CONNOTECH Experts-conseils inc.

Towards a Process Flow

for

DNS Root Zone File Signature

with

KSK Rollover Provisions

Thierry Moreau

Document Number C004711

2008/11/24

Document Revision History

C-Number	Date	Explanation
C004218	2007/09/15	Initial release of the predecessor document under the title *A (Pro?-)Position Paper re DNS Root Zone File Signature Using DNSSEC Protocols*
C004222	2007/10/09	Updates to the predecessor document prior to public distribution
C004711	2008/11/24	Major changes from the predecessor document [1] including a change in title. Removed coverage and discussion of RFC5011. Removed much discussion text related to institutional arrangements. See the introductory section for more background information.
C004711		Current version

Table of contents

1. Introduction

1.1 A Response to a Recent Development in the Field

A significant development occurred recently for DNSSEC support at the top of the DNS name hierarchy ("signing the root"): a "Notice of Inquiry" (NOI) was issued by NTIA [1], a division of the US Department of Commerce. This document is the result of a major but straightforward edition of its predecessor document [2], taking into account the contents of this NOI as it provides or suggests answers to many previously unanswered questions. This document is respectfully submitted as an integral annex to a public comment by the same author to the NOI process [3].

As a result, this document positions the author's proposal TAKREM for DNSSEC to the specifics of the DNS root controlled by ICANN, Verisign, and NTIA, respectively the *IANA function operator*, the *root zone maintainer*, and the *administrator* in the NOI document terminology.

DNSSEC is an IT security technology based on cryptographic techniques. TAKREM is a cryptographic key management scheme. In the context of the predecessor document, the foremost issue surrounding the "signing the root" project was the detailed institutional answer to the question "who controls the root." Now the focus is on effective process flows coherent with the fact that ICANN and Verisign are contractually bound to NTIA. In both cases, the TAKREM concepts are identically applicable.

The relative position of this document as an annex to the main contribution to the NOI is indicative of three simple facts 1) as a bona fide voluntary expert contribution to the advance of DNS integrity, the main contribution was first drafted as a self-contained one, and remains so in its final version with the TAKREM proposition as an option, 2) the predecessor document was conveniently edited to document this option, and 3) the option may be rejected.

1.2 Intended Audience and Purpose

This document is intended for knowledgeable readers, having a prior understanding of the DNS operations at the root, and the current institutional framework including ICANN, its specialized operational division IANA, the US government Department of Commerce (DOC), the US-based Verisign corporation, and secondary DNS root operators.

The purpose of this document is to present the TAKREM scheme (Trust Anchor Key REnewal Method) with a focus on the unique DNS root in the current context where DNSSEC deployment is envisioned, and currently being planned as described in the NOI document [1]. The

relevance of this document lies in its exposition of "better" DNSSEC root key management procedures. This is indeed a bold contribution where "better" implies the recourse to the TAKREM procedure justified by arguably stricter compliance to key management principles but using unique solution elements.
described at the institutional perspective taking the TAKREM features as a yardstick – the implied challenge is to describe better yardstick and/or description or definition for acceptable DNSSEC root key procedures.

1.3 Origin and Status of the Proposed Deployment Scheme

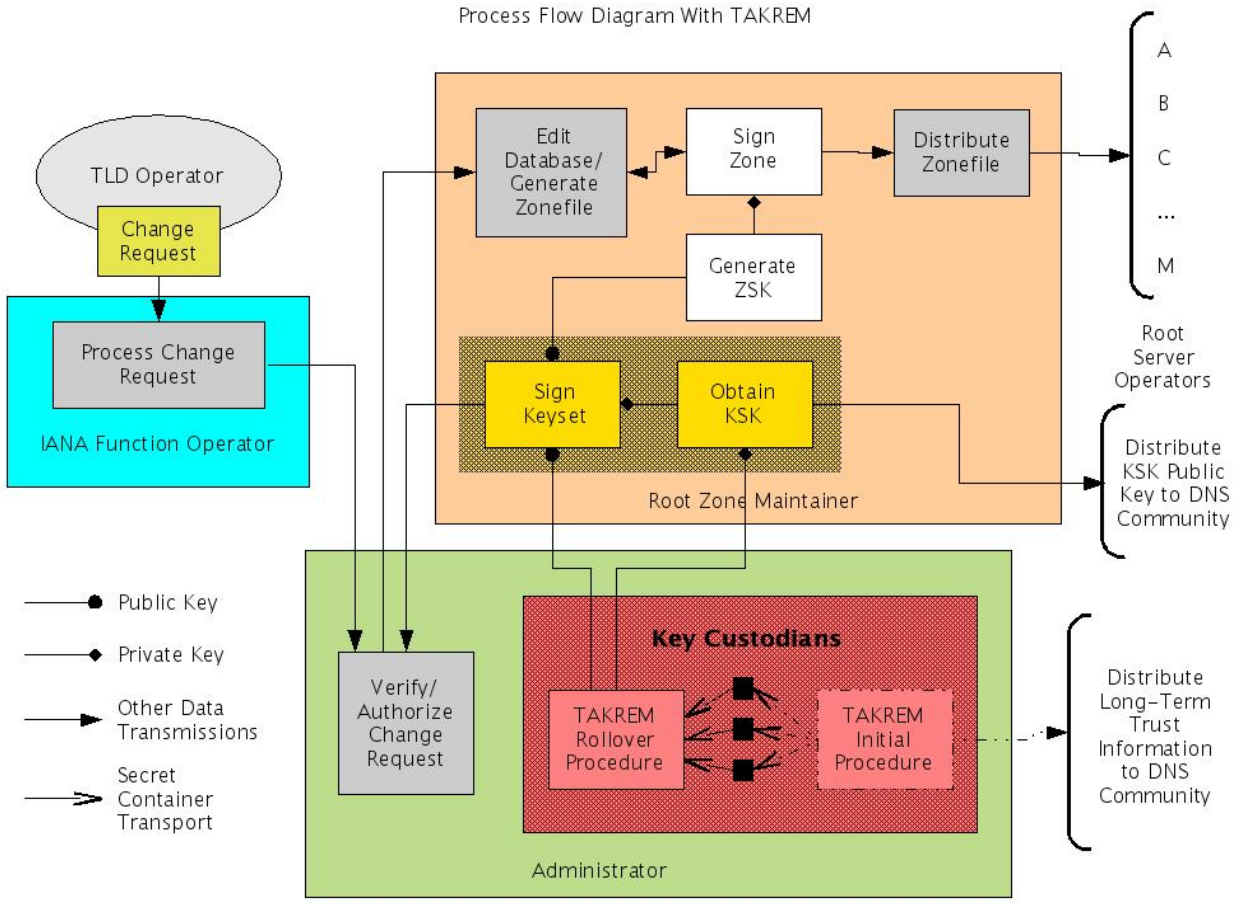
Originally, the invention of TAKREM [4] was not related to the DNS, but the applicability to DNSSEC trust anchors came quickly and turned into two Internet drafts [5] [6]. An implementation-level contribution [7] completes the picture for server-side technical details. The TAKREM proposal was not accepted by IETF DNSEXT working group as an interoperability specifications applicable generally to any trust anchor, i.e. not addressing the specific requirements of the DNS root as in the present document. Throughout this discussion, the technical validity of the proposal was never seriously challenged. If this proposal attracts attention to the TAKREM implementation details, observations made in reference [8] should not be lost.

The present document assumes the TAKREM technical validity, from security and protocol interoperability perspectives. It narrowly focuses on institutional arrangements that might apply to DNSSEC deployment support for the root. In the document [9], a different approach addresses DNSSEC deployment challenges near the top of the DNS hierarchy, including limited-scale DNS alternate root nameservice operations to palliate the *lack of a signed DNS root*. Thus, the reference [9] is orthogonal to the present one.

The effort behind this proposal is project is sunk cost project supported by private financing.

2. Institutional Perspective

This section explains the present proposal with an abstraction of the existing institutional framework for DNS root management. Another terminology is used in the NOI document, but unfortunately the present document version has not been thoroughly reviewed to adapt to it. However, the NOI document comes with neat process flow diagrams that were straightforward to adapt to the present proposal, giving the figure below.



2.1 The DNS Root Zone Management Role

In the abstracted view, a single organizational entity manages the DNS root zone file. In practice and as described in the NOI document [1], this is done partly by the IANA function operator, an operational division of ICANN, and partly by Verisign as the root zone maintainer, and with endorsement by the NTIA as the administrator.

When the DNSSEC support is added to the picture, the DNS root zone file updates require a digital signature. The NOI document assigns this role to the root zone maintainer in five out of six depicted process flows, but acknowledges a proposal by ICANN in which the signatory is the IANA function operator. The present proposal is agnostic about this question, but is documented using the root zone maintainer as the signatory.

2.2 An Authority-granting Role

NTIA, with its contractual relationship with the other two parties involved and the US government assertion of legitimacy as an Internet naming and addressing oversight authority [10], fits the abstracted view of an *authority-granting role*. At the abstracted institutional level, it is the authority granting role that enables the IANA function operator to perform the DNS root zone management role. The abstract level and the proposed cryptographic key management scheme are intended to be functionally coherent. By essence, the authority-granting role has a longer time horizon than the zone management role, and has an intuitive hands-off characteristic. Long-term key material naturally belongs to the organization fulfilling the authority-granting role.

Correspondingly, this proposal assigns new cryptographic key management duties concurrent with renewals of zone management role assignment. In practice, a root maintainer contract renewal would concur more or less with delegation formalities described in subsection 2.2.2.1 below. The overall scheme requires preparatory procedures described in subsection 2.2.1, and periodic or occasional delegations described in subsection 2.2.2.

2.2.1 Preparation Phase

Here is an account of the additional duties for the authority-granting role for DNSSEC support. These additional duties are straightforwardly derived from the TAKREM usage for DNSSEC root trust anchor. Specific implementation details are in reference [7].

2.2.1.1 A Preparation Session for DNSSEC Deployment

This operation is performed once for the expected lifetime of the DNSSEC support at the root, e.g. from 20 to 50 years. The purpose is the generation of cryptographic key material, i.e. secret information allowing the authority-granting role to be performed, and the corresponding publicly distributed configuration data (this is called *trust anchor key initial distribution message* in the reference [4]). The preparation session requires

- an ordinary computer system with specialized hardware options for random number generation,
- customized cryptographic key management software,
- a laser printer for bar code page printout,
- stationery supplies, and
- active and passive participants, respectively security experts in charge of operating the system and software and educated witnesses of varied origins for assurance of operational integrity.

The only actual output of the preparation session is

a) sealed bags or boxes of envelopes holding bar code printouts of secret key material, and
b) a few bar code pages for the publicly distributed configuration data to be publicly distributed.

All the electronics used in the session should be meticulously destroyed, so that information leakage is virtually impossible. This recourse to paper, sealed envelope, and sealed bags or boxes for the decades-long security of the global Internet is a most serious proposal. It is indeed a unique feature of the present proposal to offer an integrated DNSSEC deployment roadmap in which non-technical managers are offered simple methods for the ultimate DNS "control" implied by the DNSSEC technology: non-technical managers will seldom need computer systems or security experts after the preparation session for the fulfillment of the authority-granting role.

The computer security experts should know what to do with the item b) in the preparation session output. This is to say, the present proposal brings no noteworthy contribution to the issue of *DNSSEC priming* for the unique DNS root. The reference [9] addresses the issue of DNSSEC priming, but it remains peripheral to the present document purpose. In any event, computer security experts walk away of the preparation session with item b) in their possession.

2.2.1.2 Delivery of Sealed Bags to Key Custodians Entities

This is actually the latest portion of the above preparation session; it is described separately because it introduces the important notion of *split control* of the authority-granting role. This split control is an institutional arrangement opportunity that merely adapts an old technique in cryptographic key management, namely *split-knowledge storage of secrets* [11], or a modern number-theoretic improvement, namely *secret-sharing*. The actual solution embedded in the reference [7] is either a two-parties split-knowledge storage scheme, a three-parties split-knowledge scheme, or a two-out-of-three secret-sharing scheme (made with a trivial triplication of a two-parties scheme). The *secret components* are just the item a) in the preparation session output.

What does this mean to the simple instructions to non-technical personnel in the organization fulfilling the authority-granting role? Taking the two-out-of-three scheme for explanation purposes, the organization assigns the *key custodian* role to three organizational entities, each equipped with a safe box and internal control procedures for access to the safe box. If the organization was a corporation, the three key custodian entities might be the corporate finance department, the corporate legal department, and the external accounting auditor firm. Each key custodian entity sends two delegates to the preparation session, and receives, through these delegates, one of the sealed bag or box of

envelopes created during the preparation session. The delegates then safely carry the sealed bag or box to the safe box of their organizational entity.

2.2.2 Delegation of Authority to the DNS Root Zone Management Role

After the preparation session and the delivery of sealed bags to key custodian entities, the authority-granting role consists of periodic or occasional delegation of authority to the DNS root zone management role. As an illustrative analogy with a car rental operation, this delegation is like a car location clerk handing keys and traveling documents to the client. A concern in car rental operations is a client who never returns the car; the analogous concern in the present proposal is addressed below with the period of validity for the delegated key.

The ability to perform the authority-granting role requires the cooperation of any two of the three key custodian entities. The authority-granting role is performed mainly by manual operations devoid of technological means, so the chances of subversion by computer experts are minimized. The authority-granting role is also conceptually simple: to safeguard secrets that are gradually transferred to the zone management role on a time frequency similar to the current IANA contract renewal/option mechanism.

It should be noted that the authority-granting role is institutionally independent of the DNS root zone management role. This two-tiered institutional control implies a two-tiered accountability allocation. Notably, a serious operational mishaps in the zone management role can be recovered by a TAKREM emergency rollover procedure, ensuring continuity of DNSSEC services even if a reorganization of the zone management role was needed.

The split-knowledge storage scheme originates from cryptographic technology. The mere desirability of best available security mechanisms for the DNSSEC root private keys implies the suggestion of its application in the institutional arrangement for the DNSSEC support at the root. This logic applies to any approach to DNSSEC root private key procedures since split-knowledge storage applies to any type of secret or private cryptographic key material, and is appropriate for key material having network-wide significance.

Overall, the present proposal includes a precise fit of cryptographic key material operations and institutional roles. Combined with the technology-deprived nature of manual operations, this is advantageous for transparency and auditability of the authority-granting role. The present author suggests that a DNSSEC deployment strategy devoid of such characteristics needlessly relies on blind faith in an institution's operational integrity. In the case of the DNS root, the issue is irrelevant for the vast majority of Internet operators, but perhaps the DNSSEC deployment strategy needs to care for an influential minority.

Other DNSSEC root deployment proposals might achieve a similar fit of cryptographic key material operations and institutional roles. The main contribution to the NTIA NOI by the present author [3] is an example of specifying the desired fit starting the process flows already sketched in the NOI document, but without other characteristics found in the present proposal such as the technology deprived nature of the key custodian role.

2.2.2.1 Delegation Operation by the Authority-Granting Organization

The delegation operation described here is from the authority-granting role to the DNS root zone management role, with the delegation announcement role as an intermediate step (see subsection 2.3 below). The delegation basically grants the DNS root zone management operation the keys to operate the DNS root signature for a period *with a ritual that can be authenticated by the minority of Internet operators that counts*. As far as the authority-granting organization is concerned, that should be adequate.

For the non-technical representatives of the key custodian entities, the delegation operation is fairly simple:

- by more or less formal coordination, they come to an agreement as to when, where, and with which secret envelope they intend to gather at a delegation meeting;
- each key custodian entity sends one or two representatives to the delegation meeting, carrying a secret envelope,
- at the meeting, they (ceremoniously) scan the series of bar codes present in the envelope they brought to the meeting, using a bar code scanner connected to a then-state-of-the-art digital signature device or system, and
- they also (but less ceremoniously) scan the *public portion* present in the series of bar codes form the respective envelopes, this time using a bar code scanner connected to a computer system without special capabilities.

The difference between the last two bullets lies in the private versus public portions of digital signature keys. This is a manifestation of the fit between cryptographic principles, manual operations, and allocation of institutional accountability.

That's almost it: a skill level similar to the one of a grocery checkout clerk. There are tree additional points, linked to the assurance of good behavior in the performance of the DNS root zone management role:

a) the key custodian representatives should ear a beep or witness a visual feedback from the digital signature device or system confirming that it received sufficient secret bar code information to recover a private digital signature key;
b) the authority-granting organization, or each key custodian entity if they operate et arm's length, should make sure the digital signature device is adequate, e.g. certified according to some IT security certification program;

c) the authority-granting organization, or each key custodian entity if they operate et arm's length, should ensure that the initial delegation announcement, explained below, announces the proper period of validity for the delegated key.

Admittedly, the items b) and c) are not as technology-deprived as a non-technical representative of a key custodian entity might expect. However, these two activities are time-limited, i.e. the means to accomplish items b) and c) need not be the same over successive delegation operations, notably over a switch from one zone management entity to another, e.g. if the IANA contract was transferred to another contractor.

This gathering of key custodian representatives to merge secret information from separate envelopes is straightforwardly derived from the TAKREM recourse to split storage of secrets in reference [7]. The private digital signature key recovery mentioned in item a) above is the starting point for the TAKREM rollover operation, or *delegation announcement*, explained below.

2.3 A Limited but Pivotal Role: Delegation Announcements

From the institutional perspective, the delegation announcement is the mating point between the authority-granting role and the DNS root zone management role. This is in contrast with the authority-granting role that could be devoid of any operational involvement in trust anchor key management.

With the better understanding of DNSSEC root signature process flows based on the NOI document and its recent references (notably [12]), it is now appropriate to emphasize the dual institutional justification for the delegation announcement:

- to fulfill the DNSSEC protocol interoperability requirements through the KSK rollover operation, so that the vast majority of Internet users can benefit from higher trustworthiness of DNS data,
- to address the very specific trust anchor management expectations of *the minority of Internet operators that counts*.

To address the needs of the vast majority, KSK security breaches and change of delegation of the IANA function role can be ignored either as practically impossible events, or very exceptional events requesting DNS resolver manual reconfiguration. The minority of operators that count expects both automated DNS resolver reconfiguration and assurance that DNSSEC trust anchor keys are handled appropriately even in the exceptional circumstances.

The delegation announcement role is specific to DNSSEC and is non-existent in the current plain DNS institutional framework. The TAKREM procedure components corresponding to the delegation announcement role are the rollover operation and the rollover message. As detailed below, in the TAKREM application to DNSSEC, the needs of the vast majority are met

by KSK rollover procedures selected independently of TAKREM, and the minority expectations are addressed by the SDDA mechanism.

2.3.1 Delegation Announcements

Here is a technical description of delegation announcement. In its application to the DNS root, the TAKREM rollover operation consists of:

- preparation of two DNS RRsets, namely
  - the DNSKEY RRset augmented with the new trust anchor key – this requires the other entries in the DNSKEY RRset from the zone manager – and
  - an SDDA RRset specific to the TAKREM scheme [5] [6]– this requires the validity period for the rolled-in public signature key ;
- the DNSSEC signature operation of these two DNS RRsets with the rolled-in private signature key, producing two RRsig RRs;
- the return of these two DNS RRsets and two DNS RRSIG RRs to the zone managed by the zone manager for inclusion in the DNS root zone file for later publication by the DNS root nameservers.

What is critical for the authority-granting role is that the validity period for the SDDA RRset goes through the complete cycle up to the actual publication by the DNS root nameservers for a duration long enough so that it can be authenticated by most of the minority of Internet operators that counts. Presumably the required minimum publication duration would be in the range of one week to one month. This ensures that the delegation duration is understood by the minority of Internet operators that count.

Delegation announcement should be controlled by the DNS root zone management organization. The economy of administrative procedures precludes other arrangements such as an independent agent of the authority-granting organization. There is thus a form of *delegation of delegation announcements* implied by the present proposal. With respect to the operational considerations in the delegation announcement role, the DNSSEC root signature process flow proposal by ICANN [12] contains a suitable description of a KSK public key generation ceremony. Thus the reference [12] hints that delegation announcements could realistically be implemented by the DNS root zone management organization as a security critical operational assignment. In reference to the process flows sketched in the NOI document, either process flow number 5 or number 4 is a starting point for the allocation of the delegation announcement role proposed here. Respectively, the process flow number 5 does not change the current function allocations among IANA and Verisign, and process flow number 4 would follow the streamlined arrangement proposed in reference [12] (as indicated earlier, the present proposal is agnostic about this question).

It should be understood that a few events may trigger a rehearsal of the delegation announcement with the same rolled-in digital signature key. Mainly, this is either a change in the DNSKEY RRset after the initial delegation announcement, or a reduction of the validity period for the SDDA RRset. The former may be caused by a Zone Signing Key (ZSK) rollover. A reduction of the validity period may be caused by an emergency trust anchor key rollover or another unexpected termination of delegation to the zone management organization. At the institutional perspective, the authority-granting role includes a closer oversight over the delegation announcements than the rest of DNS root zone management operations. But the economy of administrative procedure precludes the involvement of key custodians for these operations, and correspondingly the DNS root zone management organization controls the KSK private keys.

3. Root Zone Management

The DNSSEC deployment at the root has significant implications in the management of the DNS root zone contents and in the operations of root nameservers. The present document section pertains to the trust anchor at the DNS root.

The DNS root zone management role encompasses the *concurrent compliance* with the present proposal and a simple ad-hoc KSK rollover procedure. Whenever the DNS root zone manager needs a new KSK for the rollover operation, it obtains it from the authority-granting organization, instead of generating it locally. Such coordinated operation obviously requires inter-organization planning of scheduled rollover events.

4. Sources of Guidance for DNSSEC Root Trust Anchor Key Management

A higher level of abstraction is used here to support the legitimacy of unilateral commitments to the selected DNSSEC root key process flow.

We assume a Single Organization (SO) fulfills every relevant roles in the DNS root zone management. When it comes to DNSSEC trust anchor key management, SO has to announce the *rituals* it intends to follow, and then abide by its commitment, and finally receive and handle critics that will most likely be expressed. This peculiar description of trust anchor key management departs from the simple view that an interoperability specifications tells SO what to do. In fact, the “trust” element in a trust anchor key forever remains *a belief*, despite being encoded as a configuration data element. This belief is acquired through indirect observations that some ritual has been performed appropriately. This very “trust” element may not simply be published in the DNS root zone file like other DNS data.

Hence the view that SO has to decide a trust anchor key management ritual. Generally, DNSSEC deployment starts by the nameserver side before the resolver side. In the case of trust anchor management, this extends to selection of proper rituals, i.e. SO should affirm how it intends to provide evidence of trustworthiness. Resolver-side software compliance and configuration issues are almost of secondary relevance, at least with respect to the timing of deployment.

If contrary to the above, the resolver-side expectations of acceptable DNS root trust anchor key management would prevail as a deployment strategy, at least two difficulties would be encountered. First, the DNS resolver operator community is an open-ended one, so the expectations may become extraordinary, or even frivolous or malicious. Second, the digital signature technology in DNSSEC requires the proper handling of private keys, and a commitment to demanding operating standards is better left as an assertion by the organization that must handle the private keys, and not as whish list from third parties.

5. Conclusion

TAKREM for DNSSEC, a specific trust anchor key management proposal, has been presented in sections 2 and 3, as if it was the preferred and obvious way forward. To the present author knowledge, this proposal is unique in its superimposition of cryptographic key management and institutional/contractual arrangements for DNS root zone management.

This proposal uniqueness would originate from a) the lack of security experts attention to the need to secure the applied cryptographic schemes with explicit manual key management procedures, combined with b) the tendency of institutions to look at issues in a compartmented way. Any envisioned DNSSEC deployment at the root brings an additional layer of accountability, based on principles of cryptography.

6. Acronyms

DNS
: Domain Name System

DNSEXT
: DNS EXTensions, the name of an IETF working group working on standardization of DNS protocol extensions

DNSKEY
: a technical acronym of the DNSSEC protocol referring to a public signature key entry in the DNS registry

DOC
: Department of Commerce

HSM
: Hardware Security Module

IANA
: Internet Assigned Numbers Authority

ICANN
: Internet Corporation for Assigned Names and Numbers

KSK
: Key Signing Key, a technical acronym of the DNSSEC protocol referring to a digital signature public key having special status for authentication of other keys, including ZSK

NTIA
: National Telecommunications and Information Administration

RR
: Resource Record, a technical acronym of the DNSSEC protocol referring to an entry in the DNS registry

RRset
: Resource Record set, a technical acronym of the DNSSEC protocol referring to sets of related entries in the DNS registry

RRSIG
: a technical acronym of the DNSSEC protocol referring to digital signature entry in the DNS registry

SDDA
: a TAKREM-specific technical acronym of the DNSSEC protocol referring to an entry in the DNS registry

TAKREM
: Trust Anchor Key REnewal Method

ZSK
: Zone Signing Key, a technical acronym of the DNSSEC protocol referring to a digital signature public key generally intended for authentication of DNS zone data

7. References

[1] National Telecommunications and Information Administration, US Department of Commerce, *Enhancing the Security and Stability of the Internet's Domain Name and Addressing System*, Federal Register, Vol. 73, No. 197, pp 59608-59612, October 9, 2008, available at http://www.ntia.doc.gov/DNS/dnssec.html; see also http://www.ntia.doc.gov/DNS/DNSSECproposal1.pdf, http://www.ntia.doc.gov/DNS/DNSSECproposal2.pdf, http://www.ntia.doc.gov/DNS/DNSSECproposal3.pdf, http://www.ntia.doc.gov/DNS/DNSSECproposal4.pdf, http://www.ntia.doc.gov/DNS/DNSSECproposal5.pdf, and http://www.ntia.doc.gov/DNS/DNSSECproposal6.pdf.

[2] Thierry Moreau, *A (Pro?-)Position Paper re DNS Root Zone File Signature Using DNSSEC Protocols*, CONNOTECH Experts-conseils inc., Document Number C004222, 2007/10/09, http://www.connotech.com/dnssec_root_ta_takrem_v1.pdf

[3] Thierry Moreau, *Response to NTIA Notice of Inquiry on DNSSEC*, CONNOTECH Experts-conseils inc., Document Number C004692, 2008/11/24, http://www.connotech.com/connotech_noi_resp.html

[4] Thierry Moreau, *A Note About Trust Anchor Key Distribution*, CONNOTECH Experts-conseils inc., Document Number C003444, 2005/07/05, http://www.connotech.com/takrem.pdf

[5] Thierry Moreau, *The SEP DNSKEY Direct Authenticator DNS Resource Record (SDDA-RR)*, Internet Draft (work-in-progress), draft-moreau-dnsext-sdda-rr-02.txt, April, 2006, archived at http://www.watersprings.org/pub/id/draft-moreau-dnsext-sdda-rr-02.txt

[6] Thierry Moreau, *The Trust Anchor Key Renewal Method Applied to DNS Security (TAKREM-DNSSEC)*, Internet Draft (work-in-progress), draft-moreau-dnsext-takrem-dns-02.txt, April, 2006, archived at http://www.watersprings.org/pub/id/draft-moreau-dnsext-takrem-dns-02.txt

[7] Thierry Moreau, *Server Management Tools for Trust Anchor Key Management Based on TAKREM*, CONNOTECH Experts-conseils inc., Document Number C003596, 2006/02/02, http://www.connotech.com/trustanchfoundry_09.pdf

[8] Scott Rose, *RE: Do any DNSEXT participants care about TAK rollover security?*, posting to the IETF DNSEXT working group mailing list ("namedroppers"), July 11, 2006, http://ops.ietf.org/lists/namedroppers/namedroppers.2006/msg00943.html

[9] Thierry Moreau, *Six Roles for Early Introduction of DNSSEC*, CONNOTECH Experts-conseils inc., Document Number C004006, 2007/05/15, http://www.connotech.com/six_roles_for_dnssec.pdf

[10] US Department of Commerce, National Telecommunications and Information Administration, *U.S. Principles on the Internet's Domain Name and Addressing System*, June 30, 2005, http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm

[11] See e.g the entry *split knowledge* in the glossary of terms, section 2.1 in US Department of Commerce, National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, FIPS PUB 140-2, May 2001

[12] ICANN, ICANN Proposal to DNSSEC-Sign the Root Zone, 15 September 2008, http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf