CONNOTECH Experts-conseils inc.

A (Pro?-)Position Paper

re

DNS Root Zone File Signature Using DNSSEC Protocols

Thierry Moreau

Document Number C004222

2007/10/09

Summary

The Internet DNS (Domain Name System) lacks data integrity protection; the DNSSEC protocol development effort was carried to provide a cure to this, with backwards compatibility as an essential feature. These days, open questions remain about conditions for DNSSEC support at the top of the DNS name hierarchy, or simply stated “signing the root.” This document explores these questions, through a positioning of the author's proposal TAKREM for DNSSEC to the specifics of the official DNS root controlled by ICANN. DNSSEC is an IT security technology based on cryptographic techniques. TAKREM is a cryptographic key management scheme. The foremost issue surrounding the “signing the root” project is the detailed institutional answer to the question “who controls the root.” In addition to the positioning of TAKREM in this context, an annex outlines a similar positioning of the IETF RFC5011 solution, thus facilitating a comparative study by the reader.

Document Revision History

C-Number	Date	Explanation
C004218	2007/09/15	Initial release
C004222	2007/10/09	Updates before public distribution: - updated the reference [9] - added the before last paragraph in subsection 2.2.2 - made the delegation announcement role more explicit with the insertion of subsection 2.3 and moved the former subsection 2.2.2.2 to subsection 2.3.1 - added the reference [10] and explanation of its relevance in subsection 2.3.1 - added the annex on RFC5011 [17] in section 7, acronym HSM, reference [22], and references to the annex in subsections 1.1 and section 3 - added a summary
C004222		Current version

Table of contents

1. Introduction

1.1 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, but yet neither planned nor decided. The importance of this document lies in the need for "acceptable" DNSSEC root ley management procedures. This is indeed a bold contribution where "acceptable" is 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.

For this document purpose, there are many perspectives to the DNS operations at the root, and the present document is organized according to three of them.

- The institutional perspective in section 2 explains the proposal to those concerned with the ICANN-centric institutional arrangements, without delving into the technical details.
- The DNS root zone management perspective is covered in section 3. Although many DNS zone manager, e.g. TLD registry organizations, share operational duties and concerns with the DNS root zone manager, there are very unique issues and challenges at the root, and the present proposal is centered on the root.
- The perspective in section 4 is an exploratory one, looking for possible sources of guidance for the DNSSEC deployment at the root based on the actors and their respective contributions to DNS operational rules and practices.

The annex in section 7 is offered to facilitate comparisons between the present proposal and a recent IETF specification document, using a common institutional arrangement perspective. After the limited distribution of this document initial release, it was noted that even readers very aware of DNSSEC might be in need of more explanations about DNS root trust anchor key management.

1.2 Background

At the time of this writing, the DNS evolution is characterized by a strongly felt need to deploy IDN (Internationalized Domain Names) and IPv6 (extended addressing for IP protocols) [1]. DNSSEC comes as a second-class priority.

For stakeholders wishing to see the DNSSEC deployment at the root in a reasonable time frame, a current outstanding issue is the control of the DNSSEC root trust anchor. Some commentators see the DNS root trust anchor as a highly leveraged control point for the DNS root zone file contents, while others observe that the current ICANN control is not fundamentally changed because the root zone turns digitally signed. Being in control implies accountability for those in charge. Irrespective of the political sensitivity of the root trust anchor, the aura of accountability associated with DNSSEC at the root may not be totally ignored.

1.3 Origin and Status of the Proposed Deployment Scheme

Originally, the invention of TAKREM [2] was not related to the DNS, but the applicability to DNSSEC trust anchors came quickly and turned into two Internet drafts [3] [4]. An implementation-level contribution [5] 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 [6] 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 [7], 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 [7] 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 a simple abstraction of the existing institutional framework for DNS root management.

2.1 The DNS Root Zone Management Role

In the abstracted view, a single organizational entity manages the DNS root zone file. In practice, this is part of the IANA operational division of ICANN, with the involvement of Verisign and endorsement by the DOC [8]. Reportedly, the administrative process is cumbersome, and each of the organizational triplet jealously guards its area of operational responsibility, making administrative process improvement quite challenging [9].

When the DNSSEC support will be added to the picture, the DNS root zone file updates will require a digital signature. In the institutional arrangement abstracted view, a single organization will control the DNSSEC private signature key used to sign usual DNS root zone file updates. In practice, a single member of the IANA-Verisign-DOC triplet would be the DNS root zone file signatory for usual DNS root zone file updates, presumably IANA. For the DNS root zone management role, there is a good match between the abstracted view and the anticipated DNSSEC deployment approach for the root. There are indications that the IANA technical staff is making some tests with the DNSSEC tools and techniques [10].

2.2 An Authority-granting Role

Formally, the US government DOC controls IANA as a contractor, the current duration of the contract is one year ending September 30th, 2007, and renewable at the option of DOC four times on a yearly basis [11]. This fits the abstracted view of an *authority-granting role* without which the DNS root zone management role would not be allocated to IANA. By essence, the authority-granting role has a longer time horizon than the zone management role, and has an intuitive hands-off characteristic.

Once the DNSSEC support will be added to the picture, this proposal assigns new cryptographic key management duties concurrent with renewals of zone management role contractual assignment. E.g. an IANA contract option exercise or renewal would concur 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 [5].

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 [2]). 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 [7] 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* [12], or a modern number-theoretic improvement, namely *secret-sharing*. The actual solution embedded in the reference [5] 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 is 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 authority-granting role is subject to political debate. An attempt to depict a global but simplified picture would position the US government determined to remain a key player in this area [13], the European countries with the CENTR organization [14] as a channel for their voice, and the less developed and emerging countries with the UN and IGF [15] as the appropriate venue for them. A major issue for those who challenge the global authority-granting role of a single government, i.e. the US, and perhaps even of any national government, is to create a global authority-granting constitution without recourse to treaty organizations such as the UN, ITU, or whatever. The global reach and unique characteristics of the Internet are seen by many debaters as legitimate reasons for rejecting treaty-based bureaucracies for IANA oversight. It might be fair to argue that the US government behaved in most circumstances with caution in order to account for Internet stakeholders interests, but some counterexamples boost the motivation of some participants in the debate [16].

The very presence of a political debate over IANA oversight or the authority-granting role is likely to delay DNSSEC deployment at the root. Foremostly, the DNSSEC technology comes with an aura of enhanced control and accountability. The question is not whether DNSSEC actually worsens an "unfair" control of the DNS by e.g. the US government, but rather how to deal with the opinion that it does. Indeed, to the extent that this debate falls in the field of international diplomacy, an opinion prevailing in a different part of the world can not be ignored because there is some logic which downplays the argument according to cultural values closer to the commentator.

In summary, a debate exists in which the authority-granting role of the US DOC is challenged. With the present proposal, the authority-granting role is subdivided in a small number of key custodian entities, using a key management scheme which predates the use of IT security techniques in public data networks. A step is easily taken where the authority-granting role is split in equally distributed among totally independent key custodian entities. Using our simplified depiction of the debate, a naive assignment of key custodian entities would be the US DOC, the CENTR, and a creation of the UN.

The split-knowledge storage scheme originates from the 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, irrespective of whether the authority-granting role is unified or split. 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. Other proposals might achieve an equivalent fit. 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.

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, e.g. in a diplomatic briefcase if a border has to be crossed and search and seizure is a possibility,
- 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 references [5]. 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. Maybe every engineering solution to the trust anchor key rollover requirement is deemed to have procedural provisions assigned to the delegation announcement role. This is in contrast with the authority-granting role that could be devoid of any operational involvement in trust anchor key management.

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.

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 [3] [4]– 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 zone 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 can be controlled by an independent agent of the authority-granting organization, or by the DNS root zone management organization. The difference lies in which organization receives the private signature key in the preceding delegation operation. While accountability avoidance would weight for an independent agent, economy of administrative procedures would weight for integration into the zone management organization. In either case, some operational trust in the zone management organization is needed because the minimum publication duration depends on zone management. There is thus a form of *delegation of delegation announcements* implied by the present proposal. A recent presentation of DNSSEC deployment plans by IANA for non-root zones [10] details the use of an HSM (Hardware Security Module) for zone management operations closely related to delegation announcements, namely signature of the DNSKEY RRset. Thus the reference [10] hints that delegation announcements could realistically be implemented by the DNS root zone management organization as a security critical operational assignment.

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 or the IETF-imposed trust anchor rollover ritual [17]. 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.

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 is the only zone which will always need trust anchor key management procedures. Certainly, the highest operational standards apply, given the high visibility of the root and the expectations of transparency and accountability.

The proposal introduced in the previous section using a top-down institutional approach would relieve the DNS root zone management from long-term accountability – a major operational mishaps in DNS root management would be recovered by the authority-granting organization, and not the Internet community at large.

At a more technical level, the DNS root zone management should be provided with unambiguous instructions on how to operate, at least in the narrow operational issue of trust anchor key management. The reverse specifications route should be avoided, i.e. specifying what DNS resolvers in the field expect and letting the DNS root zone management figure out how to meet these expectations.

The proposal introduced in the previous section suggests that trust anchor keys are inherited from the authority-granting organization, are included in the DNSKEY RRset in the root zone file according to DNSSEC protocol specifications, and described in an SDDA RRset also in the root zone file according to the TAKREM specifications in references [3] and [4].

Independently from the present proposal, the IETF seems to impose a trust anchor key rollover ritual specified in reference [17]. This is a configurable procedure where a number of concurrent KSKs (Key Signing Keys) exist in the DNSKEY RRset, newer keys introducing older keys. The specifications document is silent about the suitable number of KSKs, but the number 2 may appear adequate. Furthermore, there is little guidance for key management, and even less for institutional arrangements that would mitigate the accountability focus on the DNS root zone management organization for the long-term DNSSEC operational integrity. The annex in section 7 explores the reference [17] potential as the single trust anchor key management using the institutional guidelines suggested in the present document.

Assuming the DNS root zone management role encompasses the *concurrent compliance* with the present proposal and the IETF-imposed rollover ritual, two alternatives may be further investigated: independent operation, and coordinated operation.

- With the independent operation, the DNSKEY RRset contains KSK entries for the TAKREM rollover scheme, and other ones for the IETF-imposed rollover ritual.
- With the coordinated operation, whenever the DNS root zone manager needs a new KSK for the IETF-imposed ritual, it requests it from the authority-granting organization – the coordinated operation requires better planning of rollover event timing.

With either approach to concurrent support of rollover schemes, potential synergy is indeterminate, simply because the effectiveness of either one is dependent on validating resolver logic and configuration, hence outside of the control of the DNS root management organization. The important point is that concurrent support should be possible.

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

To the extent that the Internet is a public service, its governance requires input from the public, or stakeholders. Hence the mission of a number of participation-based organizations and their representatives. In addition to their representation role, some of these organizations are more directly influential on some aspects of the Internet. E.g. for our purpose: the IETF and ICANN as it was intended to evolve.

But the picture is incomplete without considerations of actors having control over portions of the Internet, both private entities and departments of governments' executive branch, *and having motivations unrelated to Internet*, i.e. economic well-being of shareholders or "national interest." E.g. for our purpose: Verisign, ICANN when perceived merely as a contractor of the US government, and the US DOC as the current IANA function authority-granting organization.

In the center of these actors, lies IANA as the organization fulfilling the DNS root zone management role. When it comes to DNSSEC trust anchor key management, IANA 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 IANA 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 IANA has to decide, or be directed to adopt, 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. the organizations which may at one point commit to DNSSEC support at the root should affirm how they intend 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.

In practice, IANA has not yet decided, and has not been directed to adopt, any trust anchor key management ritual.

Prior to the adoption of reference [17] as an interoperability specification, the IETF developed, through its usual consensus-based standards drafting procedure, a statement of requirements for trust anchor key management, now reference [18]. At least in the present author's opinion, it is doubtful that this requirements document gave adequate consideration on the actual security issue at stake for the root – interoperability issues and protocol characteristics were considered foremostly. This is perhaps due to the specialization of the IETF DNSEXT working group as an *Internet area* group and not a *security area* group. Since the IETF interoperability specification [17] reasonably meets the requirements document, the remaining issue is whether the documented requirements account for the needs of IANA, and/or ICANN and/or others who decide how the Internet is run (for our limited purpose). The short answer is no: DNSSEC deployment at the root needs high security trust anchor key rituals to be followed by the DNS root zone management organization and the authority-granting organization if its involvement may enhance the overall security. Discussions occurring outside of the IETF DNSEXT process clearly hint in this direction. In any event, the interoperability specification [17] currently stands as an IETF imposed trust anchor ritual.

A widening of horizons might allow looking forward at sources of guidance for acceptable trust anchor key rituals for the DNS root. What is missing is either operational guidelines enhancing the IETF-imposed ritual, or support for advancement of the present proposal, or something else preferably of equivalent maturity. Looking at the global picture, the Internet design and operations are influenced in a number of ways, and by an even greater number of organizations.

- Interoperability Protocols
  The IETF is not alone in this category. In addition to other standards developing organizations like W3C, software and system vendors, and service suppliers contribute to the family of interoperability protocols. In the case of DNSSEC deployment, the BIND implementation of the DLV scheme is an example [19].
- Operations Standards
  Operations standards dictate good behavior of Internet operators, target minimum performance levels, and the like. The IETF has an *operations area* including the DNSOP working group taking care of DNS issues. The DNSOP group didn't produce anything specific to DNSSEC deployment at the root. In the area of DNS, ICANN is a foremost source of operational standards, e.g. consensus policies [20]. ICANN and/or IANA has yet to issue his type of document for DNSSEC deployment.
- Contracts
  ICANN exists and works through contracts, but not only contracts (many ccTLD registries and root server operators operate outside of contractual agreements with ICANN). The use of commercial software in critical operations of the Internet also turn software license contracts into Internet governance tokens, usually with low visibility. It is unknown to which extent software license restrictions may apply in the case of Verisign software used in DNS operations [21].
- Established Practice
  Established practice in the *public* Internet has been more significant in the early days of the Internet, and played a significant role in the DNSSEC protocol design, i.e. to ensure the most complete backwards compatibility. Besides this, DNSSEC deployment at the root is fairly new and unique project, little influenced by established practice. However, established practice in the *mostly private* interactions between IANA, Versign, and the US DOC would normally have an impact on the DNSSEC deployment project [9].

The above list is superficial and incomplete as an empirical survey of Internet governance. Issues other than DNSSEC deployment guidance would call for other presentation of the material, notably additional actors. The list nonetheless shows the diversity of influences for the determination of a workable trust anchor key management ritual for the root. Since the DNSSEC root deployment project made little progress so far, contributions from any of the above perspective may be expected if DNSSEC at the root is to move at all.

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. Then, an open issue remains: is it possible at all to overcome the legal and political obstacles created by this aura of accountability. In some sense, this proposal is perhaps more a problem statement than a solution statement, i.e. is it conceivable that a root DNSSEC deployment scenario might work – taking this one as an example for discussion purposes.

In section 4, along with an ill-defined overview of Internet governance actors, we made a suggestion that long-term trust in the DNSSEC root operations could rest on rituals selected almost in isolation by the organizations already involved in plain DNS root operations.

6. Acronyms

BIND
: Berkeley Internet Name Domain, the name of an important software implementation of the DNS protocols

ccTLD
: country code TLD

CENTR
: (acronym of historical significance) an association of Internet Country Code Top-Level Domain Registries

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

gTLD
: generic TLD

HSM
: Hardware Security Module

IANA
: Internet Assigned Numbers Authority

ICANN
: Internet Corporation for Assigned Names and Numbers

IDN
: Internationalized Domain Names

IETF
: Internet Engineering Task Force

IGF
: Internet Governance Forum

IPv6
: Internet Protocol version 6, characterized notably by larger address space than IPv4

ITU
: International Telecommunications Union

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

TLD
: Top Level Domain

UN
: United Nations

US
: United States

W3C
: World Wide Web Consortium

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. Annex - The RFC5011 Alternative Revisited with the Institutional Perspective

This annex presents the possible use of RFC5011 [17] as an alternative to the present proposal. For this purpose, the informative section 6 in RFC5011 is deemed mandatory. Otherwise, the potential for trust anchor key compromise recovery potential offered by RFC5011 is unnecessarily limited. Strictly speaking, this point is not a defect in RFC5011: formal mandatory provisions in this specification document are focused on protocol interoperability between resolvers and nameservers. In contrast, the focus of the present document is ultimate security based on root zone management procedures.

In the other portions of this document, RFC5011 is referred to as an IETF imposed trust anchor ritual. Indeed, compliance to RFC5011 without consideration of its section 6 would not

achieve the full RFC5011 potential for trust anchor key compromise recovery. In this annex where the section 6 is deemed mandatory, RFC5011 is presented at par with the main proposal in the institutional aspects.

The root trust anchor ritual suggested by RFC5011 section 6 comprises a stand-by key and an active key, with the DNSKEY RRset at the root signed only with the active key. This trust anchor rollover scheme is not new. In 1998, an electronic payment security specialist disclosed [22] the same basic scheme and made the following recommendation: "storage [for active private key] and storage [for stand-by private key] are [preferably] not located in the same physical location or secured by a common security method, so that a single breach of security which allows access to one key will not allow access to the other key."

The RFC5011 is not explicitly on this point, but the *control* of the stand-by and active keys should be isolated in order to prevent simultaneous compromise. If key control isolation means separate organizations, then a delegation of authority occurs when the stand-by key control organization transfers next active key to the active key control organization.

In the institutional perspective elaborated in the main part of the document, the stand-by key control naturally falls within the authority-granting role. This allocation of operational duties allows a change in the DNS root zone management role even in the absence of collaboration from the organization losing this responsibility. However, it requires IT security systems procurement and continued support for the authority-granting role.

The control and usage of the active key as a DNS root trust anchor is part of the delegation announcement role explained in subsection 2.3. This operational assignment seems to follow the spirit of the procedures described in reference [10], while the stand-by key assignment to the authority-granting role is a suggestion that preserves the full key compromise recovery potential achievable with RFC5011.

The implementation of this arrangement requires two separate split-knowledge storage technique implementations, respectively for the stand-by key in the authority-granting role, and the active key in the delegation announcement role. Since a DNSSEC trust anchor key life-cycle according to RFC5011 starts with a stand-by phase followed by an active phase, the two split-knowledge implementations must maintain technological compatibility.

With these adaptations and the derived implementation details, the RFC5011 specification might provide a trust anchor key management scheme which can be compared with the TAKREM proposal on an similar institutional arrangement. However, the present author did not validate such a solution in any comprehensive manner.

8. References

[1] See e.g. ICANN Operating Plan at http://www.icann.org/planning/.

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] ICANN & Verisign, *Root Server Management Transition Completion Agreement*, see http://icann.org/topics/verisign-settlement.htm and http://icann.org/topics/vrsn-settlement/revised-root-transition-agreement-clean-29jan06.pdf

[9] See e.g. IANA, *IANA Root Zone Management Process High Level Process Flow*, http://www.iana.org/procedures/process-flow.html, and IANA, *Root Management*, 16 September 2003, http://www.iana.org/root-management.htm

[10] Richard Lamb, *DNSSEC @ IANA, Tech Talk, DNSSEC Deployment Working Group*, 25-Sep-07, http://www.dnssec-deployment.org/wg/materials/20071003/Lamb.pdf

[11] US Department of Commerce, National Telecommunications and Information Administration, *IANA contract*, September 2006, see http://www.ntia.doc.gov/ntiahome/domainname/iana.htm and http://www.ntia.doc.gov/ntiahome/domainname/iana/ianacontract_081406.pdf

[12] 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

[13] 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

[14] See the web page *CENTR Mission Statement*, https://www.centr.org/about/mission/

[15] See the web page *The Internet Governance Forum (IGF)*, http://www.intgovforum.org/index.htm

[16] Two examples: the debate over the .xxx TLD, opposing freedom of expression versus the ICANN ability to control the contents of the root zone file, and the debate over the whois service, opposing protection of personal information versus the ICANN ability to promulgate disclosure standards for organizations behind web site.

[17] M. StJohns, *Automated Updates of DNS Security (DNSSEC) Trust Anchors*, Internet RFC5011, September 2007

[18] H. Eland, R. Mundy, S. Crocker, S. Krishnaswamy, *Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover*, RFC4986, August 2007

[19] P. Vixie, M. Andrews, *DNSSEC Lookaside Validation (DLV)*, ISC Technical Note Series, April 16, 2006, http://www.isc.org/pubs/tn/isc-tn-2006-1.html

[20] Internet Corporation for Assigned Names and Numbers, *Consensus Policies*, http://www.icann.org/general/consensus-policies.htm

[21] See e.g. the 2006 Verisign annual report at http://investor.verisign.com/annuals.cfm, on page 23: “With regard to our Information Services business, our principal intellectual property consists of, and our success is dependent upon, proprietary software used in our registry service business and certain methodologies and technical expertise we use in both the design and implementation of our current and future registry services and

Internet-based products and services businesses, including the conversion of internationalized domain names. We own our proprietary shared registration system through which competing registrars submit .com and .net second-level domain name registrations."

[22] Tony Lewis, *Key Replacement in a Public Key Cryptosystem*, United States Patent 5,761,306, assigned to Visa International Service Association, issued on June 2, 1998