CONNOTECH Experts-conseils inc.

Opt-in Process and Nameserver System for IETF DNSSEC,

Text of Canadian Patent Application as Filed

Thierry Moreau

Document Number C004018

2007/04/20

Status of this document:

Copy of disclosure, claims, and abstract of a Canadian patent application. The inventor name is Thierry Moreau.

Document Revision History

C-Number	Date	Explanation
C004018	2007/04/20	Initial release
C004018		Current version

TITLE OF THE INVENTION

OPT-IN PROCESS AND NAMESERVER SYSTEM FOR IETF DNSSEC

BACKGROUND OF THE INVENTION

[0001] The IETF DNSSEC protocol extension to the Domain Name System is an IT security application scheme for public key cryptography, of comparable significance with the PKI model characterized by security certificates, and the PGP model characterized by its web of introducers. See Internet RFC4033, RFC4034, and RFC4035. DNSSEC is characterized by trust transition by digital signatures organized along the domain name hierarchy (actually, it's the DNS zone hierarchy as explained below). Hence, the DNSSEC public key digital signature for the DNS root becomes a focal point of attention, and large TLDs (Top Level Domain) such as .com also become critical resources to commit for large-scale DNSSEC deployment.

[0002] A DNS zone is a contiguous segment of the DNS name hierarchy that is managed by a single entity, where entity encompasses coordinated authoritative DNS nameservers and one DNS zone management organization. A DNS zone has a zone apex, like a local root in the domain name hierarchy, where public signature keys for the zone are registered, individually in DNSKEY RR (Resource Records), and collectively in the zone apex DNSKEY RRset (Resource Record Set). For DNSSEC purposes, DNS RR entries for the same type (e.g. A for IPv4 addresses, AAAA for IPv6 addresses, DNSKEY for a zone public key, ...) and associated with the same domain name are grouped in an RRset for digital signature purposes. A DNSSEC digital signature applies to a single complete RRset for a domain name and RR type; it is encoded as an RRSIG RR. Obviously RRSIG RRs themselves are not grouped in a signed RRset for a domain name and the RRSIG type because this would create

recursion and ambiguity about what is actually signed.

[0003] The above paragraph gives an overview of the DNSSEC signing process for a signed DNS zone. Unsigned DNS zones are devoid of RRSIG, NSEC, and NSEC3 RRs and are normally devoid of DS and/or DNSKEY RRs also. The signing process enforces a discipline in the DNS zone contents management because the signed zone data can not be modified without causing DNSSEC validation errors.

[0004] For a signed zone, the DNS publishing process follows the DNSSEC signature process. DNS publishing is achieved by loading (either in batch or incrementally or differentially) the DNS zone file contents in the memory (or cache or database) of one or more authoritative DNS nameserver and allowing these nameservers to respond to DNS queries with DNS responses through a network interface.

[0005] A DNSSEC-aware authoritative nameserver system is the foremost tool for DNS zone publishing when the zone is signed. Typically, it comprises the required computer equipment, software such as the well-know BIND software (Berkeley Internet Name Domain), database or indexing back-ends, and one or more network interfaces connected to the public Internet or another IP network. A nameserver is available form the IP network to which it is connected through its IPv4 and/or IPv6 address, which can be embedded in a URL. With a computer connected to the same IP network and using readily available software tools such as the “dig” utility distributed with the BIND software, it is convenient to perform ad-hoc real-time queries of the DNS data published in a zone by a nameserver at a given moment, starting with the knowledge of the DNS domain name of interest and the IPv4 or IPv6 address of the nameserver.

[0006] Since a given zone is typically served by more than one nameserver, an issue of synchronization arises, compounded by additional synchronization

requirements of specific DNS zone data with the zone parent and zone children in the DNS hierarchy. Accordingly, transient and temporary inconsistencies in the DNS are tolerated as a fact of life and the notion of “concurrent publishing” between related nameservers or DNS zones has to be understood with these temporal inconsistencies.

[0007] The best equivalent to a PKI security certificate in the DNSSEC protocols is the DNS zone “secure delegation” from a parent zone to a child zone. A secure delegation is made of 1) a public key signature, encoded as an RRSIG RR, authenticating the child zone DNSKEY RRset by one of the key present in the DNSKEY RRset, 2) a hash fingerprint of the DNSKEY RR for this signature key, the hash being registered in the parent zone in a DS RR in association with the child zone apex domain name (which is by necessity below the parent zone apex), and 3) a public key signature in the parent zone, encoded as an RRSIG RR like any other DNSSEC digital signature, authenticating the DS RRset for the child zone. A secure delegation to a signed zone requires the parent zone to be signed.

[0008] The prior art process called DNSSEC validation, or simply validation in the context of DNSSEC specifications, refers to a DNS resolver that verifies digital signatures among the DNS responses received from DNS nameservers, or cached from previous DNS responses. The complete DNS validation is usually triggered by a given DNS service request by a web browser or an application. The DNS validating resolver then verifies a chain of digital signatures, including validation of secure delegation at DNS zone cuts, starting from the domain name in the service request and upwards in the DNS zone hierarchy up to either the DNS root, or a DNS zone for which public keys are trusted, or a DNS zone having an unsigned parent. Within a single DNS zone, a link of the chain may be an RRset signed by a signature key ABC, the latter being present in the DNSKEY RRset at the zone apex, the latter being signed by signature key DEF also present in the DNSKEY RRset. In this example, the key DEF “certifies” the key ABC and may further be involved in a secure delegation from the zone parent.

[0009] By itself, the very complexity of DNSSEC is not the foremost challenge of DNSSEC deployment. Reaching a critical mass of deployment requires the commitment to DNSSEC by the zone management organizations around the top of the DNS hierarchy, in addition to support by DNS resolvers, and also applications in some usage scenarios. This turns into a clear chicken-and-egg issue in reaching a critical mass of deployed components.

[0010] In DNSSEC terminology, when a zone is signed, i.e. DNSSEC-enabled, and its parent is not, the domain is an “island of security” The issue of incomplete DNSSEC support within the DNS hierarchy has been addressed by a scheme called DLV, which is a repository for trust anchors separate from the mainstream DNS hierarchy, however accessible through modified DNS resolver software logic. See Internet RFC4431. However, the DLV scheme requires a DLV operator to provision systems to answer DNS queries from the public Internet, and as such is potentially exposed to enormous traffic growth.

[0011] Very pragmatically, the TLD zone managers under contract with ICANN as the DNS root manager are seldom free to charge extra money for establishing and maintaining secure delegations in the TLD registry (another term for the TLD zone and its computer infrastructure for registering DNS domain names). Nowadays, the DNSSEC technology is invalidated by the lack of a business model for this foremost category of participants.

[0012] Another intriguing aspect of the DNSSEC protocol is its relationship with what is known as “alternate DNS roots.” A single DNS root has been strongly advocated primarily for issues of 1) coordination of introduction of IDN (Internationalized Domain Names), 2) avoidance of discrepancies in the Internet end-user view of the DNS root zone contents, and 3) the difficulty of configuration

management for hundred of thousands DNS resolvers which must know the IP addresses of the DNS root nameservers. See Internet RFC2826. With DNSSEC, the last item seems compounded by the addition of root trust anchor key in the required configuration.

[0013] Actually, an alternate DNS root operation for the sole purpose of DNSSEC support is technically simple. The present inventor refers to such an undertaking as “DNS root nameservice substitution for DNSSEC support purposes” or simply “DNS root nameservice substitution” This is facilitated by the wide availability of the exact DNS root zone file contents, on a timely basis with respect to change schedule, thus avoiding root zone file discrepancies.

[0014] By itself, DNS root nameservice substitution has the potential to solve a major obstacle towards DNSSEC deployment. However, two difficulties arise: 1) a scaling problem with a public root nameservice that is likely to be overflowed by traffic surge if technically reliable, and 2) the resolver configuration issue.

[0015] The present inventor makes a new and useful contribution to the prior art, concurrently with the present invention, by applying the teachings of the IETF SLP (Service Location Protocol) disclosure to the task of deployment and management of DNS root nameservice substitution. The SLP concept is similar to the well understood DHCP, but on a broader scope called an administrative domain (not to be confused with a DNS domain), and with protocol standardization of authentication with digital signatures (SLP allows digital signatures of service announcements, including URLs and service attributes). By assigning the SLP UA (User Agent) role to a DNS resolver, the SLP disclosure opens the door to selective deployment of DNS root nameservice substitution within an administrative domain. Thus, the SLP scheme directly addresses the DNS resolver configuration issue. If a large corporation ABC sets up a DNS root nameservice substitution with the assistance of SLP and the word spreads that it went

smoothly, other organizations will do the same, primarily targeting their respective user base, and no single undertaking will be exposed alone to the global scaling problem. For this purpose, the DNS root zone file signing can be made by a consortium, with the nameservice operation being left to each member.

[0016] Yet another challenging aspect of DNSSEC deployment is caused by the large size of some TLD zones. For these, the DNSSEC security service called "authenticated denial of existence of DNS data," and implemented with either the NSEC or NSEC3 RR type, brings a significant processing overhead. This led to a tweaking of the specification called NSEC3 opt-out in the latest DNSSEC protocol documents. See the Internet draft draft-ietf-dnsext-nsec3-10 entitled "DNSSEC Hashed Authenticated Denial of Existence" expected to be published also as an Internet RFC. Indeed, any incomplete implementation of the DNSSEC specification is deemed to reduce the scope and/or effectiveness of its security services.

[0017] It thus remains problematic that the DNSSEC deployment is limited by important unsigned DNS zones near the top of the domain name hierarchy.

BRIEF SUMMARY OF THE INVENTION

[0018] While the prior art efforts focused on direct operational support of trust anchors for DNSSEC islands of security, the present invention aims at facilitating DNSSEC deployment by bridging the gap between a signed child zone and a signed grandparent zone, or a signed higher generation ancestor zone, when the immediate parent zone is unsigned. Like NSEC3 opt-out, the present invention opt-in strategy decreases the comprehensiveness of DNSSEC security services in favor of easier deployment path. A common public signature key value is used for trust transition between two signed DNS zones.

NO DRAWING

[0019] No drawing is provided; the present invention seems not conveniently and not constructively represented in a drawing.

DETAILED DESCRIPTION OF THE INVENTION

[0020] A public signature key is a numeric value, or small set of values, irrespective of its encoding as an ASN.1 string which affixes algorithm indications and base64 encoding and the like. In the context of the present invention, a public signature key is not systematically associated with its “owner” as is typical in academic literature (“Alice's public key ...”) and in most security protocol encoding specifications, e.g. an X.509 certificate. Notably, the invention uses a common public signature key value in two DNSKEY RRsets, in respective DNS zone apexes identified by different, and perhaps unrelated, DNS domain names.

[0021] In spite of the above, the inventive use of a common public signature key value remains secure and useful for DNSSEC validation purposes. First, because the private counterpart remains under control by an entity. Second, because it is inserted in the DNSKEY RRset of at least one DNS zone apex where it is normally validated by regular DNSSEC validation rules, e.g. a signed DNS root in a preferred embodiment.

[0022] Any DNSSEC zone administrator may insert a public signature key value in the DNSKEY RRset of its zone apex. The present invention suggests a DNS operational practice where the zone manager of e.g. example.com a) inserts the common public signature key value in the DNSKEY RRset of its zone apex, and b) has a portion of its zone file signed by the private key controlling entity. The zone administrator can do this irrespective of the DNSSEC island of security characterization and irrespective of the trust anchor distribution through DLV or out-of-band.

[0023] It is thus possible, reasonable, and legitimate for a DNSSEC validator to accept the signatures based on the common public signature key value in the second zone (example.com) from its acceptance elsewhere in the domain name hierarchy, e.g. in a signed DNS root of a preferred embodiment. Such a validation process overcomes the fact that an intermediate zone, e.g. .com, is DNSSEC-oblivious.

[0024] It should be obvious that the common public signature key value must be validated at least once using prior-art-specifications-compliant DNSSEC validation. This observation suggests an advantageous use where the common public signature key value is present in the DNSKEY RRset of a DNS rot zone apex, either from IANA or in the context of DNS root nameservice substitution.

[0025] In an example of the use of the present invention, the key controlling entity has the opportunity to have the common key included in the DNSKEY RRset at the DNS root zone apex, with a signed root, and the key controlling entity operates as a secure delegation service provider according to the present invention security scheme. The common key and/or the key controlling entity may or may not be involved in the root signing process. The manager of a second-level domain DNS zone, e.g. example.com, prepares a DNSKEY RRset including its own key(s) and the common public signature key. This second-level domain manager may sign the DNSKEY RRset with one or more of its private keys, and in all cases the key controlling entity signs the DNSKEY RRset with the common key private counterpart (credentials are presented by the second-level domain manager to the key controlling entity as is well-known for security delegation provisioning). While keeping these signatures, the second-level domain zone signing proceeds normally to add other signatures to the zone data according to the DNSSEC specifications, and the subsequent zone publishing is otherwise operationally identical to the prior art. It should be clear that if the TLD zone launches DNSSEC support at a later time, a prior-art DNSSEC secure delegation from

the TLD zone may quietly supersede the inventive secure delegation from the key controlling entity. Many variations of this usage example are possible.

[0026] A specific use of the present invention is for authenticating the IPv4 and/or IPv6 addresses of DNS root nameservers in the context of DNSSEC deployment. The difficulty is that the domain names for the relevant A and/or AAAA RRsets may reside in DNS zone(s) which are not resolvable, e.g. in an island of security. For this use, the common signature public key should be in the DNSKEY RRsets at both the root zone and any of zone containing the domain names for the relevant authoritative A and/or AAAA RRsets, the latter being called “root nameserver authoritative addressing RRsets.” Someone knowledgeable of the field may work out the details for the two solutions, respectively in which the non-root zone apex DNSKEY RRset must be signed with the common key, and in which the relevant authoritative A and/or AAAA RRsets must be signed with the common key.

[0027] The present disclosure encompasses an inventive DNSSEC validation algorithm, in the form of an improvement over the prior art validation algorithm. Simply stated, whenever the prior art algorithm is puzzled about accepting an RRSIG RR signature that has been mathematically verified with one of the public keys present in the local zone apex, it may accept the signature if the same public signature key value has been accepted for a different zone name, based on a trust anchor acceptable for the current validation context. As a matter of detail, the DNSSEC encoding specification for a “key tag” is not an appropriate basis to conclude that two key values are equal or not (e.g. if the DNSKEY RR representation of the key has the SEP bit set in one zone but not in the other). Since a broken link in the chain of digital signature may prevent the prior art validation algorithm from actually querying the zone where the common key might be accepted, the inventive algorithm should attempt a reverse direction validation. Alternately, assuming the present invention is practiced with a root-centric strategy on the nameserver side of the DNS, the candidate set of potential

common key values may be arbitrarily set at the DNSKEY RRset at the root.

[0028] In general, the data published in the DNS is used with a large degree of freedom by computers and software applications connected to the Internet or private IP networks. The DNSSEC protocol specifications include resolver behavior provisions for computing a global security status (secure, insecure, bogus, or indeterminate) from observed DNS responses, i.e. turning comprehensive data into summary data. The global security status is more useful when it is other than indeterminate. The present invention allows resolvers to come up with a useful global security status more often if they implement the inventive DNSSEC validation algorithm, to the extent that the DNS includes published data according to the present invention. It is thus obvious for any conceivable application of DNSSEC to benefit from the present invention, merely by upgrading the DNSSEC validation algorithm with the inventive one.

[0029] The technical details of the possible use of SLP with the DNS root are contained in the initial revision (00) of an Internet draft draft-moreau-srvloc-dnssec-priming-00.txt entitled “DNSSEC Validation Root Priming Through SLP (DNSSEC-ROOTP),” this draft being included herein by reference, and attached to present Canadian patent application as it is filed.

[0030] Thus, a general purpose of the invention is to provide a process of DNSSEC publishing a signed DNS zone (target zone) with a public signature key value in the DNSKEY RRset at its apex that is also present in the DNSKEY RRset at the apex of a second DNS zone (reference zone), the two zones being published concurrently, and the target zone having at least one signed RRset signed (with an RRSIG RR) using this same public signature key value, and where the private counterpart of this public signature key is controlled by an entity.

[0031] Another general purpose of the invention is to provide a DNSSEC-aware

authoritative nameserver system where a served DNS zone (target zone) has a public signature key value in the DNSKEY RRset at its apex that is also present in the DNSKEY RRset at the apex of a second DNS zone (reference zone), the two zones being published concurrently, and the target zone having at least one signed RRset signed (with an RRSIG RR) using this same public signature key value, and where the private counterpart of this public signature key is controlled by an entity.

[0032] In a variant of the present invention, the reference zone is higher in the DNS zone hierarchy than the target zone's parent, i.e. there is at least one intervening zone between the target and the reference zone and the latter is closer to the DNS root. In a further variant, at least one of the intervening zone(s) is unsigned, or at least it is published without DNSSEC support concurrently with the target zone.

[0033] In yet another variant of the present invention, the reference zone is a DNS root.

[0034] In a focused variant of the present invention, the reference zone is a DNS root, the target zone apex DNSKEY RRset is signed with an RRSIG RR using the public signature key value, and the target zone contains at least one root nameserver authoritative addressing RRset.

[0035] In an equally focused variant of the present invention, the reference zone is a DNS root, the target zone contains at least one root nameserver authoritative addressing RRset, and said root nameserver authoritative addressing RRset(s) is(are) signed with an RRSIG RR using the public signature key value.

[0036] In yet another variant of the present invention, the target zone apex DNSKEY RRset is signed with an RRSIG RR using the public signature key value.

[0037] In yet another variant of the present invention, the DNSSEC-aware authoritative nameserver system has a network interface referenced by a URL advertized by a service agent compliant to the IETF service location protocol.

[0038] While the present invention disclosure uses the DNSEXT specification as a terminology base as a matter of convenience and clarity, it is referring to the functional aspects of the protocol and security elements, and it is not limited to an embodiment in the current DNSEXT protocol specification. Unforeseen developments in the DNSSEC protocol may occur, as exemplified by precedents in the DNS evolution, i.e. KEY RR was superseded by the DNSKEY RR with similar functionality, and the NSEC RR was given the companion NSEC3 RR mainly for adding a privacy protection aspect missing in the original NSEC RR scheme. Moreover, the spirit of the present invention is independent of the current DNSSEC limitation that a RRSIG RR signature covers the complete RRset for a given domain name and RR type. Or any DNSSEC limitation that zone signing keys appear at the zone apex. Or the DNSSEC limitation on affixing attributes to signing keys (the present invention could make use of a hint bit for OPTIN like the hint bit labeled SEP in the DNSKEY RR encoding). Also, the present invention would be readily adapted by someone knowledgeable of the art to a loosely coupled directory service secured with digital signatures overlaid on a namespace hierarchy similar to DNSSEC.

CLAIMS

What is claimed is:

1 A process of DNSSEC publishing a signed first DNS zone where a public signature key value in the DNSKEY RRset at the apex of said first DNS zone is present in the DNSKEY RRset at the apex of a second DNS zone, where said second DNS zone is published concurrently with said first DNS zone, where at least one signed RRset in said first DNS zone is signed with an RRSIG RR using said public signature key value, and where the private counterpart of said public signature key is controlled by an entity.

2 A process as in claim 1 where said DNSKEY RRset at the apex of said first DNS zone is signed with an RRSIG RR using said public signature key value.

3 A process as in claim 1 where said second DNS zone is higher in the DNS zone hierarchy than the parent of said first DNS zone.

4 A process as in claim 3 where said DNSKEY RRset at the apex of said first DNS zone is signed with an RRSIG RR using said public signature key value.

5 A process as in claim 3 where at least one DNS zone above said first DNS zone and below said second DNS zone in the DNS zone hierarchy is published without DNSSEC support concurrently with said first DNS zone.

6 A process as in claim 1 where said second DNS zone is a DNS root.

7 A process as in claim 6 where said DNSKEY RRset at the apex of said first DNS zone is signed with an RRSIG RR using said public signature key value.

8 A process as in claim 7 where said first DNS zone contains at least one root nameserver authoritative addressing RRset.

9 A process as in claim 6 where said first DNS zone contains at least one root nameserver authoritative addressing RRset, and where each said at least one root nameserver authoritative addressing RRset is signed with an RRSIG RR using the public signature key value.

10 A DNSSEC-aware authoritative nameserver system where a served DNS zone has a public signature key value in the DNSKEY RRset at the apex of said served DNS zone occurring in the DNSKEY RRset at the apex of a second DNS zone, where said second DNS zone is published concurrently with said first served DNS zone, where at least one signed RRset in said served DNS zone is signed with an RRSIG RR using said public signature key value, and where the private counterpart of said public signature key is controlled by an entity.

11 A nameserver system as in claim 10 where said DNSKEY RRset at the apex of said served DNS zone is signed with an RRSIG RR using said public signature key value.

12 A nameserver system as in claim 10 where said second DNS zone is higher in the DNS zone hierarchy than the parent of said served DNS zone.

13 A nameserver system as in claim 12 where said DNSKEY RRset at the apex of said served DNS zone is signed with an RRSIG RR using said public signature key value.

14 A nameserver system as in claim 12 where at least one DNS zone above said served DNS zone and below said second DNS zone in the DNS zone hierarchy

is published without DNSSEC support concurrently with said served DNS zone.

15 A nameserver system as in claim 10 where said second DNS zone is a DNS root.

16 A nameserver system as in claim 15 where said DNSKEY RRset at the apex of said served DNS zone is signed with an RRSIG RR using said public signature key value.

17 A nameserver system as in claim 16 where said served DNS zone contains at least one root nameserver authoritative addressing RRset.

18 A nameserver system as in claim 15 where said served DNS zone contains at least one root nameserver authoritative addressing RRset, and where each said at least one root nameserver authoritative addressing RRset is signed with an RRSIG RR using the public signature key value.

19 A nameserver system as in claim 15 having a network interface referenced by a URL advertized by a service agent compliant to the IETF service location protocol.

ABSTRACT OF THE DISCLOSURE

The process of signing and then publishing a DNS zone according to the IETF DNSSEC protocols is improved by the present invention, in order to facilitate the DNSSEC deployment until most of the DNS zones are signed. The prior art situation is that a second-level domain, e.g. example.com, often faces an unwanted status of “DNSSEC island of security,” and a challenging task of “trust anchor key” out-of-band distribution. The invention somehow fixes such broken DNSSEC chains of trust, e.g. it fills the gap between a DNSSEC island of security and its signed grandparent or ancestor. The invention is deemed useful for the introduction of DNS root nameservice substitution for DNSSEC support purposes, and allows opt-in while NSEC3 opt-out is awaiting deployment in large TLDs.

INTERNET DRAFT
Document: draft-moreau-srvloc-dnssec-priming-00.txt
Category: Experimental
Expires: October 19, 2007

Thierry Moreau
CONNOTECH

April 19, 2007

DNSSEC Validation Root Priming Through SLP (DNSSEC-ROOTP)

draft-moreau-srvloc-dnssec-priming-00

Status of this Memo

Copyright Notice

IPR Disclosure Acknowledgment

Abstract

By assigning the SLP (Service Location Protocol, [RFC2608]) UA (User Agent) role to a DNS resolver, the present document opens the door to selective deployment of DNS root nameservice substitution within an administrative domain. This SLP scheme directly addresses the DNS resolver configuration scaling issue. It is envisioned that various DNS root nameservice substitution undertakings target their respective user base, and no single one will be exposed alone to the global scaling problem. Usage is limited to DNSSEC-enabled root

nameservice. Moreover, from the SLP security features, the proposed scheme expands the set of DNS root trust anchor key rollover options.

Table of Contents

1. Introduction

The present document addresses well-known DNSSEC deployment and scaling issues. DNSSEC is the DNS security protocol ([RFC4033], [RFC4034], and [RFC4035]). The Service Location Protocol version 2, or SLP ([RFC2608]), is applied to tame some of the issues.

For the purpose of the present document, and at the time of writing, the DNSSEC still lacks an accepted standards-based rollover procedure for the DNS root trust anchor key. The timers-based rollover ([TIMERS-ROLL]) is submitted to the IESG wisdom for adoption, and the present author's TAKREM proposal ([SDDA-RR], [TAKREM-DNSSEC]) remains available, at least as a proprietary rollover scheme.

The present document then makes contributions in a number of ways:

- it discusses the opportunity to operate limited-scope DNS root authoritative nameservers for DNSSEC purposes;
- it details the use of SLP to facilitate the deployment of such undertakings;
- it investigates the interaction between the SLP security features and DNSSEC root trust anchor initial distribution;
- in doing this investigation, it revisits the root trust anchor rollover issue, and while doing so it brings a new solution; and
- it provides, in appendix A, a draft formalism for DNNSEC root priming, and while doing so it comes up with a root operational recommendation and a special validating resolver logic for root priming.

2. Overview and Rationales

2.1 DNS Root Nameservice Substitution and Motivations

Recently, a model was revisited for DNSSEC deployment near the top of the DNS hierarchy. It relies on the observation that the operation of a small-scale DNSSEC-aware root nameserver is relatively easy. It can be described as DNS root nameservice substitution for DNSSEC support purposes.

The technical requirements for a small scale DNS root nameservice are easily met. It is the global reachability objective that is difficult to meet. In summary, an authoritative nameserver operator 1) retrieves the root zone file contents from the Internic ftp site, 2) edits or replaces a few resource records, i.e. SOA record,

authoritative NS records, and authoritative A records, and 3) serves the edited root zone contents from the nameserver(s) indicated in the edited A records. A DNS resolver may use this substitute nameservice if it is properly configured.

If DNSSEC enters in the picture, the editing step 2) above is augmented with the addition of DNSKEY records for the digital signature keys, and DS resource records for secure delegations to TLDs that support DNSSEC. Furthermore, a step 2.1) is added for the root zone file signature operation. These DNSSEC-specific actions are required when managing any DNS zone contents. A DNS resolver using this substitute DNSSEC-aware nameservice must further be configured with the appropriate trust anchor data.

The substitute DNS root nameservice may be recursively extended to lower zones when this make up for missing links in the chains of DNSSEC signatures, e.g. in the case of infrastructure zones .arpa, and in-addr.arpa. The same idea applies to the .int zone as soon as a first international organization launches DNSSEC support. These three sample zones are currently managed by IANA, and are available from the Internic ftp site.

The above is a duplication of DNS zone management efforts that were anticipated from IANA. If there is added value in this duplication, it lies in early adoption of DNSSEC and in the opportunity for oversight by some decentralized management. The latter is a substitution for the global oversight management expected from IANA. Maybe the global expectations are so extensive and diversified that DNSSEC support at the root by IANA is not foreseeable.

2.2 Rationale for Departure from the Single DNS Root Dogma

An explanation of arguments for a single DNS root is found in informative reference [RFC2826].

An argument is the desirability of coordinated DNS root zone updates. The present proposal for DNS root nameservice substitution is limited to DNSSEC support purposes, and aims to remain fully compliant with IANA coordinated updates of the root zone contents.

The last argument for a single DNS root is the practical difficulty of relocating the root nameservers in the IP address space. This is addressed in the present proposal with the recourse to the SLP (Service Location Protocol) as explained below.

2.3 Rationale for SLP Usage

The present document applies SLP to the task of priming the DNSSEC configuration in resolver systems, in the scope of an

administrative domain, e.g. a medium or large organization, a government, a consortium of ISPs. See appendix A for a formalization of DNSSEC root priming prior to the introduction of SLP in the picture.

It should be noted that the term "domain" in the SLP applicability statement refers to an administrative domain, and is encoded in the "scope" field of the SLP frame format. In the present document, we disambiguate the SLP domains from DNS domains by using the phrases "administrative domain" and "DNS domain" respectively.

The SLP functionality is sometimes compared to DHCP, DNS SRV records, and out-of-band configuration, for instance see informative reference [RFC3105]. For our purpose, there are, broadly speaking, two attractive aspects of SLP:

- a good fit between the SLP administrative domains, and the task of DNSSEC priming for DNS root nameservice substitution, and
- the SLP security features.

With the use of SLP, the control of DNSSEC priming within an administrative domain, both for caching resolvers and DNSSEC-validating resolver functionality that may appear in end-user applications in the future, potentially remains in the hands of administrative domain management. This may facilitate the phasing out of DNS root nameservice substitution once DNSSEC support is offered by the IANA root.

In essence, the SLP security is an optional digital signature affixed by an SLP SA (Service Agent) on its announcement of URLs for a given service, and on service attributes associated with a given service URL. This simple SLP security scheme does not provide any public signature distribution mechanism, but it may accommodate X.509 security certificates affixed to the digital signature value.

The security of SLP is considered inadequate when SLP is applied to the priming of connections for block storage protocol, see informative reference [RFC3723] where IPsec is recommended as a security scheme underlying SLP. For DNSSEC priming, somehow surprisingly, we make good use of the minimalist and optional SLP security feature, i.e. a digital signature affixed to a service announcement. Actually, the surprise would not resist a deeper analysis with the realization that DNSSEC priming is a security scheme priming, and the further recourse to any full-blown security mechanism would merely push back the perils of security bootstrap.

A later section of the present document explains four security models that are not strictly mutually exclusive. It is expected that an administrative domain selects a security model and then adheres to it for a 1) initial DNSSEC priming, and 2) in the case

of subsection 4.4, DNSSEC root key rollover operation.

The DNS resolver operators within an administrative domain refer to it with an SLP scope identifier. The SLP scope identifier thus selects a DNSSEC-enabled root nameservice. It is strongly recommended that a DNS resolver operator be offered a very small selection of scope identifiers. E.g. only "IANA", for the ICANN accredited root nameservers, and "INTERNAL", for whatever the corporate IT department selects as a DNS root nameservice substitution. In the case of the rollover scheme introduced in subsection 4.4, the security foundation for trust anchor key management can be common to more than one scope identifier. But this is an exception, and furthermore it is difficult to counter the operational threat of maliciously inducing a DNS resolver operator to select a rogue SLP scope identifier.

2.4 Non-Goals

The present proposal attempts to be focused on a single goal, i.e. providing end-to-end DNSSEC deployment in a context where DNSSEC support at the root is not foreseeable. Accordingly, non-goals are readily identified.

- The present proposal is not intended to support alternate DNS roots nameservice where DNSSEC support is not provided. The assumed value added in the case of DNSSEC deployment support (section 2.1) is absent for insecure alternate DNS nameservice.

- The present proposal is not intended to assist configuration of DNSSEC trust anchors other than for the DNS root domain. Other solutions are provided in this area. Moreover, support for DNSSEC island of trust other than the root would be hard-to-justify duplication of DNS zone management effort.

3. Use of Service Location Protocol for DNSSEC Priming

Document editing note: This section is in draft form. The review of the technical details for validating the concept is nearing completion to the point where the adage "the evil is in the details" has been addressed. Part of the specification refinement exercise is a template per [RFC2609] to be submitted for IANA registration.

A SLP UA (User Agent) entity is co-located with the DNSSEC-aware resolver. It is expected that existing SLP SA and DA software and systems can be readily applied to the proposed use, except when the use is made of the recommended addition of algorithm RSA with SHA-1.

3.1 SLP Service Announcement with Attributes

Each IPv4 or IPv6 addresses of authoritative root nameservers should be encoded in a URL, with the respective nameserver DNS domain names encoded as the later part of the url, e.g. "service:dnssec://193.0.14.129/k.root-servers.net." (the reader should not yet take this example for granted). The set of DNSSEC trust anchors for the DNSSEC root nameservice at this URL is an SLP attribute by the name "TA" containing an opaque value for SLP service selection or filtering purposes.

Three SLP attributes are used to convey the type of trust anchor rollover support:

- a presence-only attribute by the name "TIMERS" for a DNS root nameservice compliant to [TIMERS-ROLL],
- a presence-only attribute by the name "TAKREM" for a DNS root nameservice compliant to [SDDA-RR] and [TAKREM-DNSSEC], and
- a string attribute by the name "SLP-ROLL" for a DNS root nameservice announced an SLP SA compliant with the rollover scheme in subsection 4.4, where the attribute value is the SLP SPI (Security Parameter Index).

These are not mutually exclusive.

The present document specifies the addition of the algorithm selection RSA plus SHA-1 in the protocol option set in the SLP deployment, for sake of consistency with the mandatory algorithm in DNSSEC. This is reflected in the IANA considerations section.

3.2 SLP Usage Rules

The SLP attribute request protocol feature is used only in its variant where an explicit service URL is provided by the SLP UA (this is required whenever an attribute signature is to be validated, so we make it a general rule).

A simple SLP UA (User Agent) implementation is required.

The basic DNSSEC priming service discovery uses the SLP request messages "Multicast SrvRqst" and "Unicast SrvRqst". The latter is available if the SLP DA (Directory Agent) address is known, which can be obtained via DHCP ([RFC2610]), or through the SLP service discovery itself as indicated in the SLP specification. The expected answer is a SLP response message "Unicast SrvRply" containing the service URL(s) indicated above.

4. DNSSEC Priming Operation vs Trust Anchor Key Management

Unless otherwise specified herein, the DNSSEC root nameservice service discovery operation should not be triggered without operator intervention by a DNSSEC-aware resolver system. In

addition, the operator should be fully aware of the SLP scope used by the SLP UA for priming the DNSSEC-aware resolver. This is recommended so that a DNSSEC root nameservice substitution has a well-known name.

4.1 Un-authenticated Priming

The unauthenticated SLP service discovery may be an option for an administrative domain management, or it may be the only option available because the DNS resolver system that needs DNSSEC priming lacks the appropriate SLP SPI public key or the functionally analogue TAKREM TAK-i configuration data. In either case the security implications of un-authenticated priming should be weighted against the alternatives.

4.2 Priming with SLP Digital Signature Validation

This is a straightforward application of SLP security features. The public signature key to be used for signature must be configured in the DNS resolver prior to the priming operation. The public signature key is identified by the SLP SPI protocol field. If SLP is already deployed in the system hosting the DNS resolver, an SPI value and the corresponding public key may already be available for authenticating the DNSSEC priming.

4.3 Priming with Implied TAKREM Trust Anchor Management

No SLP attribute is defined for distributing the TAKREM TAK-i configuration data to DNSSEC-aware resolver.

However, if TAKREM TAK-i configuration data pre-exists in a DNSSEC-aware resolver, priming with SLP need not use the SLP security option.

4.4 Priming and Rollover with SLP Digital Signature Validation

If DNSSEC priming becomes "easy" and adequately secured with the SLP security option, a spontaneous trust anchor key rollover scheme emerges: repeat the DNSSEC priming operation whenever a trust anchor key rollover is deemed required.

Indeed, this is an instance of this classical security scheme: the long-term signature key periodically endorses a fresh operational key. In this instance, the rollover scheme catastrophic failure mode is a compromise of the SLP signature verification key. The rollover scheme implementation guidelines are obvious to deduce: use a larger key size for SLP than for DNSSEC, and restrict the key usage as much as possible.

Inherited from the notion of SLP administrative domain, this

rollover scheme is born with a flexible security authority management capability: the administrative domain that "controls" rollover may be separate from the DNS root zone operator. The SLP administrative domain may indeed migrate the DNSSEC service from a root operator to another one without DNS resolver operator involvement, e.g. upon a scheduled trust anchor rollover operation.

5. Security Considerations

The DNSSEC priming operation is a security critical operation subject to "social engineering" attacks (e.g. induce the DNS resolver operator to perform priming using a bogus procedure). This is especially true when the operator is expected to select an SLP SPI identifier.

In deploying the scenario of section 4.4, confidence in the overall security would be increased with no operator selection of SLP SPI identifier, i.e. if there is a single one.

6. Internationalization Considerations

No internationalization consideration has been identified at the time of writing the initial revision of the present document. It is expected that the final version will restrict the SLP usage to the English language.

7. IANA Considerations

No IANA consideration arises from the SLP notion of an administrative domain, including the namespaces for SLP scope field values and SLP SPI (Security Parameter Index).

In a later revision, the present document would require an allocation for a service scheme registration per [RFC2609], for reference to the DNSSEC root nameservice. Then a template per [RFC2609] would be filled.

In a later revision, the present document would require a allocation for a Cryptographic BSD (Block Structure Descriptor) Codes per [RFC2608] for the digital signature specifications that is mandatory in DNSSEC, i.e. RSA with SHA-1. This is justified by the avoidance of implementation burden of the DSA digital signature scheme in the SLP UA software that would typically be embedded in DNSSEC resolver software. The whole DNSSEC deployment effort is based on RSA with SHA-1. In the DNSSEC specification, the RSA signature with MD5 is not allowed for DNS zone signing.

No IANA consideration arises in relation with DNS or DNSSEC specifications.

Appendix A - A Primer on DNSSEC Root Priming

The present appendix contains a preliminary specification for DNSSEC root priming. Such a specification seems to lack from the DNSSEC document set.

If the initial configuration of a DNS resolver can be seen as a local matter with respect to protocol standardization, it is nonetheless a significant impediment to DNSSEC deployment. Indeed, in bringing up the following specification, an operational issue came up, with a related recommendation, about DNS root zone management in the context of DNSSEC deployment.

The specifications language used in the present appendix is both technical and high-level. In a later document revision, it should be complemented with more specific references to the DNSSEC protocol features.

DNSSEC is about validating digital signatures for data retrieved from the DNS, e.g. authoritative A RRsets for a domain name, so that name-to-address translation is trustworthy.

Let's refine by adaptation to the authoritative nameservers for a DNS domain name that is a DNS zone apex: DNSSEC is sometimes applied to validate the digital signatures for A and AAAA RRsets from DNS domain names that are listed in the NS RRset in the zone apex, the latter RRset deserving signature validation as well.

Let's further refine to DNSSEC priming for an island of trust: when the above process for validation of authoritative nameservers is applied to an island of trust, validation of signatures stops at the KSK(s) found and self-validated in the DNSKEY RRset in the zone apex. Some or all of these KSK(s) may need to be backed by an authentication procedure outside of DNSSEC, either a priori or a posteriori.

Oops, this introduces a potential corner case: the DNSSEC priming process for an island of trust may encounter a different island of trust for the authoritative nameserver addresses than for the zone apex.

This suggests an original DNSSEC operational recommendation for an island of trust: if the DNS domain name of an authoritative nameserver is neither within the zone itself nor within a descendant zone for which a chain of trust exists, the zone containing the authoritative nameserver should have the same public key value as the trust anchor in its DNSKEY RRset, and the DNSKEY RRset should be signed with it. It is the signature public keys that should match, not the DNSSEC RR itself.

The following refinement it then made: in the DNSSEC priming process for an island of trust, when the DNS domain name of an authoritative nameserver is within neither the zone itself nor a descendant zone for which a chain of trust exists, the DNSKEY RRset at this other zone apex deserves special validation with the same signature public key as found in at least one of the KSK(s) for the original zone.

Now, we can formulate the two requirements for DNSSEC root priming:

- The DNS root zone management should follow the above recommendation about signature public key. In practice for the IANA root nameservice, this would be done by adding an appropriate DNSKEY RR in the DNSKEY RRset of the DNS zone "root-servers.net.", signing the resulting RRset with the private key counterpart, and serving the DNS zone "root-servers.net." with the RRSIG RR included.
- For a resolver, the DNSSEC root zone priming is the above process applied to the root zone.

In summary, DNSSEC root priming starts with an IP address for a root nameserver; the end-result of DNSSEC root priming is the validated list of DNS domain names and addresses for root nameservers; this validation is trustworthy to the extent that the KSK(s) on which it relies are backed by an authentication procedure outside of DNSSEC.

The DNSSEC root priming process should occur in the following cases:

- upon installation of a DNSSEC-aware resolver entity,
- on a timer expiry basis, as implied by the smallest TTL value observed in DNS RRsets relied upon in the previous instance of root priming, and
- in relation with root trust anchor key rollover, whenever a change occurs in the set of trusted KSK root keys.

Normative References

[RFC2608] E. Guttman, C. Perkins, J. Veizades, M. Day, "Service Location Protocol, Version 2", RFC2608, June 1999

[RFC4033] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005

[RFC4034] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005

[RFC4035] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005

[TIMERS-ROLL] M. StJohns, "Automated Updates of DNSSEC Trust Anchors", internet draft draft-ietf-dnsext-trustupdate-timers-05.txt, November 29, 2006

[SDDA-RR] T. Moreau, "The SEP DNSKEY Direct Authenticator DNS Resource Record (SDDA-RR)", work-in-progress, Internet Draft draft-moreau-dnsext-sdda-rr-02.txt, April 2006

[TAKREM-DNSSEC] T. Moreau, "The Trust Anchor Key Renewal Method Applied to DNS Security (TAKREM-DNSSEC)", work-in-progress, Internet Draft draft-moreau-dnsext-takrem-dns-02.txt, April 2006

[RFC2609] Guttman, E., Perkins, C. and J. Kempf, "Service Templates and service: Schemes", RFC 2609, June 1999

Informative References

[RFC2826] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", May 2000

[RFC3105] J. Kempf, G. Montenegro, "Finding an RSIP Server with SLP", RFC3105, October 2001

[RFC3723] B. Aboba, J. Tseng, J. Walker, V. Rangan, F. Travostino, "Securing Block Storage Protocols over IP", RFC3723, April 2004

Author's Address

Thierry Moreau
CONNOTECH Experts-conseils inc.
9130 Place de Montgolfier
Montreal, Qc, Canada
Tel.: +1-514-385-5691
e-mail: thierry.moreau@connotech.com

IPR Notices

Intellectual Property

Copyright Notice

Disclaimer