", and "DNSSEC Practice Statement for the Root Zone ZSK operator" which can be found at http://www.root-dnssec.org/documentation/

[4] The Delegation Signer (DS) Resource Record Set (RRSet) is a cryptographic representation of a child zone's KSK; in this case, the child is a TLD.

[5] The DNSKEY RRSet contains the public part of both Zone Signing Key (ZSK) and Key Signing Key (KSK) key airs, and is accompanied by a signature from the KSK.

[6] Copies of presentation materials can be found at http://www.root-dnssec.org/presentations/

Documentation

Interim, draft documentation has been made available to the Internet technical DNS community periodically as the approach was under development, and all suggestions provided to the design team have been considered and, where appropriate, incorporated.

The presentation format of some technical documents, specifically those whose target audience was primarily from the Internet engineering community, was chosen to be consistent with the technical documentation conventions of the Internet Engineering Task Force. These documents were formatted as plain text with two-digit, monotonically-increasing, integer version numbers starting at zero.

The project documentation submitted to DOC for consideration in support of this document is as follows. All documents are available in full at http://www.root-dnssec.org/documentation/.

Date	Revision	Title
2010-05-07	1.3	DNSSEC Root Zone High Level Technical Architecture
2010-05-07	01	DNSSEC Trust Anchor Publication for the Root Zone
2010-05-07	01	Root Zone DNSSEC KSK Ceremonies Guide
2010-05-05	02	DNSSEC Deployment for the Root Zone
2010-05-17	02	DNSSEC Practice Statement for the Root Zone ZSK Operator
2010-05-21	02	DNSSEC Practice Statement for the Root Zone KSK Operator
2010-05-11	01	DNSSEC Key Management Implementation for the Root Zone
2010-04-08	01	Trusted Community Representatives – Proposed Approach to Root Key Management
2010-05-12	00	DNSSEC Test Plan for the Root Zone
2010-05-07	01	Resolver Testing with a DURZ
2010-02-17		IANA TLD Modification Template
2010-05-08	00	Placing TLD Trust Anchors in the Root Zone
2010-05-01		RFC 5011 Testing, Interim Report

Date	Revision	Title
2010-05-26	1.6	Final Report on DNSSEC Deployment Testing and Evaluation in the Root Zone

Testing and Implementation

The Design Team proposed and moved forward with a staged, incremental testing of DNSSEC deployment in the root zone.[7] DNSSEC information was introduced into the root zone one group of root servers at a time, and each transition was scheduled to allow substantial time for measurement and analysis.

This staged testing implementation required the involvement of the Root Server Operators. The Design Team has productively engaged the Root Server Operators since the early stages of the project. Together, the Design Team and the Root Server Operators worked constructively to ensure that the operational measurement and deployment tasks required of the implementation plan were executed on schedule and in an operationally responsible manner.

Testing was supported by the largest coordinated measurement exercise ever attempted on the DNS's root server system. Substantial volumes of source data were collected from all 13 root servers as part of this implementation, and centralized storage and analysis facilities were secured which ensure that the data will remain available to a controlled but open community[8] for at least ten years following collection, to support ongoing research and analysis.

The DNSSEC information that was rolled out to groups of root servers was carefully chosen to be representative and to allow meaningful testing, but also to avoid the possibility that Internet users might treat the test deployment as production and use it to perform validation. Early validation would make it difficult to roll back to an unsigned root zone without harming that validating user base. The root zone, so-constructed, is described in project documentation as the Deliberately Unvalidatable Root Zone (DURZ). The deployment of DNSSEC using the DURZ has made it possible to focus testing on the stability and reliability of the DNS itself, making sure normal DNS resolution is not made less reliable by testing DNSSEC deployment in the root zone.

[7] Details of the staged deployment approach, including a detailed timetable for the associated maintenance work for each root server are described in "DNSSEC Deployment for the Root Zone", published at http://www.root-dnssec.org/documentation/.

[8] Data collection and centralized storage is being coordinated by the DNS Operations, Analysis and Research Centre, DNS-OARC, by OARC Inc. under contract from ICANN. The controls on how data is made available are described in the "OARC Proprietary Data Agreement", https://www.dns-oarc.net/files/agreements/OARC-proprietary-data.pdf

ICANN proposed a provisional framework for the involvement of external parties in KSK ceremonies[9], referred to in documentation as Trusted Community Representatives (TCRs). ICANN solicited involvement from the DNS technical community world-wide and selected individuals who have technical standing in their regions to participate. The result is a geographically-diverse set of trusted people, whose involvement will increase transparency and awareness of the processes by which critical key materials are handled.

The involvement of these TCRs, as provisionally-defined, requires a greater degree of logistical planning than is usually necessary for key ceremonies commonly executed within the Certification Authority industry. ICANN consulted experts in security engineering and has completed an extensive series of rehearsals in order to ensure that the ceremonies are appropriately designed and executed. ICANN also retained auditors in preparation for gaining SysTrust accreditation for the design and implementation of the KSK management processes and systems.[10]

Solicitation for TCRs began in May 2010, and background checks and final selection were completed by the end of that month. The first event at which TCR participation is required is the first production KSK ceremony, which is scheduled to occur on 2010-06-16[11].

Test Results

The test plan for the implementation of DNSSEC in the root zone is included in the supporting documentation accompanying this report[12]. We summarize the results of all tests specified in that test plan as one of:

- Success: the tests were completed and all success criteria were met;
- Partial Success: the tests were completed, and although some success criteria were not met, the impact of any failures were mitigated, or were assessed and judged to pose insufficient concern to recommend that deployment not proceed; and

[9] Various types of KSK ceremony require the presence of TCRs, including HSM Initialisation, Key Initialisation and KSR Processing. A more detailed treatment of the roles of TCRs and ICANN staff can be found in "Root Zone DNSSEC Ceremonies Guide", published at http://www.root-dnssec.org/documentation/.

[10] The functions carried out by TCRs have been tested extensively during key ceremony rehearsals using ICANN staff not familiar with the project in place of actual TCRs. In ceremonies, TCRs will have extensive guidance from ICANN staff to ensure that their roles are well-understood and correctly executed.

[11] TCRs will also be available the following day, 2010-06-17, in case any unexpected event delays completion of the ceremony on the scheduled day.

[12] See "DNSSEC Test Plan for the Root Zone", published at http://www.root-dnssec.org/documentation/.

- Failure: the tests were completed, and one or more success criteria were not met, the particular failures being sufficiently serious to merit concern;
- Incomplete: the tests were not completed as of the time of this report.

Section references in the summary table which follows correspond to section numbers in the test plan. Please consult that document for more detailed explanation of each test, and its corresponding success and failure criteria. Test results that are qualified or otherwise merit additional discussion are expanded upon in the corresponding footnotes.

Section	Description	Results
5.1	Root Server Incoherence	Success
5.2.1	Generation of DURZ	Success
5.2.2	Distribution of DURZ	Success
5.2.3	Serving the DURZ	Success
5.2.4	Rollback to unsigned from the DURZ	Success[13]
5.2.5	Resolver Behavior	Success
5.3.1	Long-Term Primary Query Collection	Partial Success[14]
5.3.2	Tactical Full Request Capture	Partial Success[15]
6.1.1	Transmission of KSR	Success

[13] The specific scenario whereby the DURZ is rolled back to unsigned was tested in a lab environment. This was a conscious decision intended to avoid unnecessary changes to the production DNS. All lab testing was successful. The individual component systems that generate, sign, blind and distribute the root zone were extensively tested in production.

[14] 12 out of 13 root servers (all except "B root") collected priming queries over an extended period and submitted them for storage and analysis. However, despite incomplete participation by all root server operators, the Design Team was still able to collect sufficient data to meet the objectives of the collection: we were able to confirm that there were no significant changes in the pattern of priming queries to the root server system, which indicates success.

[15] Several tactical packet captures were executed before, during and after the phased deployment of the signed root, but not all root servers participated in every session. Fortunately, there was full participation by all root server operators for two sessions near the end of the planned group of sessions. However, despite incomplete participation by all root server operators, the Design Team was still able to collect sufficient data to meet the objectives of the collection: we were able to confirm that there were no significantly anomalous traffic patterns that would indicate widespread problems with the incremental deployment of the signed root zone.

Section	Description	Results
6.1.2	Transmission of SKR	Success
6.1.3	Authorization of SKR by US DoC NTIA	Incomplete[16]
6.2	ZSK Rollover	Success
6.3	KSK Rollover	Success
6.4.1	Failure of one HSM	Success
6.4.2	Failure of both HSMs at one location	Success
6.4.3	Loss of all HSMs at both locations	Success
6.5.1	Key Management Ceremonies Prologue	Success
6.5.2	HSM Initialization	Success
6.5.3	HSM Decommission	Success[17]
6.5.4	Key Generation	Success
6.5.5	Key Signing/KSR Processing	Success
6.5.6	Private Key Deletion	Success
6.5.7	Key Management Ceremonies Epilogue	Success
6.5.8	Safe Security Controller Enrollment	Success
6.5.9	Safe Security Controller Replacement	Success

[16] US DoC NTIA will authorize the SKR generated by ICANN by connecting to a web site run by VeriSign. Because of the importance of the key material being authorized, it is vital that NTIA personnel be strongly authenticated; therefore, the Design Team decided that access to the web site will make use of the certificate on an individual authorizer's PIV card. All necessary equipment to support PIV card use has only recently been procured and installed, so this testing has not been able to be completed. However, we have every confidence that this authorization will be successful: the web site has been extensively tested by VeriSign engineering's quality assurance (QA) team. In addition, there is a workaround, if necessary: NTIA personnel could manually authorize an SKR by contacting VeriSign (e.g., by sending a digitally signed email with the authorization).

[17] In order to facilitate continued testing and key ceremony rehearsals without the cost and inconvenience of hardware replacement, the HSM tamper barrier was not violated as part of this testing. We note that tamper barrier testing for the specific type of HSMs being used were tested as part of their FIPS-140 certification, however.

Section	Description	Results
6.5.10	Crypto Officer Enrollment	Success
6.5.11	Equipment Acceptance	Success
6.6	Trust Anchor Publication	Success
7.1	Receipt and Validation of DS RDATA by IANA	Success
7.2	TLD DS Change Request Workflow	Incomplete[18]
7.3	Generation of Signed Root Zone	Success
7.4	Distribution of Signed Root Zone	Success
7.5	Rollback to Unsigned from Production Signed Zone	Success

Summary of Findings

A primary objective of the staged implementation testing approach designed and implemented by the Design Team was to be able to identify any potential harmful effects of the deployment quickly, and to be able to react promptly to mitigate any such effect in a controlled manner in order to safeguard the stability and security of the DNS.

Following extensive data collection and observation of the reaction of the DNS to the changes that have been made, no harmful effects of the staged test deployment of DNSSEC have been identified.

[18] This testing is scheduled to begin on the day this Final Report was due to be submitted. We have every confidence that this testing will be successful: DS records are processed in the same manner as other root zone change requests, which is a process that all three parties involved in the processing are quite familiar and proficient with.

Request for Authorization to Proceed

This document summarizes the results and observed effects of the staged DNSSEC deployment testing in the root zone of the DNS, and hereby requests authorization for the implementation to proceed into production. Specifically,

1. that the key materials generated during the first successful KSK ceremony held by ICANN, as IANA Functions Operator, be acknowledged as being authentic and proper by NTIA for use as the KSK in the root zone of the DNS;

2. that VeriSign, as Root Zone Maintainer, produce a signed root zone based on those key materials, following the procedures referred to by this document;

3. that VeriSign, as Root Zone Maintainer, execute the necessary procedures to transition from DURZ to production signed zone on 2010-07-15 or whichever other date is subsequently agreed upon by the Design Team;

4. that ICANN, as IANA Functions Operator, publish the first root zone trust anchor, following the procedures referred to by this document;

5. that ICANN and VeriSign each make public announcements following the successful publication of the first root zone trust anchor.