CONNOTECH Experts-conseils inc.

Six Roles for Early Introduction of DNSSEC

Thierry Moreau

Document Number C004006

2007/05/15

Document Revision History

C-Number	Date	Explanation
C004006	2007/05/15	Initial release
C004006		Current version

Table of contents

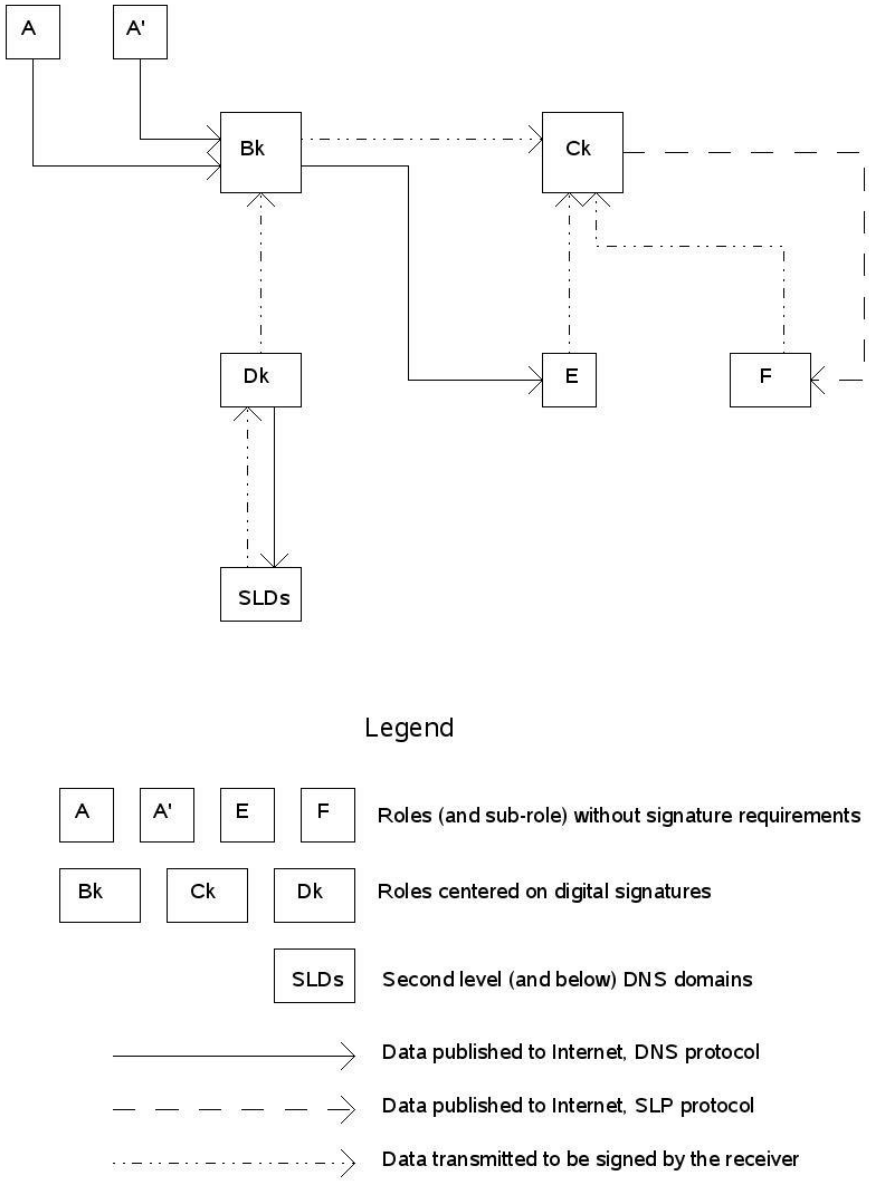

Figure 1) Relationships between the six roles for early introduction of DNSSEC

1. Introduction

1.1 Background

The Internet grew out of innovation and experiments, in ways that challenged established business principles and traditional public service operations. Out of these experiments, the more mature portions of the Internet technology settled in operational/institutional models that might be qualified "proven" despite their young age.

The DNSSEC deployment near the top of the DNS hierarchy is both very new, and constrained by the technological and institutional maturity of the DNS. The DNSSEC novelty lies in a new application scheme for the public key cryptography digital signature technology, with the both modest and ambitious goal of fixing the "unsecured DNS integrity vulnerability." The goal is modest considering the limited effective security services provided by DNSSEC, and ambitious considering it was never done before and DNSSEC is not trivial to implement and deploy.

In this context, the present document describes an innovative set of roles, with interrelationships, for assisting the DNSSEC deployment near the top of the DNS hierarchy. Here is a sequential account of proposals and documents, in the innovative and experimental category, of the present author:

The TAKREM for DNNSEC Proposal

> After a fortuitous invention of TAKREM in the field of cryptographic key management in 2005 ([1]), the DNSSEC trust anchor key rollover requirement was quickly identified as a possible field of application ([2], [3]), and triggered the present author involvement as a participant in DNSSEC discussion forums.

The SISATA "Proposition"

> The SISATA document ([4]) is more important as a survey of the "DNS Global Support Sector," and other background information than for the deployment scheme proposition that was explicitly documented to be put on the shelf. The SISATA document is indeed providing background information relevant to the present document.

The six roles for early introduction of DNSSEC

This refers to the two original technical proposals which are at the origin of present document. One is an Internet draft ([5]) covering the two roles tied to the SLP (Service Location Protocol). For the DNS root trust anchor key rollover, these two roles bring an alternative to both TAKREM and its IETF DNSEXT preferred protocol alternative (i.e. [6]). In other words, TAKREM for DNSSEC is somehow deprecated by the six roles. The other technical proposal is currently only documented in a patent application ([7]), and provides an opt-in secure delegation scheme.

1.2 What Is Early Introduction of DNSSEC?

If nothing special is done, the deployment of DNSSEC at a significant penetration rate is likely to be postponed indefinitely, mainly for two reasons: a) the political debates surrounding the control of the DNS root zone file updates, and b) for gTLD registries, the lack of business incentives attached to DNSSEC deployment. Thus, the critical mass of DNSSEC deployment is seldom reachable due to lack of DNSSEC support near the top of the DNS hierarchy, i.e. at the DNS root and important TLDs. For a given DNS domain administrator wishing to have its DNS data protected against the integrity vulnerabilities, the important TLD is the parent of the relevant domain, e.g. the .com TLD in the case of most e-commerce operators.

The overall goal of the six roles is to circumvent the lack of DNSSEC support near the top of the DNS hierarchy, without creating unnecessary difficulties. Because the six roles include DNS root nameservice substitution, they share with “alternate roots” a scaling issue for the task of DNS resolver entity configuration. Two of the six roles are mitigating the scaling issue in DNS resolver configuration.

Early introduction of DNSSEC is thus proposed as a model for DNSSEC usage before the required organizational and technological infrastructure is put in place. The present document briefly explains the six roles and their relationships, without attempting to educate the reader in the underlying technologies, protocols, and security techniques.

1.3 Nomenclature for the Six Roles

The six roles announced by the title are enumerated below, with a brief description. Their relationships is depicted in the figure on page 3, where roles are indicated by labeled boxes. Three of the roles involve digital signature operations using a private signature key, making the security backbone of the proposed DNSSEC deployment.

(A and A') Root Zone File Preparation

DNS root zone file (RZF) preparation is currently done by a centralized organization, ICANN. The introduction of DNSSEC relies on this central RZF preparation, but expands it to secure delegation data collection.

Until an institutional commitment emerges for DNSSEC support at the root, secure delegation data collection is a RZF preparation *sub-role* (label A' in the figure on page 3) for which ICANN is of little assistance.

(Bk) Root Zone File Signature

Technically, the RZF signature role is specified in section 2 of RFC4035 ([8]). Once the RZF contents is established and verified, including secure delegation data, the foremost remaining issue is control of private signature key. The RZF signature role requires no on-line presence.

(Ck) Off-Line Signatures for SLP

The off-line signature for SLP role comprises signature operations supplemental to the RZF signature role. It is the digital signature operation portion of the DNSSEC nameservice advertizement specified in the reference [5]. The core data signed for SLP pertains to the DNSSEC root nameservice and its trust anchor keys. But there is other miscellaneous data which needs to be signed, mainly for formal compliance with the SLP specifications.

(Dk) Opt-in Secure Delegation Operations

The opt-in secure delegation scheme is a novel alternative to DLV ([9]), i.e. a scheme intended to facilitate DNSSEC deployment while a large number of DNSSEC islands of security exist because important TLDs are left unsigned. In the more recent and intricate refinements of the DNSSEC protocol development, the NSEC3 opt-out protocol provision (section 6 in [10]) fulfills a related requirement, i.e. minimizing the DNSSEC performance impact for large *signed* TLD registries while a small portion of second-level zones are signed. The opt-in secure delegation scheme has a similar impact, while not strictly replacing the NSEC3 protocol provision.

In the context of the six roles, the opt-in secure delegation operations role represents a secure delegation *provisioning service* to be offered to second-level (and below) domain managers who whish to support DNSSEC in their respective zones. Thus, opt-in secure delegation operations require on-line presence in a name registration provisioning context,

including required authentication security and digital signature generation capabilities. However, and unlike DLV, the opt-in secure delegation scheme requires no on-line presence for DNS name resolution support.

(E) Authoritative DNS Root Nameservice

The DNS root namesevers that currently support the public Internet are operated by organizations that commit critical resources for stability of global DNS services. Besides these ICANN recognized high traffic nameservers, possibilities exist for a) DNS root nameservice on a very limited scale, e.g. laboratory experiments or private roots, with little added value besides the nameserver operator pride, and b) “alternate roots” motivated either by a challenge to ICANN legitimacy in determining the RZF contents, or a whish to counterbalance the US government oversight of RZF updates.

In contrast with alternate roots, the single motivation for the six roles is the postponing of DNSSEC deployment near the top of the DNS hierarchy. In the context of the six roles, it is assumed that the authoritative DNS root nameservice role can be fulfilled by interim operational entities while the unique root lacks DNSSEC support, and perhaps while the opt-in secure delegation scheme remains a necessity because large TLDs are lacking DNSSEC support. This is deemed to be a reasonable scale undertaking, notably when deployment is assisted with the SLP service agent operations role.

(F) SLP Service Agent Operations

The SLP (Service Location Protocol) is a stable IETF protocol specification intended to facilitate largely automated deployment of host computers, not unlike DHCP (Dynamic Host Configuration Protocol). The SLP functionality applied to DNSSEC deployment avoids the circular arrangement that would occur if the DNS SRV record type was used to advertize the network address and other characteristics of DNSSEC-aware DNS root nameservice.

In the six roles for early introduction of DNSSEC, the SLP service agent operations addresses the DNS resolver configuration scaling issue. It is based on SLP compliant implementation, somehow extended by mandatory use of the optional SLP digital signature scheme, furthermore with signature algorithms, modes of operation, and key sizes that are not usually found in SLP implementations.

2. DNS Root Nameservice Substitution for DNSSEC Purposes

Three of the six roles contribute to "DNS root nameservice substitution for DNSSEC purposes," i.e. those labeled A (including sub-role A'), Bk, and E. Respectively, they represent what ICANN should do to maintain, sign, and publish a DNS root with DNSSEC support. In a substitution mode of operation, the separation of the three roles provides flexibility, efficiency, and scaling capability as explained below.

(A and A') Root Zone File Preparation

The central root zone file preparation done by ICANN is represented in the figure on page 3 by the box labeled A, and the currently missing secure delegation data collection by the sub-role box labeled A'. The pre-DNSSEC root zone file is available on the Internic ftp site ([11]). Collecting secure delegation data for the root zone file (sub-role A') means monitoring the TLDs that support DNSSEC for any update in their trust anchors, and ascertaining the genuineness of any such update.

Eventually, the A' and A roles would be merged, the sooner the better. Actually, the ICANN organization may be advised to maintain a public record of secure delegation data for the RZF without signing the RZF, for some time prior to the launch date of DNSSEC support at the root.

(Bk) Root Zone File Signature

The key pairs used for RZF signature operation preparation include a DNS root trust anchor. The six roles diminishes the criticalness of the security experts debate over the separation of control between the KSK (Key Signing Key) and ZSK (Zone Signing Key), multiple storage of private key components, certification of cryptographic hardware, and even trust anchor key rollover. This is caused by the RZF signature role being introduced and authenticated by the two SLP roles (this document section 3), the latter having a non-global scope.

Stated differently, there is low barrier to entry in the RZF signature role, and the SLP roles act as independent agents between suppliers and consumers. Thus, the DNSSEC key management separation between KSK and ZSK is transferred to the role separation between the RZF signature and the off-line signatures for SLP. This separation combined with the non-global scope of SLP provides flexibility that should turn into scalablity.

In reference to the figure on page 3, the arrow pointing upwards to the RZF signature role

labeled Bk depicts the inclusion of a special public key in the DNS root keyset. This signature public key with an unusual justification is transparent to DNS root nameservice and name resolution. However, it allows the introduction and authentication of the opt-in secure delegation role (this document section 4).

The end-product of the RZF signature is delivered to one or more authoritative DNS root nameservice organizations (label E in the figure on page 3). Normally, each DNS root nameservice organization would have its own set of DNS authoritative nameservers; accordingly, the RZF signature needs to be adjusted according to the recipient organization.

Also part of the RZF signature deliverables, the root nameserver addressing information is sent to the off-line signature for SLP organization(s). In a complete six roles scheme, there is one (or more) off-line signature for SLP organization for each authoritative DNS root nameservice organization. The root nameservice configuration data sent along this route includes trust anchor and addressing data, and is intended for both publication (service advertizement with SLP) and authentication with digital signatures.

(E) Authoritative DNS Root Nameservice

This role is not modified by its inclusion in the six roles. Strictly speaking, it does not exist currently on a global scale because the ICANN DNS root does not support DNSSEC. However, a few ccTLDs do support DNSSEC, the Swedish one being the first and foremost example.

3. Service Location Protocol Support for Deployment

(Ck) Off-Line Signatures for SLP

The SLP protocol specification ([12]) allows digital signatures for service advertizement and service attributes. In the case of the six roles, this is further specified in section 4 in reference [5]. The “off-line” qualification refers to the generally agreed principle that a private signature key is less subject to compromise if the signature operation can be performed by a computing device with no or minimal network connectivity.

This role provides DNS root trust anchor key management.

On the figure on page 3, the arrow pointing upwards from the nameservice (label E) to off-line SLP signature (label Ck) refers to the IP addresses of the authoritative DNS root nameservers (this same information could also be obtained through the RZF signature role). Similarly, the arrow pointing from the SLP service agent (label F) to off-line SLP

signature (label Ck) refers to the SLP scope strings which define SLP administrative domains. From a security design perspective, the delineation of signed data appears less carefully crafted in SLP than in DNSSEC, and the known rationale for SLP scope value signatures is the mere formal Internet RFC compliance.

(F) SLP Service Agent Operations

From the perspective of specifications compliance, based on the SLP specifications, this role is not modified by its inclusion in the six roles. However, deployment guidance recommendations would be welcome since the SLP service agent role is intended to address the DNSSEC resolver system configuration scaling issue. Although SLP currently has a user base for other service advertizement uses, the guidance recommendations applicable to DNSSEC can only be established through experimentation and early deployment experience.

4. Opt-in Secure Delegations

(Dk) Opt-in Secure Delegation Operations

In reference to the DNSSEC protocol terminology, an opt-in secure delegation occurs when a SLD domain manager prepares a revision of SLD zone keyset, i.e. the DNSKEY RRset at the zone apex. The opt-in service provider has a direct delegation signature key pair, and the SLD domain manager includes this direct delegation public key in the SLD zone keyset, i.e. a DNSKEY resource record for a signature key that is exceptionally not controlled by the zone manager. The SLD domain manager sends the revised keyset to the opt-in service provider. The latter authenticates and checks the authorization status of the SLD before digitally signing the DNSKEY RRset with its direct delegation signature private key, and returns the signature to the SLD domain manager, i.e. the service provider sends an RRSIG resource record. The SLD manager includes the received direct delegation signature in the zone file and serves the DNS zone through the authoritative nameservers as usual.

5. Conclusion

Out of the six roles presented here, three should be performed for the ICANN root when DNSSEC support is introduced. The two roles related to the Service location Protocol are intended to spread the Gordian knot of trust anchor management and DNS resolver configuration among separate roles with limited scope instead of a single global Internet undertaking. The fundamental challenges do not magically vanish; they are hopefully made more manageable.

The original DNSSEC opt-in scheme fits well in the proposed early deployment of a signed DNS root.

The present document merely introduces the six roles and their interrelationships. It is perhaps challenging to the reader to delve into the details to make his/her opinion on the extent to which the various components gracefully interwork. At the very least, many details are left unspecified about public key and signature updates among the three signatory roles.

6. References

[1] 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

[2] 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

[3] 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

[4] Thierry Moreau, *The SISATA Institutional Development Proposition for DNSSEC Deployment Facilitation*, CONNOTECH Experts-conseils inc., Document Number C003957, 2006/11/15, http://www.connotech.com/sisata_proposition.pdf

[5] Thierry Moreau, *DNSSEC Validation Root Priming Through SLP (DNSSEC-ROOTP)*, Internet Draft (work-in-progress), draft-moreau-srvloc-dnssec-priming-01.txt, May 9, 2007, archived at http://www.watersprings.org/pub/id/draft-moreau-srvloc-dnssec-priming-01.txt

[6] M. StJohns, *Automated Updates of DNSSEC Trust Anchors*, internet draft (work-in-progress) draft-ietf-dnsext-trustupdate-timers-06.txt, April 2, 2007, archived at http://www.watersprings.org/pub/id/draft-ietf-dnsext-trustupdate-timers-06.txt

[7] Thierry Moreau, *Opt-in Process and Nameserver System for IETF DNSSEC, Text of Canadian Patent Application as Filed*, CONNOTECH Experts-conseils inc., Document Number C004018, 2007/04/20, http://www.connotech.com/optin_for_dnssec.pdf

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

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

[10] B. Laurie, G. Sisson, R. Arends, D. Blacka, *DNSSEC Hashed Authenticated Denial of Existence*, internet draft (work-in-progress), draft-ietf-dnsext-nsec3-10.txt, January 2007, archived at http://www.watersprings.org/pub/id/draft-ietf-dnsext-nsec3-10.txt

[11] ftp://ftp.internic.org/domain/root.zone.gz

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