CONNOTECH Experts-conseils inc.

The SISATA Institutional Development Proposition

for

DNSSEC Deployment Facilitation

Thierry Moreau

Document Number C003957

2006/11/15

Table of contents

Document Revision History

C-Number	Date	Explanation
C003957	2006/11/15	Initial release
C003957		Current version

1. Introduction

1.1 Background of this Document

The present document provides information about an *institutional development proposition* aiming at securing the global DNS. Actually, the SISATA proposition is intended to facilitate the deployment of the DNSSEC protocol as an alternate strategy for the challenges of DNSSEC protocol support by the DNS root zone administration.

The term SISATA "proposition" is preferred over "proposal" because the present author, and CONNOTECH Experts-conseils inc., seeked no alliance with early supporters. In other words, the present document describes a somehow orphaned proposition, and the SISATA proposition is documented mainly to be available for an interested party to pick up.

Nonetheless, and fundamentally, some attractive features should be noted:

- an enabling approach for TLD administrations (and perhaps SLD administrations for significant SLDs) for DNSSEC deployment;
- integration of institutional, operational, and technical features for enhanced IT security assurance;
- forward compatibility with both 1º the IETF-backed DNSSEC protocol refinements and 2º eventual DNSSEC support by DNS root administration, if and when either development actually occur;
- a focused undertaking with a manageable scope.

The present document is intended as a positive contribution towards security enhancements in the global Internet. In this spirit, it falls beyond the purpose of the present document to present a comparative analysis of the SISATA proposition with alternate strategies, since such analysis might unexpectedly cast doubt on elements of IT security in the reader's mind, which may be counterproductive in the absence of interaction between a reader and SISATA proposition supporters.

1.2 Introduction for the Knowledgeable Reader

The reader may already know the central role of the DNS, Domain Name System, as a support function for daily operations of the global Internet, with the DNS root being a critical facility. The DNSSEC protocol is an emerging extension to the DNS protocol specifications; DNSSEC "deployment" comprises the required technical, operational and institutional adjustments required for DNSSEC to go out of the laboratory to the field at a significant penetration rate, i.e. a penetration rate at which the DNSSEC has actual impact for non-technical Internet users. Among the required institutional adjustments required for DNSSEC deployment, ICANN, as the DNS root zone administration, should turn on DNSSEC protocol support for the DNS root. This is referred to as "signing the DNS root," a seemingly straightforward technical operation with nonetheless far-reaching policy implications. In a sense, the proposition to deploy the DNSSEC protocol extension is easily justified from a strict engineering perspective, but the corresponding institutional commitment is harder to obtain for the DNSSEC support at the DNS root, as discussed in document subsection 4.2 below.

Accordingly, the present document addresses institutional development issues rooted in protocol and IT security engineering issues. The document is organized and written to leave engineering issues as subsidiary to institutional and policy issues. The reader is thus directed to other documents and information sources about the detailed technological aspects, including about our TAKREM procedure and technology. TAKREM is one of the foundation for the operational aspect of the SISATA proposition, but it is almost merely mentioned in here (e.g. subsection 5.3) as a known implementation for a security procedure that is conveniently abstracted in the scope of the present document.

Comparisons are possible between the X.509 security certificate technology, also known as PKI (Public Key Infrastructure) and the DNSSEC technology. The two apply public key digital signatures, but were designed with very different foundations and are incompatible at the protocol interoperability level. A comparative analysis is way beyond the scope of the present document. Nonetheless, we sometimes refer to the PKI technology when describing a DNSSEC conceptual refinement.

The SISATA proposition and the present document focuses on TLD administrations since TLD registries are the first organizations to deploy DNSSEC. The term "DNS zone administration" is preferred to "DNS registry" because the SISATA proposition is justified first by institutional constraints, to which the technical aspects are adjusted.

1.3 Document Organization

The document organization comprises background material in sections 2 to 5. This background material presentation is oriented towards the problem area addressed by the SISATA proposition, selectively omitting unrelated aspects and inflating the relative importance of others based on our view of the DNSSEC evolution. Accordingly, sections 2 to 5 should not be taken as a general introduction to the DNS and DNSSEC.

The main DNSSEC deployment analysis is found in sections 6 and 7, respectively investigating an aspect of the DNSSEC landscape and introducing alternatives for DNSSEC deployment. The SISATA proposition itself is introduced as an alternative in the subsection 7.4, and covered extensively in section 8.

Some portions of the present document contain original material. Within the background material, the listing of DNS global support sector participants (subsection 3.1) is perhaps a unique perspective, and the DNSSEC trust anchor key management discussion (subsection 5.3) is material seldom found elsewhere. The analysis sections 6 constructs the original definition of "stable island of trust." Obviously, the SISATA proposition itself (subsection 7.4 and section 8) is also original.

The present document uses both footnotes and bibliographic references grouped in section 10 on page 45. Footnotes indicate support material, sometimes even of anecdotical nature, for interpretations of current trends and opinions. Bibliographic references in section 10 provide material deemed more significant for a broader understanding of the covered subject matter.

1.4 What's in a Name

The SISATA acronym stands for "Stable Island of Security Agency for Trust Announcements."

- The term "island of security" is formally defined in the Internet standard document RFC 4033 [1] and is equivalent to the colloquial term Island of Trust (IOT) used throughout the present document (see document subsection 5.2 for an explanation of IOTs). An IOT is a DNS zone, of which the administrative aspect is relevant to the SISATA proposition, so the island of security embedded in the SISATA acronym refers to a DNS zone administration.

- The qualification "stable" applied to an IOT refers to an expectation of stability over a multi-year time horizon for the IOT as an administrative body, and the domain name for the IOT. This notion is introduced in the present document

section 6.

- The name “agency” applies to the new institution envisioned by the present institutional development proposition, as an agent for stable IOT administrations. The new institution authority comes from its role as an agent of IOT administrations (the SISATA acronym does not refer to a governmental agency in any way). This is introduced in document subsection 7.4.

- Some “trust announcements” are among the foremost operations performed by the envisioned agency on behalf of stable IOT administrations. Such trust announcements are intended to perform the DNSSEC trust anchor out-of-band distribution mentioned in section 4.4 of Internet standard document RFC 4035 [3]. The details of the SISATA proposition with respect to trust anchor distribution are discussed in the present document subsection 8.1.

2. Background on DNS and DNSSEC

2.1 DNS Basics

The DNS (Domain Name System) is an important component of the global Internet. It is sometimes described as an on-line global database of domain names with core functionality being name to IP address conversion or resolution (IP: Internet Protocol). The DNS is like a master directory for the global Internet. Actually, there are many other uses of the DNS as a global Internet infrastructure facility, e.g. providing details of services available from server systems in an organizational unit identified by a domain name.

The domain name space follows a hierarchical organization (www.example.com is subordinate to example.com which is subordinate to com which is subordinate to the DNS root at the top of the hierarchy). The “DNS nameserver” are on-line systems providing (hopefully up-to-date) DNS data to the public Internet. An “authoritative” DNS nameserver serves one or more “DNS zones,” which are sections of the name hierarchy with a single “parent zone” and perhaps one or more “child zones.” For sake of 24/7 continuity of operations, it is recommended that a DNS zone be served by a few authoritative nameservers, and the DNS root is served by thirteen of them. Every nameserver for a given DNS zone must provide the same data, and there is a single administrative authority for any DNS zone. A DNS zone administration is ultimately in charge of maintaining a DNS zone contents up to date.

In addition to the task of operating nameserver systems and coordinating their contents, a

DNS zone administration is responsible for namespace management within its section of the name hierarchy, either allocating names for which it remains authoritative or allowing names for child zones through a DNS delegation. E.g. the DNS zone administration for .museum also manages history.museum, but delegates springfieldart.museum to a child zone administration. Although DNS name resolution principles are not directly reflected in web site contents, the reader may compare http://about.museum/, http://history.museum/, both in the same zone, and the child zone http://springfieldart.museum/.

Important institutional arrangements are in place for the DNS root zone and the few hundred TLD zones positioned just below the root in the hierarchy (TLD: Top Level Domains). These DNS zone administration near the top of the hierarchy are subject to intense policy debates about issues such as pricing for name registration, enforcement of trademark rights, and the like.

The DNS serves the global Internet community and requires, among other, a) interoperability specifications, b) operating guidelines to encourage efficient use of resources committed to DNS operations, and c) an institutional framework for management. The interoperability specifications are made of the many Internet RFCs that update the core DNS specification, RFC 1035 [5], which were created by the IETF DNSEXT working group. Operating guidelines are less formal, and maintained by the IETF DNSOP working group. Actually, because the public Internet has little enforcement facilities, a prevailing DNS operational practice may become a de-facto standard, and eventually become part of the interoperability specifications. At the other end of the formalism spectrum, the institutional framework evolves by itself, and seems to escape any definition attempt.

2.2 The DNS Integrity Vulnerability

It is well known that data retrieved from the DNS is not protected by any integrity mechanism that would prevent data tampering between zone data publication by the DNS zone administrator and Internet user reliance on this data. This is the *DNS integrity vulnerability*, a serious IT security concern for many Internet experts. DNS cache poisoning is a type of IT security attack that exploits the DNS integrity vulnerability.

Does the DNS integrity vulnerability really matter? In discussing this question, we get a sense of the demand for IT security technology, i.e. an intriguing paradox between the ever increasing set of attacks on e-commerce operators (including e-government and online banking) and the limited effectiveness of any workable IT security mechanism. A magic fix of the DNS integrity vulnerability would directly solve a limited set of attacks, but it is doubtful that any encompassing approach to e-commerce security can be drafted

without addressing the DNS integrity vulnerability. While the DNS integrity vulnerability definitely needs to be addressed from the perspective of an educated observer of Internet security, the application use of any DNS integrity mechanism is currently absent, and the impact on human factors still needs attention. In summary, some latent demand exists for improving DNS integrity as an e-commerce strengthening measure; the timing is as soon as possible; but the measurable benefits are indirect and contingent on application support of DNS services not currently available.

2.3 DNSSEC Basics

DNSSEC is a security protocol extension to the DNS interoperability specifications, addressing the DNS integrity vulnerability. The DNSSEC specifications applies modern digital signature technology, known as "public key cryptography," to the data retrieved from the DNS hierarchical database. DNSSEC is the only proposal that addresses the DNS integrity vulnerability, originated from a decade-long protocol development effort in the IETF (references [1], [2], and [3]), notably with the bind software supplier as a flagship open source implementation (reference [4]).

The DNSSEC security architecture is both conceptually simple and intricate at the implementation level. In a nutshell, the DNSSEC services are provided with the public key digital signature technology applied in batch mode, i.e. the DNS data is digitally signed when it is changed in the distributed database, and not when it is requested in an individual DNS database query. Moreover, the DNSSEC chains of digital signatures are structured along the DNS hierarchical name space: this superimposes a trust model over a delegation scheme that was originally intended for database maintenance operational duties.

There is still on-going work on DNSSEC protocols. Progress is being made on the NSEC3 work item, a privacy enhancement mechanism, more specifically a countermeasure against unauthorized collection of every domain name in a given DNS zone, a possibility inadvertently introduced in the DNSSEC protocol ("privacy" is not to be confused with "confidentiality" in the context of NSEC3). In addition to providing some privacy protection (preventing "zone walking") for DNS name registrants in a zone, NSE3 also provides a so-called "opt-in" capability that allows a DNS zone administration to limit the processing load associated with DNSSEC zone signing. This capability is important for large TLD zones.

Progress is less clear for the issue called "trust anchor key management," (an alternate term is "automated trust anchor key rollover," focusing on the required technical functionality). The SISATA proposition is a contribution addressing this last issue, which is covered more extensively starting with section 5.

Moreover, DNSSEC, as a global service upgrade in the Internet, faces the chicken-and-egg acceptance paradox, where the end-user benefits seems to materialize only when a critical mass of DNS nameserver support is reached. In addition, and DNSSEC is not really different from many other Internet services in this respect, the DNSSEC direct benefits accrue to end-users while the DNSSEC operational burden accrue to nameserver operators.

Other important issues for effectiveness in providing DNS data assurance include application software support, and an unbounded security awareness campaign: it is often the end-user who makes the ultimate decision to rely on computer results based on DNS provided data.

3. "DNS Global Support Sector"

We tentatively define the "DNS global support function" as the set of Internet related activities that sustain the global DNS as an effective component of public Internet connectivity.

3.1 DNS Global Support Sector Participants

A number of very diverse organizations are involved in the DNS global support function, and the present section surveys them, perhaps with some minor bias towards the purpose of the SISATA proposition. Note that our list of DNS global support sector participants includes no standard drafting organization, not even the IETF.

3.1.1 Direct Participants

Direct participants support the DNS at the root and TLD levels. Somehow arbitrarily, we differentiate the administrative units (involved in management decisions and policy) from the operational units (involved in systems operations).

3.1.1.1 ICANN

ICANN (Internet Corporation for Assigned Names and Numbers) is a USA-based nonprofit organization that inherited a central role in the DNS support function from US government. In a nutshell, ICANN is the DNS root zone administrator.

3.1.1.2 DNS Root Nameserver Operators

DNS root nameserver operators might be seen as ICANN agents for DNS root sone support, but in practice the Internet history for the establishment of root operators is more intricate than usual contractual arrangements. Root operators provide, maintain, and operate high availability on-line systems that disseminate DNS root zone data to the public Internet.

Currently, the 'A' root server, the master authoritative nameserver for the DNS root, is operated by a private sector organization, Verisign inc., that is also formally responsible for DNS root zone file contents editing. This situation that places Verisign inc. in a strategic position with respect to the decision to introduce DNSSEC support at the root.

3.1.1.3 TLD Administrations

TLD administrations are involved in management decisions and policy for TLD zones. TLD administrations are of two kinds depending on how they initially got their TLD name in the root zone:

- generic TLDs, or gTLDs, having a formal contract with ICANN, this category being subdivided into
  - genuine gTLDs:
    .com, .net, and .info
  - gTLDs with some bias on the child zones that are registered under the TLD name:
    .org, .name, .pro, and .biz
  - formally sponsored gTLDs, or sTLDs, and have a well-defined bias on the child zones that are registered under the TLD name:
    .cat, .aero, .coop, .jobs, .mobi, .museum, and .travel

- generic TLDs, having an history dating to the early days of the DNS, and which didn't evolve into arm's length contract with ICANN
  - .gov, .edu, .mil are United States sectorial TLDs
  - .int is a little used TLD for treaty-based international organizations

- country code TLDs, or ccTLDs, are listed in the two-letter ISO registry of country codes (.uk, .de, .ca, .fr, ...) and are administered by organizations that happen to be recognized by ICANN.

- finally, there is the .arpa "infrastructure zone" for Internet self-management.

3.1.1.4 TLD Registry Operators

Actually, the TLD registry operator function is part of the respective TLD administration duties. There is less separation between administration and registry for a TLD than for the root.

3.1.1.5 DNS Nameserver Operators Acting as Secondaries for TLDs

The secondary nameservers for each TLD are operationally nearly as critical as the primary TLD registry operator, and not necessarily included in our definition of DNS global support sector (e.g. a secondary DNS nameserver operator may be unrelated to any TLD administration).

3.1.2 Participants in the DNS Policy Process

The management and governance of the DNS is a highly debated subject area. Some participants in the DNS global support sector are involved mainly at the management and governance level. The following subsections list such organizations.

3.1.2.1 US Government NTIA as an Influential Government Organization

The foremost participant in the DNS Policy Process is the executive branch of the United States federal government, through the Department of Commerce NTIA branch (National Telecommunications and Information Administration), to the extent it provides legitimacy for ICANN oversight of critical Internet resources, up to the detailed contractual arrangements required by ICANN for its operations.

3.1.2.2 IAB, Internet Architecture Board

In the IETF constellation of institutions, the IAB (Internet Architecture Board) is involved in two ways related to ICANN for the DNS global support function:

1) as a liaison for IETF standardization activities, and

2) as an IANA (Internet Assigned Numbers Authority) overseeing body.

The IANA function is actually performed by an ICANN department. The IAB role is perhaps a mere affirmation of jurisdiction in the IETF view of accountability, since the ICANN operation of the IANA function is legitimized also by a contract with the US government.

3.1.2.3 United Nations Initiatives

The United Nations organized a few WSIS meetings (World Summit on the Information Society), and launched the new IGF initiative (Internet Governance Forum). The primary drive for these UN initiatives is the concerns of many stakeholders, especially outside of the United States, about a single-government control of the global DNS. The effective influence of the IGF is yet to be seen.

3.1.2.4 Alternate DNS Root Nameserver Operators

The mere idea of an alternate DNS root is controversial. The ICANN nearly official position is that alternate roots are detrimental to the global Internet in every single aspect of their motivation, existence, and operation ([18]). However, alternate DNS root initiatives could have a more-than-negligible impact on the DNS global support function, ans as such they would qualify as participants in the DNS policy process, mainly for their indirect influence on DNS management and governance.

3.1.2.5 ISC as an Early Adopter DLV Operator

In the early development of the Internet, a protocol proposal already deployed had greater chances of becoming a “standards track” Internet RFC than a well engineered one. Although this is certainly lesser the case as the global IP network grows in size and criticalness, the DNSSEC scene has recently experienced this deployment-first strategy with the “DLV operation” run by ISC (Internet Systems Consortium) ([6]). This is a push for one of the alternatives for DNSSEC deployment by TLDs (subsection 7.2). This places the ISC as an influential organization for DNS policy processes.

3.1.3 DNS Software Participants

For software participants, our listing is biased towards the DNS software components critically needed for the purposes of SISATA proposition.

3.1.3.1 Wholesale DNS Software Suppliers

The foremost DNS software supplier is ISC, a California based non-profit organization that distributes the bind software as BSD-style licensed open source software. Other DNS software suppliers exist, including PowerDNS (licensed as GPL'ed open source software), and proprietary software offerings by Nominum, inc. These organizations supply somehow raw technological capabilities to operating system distributors and system integrators (see following entry in the present list of DNS global support sector participants.

3.1.3.2 Operating System Distributors and System Integrators

These are participating in the DNS global support function by integrating DNS software and providing relevant configuration support, e.g. IP addresses of DNS root servers, and (once DNSSEC gets deployed) default security settings. Such global DNS interoperability configuration is a small portion of system installation procedures, so there are potential improvements in deployment burden avoidance through early involvement of OS distributors and system integrators in the DNS global support function.

3.2 Services by the DNS Global Support Sector

3.2.1 Name Registration Services

The name registration services are provided to DNS registrars, and ultimately to name registrants (we exclude DNS registrars from the DNS global support participants since no single registrar has strict requirements to offer registration on a global basis). In essence, the name registration service provides determinism of name ownership in a limited namespace. The aftermarket for unused and expired names is a consequence of the DNS global support function primary supply of name registration service.

The DNS registrar industry was created by the ICANN dedication to introduce competition in the name registration service. Nowadays, the DNS registrar industry is very diversified, and operates on a highly competitive environment with low margins. In many instances, the name registration service is a portion of a set of network services offerings. In the strict perspective of DNSSEC deployment, the DNS registrar industry seems to introduce complexity without added value. In any event, the present document does not address this issue any further.

3.2.2 Reachability Support from the Global Internet

The overall DNS operations provide reachability from the global Internet (kind of an electronic doorstep) to support Internet presence of organizations. From the DNS global support sector standpoint, this reachability service is provided mainly to secondary level domain (SLD) operators.

3.2.3 Internet Application Support, General-purpose Applications

Ultimately, the DNS reachability support provides service to Internet end-users through their application software. The DNS global support sector contributes to the application support through the supply of core DNS software, and its integration into operating systems and system configuration procedures. With the DNSSEC focus of the present

document, it is useful to segregate security-oriented application of DNS services (see following paragraph) from general-purpose Internet applications such as web browsers.

3.2.4 Internet Application Support, Niche Security-focused Applications

Just like general-purpose applications, emerging security-focused Internet applications rely on the DNS for global reachability of domain names. Developments in this area could contribute to resolving problems in email based SPAM and public-key and certificate management for encrypted communications systems.

In the case of unsolicited bulk e-mail filtering, two protocol development initiatives can be cited:

- DKIM (DomainKeys Identified Mail Signatures) (reference [7]), and
- SPF (Sender Policy Framework) (references [8], [9], [10], [11], and [12]).

In the case of message encryption supported by DNS distribution of cryptographic keys, some of the current protocol developments can be cited:

- an update to a general purpose specification for storing cryptographic keys in the DNS, intended notably to support OpenPGP public encryption keys (reference [13]),
- the opportunistic encryption protocol development, which appears as a comprehensive application development initiative (references [14] and [15]),
- an enhancement to the SSH (Secure SHell) that uses the DNS as a trust distribution mechanism for public encryption keys (reference [16]), and
- the current HIP (Host Identity Protocol) architecture development also relies on the DNS for trusted public key distribution (reference [17]).

The unique aspect of security-focused applications is the immediate benefit gained from the eventual DNSSEC deployment by the DNS global support sector. This immediate benefit is strengthened security while the security-focused application already provide defined security services with the plain DNS.

Note that such security-focused application might need to embed the DNS resolution function within the application itself, instead of relying on a DNS resolver software somewhere in the end-user environment, where the DNS service may be shared and caching techniques may be applied to reduce the query load on the various authoritative nameservers. If this embedding of DNS resolution function within end-user applications becomes a trend, the DNS query traffic on the public Internet may increase accordingly. No attempt has been made to estimate the potential traffic increase.

3.3 Organizations Benefitting from DNSSEC Services

The following subsections list the Internet participants that would benefit most from the DNSSEC solution to the DNS integrity vulnerability. This list is far from definitive.

3.3.1 E-Commerce Operators

E-commerce operators are increasingly targeted by hackers, especially in the form of phishing and pharming attacks ([19]). This includes e-government and e-banking. Although a clear case has yet to be documented for DNSSEC as a solution element for the e-commerce security, the DNSSEC cure to the DNS integrity vulnerability is definitely part of sensible medium-term solution approach.

3.3.2 Sponsored TLD Administrations

A “sponsored” TLD is an organizations with a more specific mission than an “unsponsored” generic TLD or a typical country code TLD (some ccTLDs for tiny countries are administered as if they were sponsored TLDs). Examples of sponsored TLDs include .museum, .aero, .mobi. An example of a quasi-sponsored ccTLD is .tv. A sponsored TLD mission may, by itself, imply an emphasis on security, in which case the DNSSEC deployment becomes an attractive proposition. For instance, the air transportation service industry has the .aero sponsored TLD and there are reports of interest in DNSSEC motivated by a very high emphasis put on security in the air transportation industry. In summary, a sponsored TLD penetration strategy may adopt the DNSSEC proposition as a differentiation element well suited to its sponsorship mission.

3.3.3 User Communities for Security-focused Internet Application

Security-focused Internet application were introduced in above subsection 3.2.4. The user communities for some of these might spur focused initiatives of DNSSEC deployment.

3.3.4 Large Organizations

The overall DNS integrity improvement capability of DNSSEC is perhaps relevant to IT managers of large organizations for whom the negative productivity impact of security incidents is significant. Perhaps the US government specification of DNSSEC in procurement-oriented standards ([20], [21]) falls into this large organization overall security concern.

4. DNSSEC Policy Background

4.1 Overview of DNSSEC Impact on DNS Zone Administration

4.1.1 The Essence of DNSSEC

The technology perspective teaches us that DNSSEC enhances plain DNS delegations with parallel *secure* delegations. DNSSEC thus extends the DNS administration focus on namespace management with *accountability of online delegation database management*. Specifically, the addition of secured "DS resource records" alongside the previously insecure "NS resource records" means that a "digital signature" enters the picture. The accountability element is introduced in part by the aura of accountability surrounding the term "digital signature." The accountability element enters the picture in spite of the explicit intent of the authors of DNSSEC specifications to restrict the DNSSEC security service to "data origin authentication," in contrast with the "non-repudiation" service that would characterize a security scheme with accountability built-in by design.

Closer examination is deserved for the notion of "accountability of online delegation database management." Well before the information revolution, public institutions of all kinds were required by governmental authority to register persons, businesses, land sections, or whatever, in accordance to some criteria (e.g. a person's competence in a given professional activity). In many cases, the institution is further mandated to make publicly available the record book so maintained, usually with liability-waiving provisions for errors and inaccuracies in the published records. The DNS zone administration role is just another example, with "minor details" such as the global reach of the Internet and the many operational aspects provided in IETF standard documents. Entries in a parent DNS zone file are delegations to child zone administrations. DNSSEC comes with an aura of increased accountability for the contents of the parent zone file as it becomes "digitally signed."

In practice, if DNSSEC is successfully deployed on a global scale, it will be harder for a DNS zone administration (at any point in the DNS name hierarchy) to blame erroneous DNS data on someone else if the data is digitally signed according to DNSSEC. The converse observation is well understood by early adopters and field trial participants: DNSSEC deployment forces DNS zone administrations to review their internal zone management procedures, and fix inconsistencies and error-prone procedural elements.

What is the core lesson? The introduction of DNSSEC in the picture grants a new property to the DNS root and TLD zones, i.e. they become a focal point for trust, co-located with the existing focal point for name resolution.

4.1.2 Burden of Deployment

In addition, the DNSSEC technology brings change to the daily operational duties of DNS zone administrators. As with any other cryptography-based security scheme, DNSSEC brings strong *information controls* that stand in the way of operational procedures (assuming the cryptographic key material is handled reasonably in compliance with the recommended practice). Hence, DNSSEC introduces subtle impacts on DNS zone operations that are actually challenging organizationally, e.g.

- a high error rate in a DNS registry must now be addressed in a more systematic and disciplined way,
- the DNSSEC private key management (i.e. cryptographic key material handling) arises as a new operational responsibility,
- DNS zone administration partners must be solicited for DNSSEC adoption if not already done, i.e. parent zone administration and secondary nameservers,
- in the case of a TLD registry, DNSSEC effectiveness is dependent on DNSSEC adoption by at least one of the registrars offering name registration for the TLD.

These challenges are compounded by the inherent difficulty with economic justification of DNSSEC as an IT security scheme.

The DNSSEC business case would obviously have to consider the purely technical impact of DNSSEC (e.g. incremental system and connectivity capacity planning). Typically, the cost of technical impact is absorbed as a recurrent requirement to stay current with evolving technologies and/or the general declining cost trend in information technologies. In the IT field, this cost decline trend has consistently facilitated the deployment of technological advances that were first applied to niches where the demanding systems requirements were offset by higher valued benefits. This should apply to DNSSEC, but not 100% because DNSSEC introduces database contents authenticity validation which can not be completely eliminated by automation.

Another challenging aspect of DNSSEC business justification is the unbalanced allocation of costs and benefits among DNS zone administrations, bearing the costs, and end-user communities, benefitting from enhanced confidence in the data retrieved from the DNS.

4.2 DNSSEC Deployment Policy at the Root

The DNS root level can be seen as yet another DNS registry administration, and the concerns of the preceding subsection apply to it. However, the root is especially subject to policy because its global impact implies a potential leveraged control on some aspects of the global Internet.

For sake of focus on the alternate deployment strategy, we omit a lengthy discussion of DNS root policy. Our conclusion is simple: with respect to DNSSEC deployment at the root, ICANN is stalled indefinitely by the influence of US government. Here are some recent empirical observations supporting this conclusion:

- Recently, the US government reaffirmed its continued control over the IANA function, especially for the DNS root zone file contents[1].
- In line with a consistent behavior, ICANN staff response to a written inquiry by a gTLD about DNSSEC deployment omitted any bit of information about the DNSSEC support at the root level[2].
- Same behavior occurred in an ICANN public meeting when the general manager for an important ccTLD administration asked verbally and clearly about an appropriate forum or venue for discussion about DNS root signing[3].
- In the process of updating a yearly operational plan, the ICANN staff reworded the DNSSEC deployment milestone from "Implement signing of the root .." with the addition of "Determine timetable, coordination requirements and costs for full deployment."[4].

In short, there is almost no indication of ICANN intent to progress towards "signing the root," i.e. deploying DNSSEC at the root.

Another way to support our conclusion is to anticipate the required steps for DNSSEC

---

[1] Monika Ermert for Intellectual Property Watch, *US Government On Internet Control: ICANN Can Go, IANA Is Ours*, 28/7/2006, http://www.ip-watch.org/weblog/index.php?p=375&res=1280&print=0 . Also, the root transition agreement from Verisign to ICANN, http://www.icann.org/topics/vrsn-settlement/revised-root-transition-agreement-clean-29jan06.pdf , is also connected to the IANA control by the US government, this root transition agreement awaiting approval by the US Department of Commerce as an integral component of a lawsuit settlement between ICANN and Verisign.

[2] Letter from Tina Dam to Edward G. Viltz, *PIR Plans for DNSSEC Implementation*, 14 August 2006, http://www.icann.org/correspondence/dam-to-viltz-14aug06.pdf

[3] See the Sabine Dolderer intervention in ICANN, real-time captioning taken during the Workshop on DNSSEC held on 28 June 2006 in Marrakech, Morocco, http://www.icann.org/meetings/marrakech/captioning-dnssec-28jun06.htm

[4] Compare ICANN, *ICANN Annual Operating Objectives*, Draft dated 20 March 2006, http://www.icann.org/announcements/operating-plan-21mar06.pdf with ICANN, *ICANN Annual Operating Objectives*, Draft dated 22 Jun 2006, http://www.icann.org/announcements/operating-plan-rev-22jun06.pdf

introduction at the root: in order for ICANN to "sign the DNS root," there will be at some point a "ICANN intends to sign the root" report issued by ICANN for public comments. We can anticipate that there will be numerous questions triggered by the proposal, compounded by a prevailing lack of understanding of the DNSSEC technology (e.g. the limited significance a "digital signature" in the context of DNSSEC). It is hard to predict the tone and intensity of the public debate to occur. For instance, it is very unlikely that a debate can be avoided, or even just kept reasonably productive, about who controls the DNS root zone private signature key.

A little historic comparison with the PKI security model is perhaps relevant. When the foundation of the PKI security model was laid, mainly in the 1990's, it was envisioned to have a handful of high level certification authorities (CA), using cross-certification agreements among intermediate-level CAs, providing a global scheme for distribution of trust in the Internet. It turns out that the trust agreements between CAs are difficult to reach, and thus web browsers are configured with large number of "root certificates," each one implying a kind of trust endorsement by the end-user (these are "self-signed" certificates, but they are not trustworthy by virtue of being self-signed).

Turning the PKI lessons to the DNS, the high level CA equivalent is the DNS root administrator *as the single candidate*. The absence of widely recognized high profile root CAs is as a sign of institutional failure, by the government agencies, financial institutions and foremost network operators, to address the intricate policy issues embedded in a high level CA mission. The transfer of this institutional failure observation to the DNS suggests that DNSSEC support by the DNS root administration is unlikely.

4.3 DNSSEC Deployment Status among TLD Administrations

The TLD administrations are autonomous organizations or independent businesses, but not isolated from ICANN politicking. In this respect, there are two categories of TLDs:

- TLD administrations bound to ICANN through a contractual arrangement, including generic TLDs (gTLDs) and sponsored TLDs (sTLDs), and
- Country code TLDs (ccTLDs) which exist by virtue of a two-letter country code being allocated by the International Standard Organization (ISO) to any country in the world [ref ISO].

A ccTLD is not formally bound to ICANN by a contract, but their freedom is not unlimited. The institutional support of ccTLD administrations is a study area by itself ([ref Fromkin]).

The Swedish ccTLD, .se, has been the first TLD to deploy DNSSEC in a production environment and is still alone in this position (commitment to maintain DNSSEC support was announced for a 12-month period). Other ccTLD administrations announced plans or

showed interest in DNSSEC deployment, but none actually turned on DNSSEC-aware nameservers in production environments. In our analysis of primary motivations for DNSSEC deployment (above subsection 3.3), the .se early adoption of DNSSEC would presumably fall under the e-commerce operator motivation, based on an assumption that the Swedish state is keen on e-government projects and would provide resources to the .se ccTLD administration for DNSSEC deployment, primarily as an indirect mean of securing e-government operations (this has not been validated). Alternately, our listing for DNSSEC deployment motivation is incomplete, e.g. in the case of early adopters who might perceive the DNSSEC proposal in unexpected ways.

The sponsored TLDs and the ccTLDs pursuing a sponsored-type strategy (e.g. the .tv TLD acronym has been actively marketed as an affiliation indication for television related activities, without reference to the formal Tuvalu country designation) may have their own justification for DNSSEC deployment (see document subsection 3.3.2).

4.4 Policies for Secure Delegations from the Root to TLDs

For complete deployment at the top of the DNS hierarchy, DNSSEC requires, in addition to DNSSEC support both at the root and at a significant portions of the TLDs, secure delegations from the DNS root to TLD zones.

We learned recently that the gTLD administrations are discriminated in their ability to deploy DNSSEC by virtue of their contract with ICANN. Indeed, an ICANN staff member stated that the DNSSEC service offering by the .org gTLD must be scrutinized according to the ICANN Registry Services Evaluation Process (RSEP) ([22]). The RSEP is a bureaucratic review process applicable to gTLDs that are contractually bound to ICANN (which is not the case for ccTLDs). The RSEP, which is coming into force these days, has certainly not initially been intended as a DNSSEC deployment regulatory tool for TLD administrations, but it might have this impact. Presumably, if a gTLD administration obtains an RSEP clearance for DNSSEC deployment, there would be no other condition for a secure delegation from the DNS root zone (once DNSSEC support is provided at the root).

For ccTLD administrations, the situation is different. A ccTLD administration need no RSEP clearance for DNSSEC deployment, but a secure delegation from the root need not be automatic for them. Given that ICANN is looking for ways to enter into contractual arrangements with ccTLD administrations, the question remains open about the ease with which a DNSSEC-compliant ccTLD zone will get a secure delegation in the root zone file. It is thus conceivable for a TLD and the DNS root to be both DNSSEC-compliant, but no secure delegation from the root zone file to the TLD (this is allowed by the DNSSEC protocol specifications).

4.5 Higher Level Governance Issues

At the global policy and world diplomacy level, the cross-jurisdictional reach and scope of the Internet triggers challenges to the US government oversight of ICANN. Specific initiatives include the WSIS (World Summit on Information Society) and its offspring IGF (Internet Governance Forum). WSIS and IGF meetings were held with resources committed by host countries (e.g. the first IGF meeting was held recently in Athens, Greece) and legitimized by United Nations SG (Secretariat General).

It is obviously beyond the scope of the present document to discuss the forces and tensions at this higher level governance level. It is nonetheless useful to relate to some principles that are carried from the US-centric Internet governance to the IGF level:

- the national sovereignty with respect to ccTLD policies has been affirmed in IGF preparatory documents[5],

- the IGF seems to adopt the culture that was fertile ground for the emergence of the global Internet through technological innovation and spontaneous initiatives by more or less formal groups.

Accordingly, if the Internet governance at the IGF level was to become somehow influential for DNSSEC deployment policies, there is currently no indication that this would be an impeding influence.

4.6 Miscellaneous DNSSEC Deployment Policy Issues

The present author made representations to the US government NTIA about DNSSEC deployment versus DNS and Internet governance ([23]). In doing so, three recommendations were put forward to whichever organization has formal authority over ICANN. These recommendations read

1) Don't use DNSSEC support at root level for to control encryption key distribution.
2) Help the emergence of a "DNSSEC business model."
3) Avoid contractual restrictions on DNSSEC secure delegations from the root.

We refer the reader to the reference [23] for more information about recommendation 1).

[5] See paragraph 63 in, WSIS, *Tunis Agenda for the Information Society*, Document: WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 November 2005, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

Recommendation 2) is about business models. Among the DNS global support sector participants, there are non-profit organizations and regular businesses. For non-profit organizations, a business model boils down to funding or cost recovery for DNSSEC deployment efforts. For regular businesses, a more comprehensive economic justification is needed. Not all costs of DNSSEC deployment can be absorbed by productivity increase originated from technological advances (see section 4.1.2). Since ICANN has been a significant actor in the price regulation in DNS name registration market, and it has not yet stated a position on DNSSEC cost structure allocation, it remains an open question whether a price differential is allowed for gTLD registry services with a "DNSSEC option."

Recommendation 3) above refers to eventual contractual barriers to registration of DNSSEC secure delegation for TLD in the root zone file, and recursively for secondary level domains (SLD) in TLD zone files. Already, an issue of contract clause interpretation has been discussed in the case of data escrow provisions for DNSSEC key material. The recent introduction of the ICANN RSEP (discussed in above subsection 4.3) is another contractual hindrance of unknown impact. The fewer such issues, the better fate for DNSSEC among TLD administrations.

5. DNSSEC Technology Background

This section contains technical information about the DNSSEC protocol, with focus and sufficient details for introducing the notions of DNSSEC Islands of Trust (IOT), Trust anchor key (TAK) management, and the specific TAK rollover procedure used in the present institutional development proposition. In essence, the relevance of the IOT technical notion is increased by the institutional failure to make progress in DNSSEC deployment at the root.

5.1 Chains of Digital Signatures along the Name Hierarchy

In simple terms, the DNSSEC security model is a chain of digital signatures following the DNS name hierarchy up to the root.

DNSSEC digital signatures, like any other application of public key cryptography, use public keys associated with entities or system objects, a DNS zone administration or a DNS authoritative nameserver for a given domain name. The association is operative through the private key counterpart of the public key, by virtue of the strict control of private key usage by the legitimate entity or system object. Colloquially, a "public key," "signature key," or "zone key" refers public portion of the public/private key pair, but when the context refers to the digital signature operation, these terms may extend to the

private counterpart.

The DNSSEC specifications make a distinction between KSK (Key Signing Key) and ZSK (Zone Signing Key), with no mandatory protocol provision associated with the distinction. We find the KSK versus ZSK distinction unfortunate because its use is optional and its specifications text is not very clear. In any event, if the KSK versus ZSK distinction is somehow enforced, the SISATA proposition deals exclusively with DNS zone keys that would qualify as KSK digital signature public keys.

5.2 From Island of Trust to Trust Anchor Key Management

Let's go back to the simple DNSSEC security model as a chain of digital signatures following the DNS name hierarchy up to the root. Actually, there is little oversimplification in this explanation, except for the complexities introduced by broken chains that are inevitable a) until the DNSSEC protocols are widely deployed, and b) since the DNS root is unlikely to be signed anytime soon. Broken chains create IOTs (Islands Of Trust).

The notion of IOT is introduced in the DNSSEC introductory document RFC 4033 [1], as a definition for "island of security." A DNS zone that supports DNSSEC either has a secure delegation from its parent zone (which is possible only if the parent zone itself supports DNSSEC), or is an island of trust. The DNS root can only be an island of trust, simply because it has no parent zone. The DNSSEC protocol operations document RFC 4035 [3] states the obvious about islands of trust: "Validating signatures within an island of security requires that the validator have some other means of obtaining an initial authenticated zone key for the island." This introduces the notion of *trust anchor* or *trust anchor key* (acronym TAK) as a zone key for an island of trust (the term "trust anchor" is also defined in RFC 4033 [1]).

Turning to the administrative side of the DNSSEC support for an island of trust, the term "trust anchor key management" (TAK management) refers generally to the procedures to be followed by IOT DNS zone administrators for to enable validators (i.e. software in the end-user environment, also called DNSSEC-aware resolvers) to obtain, hopefully in a trustworthy way, the relevant trust anchors, and to maintain them over a multi-year time horizon.

As DNSSEC should deploy gradually to a larger scale, it is expected that many islands of trust are eventually going to turn into normal secure zones. In this perspective, the launch of DNSSEC support for the largest TLD zones will be very significant milestones, even more than DNSSEC support at the root (even if the latter would definitely be a high visibility milestone). The more islands of trusts are expected, the more pervasive are the

trust anchor key management issues.

To say the least, TAK management does not scale well as the number of IOTs grows. Something has to be planned for the expected proliferation of trust anchors, before the DNSSEC technology can be claimed ready for deployment. This is an issue with two faces: for SLD zone administrations, it is mainly an issue of ensuring DNSSEC adoption by TLD administrations; for TLDs, the DNSSEC adoption by the DNS root zone administration being uncertain. Hence the need for an *IOT support scheme* for TLDs, and the SISATA proposition comes to the rescue.

The present institutional development proposition is intended to facilitate TAK management in the absence of DNSSEC support at the root. So, we delve into the technical details of TAK management which are relevant to shape the institutional design.

5.3 TAK Management in the Context of DNSSEC

Generally speaking, well applied cryptographic techniques coerce the locus of control, within an organization, at focal points dictated by the key management principles in the security scheme. The locus of controls is tied to cornerstone cryptographic keys, i.e. with DNSSEC, the TAK private counterpart for an IOT like the DNS root. In practice however, the locus of control usually falls in the hands of a computer system administrator who becomes overly empowered, whereas the locus of control should remain in the management hands for an application area. In stressing the bind between cryptographic key management principles and roles within an organization, we are not pleading for the widespread adoption of "role-base access control" systems: cornerstone keys are so few in numbers that related security processes do not require automation. We applied these ideas when designing the TAKREM scheme for TAK management, and the SISATA scheme as an IOT support scheme: the key management design came first, then the roles were allocated accordingly among the global DNS support sector participants.

There are basically two operations needed for TAK management in the context of DNSSEC: initial TAK distribution, and automated TAK rollover (renew the actual TAK value while maintaining or increasing its trustworthiness). In the broader scope of cryptographic key management principles, a TAK being similar to the "master key" in a key management scheme, other operations should be considered as well (e.g. key removal without the introduction of a successor key as in rollover). However, a few factors brings us to the limited-scope TAK management in the context of DNSSEC.

1) Security functional limitations are created by the limited capability of the underlying DNS protocol, i.e. one-way-ness of persistent data transmission from the nameservers to the end-user environment.
2) Formally, a distinction should be made between *emergency* and *scheduled* TAK

rollover operations, but the DNS protocol lacks an alerting mechanism. Also, we believe that TAKREM applied to DNSSEC, our instantiation of the TAK management model, adequately handles key lifetime, in a way that allows the amalgamation into a single concept of TAK rollover.

3) We exclude specific key management procedures associated with a disruptive change of control for an IOT administration, defined as a change in the IOT DNS zone administration without mutual consent between the old and new administrations for a secure transfer of relevant cryptographic key material. This issue is further discussed in following document section 6.

Instead of introducing the TAKREM details, we base the present document on an abstract model for TAK management, made of initial TAK distribution and automated TAK rollover. In the cases where the TAKREM solution enhances the abstract model, this fact is mentioned without delving into the technical details.

For each DNSSEC IOT, the initial TAK distribution requires the configuration of some data, notation TAK-i, in the DNS resolvers. The TAK-i data might be made of one or more public keys, or other data allowing the future validation of public keys. We can make some observations on the initial TAK-i distribution process.

1) The DNS global support sector participants that are in the best position to provide TAK-i distribution are the software suppliers, software distributors, and system integrators. We can observe that some of these participants' involvement in the DNS has been marginal up to now (before the deployment of DNSSEC at any noticeable penetration rate).
2) TAKREM, in contrast with other DNSSEC TAK management schemes, allows TAK-i data that remain stable over time. Accordingly, TAKREM is less likely to introduce “shelf life expiry date” for software distribution.
3) Furthermore, with some boldness in cryptographic key management planning and institutional undertaking, TAKREM makes it possible to establish and distribute TAK-i data for IOT DNS zones *in advance of DNSSEC support* by the respective zone administrators (ICANN analogously reserved ccTLD codes to some countries before they run a TLD registry). See document subsection 8.3.4 for more information.

The other TAK management operation is automated TAK rollover, an operation needed to maintain the global trust in an IOT in the medium and longer term. In our abstract model, this is the distribution of relevant data, notation TAK-r, using the DNS (similar to data broadcast). The TAK-r distribution occurs in-band, i.e. it uses the DNS protocol as the data transmission means (an IOT support scheme relying on out-of-band means for TAK rollover would face irrevocable rejection by DNS global support sector participants). The TAK-r distribution is a task assigned to an IOT DNS zone

administration. The "automated" portion of a TAK rollover occurs in DNS resolver software in the end-user environment, but only if a given DNS resolver software has been configured with the TAK-i data for the IOT.

Some TAK management schemes may require that a DNS resolver processes each TAK-r data broadcast in sequence so that it actively stays current, but this restriction is absent from TAKREM.

Incidentally, avoiding TAK rollover is not considered an option. The complete justification for the TAK rollover operation is out of scope for the present document, but we can observe that no DNSSEC deployment expert would suggest that the short-term trust in a given TAK is valid over the medium and long term, in which case the TAK rollover operation would not be required in the first place. In other words, there is an element of conventional wisdom in the need for TAK rollovers, and it is assumed highly counter-productive to go against the prevailing view on this issue.

In summary, we present a simple abstract model comprising TAK-i distribution by the software provisioning chain and TAK-r data broadcast as an IOT DNS zone administration duty, actually a small part of DNSSEC support activities. We hint that TAKREM is well-suited to instantiate the abstract model, with operational efficiencies not present in other schemes. The SISATA proposition builds on the TAKREM capabilities to address the fundamental issue with IOT TAK management, i.e. the distribution of trust anchors for multiple IOTs does not scale well. See following document subsection 7.4 for SISATA introduction, and section 8 for a comprehensive explanation. Further details about TAKREM can be found in references [24], [26], and [25].

6. Stable IOTs Are a Special Case

The IOT status of a given DNS zone is a byproduct of the DNSSEC technology -- a DNS zone administration would actively seek an IOT status only in exceptional cases (e.g. in a private trust arrangement, targeted at an end-user audience for which specific out-of-band configuration of trust information is feasible; see also subsection 8.3.3). This is why the notion of IOT was not introduced in the preceding document section 4 about DNSSEC policy background.

Given that a DNS zone administration wishes to support DNSSEC, one of the first relevant question is whether the DNS parent zone supports DNSSEC, or intends to support it within an acceptable time frame. (We ignore a secondary question about any unexpected condition for the parent zone administration to "grant" a DNSSEC secure delegation in addition to the existing normal DNS delegation from the parent to the

child.) If the DNS zone administration gets a negative answer from its parent (i.e. no DNSSEC support within an acceptable time frame), it faces the burden of becoming an IOT DNS zone.

In this respect, the DNSSEC technology lacks the flexibility of the PKI where an entity can request an "intermediate-level CA" security certificate (i.e. the PKI equivalent to a DNSSEC secure delegation) from more than a single certification authority before reverting to a "root CA" status (i.e. the PKI equivalent to an IOT).

The essence of the SISATA proposition is the facilitation of DNSSEC deployment for IOT DNS zone administrations. However, not every DNS zone is a good candidate for IOT status supported by the SISATA scheme.

For most SLDs and lower level zones, lack of DNSSEC support by its parent is the end of discussion about DNSSEC adoption, except for the very limited circumstances where a change of domain name is conceivable (e.g. from example.com to example.se). The SISATA proposition can hardly assist the desperate situation of SLDs and lower level zones that are isolated in their IOT status.

It is useful at this point to introduce data turnover in a DNS parent zone with respect to delegations to child zones, both normal DNS delegations and DNSSEC secure delegations. The data turnover is a distribution of the average DNS data change intervals for each domain name delegation in the DNS parent zone file. The DNSSEC protocol is designed with independence between the turnover rate for normal delegations (made of "NS" records and "associated glue address" records [3]) and the rate for secure delegations (made of "DS" records and associated signature records). In other words, in the DNS parent zone management, a secure delegation need not be updated when only the normal DNS delegation is updated (the "NSEC" or "NSEC3" record rules with respect to DNSSEC zone signing do not contradict this secure delegation independence, as they apply irrespective of the DNSSEC status of the child zone). Indeed, a secure delegation merely ascertains the bind between the DNS zone name and a public signature key, and this nonetheless provides end-to-end data assurance. Part of the trick is that the child zone "authoritative NS record," at the zone apex are ascertained with a child zone digital signature, so a parental signature update is not needed when NS values are changed. We refer the reader to the relevant DNSSEC protocol specifications -- the relevant facts are that DNSSEC is subject to delegation data turnover in a narrow definition of "secure delegation," this secure delegation data turnover is lesser than the overall data turnover

TAK management and IOT support schemes apply when the parent zone is not signed, but the data turnover for secure delegations from a would-be signed parent zone is still relevant. The best TAK management and IOT support scheme combination is an

imperfect substitute to signed DNS parent zone, and the analysis of secure delegation data turnover reveals where are the shortcomings.

The itemized list below describes the various contributions by a child zone to its parent zone's secure delegation data turnover, along with observations on handling in the context of

a) a DNSSEC-compliant parent zone,
b) TAK management according to IETF model,
c) TAK management according to the TAK-i / TAK-r model introduced in above subsection 5.3, and
d) an IOT support scheme such as the present SISATA proposition.

- **Creation of a New Secure Zone**

  The creation of a new secure zone is a routine operation in the case of a DNSSEC-compliant parent zone, i.e. the addition of a new DS record alongside the NS record needed for an plain DNS delegation. In the case of TAK management, the creation of a new secure zone triggers a need for TAK-i distribution, which is an area where an IOT support scheme should help. An IOT support scheme may make a distinction between a completely new zone that is initially created with DNSSEC support, and an existing DNS zone that turns DNSSEC-aware. E.g. the SISATA proposition supports anticipation of future DNSSEC support for an existing zone, but is less effective for the expeditious launch of a completely new IOT zone.

- **Rollover of a Secure Zone Key (KSK, Key Signing Key)**

  In the case of a DNSSEC-compliant parent zone, a child zone KSK rollover should be a routine operation, likely to be fully automated. In the case of an IOT, the equivalent operation is an automated TAK rollover, e.g. the TAK-r component of the TAK-i / TAK-r model introduced in above subsection 5.3. The SISATA proposition does not interfere in the automated TAK rollover.

- **Redelegation of a Secure Zone to a Different Administration**

  In DNS zone management terminology, a redelegation is a change in a child zone administrative responsibilities (recall that a change limited to child zone operational parameters has typically no impact on the secure delegation). For any DNS zone that supports DNSSEC, there is critical cryptographic key material (e.g. a computer data media holding the private key for the zone KSK) that should be tightly controlled by the DNS zone administration. We define a disruptive

redelegation as one where a secure transfer of the critical cryptographic key material is not feasible (e.g. the old and new administrations can't agree on conditions and means of key material transmission).

In the case of a DNSSEC-compliant parent zone, the redelegation of a secure zone is a well-defined operation, even if there might be transient difficulties in DNSSEC validations due to cached DNS data. The disruptive nature of a given redelegation may be challenging at the administrative level, but the DNSSEC protocol operations are not impacted.

For the IOT equivalent of a redelegation, it is advantageous to avoid a disruptive change in zone administrative responsibilities: the TAK configuration in end-user environment is invalidated as a consequence of the disruption, and this might mean a serious security incident since there is no agreed-upon mechanism for the new administration to alert DNSSEC-aware resolvers of the situation.

For an IOT support scheme, a non-disruptive IOT equivalent of a redelegation is either a non-event, or seen as a occurrence of a secure zone KSK rollover.

- **Retirement of a Secure Zone**

  The retirement of an IOT DNS zone is a problematic event from a security perspective, because once a DNS zone is removed, its former administration has no means of announcing its retirement, and unsuspicious end-users are faced with a variety of replay attacks. This observation is among the justifications for IOT status avoidance in the first place. Indeed, removal of a secure zone is handled smoothly in the case of a DNSSEC-compliant parent zone.

We define a “stable IOT” as a DNS zone having an administration that is unlikely to experience retirement or disruptive redelegation. Actually, the IOT status is independent from its stability; it came into the terminology because there is no need to assess the stability of a DNS zone having a secure delegation. Obviously, there is no rational criteria to distinguish a stable IOT from an unstable one, because there are no measurement means for administration life expectancy.

In order to support secure DNS zone retirement and disruptive redelegation, the design of an IOT support scheme is likely to turn into a “me too” DNSSEC-compliant parent zone, e.g. through reliance on cryptography-based mechanisms of similar scope as DNSSEC itself. This is not the case of the SISATA proposition.

The present SISATA proposition is targeted at DNS zone administrations facing the

dilemma between no DNSSEC support or an IOT status. More specifically, the proposition targets stable IOTs because IOT support schemes are less effective for other IOTs.

7. Alternate Strategies for DNSSEC Deployment by TLDs

The following document subsections briefly describe various approaches for the facilitation of DNSSEC deployment at the TLD and DNS root. The focus is put on institutional status of respective strategies.

7.1 ICANN Root with DNSSEC Support

The textbook approach for DNSSEC deployment is DNSSEC support at the root early in the deployment campaign. This involves the establishment of a trust anchor key for the DNS root, and compliance with a TAK rollover scheme for medium term and long term maintenance of trustworthiness.

Currently, ICANN is the formal DNS root zone administration, but the root zone file editing and publishing is performed by Verisign, with oversight from the US government Department of Commerce. If ICANN was to sign the DNS root, either by itself or in collaboration with Verising, it would be under its IANA mandate (Internet Assigned Numbers Authority). Earlier in this document subsection 4.2, we listed some of the policy issues that bring us to suspect an indefinite delay in the DNSSEC support at the root. It is precisely about the IANA function that the US government reaffirmed its intention to remain in control of ICANN activities.

7.2 Reliance on DLV Registry Operation

In the absence of progress towards DNSSEC support at the root, a temporary workaround scheme emerged where a collection of IOT TAKs are published as special DNS data in a dedicated zone. This scheme is named DNSSEC Look-aside Validation, or DLV. This scheme is not intended to support any form of TAK rollover for the IOTs, and is being put forward as a temporary solution by contributors who see a signed DNS root as the preferred way.

ISC, one of the major software supplier participants in the DNS global support sector (see document subsection 3.1.3) is also an operator for such a DLV registry scheme ([6]). The specifications for the DLV scheme are not published in a way that would facilitate implementation interoperability ([27]), e.g. at the implementation design, development and test. Indeed, given the ISC special status as the BIND software supplier,

implementation interoperability turns out as an internal issue within the ISC organization.

The ISC operation of a DLV scheme has been questioned, notably for operational aspects that may influence its perceived trustworthiness (i.e. procedural checks fo DLV registry data accuracy). While the DLV scheme appears unbiased towards stable or unstable IOT DNS zones as defined in above section 6, it is deemed to be operationally challenging to keep track of a large number of IOTs at the SLD level. In any event, the DLV proposal and its operation by ISC is presented as an interim, short term solution for early start on DNSSEC deployment.

7.3 Alternate DNS Root with DNSSEC Support

Within DNS governance circles, "alternate DNS roots" is a recurring subject of discussion, always surrounded by an aura of controversy. From a quick survey of the alternate DNS root initiatives that lived for a while, past, current, and suspected, we concluded that each alternate root project exist as an attempt to soften an irritating aspect of ICANN behavior:

- alternate roots attempted to add new types of TLDs because it was felt that ICANN was too restrictive in allocation of new TLDs,
- a Chinese alternate root is alleged to exist today because ICANN appears too slow for enabling IDN (Internationalized domain names) in the DNS,
- at least one alternate root exist based on the fear that the ultimate control of the US government over the root zone file contents might *eventually* turn DNS root zone control into an ill-advised means of international policy implementation.

Actually, the DNS root zone file is of a fairly reasonable size, and its data turnover rate is also quite reasonable. If only a tiny portion of DNS resolvers are configured to direct DNS root queries to an alternate root server, an alternate DNS root zone operation is a manageable undertaking. Indeed, the difficulties with any alternate DNS root zone operation seems to start with any minute departure from the ICANN operations, when the penetration rate of the alternate root increases above an infinitesimal level.

It is unlikely that an alternate root initiative would be triggered by the ICANN slow progress towards signing the root. Firstly, the DLV offering described in the preceding section is already filling this void with a similar spirit of challenge to institutional inertia. Second, the signature key for the alternate root and the ICANN root would conflict, which means planned trouble for early adopters when ICANN finally supports DNSSEC. Third, alternate root operators have generally less extensive technological capabilities than what would be required for DNSSEC deployment in coordinated root nameservers. But again, alternate DNS root is viable on a tiny scale, e.g. for coordinated experimentation, which can include DNSSEC trial. Such tiny scale experimentation does not qualify as a noteworthy institutional development for the purpose of the present

document.

An inverse but related question arises if we considers the impact of an ICANN signed root on alternate roots. Once a zone is signed (i.e. it supports DNSSEC), its contents is protected against intentional or inadvertent modification, for those DNS resolvers which are operating in DNSSEC-aware mode. So, if a resolver refers to an alternate root and becomes DNSSEC-aware, it will suddenly detect modifications made by the alternate root operator, and this would likely defeat the very purpose of the alternate root (for technical accuracy, not every zone file change would be detected as explained in section 6, but without practical impact on DNSSEC integrity protection for DNS data retrieved from an alternate root nameserver). In other words, DNSSEC support at the ICANN root is a step towards limiting the proliferation of alternate root initiatives.

7.4 The SISATA Proposition

We are now ready to introduce the core principle for the present institutional development proposition: a federation of stable islands of security (IOT) for global trust dissemination. The main target of the SISATA proposition is the TLD administrations wishing to deploy DNSSEC in advance of DNSSEC support at the root. The core operating principles are straightforward:

- each TLD wishing to operate an IOT establishes the relevant TAK-i data for long-term trust support;
- every such DNS zone administrations designate the novel institution as its agent for TAK-i distribution; and
- the novel institution distributes the collection of TAK-i configuration data to the software supply chain participants.

Basically, that's it. The novel institution is empowered by its agent role for the TLD constituents, and has the potential to overcome the IOT scaling problem by virtue of offering an exclusive path towards global DNSSEC deployment. The lasting trust property of the TAK-i data allows the new agency to play a minimal yet instrumental role in the DNSSEC deployment, which is why TAKREM is the preferred automated trust anchor rollover procedure in the SISATA context.

The SISATA institutional development proposition is described in the present document, and is available for interested parties to support and plan for effective implementation. There is yet no alliance supporting it since its principles are first detailed in the present document. Indeed it is the only alternative for DNSSEC deployment by TLDs that is not yet influenced by participants in the DNS policy process.

8. SISATA: a Federation of IOTs for Global Trust Dissemination

8.1 Role of the New Agency

The SISATA acronym stands for "Stable Island of Security Agency for Trust Announcements" which is explained in the introduction subsection 1.4. In here, we detail the role of the new agency.

The primary role of the new agency is to *centralize and coordinate the distribution of initial trust information* for enrolled IOTs. Enrolled IOTs are essentially among TLD administrations. The distribution of initial trust information is a foremost requirement when turning on the switch for DNSSEC support in the end-user environment: a trust anchor is the very first configuration item of any DNS resolver software for DNSSEC support, as is explained in DNSSEC core specifications documents (reference [1] subsection 3.1, 5, and 6, reference [3], subsections 4.4, 5, 5.1, and 5.3.1). In a perfect world, this is not needed for TLDs because the DNS root zone administration supports DNSSEC, hence TLDs are *not* IOTs in the first place, and any centralization and coordination is done by the DNS root zone file management. In the real world, the new agency is positioned as a more expeditious institutional development route for DNSSEC support among TLDs.

An IOT support scheme requires the distribution of this initial trust information (notation TAK-i distribution in above subsection 5.3). Realistically, large-scale DNSSEC TAK-i data configuration in end-user environment can only occur concurrently and transparently with new software installation or software upgrade. A typical example is the preparation of a Linux distribution with the binary distribution of the BIND software release and its default configuration files. Generally, this is a typical function of software participants in the DNS global support sector (see subsection 3.1.3). In order to achieve effective "centralization and coordination" for TAK-i distribution, the new agency needs to establish itself as a de-facto source of collection of TAK-i configuration data for the broadest possible set of stable IOTs, and then turn to software participants in the DNS global support sector for actual distribution.

The notion of stable IOTs is introduced in the present document section 6; it is important for the new agency trustworthiness: the new agency should attempt to represent only "stable" IOT administrations. This is because the TAK-i data collection distributed by the new agency represents long-lasting trust information for the enrolled IOTs.

A special care should be exercised by the new agency for the timeliness of TAK-i data

distribution for any given IOT, the sooner being the better. As soon as a TLD administration anticipates to deploy DNSSEC anytime in the future, it should enroll in the new agency TAK-i data distribution program, so that if and when the IOT zone turns DNSSEC-aware, it is immediately supported by a portion of Internet users. The new agency should undertake a targeted education and awareness program for the purpose of early TAK-i data distribution among DNS zone administrations which might expect to become a stable IOT.

The timeliness argument in the preceding paragraph might even be extended to TAK-i data distribution *in advance of* IOT administration agreement to be serviced by the new agency. A closer examination is perhaps deserved before this possibility is put aside: from an IT security perspective, the precise key management principles embedded in the TAKREM technology and procedure suggest an operational framework for establishing and safeguarding the required cryptographic key material in advance of its use by an IOT administration. This is further discussed in following document subsection 8.3.4.

The new agency is not involved in any way in the automated TAK rollover operation which is part of the DNSSEC protocol operational aspect (notation TAK-r introduced in subsection 5.3). The new agency operational involvement is thus very limited, with no specific on-line presence requirements. Moreover, this is coherent with the principle that the SISATA relevance vanishes if the DNS root turns DNSSEC-aware: in this event, a) TAK-i distribution for stable IOTs is intrinsically centralized since the root would be the only stable IOT, b) ICANN needs no agent for TAK-i distribution, and c) in any case no IOT administration relies on the new agency for automated trust anchor key rollover.

While SISATA proposition may be described at a high level with the abstract notions of TAK-i data distribution by the new agency and in-band (i.e. within the DNS) automated TAK-r distribution, the TAKREM procedure and technology adds significant value to the proposition when looking at the details, e.g.

- TAKREM allows TAK-i data distribution in advance of DNSSEC support;
- with TAKREM, the TAK-i data is valid indefinitely for stable IOTs;
- accordingly, TAKREM spares the SISATA entity any involvement in TAK rollover;
- TAKREM provides well-defined manual key management procedures (incidentally addressing many concerns within a debate to occur about DNS root private key control);
- TAKREM allows the SISATA to support non-disruptive redelegation of IOT DNS zone administrations.

It is expected that some of the TLD administrations will be the first adopters of the DNSSEC protocol for their respective DNS registries. The new agency is indeed

suggested as an organization serving, *and controlled or at least influenced by*, stable IOT administrations, i.e. mainly TLDs.

8.2 Not an Alternate Root Initiative

The SISATA proposition shares little, if any, with alternate root initiatives. As indicated in subsection 4.1.1, DNSSEC at the root adds a somewhat independent role to the DNS root management, i.e. DNSSEC introduces accountability of online delegation database management. The section 6 provides further details on this separation of roles when looking at the components of data turnover in a zone file contents, and this analysis is relevant to the root as well.

Alternate roots are attempts to take over the existing role for DNS root zone management. The SISATA proposition assists TLD administrations because they face the IOT status while the root lacks DNSSEC support. Actually, the SISATA proposition is compatible with alternate roots until the genuine DNS root administration deploys DNSSEC (at which point the issues become more complex as DNSSEC-specific discrepancies between root operators enter the picture).

8.3 Strategy for Institutional Development

8.3.1 New Agency Constituents or Members

The SISATA proposition is organized around an agency entity acting as a representative for participating TLD administrations. Thus, the new agency may be formed as a consortium or joint venture of its constituents, i.e. the new agency members are the participating TLD administrations.

It would be reasonable for the new agency founding members to be a small group of TLD administrations, either already supporting DNSSEC in their respective zones, or in the planning stage for such support. It is deemed preferable to keep an arm's length relationship between the participating TLDs and the DNS software suppliers and distributors. Presumably, this would facilitate the new agency support mission for DNSSEC, since TLD administrations are key players for initiating DNSSEC deployment momentum.

In addition to regular members, the new agency envisioned in the SISATA proposition should attempt to enroll “candidate members,” i.e. TLD administrations not currently planning to deploy DNSSEC but reserving trust anchor initial information, to be used if and when the TLD introduces DNSSEC support at a later time.

The new agency might also consider another group from which new members can be accepted, namely stable SLD administrations that face an IOT status because their TLD is unlikely to support DNSSEC in a foreseeable future. However, this should be done on an exceptional basis, if at all, because the SLD count is very large, and any operational definition of "SLD stability" is deemed to be criticized and a source of false positive evaluations (i.e. an SLD that is classified as stable and later experiences retirement or disruptive redelegation as explained in section 6).

8.3.2 Motivations for Institutional Development

The foremost motivation for the SISATA institutional development is DNSSEC deployment in a context where the DNS root administration is not expected to provide DNSSEC support at the root in a foreseeable future. Implicit in this deployment motivation is a willingness to "do it right," i.e. to adopt adequate security procedures for IOT support. "Do it right" is a requirement because DNSSEC integrity assurance is a last line of defense in the Internet security landscape, coming late in the security enhancement process, both chronologically and according to relationships in IT controls. Procedural security emphasis is a requirement because IOT support can not be an completely technology-centric activity.

We have seen that TLD administrations are the first parties interested in DNSSEC deployment, and the candidate constituents for the SISATA institutional development. Among them, some sponsored TLDs and sponsored-like ccTLDs perceive more acutely value of DNSSEC integrity assurance (see document subsection 3.3.2). In addition, some of the DNSSEC dependent security-focused Internet applications (see document subsection 3.3.3) might find support from sponsored TLD administrations.

The SISATA proposition comes with a well-defined path to a critical mass of DNSSEC deployment, and thus offers a unique enabling proposition for addressing the DNS integrity vulnerability. This should attract some support for the present institutional development proposition.

8.3.3 Protection Against IOT Status Uncertainties

In the above subsection 4.4, we saw a possible situation where the DNS root is signed, but the TLD lacks a secure delegation from the root, and thus remains an IOT. Generally, for any DNSSEC-aware zone, there is an operational risk associated with the loss of secure delegation from the parent zone, including cases where the parent zone stops supporting DNSSEC. We refer to this as the IOT status uncertainty.

An alternate trust dissemination strategy, such as the SISATA proposition, may offer

some protection against the IOT status uncertainty for a TLD, or a stable SLD.

8.3.4 Strategy for establishing trust base in advance of DNSSEC adoption

In order to expand its support of future DNSSEC deployment beyond regular TLD members and candidate TLD members, the new agency might consider going one step further, i.e. by preparing trust information (TAK-i configuration data) for TLD administration in advance of their enrollment. The critical security measure for following this strategy is the safeguarding of the private counterpart of the TAK-i data by independent custodians (e.g. three of them) that strictly adhere to key management principles and code of conduit, so that when the TLD administration realizes that DNSSEC deployment requires an IOT support scheme, they can feel confident that the already distributed TAK-i configuration data is a good trust basis for them. In the rest of the present document subsection, we provide details about the implementation of this basic idea, with an implicit concern about any harm potentially caused by this advanced TAK-i data distribution.

In the end-user environment receiving such advanced TAK-i configuration data for a would be IOT TLD, the TLD should be flagged as disabled by default (see document subsection 8.4.1 for the context in which this suggestion applies). If it is inadvertently enabled by configuration management personnel while the TLD is either not supporting DNSSEC or supporting a TAK rollover scheme other than TAKREM, there should be no operational impact other than introducing minor confusion during issue troubleshooting with this IOT TLD (assuming there is an issue to investigate in the end-user environment).

As indicated, independent custodians should be hired to handle the private counterpart of the TAK-i. Once the initial arrangement is completed (including generation of cryptographic key material for the TLD according to the TAKREM scheme), each of the custodian is completely independent from each other, with a role is limited to

a) safeguard one component of the TAK-i data private counterpart,
b) upon a request for action by an alleged TLD administration, validate identity and authority of requestor as a representative for the legitimate TLD administration,
c) following the choice made by the legitimate TLD administration, perform one of the following action:
    1º destroy the safeguarded component of the TAK-i data private counterpart for the TLD,
    2º transfer the complete component of the TAK-i data private counterpart for the TLD to the address indicated by the TLD representative, or
    3º as in 2º above, but transfer only a portion of the component (the TAKREM TAK-i data private counterpart encompasses key material for a number of

TAK rollover operations, and the transferred portion covers a single one),

d) charge a reasonable price for these activities, above transfers c) 2º and c) 3º being charged to the receiving TLD entity, other activities being charged to the SISATA entity except if a TLD entity prefers to pay for the IOT support assurance provided by the custodian role,

e) in case of a collapse of the SISATA entity, destroy any remaining component of the TAK-i data private counterpart for every TLDs that never requested a partial transfer per above c) 3º.

Even if due care is needed for the fulfillment of these duties, the above role comprises no decision making. Also, there is no system technology involved, beyond a safe box with appropriate access controls: the TAKREM scheme defines the components as physical dead storage units, e.g. sealed envelopes with pages of printed bar codes (seemingly meaningless). Preferably, the independent custodians should be based in different countries.

Thus, this arm's length arrangement needs a mostly mechanical implementation by independent custodians. It offers to the TLD administrations freedom to enroll in a very effective IOT support scheme, and significant security assurance in any event. While a TLD administration does nothing, its potential TAK-i configuration data remain ready for later DNSSEC implementation plan support. If a TLD administration finds itself interested in future recourse to the TAK-i configuration data, it should consider becoming a candidate member of the SISATA entity. While, at any time, the TLD administration may take complete safeguarding responsibility for its TAK-i data private counterpart (i.e. requesting transfers c) 2º from every custodians), it is perhaps convenient to continue the reliance on one or more independent custodians already trained and equipped for in key material handling (i.e. requesting transfers c) 3º from one or more custodians at every TAK rollover event, e.g. on a yearly basis). In case a TLD administration declines any reliance on the TAK-i configuration data prepared in advance of its DNSSEC support, it is sufficient to request a single custodian to destroy the safeguarded component of the TAK-i data private counterpart for the TLD.

These details may look as operational subtleties of little interest to the reader, perhaps barely understandable unless the TAKREM scheme is already understood. Nontehtless, these are important details for cryptographic key material handling for *any authority having its trustworthiness based on a trust anchor key*, not just for a DNSSEC IOT (e.g. a PKI trusted CA[6]. What is specific to the present context is this spread of operational

[6] Thierry Moreau, *Trust Anchor Key Renewal Method Applied to X.509 Self-signed Certificates (TAKREM-X.509)*, September, 2005, internet draft draft-moreau-pkix-takrem-01, archived at http://www.watersprings.org/pub/id/draft-moreau-pkix-takrem-01.txt

duties assignments that isolates a TLD administration from SISATA interference, and at the same time provides the benefit of early distribution of trustworthiness configuration data. Accordingly, the basic idea of establishing trust base in advance of DNSSEC adoption is applicable also to the DNS root itself.

8.3.5 Intellectual Property Impact on Institutional Development

The impact of patents is actually beneficial to the SISATA proposition. In essence, the current challenges of DNSSEC deployment is to reach a critical mass in a context where the root can not be relied upon. Besides the DNS root administration, there are no evident centralized entities that can be leveraged upon to advance DNSSEC deployment. Any scheme for which there are low barriers to entry, if it also has chances of success, is deemed to be initiated independently by diverse groups (a possible instance is the DLV scheme described in subsection 7.2). This fragmentation threat compounds the difficulties towards a desirable DNSSEC deployment critical mass. Accordingly, an artificial monopolistic status adds value to an IOT support scheme such as the SISATA proposition. A temporary artificial monopoly is precisely what a patent provides, allowing the patent owner some control over the use of the patented matters, even with protection from anti-trust effect.

Generally, the control afforded by a patent is associated with higher prices for the technology and lesser availability. But this need not be the case in practice: a patent allows a more orderly innovation launch and monopolistic pricing is influenced by market forces such as pre-existing substitutes. The present SISATA proposition is indeed an attempt to orderly deploy DNSSEC with IOT support based on the patent-pending TAKREM rollover procedure.

8.4 Elements of Management Strategy for SISATA Entity Operations

Miscellaneous elements of management strategy for SISATA Entity operations are indicated in the following document subsections. They are generally independent from each other.

8.4.1 Involvement of Software Participants in the DNS Global Support Sector

The SISATA proposition relies on software participants in the DNS global support sector for initial TAK-i distribution service. Actually, software participants are called for much broader involvement in DNSSEC support, including significant software development, testing, release, and support. Furthermore, among the DNSSEC-specific software developments, there are incomplete specifications, such as the NSEC3 protocol refinements for privacy protection. The specifications uncertainty is even more acute with

respect fo automated TAK rollover needed for IOT support, where two foremost solutions are being put forward (the most likely IETF one and the TAKREM scheme) with anyone hardly able to seriously predict an end result.

In this last respect, the SISATA proposition can be mistaken as an attempt to back the TAKREM scheme with a made-to-fit institutional development; in fact, it is the reverse: the SISATA institutional development is attractive because it allows the TLD administration to move forward with a stable IOT support scheme, and then the TAKREM automated rollover becomes a requirement.

Accordingly, it is the adoption of the SISATA proposition by TLD administrations that would indicate the desirable developments to software participants in the DNS global support sector. The main elements of their task would be

1) support of the TAKREM procedure
2) provision of an IOT configuration management dialog (or equivalent) in DNS resolver software, and
3) distribute the TAK-i configuration data provided by the SISATA entity.

With respect to the IOT configuration management, this is an implementation of a "local policy" selection capability ("local policy" refers to choices made by a system administrator that do not impede interoperability according to a data communications standard). The design of this IOT configuration management should be influenced the SISATA institutional arrangement in the following way:

- each IOT should be configured independently because the SISATA entity is an agent for independent constituents,
- for each IOT, a state indication should be available for user control, with the possible values "disabled," "enabled," and "enabled and superceding secure parental delegation," this last state being possible only allowed by the IOT zone administration as it is an assertion of specific trust arrangement, this possibility being recorded in fixed information in the TAK-i configuration data, and
- for IOTs that are not formally enrolled in the SISATA scheme (see document subsection 8.3.4), a configuration change from "disabled" to "enabled" should be allowed only after the user agrees to a warning window (actually a disclaimer) requesting the user to obtain independent confirmation that the IOT administration indeed enrolled in the SISATA scheme.

The reader may get the impression that such a configuration dialogue creates more chances for errors than a signed DNS root which automates the implied trustworthiness assessment decisions. Indeed that impression is correct; DNSSEC support at the root is the preferred way. An analogy with the configuration of trusted CA certificates in web browsers, where each trusted CA is controlled independently, may be extended to the institutional perspective, where the absence of a single globally recognized trusted CA is

analogue to the absence of DNSSEC support at the root.

8.4.2 Compatibility with Likely IETF Automated TAK Rollover Solution

One of the outstanding issues in the DNSSEC protocol specifications is the automated TAK rollover procedure, and the IETF DNSEXT working group has been working on it for a few years. Although the IETF standard-drafting activities for this work item recently came to a halt, there is an automated TAK rollover solution ([28]) that appeared as the most likely solution to be adopted by the IETF.

The likely IETF automated TAK rollover solution is different from the TAKREM solution for about the same protocol functional requirements. An historical review and a comparative analysis would go beyond the purpose of the present document. But the likely IETF solution can be used as a compatibility test for the SISATA proposition (the SISATA proposition relies on TAKREM).

For an IOT zone managed with the TAKREM automated rollover scheme, it is possible to apply simultaneously the likely IETF TAK rollover scheme. Such simultaneous rollover scheme operation applies on the IOT DNS zone administration side. On the end-user side, a DNS resolver software instance (made of a specific implementation version and configuration state) would typically support a single one, as a "local policy." This compatibility does not mean that the SISATA proposition is an IOT support scheme assisting the deployment of the likely IETF TAK rollover scheme. But the recourse to the SISATA scheme does not prevent concurrent support of the likely IETF TAK rollover scheme.

8.4.3 Compatibility with DNSSSEC Support at the Root

The purpose of the SISATA proposition vanishes is DNSSEC support becomes available from the DNS root administration, including easy conditions for TLDs to obtain a secure delegation from the root. The rest of this document assumes a lack of institutional commitment to such DNSSEC support by the DNS root administration. In the present document subsection, we consider the possibility of DNSSEC support introduction at the root *after* the implementation of the SISATA proposition.

The compatibility between an operational SISATA entity and DNSSEC support introduction at the root is a two-sided issue:

1º the required graceful transition from an IOT status to a normal secure zone (i.e. having a secure delegation from its parent) for the TLDs that introduced DNSSEC support before the root, and

2º the IOT support scheme for the DNS root.

The issue 1º, transition from an IOT status to a normal secure zone, is well taken care of by the TAKREM automated rollover scheme. This takes care of the SISATA entity duty of deference for the DNS root administration role. If a number of TLD administration sees value in the IOT status uncertainty protection offered by the SISATA scheme (see document subsection 8.3.3), they should commit resources for the SISATA entity operations after DNSSEC support introduction at the root.

With respect to the issue 2º, the IOT support scheme for the DNS root itself, the root is necessarily an IOT DNS zone for DNSSEC purposes. We previously indicated, in subsection 5.3, that avoiding TAK rollover is not considered an option. This is particularly so for the DNS root administration, due to its unavoidable exemplary status for IT security management. Thus, an IOT support scheme for the DNS root should encompass mechanisms for initial distribution of trust information, and a TAK automated rollover scheme. In this context, the SISATA proposition is either an ignored initiative, or an alternative considered to its own merit. This is why the DNS root zone is mentioned in document subsection 8.3.4 as a possible target of anticipated enrollment in the SISATA IOT support scheme. Otherwise, the present document focus on TLD administrations as early adopters of DNSSEC, and the SISATA potential as IOT support scheme for the root is not discussed any further.

8.4.4 Termination of the SISATA mission

The SISATA proposition is carefully crafted to fulfill a specific need in the DNSSEC deployment with little disruption in existing roles in the DNS global support sector, and new roles implied by the DNSSEC introduction. Correspondingly, the SISATA entity operations require no on-line presence. Moreover, for a TLD administration that relies on the SISATA entity for IOT support, the foremost dependency on the SISATA entity lies with the initial distribution of trust information, i.e. inclusion of its own TLD information in the collection of TAK-i configuration data that the SISATA entity distributes to the software participants in the DNS global support sector. After a critical period when this distribution occurs to a significant portion of the software participants, a TLD administration is less dependent on the SISATA entity.

If the SISATA entity ever collapses, the already distributed collection of TAK-i configuration data remains configured in end-user environment and disseminated among software participants for new software installations. Indeed, TAK-i configuration data set remains valid (in the case of TAKREM at least), except for the circumstances that distinguish an unstable IOT from a stable one, i.e. IOT retirement or disruptive redelegation. The SISATA proposition foremost benefit is the *centralization* of collection and dissemination of trust information, useful until the DNS root supports DNSSEC, and thereafter if some members are interested in IOT status uncertainty protection.

9. Want to Know More?

The present document is presented "as is" with the expectation that interaction can occur among interested participants in the DNS global support sector. In applying a documentation procedure starting with policy motivations and then moving to the envisioned SISATA institutional solution, many aspects of the underlying technologies were incompletely covered. That was done on purpose: we avoided the usual approach of pushing a security technology solution in need for an application market.

We are obviously interested in getting feedback, and answering questions from those involved in the DNS global support sector.

10. References

The present document uses both footnotes and bibliographic references grouped below. Footnotes indicate support material, sometimes even of anecdotical nature, for interpretations of current trends and opinions. The following bibliographic references provide material deemed more significant for a broader understanding of the covered subject matter.

[1] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *DNS Security Introduction and Requirements*, RFC 4033, March 2005

[2] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *Resource Records for the DNS Security Extensions*, RFC 4034, March 2005

[3] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, *Protocol Modifications for the DNS Security Extensions*, RFC 4035, March 2005

[4] Internet Systems Consortium, *ISC BIND*, http://www.isc.org/index.pl?/sw/bind/

[5] P. Mockapetris, *Domain Names - Implementation and Specification*, RFC 1035, November 1987

[6] Internet Systems Consortium, *ISC Launches DLV registry to kick off worldwide DNSSEC deployment*, announcement 2006-03-27, http://www.isc.org/about/press/?pr=2006032700

[7] E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, M. Thomas, *DomainKeys Identified Mail Signatures (DKIM)*, October 20, 2006, internet draft draft-ietf-dkim-base-06, archived at

http://www.watersprings.org/pub/id/draft-ietf-dkim-base-06.txt, see also http://www.ietf.org/html.charters/dkim-charter.html

[8] Mark Delany, *Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys)*, 25 July 2006, internet draft draft-delany-domainkeys-base-06, archived at http://www.watersprings.org/pub/id/draft-delany-domainkeys-base-06.txt

[9] E. Allman, H. Katz, *SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message*, RFC4405, April 2006.

[10] J. Lyon, M. Wong, *Sender ID: Authenticating E-Mail*, RFC4406, April 2006.

[11] J. Lyon, *Purported Responsible Address in E-Mail Messages*, RFC4407, April 2006.

[12] M. Wong, W. Schlitt, *Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1*, RFC4408, April 2006.

[13] S. Josefsson, *Storing Certificates in the Domain Name System (DNS)*, RFC4398, March 2006

[14] M. Richardson, *A Method for Storing IPsec Keying Material in DNS*, RFC4025, March 2005

[15] M. Richardson, D.H. Redelmeier, *Opportunistic Encryption using the Internet Key Exchange (IKE)*, RFC4322, December 2005

[16] J. Schlyter, W. Griffin, *Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints*, RFC4255, January 2006

[17] P. Nikander, J. Laganier, *Host Identity Protocol (HIP) Domain Name System (DNS) Extensions*, October 17, 2006, internet draft draft-ietf-hip-dns-08, archived at http://www.watersprings.org/pub/id/draft-ietf-hip-dns-08.txt

[18] ICANN Security and Stability Advisory Committee (SSAC), *Alternative TLD Name Systems and Roots: Conflict, Control and Consequences*, SSAC Report SAC009, March 2006, http://www.icann.org/committees/security/alt-tlds-roots-report-31mar06.pdf

[19] Aaron Emigh, *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*, Radix Labs, October 3, 2005, available at http://www.antiphishing.org/Phishing-dhs-report.pdf -- note that some experts involved in the preparation of this report acknowledged the editorial oversight of omitting

DNSSEC as a countermeasure for the DNS integrity vulnerability.

[20] NIST Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

[21] NIST Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, public draft, March 2006, http://csrc.nist.gov/publications/drafts/800-53-rev1-ipd-clean.pdf, where secure name lookup service is referred under acronyms SC-20 and SC-21, respectively for DNS authoritative source and DNS resolution.

[22] ICANN, *Registry Services Evaluation Policy*, 25 July 2006, http://www.icann.org/registries/rsep/rsep.html

[23] Thierry Moreau, *DNS Transition Notice of Inquiry Contribution -- re DNSSEC Deployment at the DNS Root*, Letter to NTIA, June 28, 2006, public comment archived by NTIA at http://www.ntia.doc.gov/ntiahome/domainname/dnstransition/comments/dnstrans_comment0080.htm or http://www.ntia.doc.gov/ntiahome/domainname/dnstransition/comments/dnstrans_comment0080.pdf

[24] 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

[25] 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

[26] 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

[27] M. Andrews, S. Weiler, *The DNSSEC Lookaside Validation (DLV) DNS Resource Record*, RFC4431, February 2006

[28] M. StJohns, *Automated Updates of DNSSEC Trust Anchors*, internet draft draft-ietf-dnsext-trustupdate-timers-03.txt, July 16, 2006, archived at http://www.watersprings.org/pub/id/draft-ietf-dnsext-trustupdate-timers-03.txt