DNSSEC Lives. Now what? How to avoid certain failure.

Dr. Richard Lamb

ICANN, Marina del Rey CA 90292, USA,
richard.lamb@icann.org

Abstract. With the healthy deployment of DNSSEC well on its way and serious efforts to make use of the resulting global PKI to expand the benefits of cryptographic security to the masses, DNSSEC has the potential of becoming a critical link for a wide range of industry applications. However, many of the current practices employed and mindset in the current chain from registrant to root are inadequate and need to improve if the Internet is to reap the full benefits from DNSSEC. This paper will seek to identify the weak links in this chain and to outline approaches various entities can take to strengthen them.

Keywords: DNSSEC, DPS, SysTrust, WebTrust, DNS, IT Security, Processes and Practices

Disclaimer: The views expressed in this paper are those of the authors and do not represent those of their employer. Topics: DNS and Cybercrime, DNS Cyber Threats and Vulnerabilities, DNS Defense, DNSSEC (all aspects), Impact of DNS on Critical Infrastructures (Energy Systems, Finance etc.)

1 Introduction

At the time of this writing, 72 out of 310 TLDs have deployed DNSSEC. Due to the popularity of some of those TLDs, over 80 percent of the domain names on the Internet have the ability to deploy DNSSEC. However, since it is still a relatively new technology, less than 1 percent of domain names have DNSSEC deployed on them. This is both a drawback and an opportunity.

Our increasing reliance on the Internet, and its protocols, for critical applications encompassing everything from financial and health care systems to new applications, such as smart grid in the electric utility space, make it imperative that the Internets infrastructure needs to be improved. DNSSEC is a big step in that direction.

Unfortunately, many of the current practices employed in the chain of trust (Registrant to end user) are inadequate. Reaping the full benefits of DNSSEC will require enhancement. This paper will identify the weak links in this chain and outline approaches entities can take to strengthen them.

Given the early stages of overall deployment, the goal of this paper is to encourage a race to the top with the establishment of best practices instead of

one to the bottom (untrustworthy deployment leading to little value and minimal adoption) by raising awareness and learning from and building on existing sources of trust on the Internet.

2 DNSSEC Lives! - Nirvana?

With the root signed [ICANN root] and a healthy implementation rate on TLDs, we believe full DNSSEC deployment, at least at the top level, is an eventuality and the benefits from a trusted DNS will be realized.

Future innovative efforts to develop a range of global security and authentication solutions based on a DNSSEC secured DNS will increase security and improve the overall Internet experience [VCandDK].

Although the idea of using the DNS to provide more than just IP addresses and domain names has been around for some time, the concept of using the DNS to deliver key material was cited as early as [Schlyter Cert]. The expansion to other cryptographic applications [IPSEC] [DKIM] quickly followed with the view that DNSSEC would someday become a reality.

It should be noted that the desperate need for a global source of identity on the Internet (e.g., e-mail addresses) has had vendors relying on the unsecure DNS for some time as a validation mechanism for creating accounts on web sites and even as part of acquiring digital certificates attesting to the owner of a web site. As the only source of globally unique generic identifying material on the Internet, the vendors had little choice but to attempt to make use of the DNS in this way.

Once DNSSEC is fully deployed, the technical underpinnings will finally be in place to trust the DNS for such transactions but this requires that DNSSEC be deployed and managed carefully.

2.1 SSL

Given the availability of this newfound secure, global database in the DNS, the first natural step is to find ways to extend and improve upon existing sources of trust on the Internet. Currently the only widespread source of such trust is Certificate Authorities (CA) providing SSL digital certificates.

Digital certificates provide a mechanism for a CA to cryptographically attest to the identity of the certificates owner. The certificate and associated key data is deployed by a web site owner to provide a way for the end users browser to validate the sites owner.

While the inclusion of a CAs public key or root key to validate certificates in an operating system (OS), or its removal in the case of CA compromise, is often a difficult and lengthy process, the addition, update, or removal of records from the DNS is easy and can be dynamic.

Problems with OS distribution include, but are not limited to, dependence on update release cycles, expensive audit requirements (not necessarily bad), inability to reach static installations, and flawed certificate revocation systems.

Placing CA root key material in a DNSSEC secured DNS provides the ability to easily update key material quickly and at little or no expense. This not only improves CA key management but also has the potential of greatly increasing the number of SSL protected sites (currently only 4M [SSL obs] out of over 200M) by reducing certificate distribution costs.

Interest in being able to indicate to OS or browsers which CA root key to trust for a particular domain has recently increased with the spate of CA compromises [comodo]. Competition among the large number of CAs (1482 [SSL obs]) has often resulted in the use of inadequate methodologies to verify the identity of domain name holders. This has, at times, reduced the quality of a CAs attestation [DV SSL] and hence certificates issued by it, making it hard to distinguish which CA to trust. Using data from DNS to decide which CA root key to validate against provides a level of trust agility in the face of changing trust models and threats.

Linking DNSSEC and SSL CA services and having combined operations (e.g., a Registrar that offers DNS hosting and is a CA) can lead to synergies such as increased assurance that a certificate is associated with the actual domain name owner; reduced costs using shared facilities and procedures between DNSSEC and CA; reduced certificate management costs via DNSSEC distribution; and marketing and additional product opportunities for an entity.

Standards, that are in the final stages of approval, have been collaboratively developed between Internet standards organizations such as the IETF and CA organizations for DNSSEC based certificate distribution and management [DANE SSL].

Although support for SSL certificates drawn from or validated in DNS is not yet supported in popular operating systems, demonstration software [DANK BH] and experimental efforts building DNSSEC SSL support directly into browsers [CHROME] has shown promise.

2.2 SMIME

SMIME is a mature secure email system supported by many email packages. Although it has been in existence for some time, difficulties in distributing and managing the PKI key material needed to support SMIME, not to mention being able to exchange such material across different organizations, have kept widespread SMIME use out of reach.

Just like SSL, SMIME uses certificates with a chain of trust to root keys. Each email sender has its own certificate that is used by recipients to validate the sender. If a sender can look up a recipients certificate, it can also encrypt email destined for that recipient.

The difficulty here is how to easily lookup the certificate of a recipient or sender across disparate systems on the Internet. Currently enterprise certificate distribution mechanisms vary between systems and have unique access control regimes that make interoperability difficult. A single common secure mechanism might finally let SMIME reach its full potential.

DNSSEC to the rescue! Similar to the SSL efforts above, work is being done to place SMIME certificates (or cryptographic hashes uniquely identifying them) into the DNSSEC secured DNS in a standardized format [DANE SMIME]. This would then remove technical barriers to a truly cross-organizational, transnational secure email system built on an installed base of existing products.

As with SSL certificates, the ability to draw certificate information from the DNS is not part of currently popular operating systems, but demonstrations of this approach have been successful and show promise [DANK BH].

2.3 Other applications

If DNSSEC is widely deployed in a trustworthy manner, we believe many other applications, in addition to SSL and SMIME, will hang their keys in the DNS. Standards for IPSEC [IPSEC], DKIM [DKIM], and discussions on how to secure the ever expanding percentage of VoIP phone calls are either already in place or in process.

On a broader scale, DNSSEC may provide support to the quest for improved identity mechanisms in cyberspace that many governments are taking on in response to public cybersecurity concerns.

Regardless of the focus we believe the open, hierarchical, bottom-up, multi-stakeholder nature of DNS and DNSSEC lends itself to becoming a platform for innovative security solutions that will go far beyond simply securing DNS lookups.

3 Reality Check Failure?

Every one of the above applications relies on being able to trust responses from the DNS thus placing ever greater pressure on its various entities to operate in a trustworthy manner.

The cryptographic algorithms used in DNSSEC provide mechanisms to ensure this technically. However, the management of the key material associated with DNSSEC is, by its nature, one with opportunities for missed updates and compromise which could lead to failure and mistrust.

The combination of this added complexity with the additional material (e.g., keys) that must be accurately exchanged via administrative/out-of band interfaces between entities in the hierarchy makes the nirvana described above an empty hope if these issues are not given adequate consideration.

We believe the current early stage of DNSSEC deployment at the Registrant level is an opportunity to develop an environment to encourage the implementation of secure processes and practices before DNSSEC comes to be widely deployed and critically relied upon.

With the potential for such high levels of reliance on a DNSSEC secured DNS, it is better to work to set the bar high from the start.

3.1 Chain of Trust

When an end user goes to a web page he/she begins a series of actions that rely on many entities in the Internet ecosystem. The first step typically involves querying the ISPs local DNS resolvers. The DNS resolvers will retrieve the requested information on behalf of the user. If DNSSEC is enabled on the resolver, it will also attempt to cryptographically validate the response before returning it to the user.

If this is a new request for the resolver, it will then query root, Registry and Registrant DNS servers until it has tracked down the requested information and, for the DNSSEC, validate each intermediate response against prior ones in the DNS hierarchy and terminating with the root key. Since Registrars are responsible for processing Registrant requests and data into Registries, they too are in the path.

From the perspective of DNSSEC validation, the end user relies on the ISPs resolver to lookup DNS records. The resolver ultimately relies on the root key to validate the DNS result. The root uses its key to attest to the Registry keys. The Registry uses its key to attest to key material received from the Registrar who handles keys controlled by the Registrant. This forms a chain of trust from Registrant to end user.

Registrant → Registrar→Registry→Root→ISP/resolver→End User

(or by way of example: mybank.se→GoDaddy→IIS .SE Registry→ICANN→City DSL→mybank account holder)

In order for a DNSSEC response to be trusted, each entity along this chain of trust must not only support DNSSEC, but do so in a trustworthy manner. As a chain of trust, the level of trust placed by the end user in a response is set by the weakest link in the chain.

What follows is an overview of possible weaknesses at each link in the chain in the context of DNSSEC.

3.2 Registrant

Each Registrant is responsible for deploying DNSSEC on its domain name. This means either putting together its own DNSSEC signing system, complete with key generation and management systems, or outsourcing these operations to a third party.

The current DNS mentality of set and forget for what has been effectively a static file does not work for DNSSEC. Specifically, the time dependent nature of DNSSEC signatures requires regular updates and key rollover. Failing to do so can leave the domain name unreachable. For many Registrants, the skills for these additional tasks may not exist or exceed either current human or financial resources. This can lead to inadequate or insecure implementations that may lead to the eventual removal of DNSSEC functionality due to cost or potential reputational harm.

Alternatively, for the vast majority of Registrants, the complexity of DNSSEC key maintenance and other duties will relegate DNSSEC operations to a third party just as Web and DNS hosting is done now.

However, this simply moves the problem to the DNS provider who may have only a limited interest in trustworthy DNSSEC operations while the Registrant still bears the bulk of its own reputational responsibility. The Registrant should therefore carefully consider its agreement with and the reputation of the DNS provider.

Unfortunately, without building awareness in the end user and Registrant communities, providing such services quickly becomes a race to the bottom for the DNS operator who would only be driven to provide a minimal implementation with little concern for trustworthiness and no overall benefit to the end user.

3.3 Registrar

As the interface between Registry and Registrant, without the support of the Registrar, DNSSEC has little hope of widespread deployment.

Many Registrars point to a lack of demand for DNSSEC as the primary reason for not supporting it. Registrants, conversely, point to the lack of Registrars supporting DNSSEC as a barrier to deployment. Without sufficient support and deployment by these entities, end users will not reap the benefits of DNSSEC or any subsequent innovation.

An isolated view of support and deployment costs for Registrars and Registrants also enters into this standoff.

Unfortunately this mindset can again lead to either forgoing the benefits of DNSSEC altogether due to lack of support or building untrustworthy end user/registry interfaces and operations to support it. In the early stages of DNSSEC deployment, an excessive number of failures and/or unprofessional handling of incidents would be a death knell for further DNSSEC deployment efforts. With a loss in perceived benefit, Registrants would cease to request DNSSEC and Registrars drop support for it. Without a widely deployed, secure and trustworthy DNSSEC infrastructure, the promise of innovation in the prior section becomes a pipe dream.

3.4 Registry

Registries responsible for the TLDs have many of the same concerns as Registrars regarding the lack of demand and cost.

However, the adoption rate here is not so bleak. The decades of DNSSEC development by the Internet community has brought along with it awareness for those operating TLDs. Most Registries accept that they will need to eventually deploy DNSSEC [ccnso survey].

Due to cost constraints, some of the smaller TLDs may forgo deploying DNSSEC or end up with untrustworthy deployments. As will be described later, there are multiple approaches to overcoming cost issues.

Deployment need not be expensive if proper practices are put into place and expectations set appropriately. There are also multiple inexpensive or free secure [ccTLD PCH] outsourcing options.

3.5 Root

DNSSEC was deployed on the root July 15 2010 [ICANN root] and supported by a key management process requiring the direct involvement of 21 trusted community representatives from around the world. This ensures trustworthy management of the root keys with global buy-in in a way that encourages a simple validating structure relying on one key.

Feedback and suggestions for improvements on this system is continually taken by ICANN from the Internet community.

3.6 ISP

The ISPs direct relationship with the end user places it in a position of trust. In this position, the ISP typically operates a DNS caching resolver on behalf of end users to take advantage of aggregation and speed up DNS response time. To support DNSSEC and thus cryptographically validate responses before passing them to the end user, the ISP need only enter a copy of the root key and switch on this capability. Unfortunately, few ISPs have done so, fearing additional support calls and additional, albeit minor, maintenance in installing DNSSEC root key material in their resolvers.

Making the leap to turning on DNSSEC validation should be considered carefully since mis-configuration of the ISP resolver would lead to DNS lookup failures and bad end user experiences. The danger of which may be a major setback for turning on DNSSEC validation again and hence keeping DNSSEC benefits from the masses.

3.7 End User/Relying Party

The end user or relying party is the most influential entity in the chain of trust. Although in an ideal setting, where DNSSEC has been fully deployed on the Internet, the end user would see no signs of DNSSEC, without end user awareness of the benefits of DNSSEC, it may never reach the critical mass needed for innovation to flourish.

The end user, unaware of DNSSECs benefits, might point to this new DNSSEC service as a problem during its rollout by, say an ISP, where a poorly operated external domain name may have failed validation by no fault of the ISP. As a result, the end user and ISP may simply turn off validation as an expedient approach to avoid any more support calls. This would further frustrate DNSSEC deployment and block the future benefits it could bring.

Conversely, an end user who is aware of DNSSECs benefits (either through Registrant, ISP, Registry or other education) can drive adoption and subsequent DNSSEC application development that will provide a better Internet experience for all.

4 How to avoid failure Raising the bar

Although the previous section did not paint an encouraging picture for the new-found DNSSEC infrastructure ever becoming a source of trust on the Internet, let alone playing a role in critical applications, there is hope.

DNSSEC deployment can be used as an excuse to revamp or improve the processes and practices surrounding DNS operations to become a cornerstone for security on the Internet and to be relied upon for critical applications. By applying practices used by established sources of trust on the Internet and benefiting from their lessons learned, we can transfer and even improve upon many of the same qualities to DNSSEC.

Borrowing from the many decades of experience CAs have developed in selling trust and all the legal, financial, and reputational aspects that entails allows us to bootstrap that same trust into DNSSEC operations. This has been done at the root as well as a few top level domains.

Armed with this experience, below are suggestions for each of the entities in the chain of trust described in the previous section.

4.1 For End Users/Relying Parties

Finding a path toward building trust into DNSSEC deployment is only half the solution toward a trusted DNSSEC infrastructure that benefits all. The other half is encouraging the relevant entities to take the path and implement the processes and procedures borrowed from the CA community.

As the largest beneficiary of a trusted infrastructure, it is the 2B [pingdom] end users of the Internet that need to demonstrate their interest in security by gravitating toward secure Web sites, ISPs, and other solutions on the Internet. By doing so, entities in the chain of trust will be incentivized to take the path that builds trust in their offerings.

Therefore, building end user awareness regarding the benefits of a trusted DNSSEC infrastructure is the key step in ensuring that trustworthy DNSSEC deployment becomes a race to offer the best product instead of a race to the lowest cost and quality service resulting in an untrustworthy deployment.

4.2 For the ISPs

For ISPs, the steps needed to support DNSSEC are deceptively simple. Since the majority of DNS resolver implementations already support DNSSEC, it is only a matter of switching on DNSSEC validation functionality. This will ensure that records for domains with DNSSEC deployed on them must be validated before passing to the end user.

There will likely be increased computational load on the DNS resolvers, that may require additional servers. However, given the gentle uptake of DNSSEC this can be an incremental process.

Due to the public facing nature of ISPs, which can greatly amplify even the slightest misunderstanding on the part of the end user, additional education for

support staff regarding DNSSEC should accompany a decision to offer DNSSEC validating service on an ISPs resolvers.

For example, as Registrants progress along the DNSSEC learning curve, there are bound to be situations that make the Registrants site temporarily fail to validate and thus become unreachable by no fault of the ISP. But the complaint reaches the ISP first.

Large ISPs have already begun to roll out support for DNSSEC in their resolvers [Comcast] or are the process of considering it.

Finally, ISPs can use this relatively minor investment by promoting DNSSEC as a differentiator amongst products and competing providers.

4.3 For Registrants

Registrants have a number of options for trustworthy DNSSEC deployment on their domain name.

They can build their own DNSSEC signing system adopting the same practices used by Registries and the root. As will be described below, depending on individual requirements and risk profiles, this need not be costly but it must have transparency and thorough documentation among its key aspects.

Much of the software and equipment needed, as well as training, is readily available.

Rolling your own DNSSEC deployment might be appropriate to high security domain names where financial, legal, patient, or other critical information is regularly exchanged. However, for the vast majority of Registrants outsourcing the generation, use, and rollover of DNSSEC keys and domain signing will be the only reasonable option.

Here various reputable options exist including some with estimates as low as 2USD/year [VRSN DNSSEC] or as part of packages [GoDaddy]. DNSSEC signing services may also be provided by the DNS and Web hosting providers currently being used by the Registrant. In each case, the Registrant should check the suitability of any public documents describing the signing services for linking to its own site since its own reputation will depend on them. This would be particularly important if legal or reputational issues rely on the integrity of services provided via the Registrant's Web site.

Similarly, the ability to seamlessly move DNSSEC operations from one operator to another is critical to protect against operator system or reputational failure. This is often an afterthought but it should not be [DNSSEC Koch].

Finally, Registrants can differentiate their Web site and other services from competition by promoting the security afforded by DNSSEC, whether home grown or riding on the reputation of the outsourced DNSSEC provider.

4.4 For Registrars

As the interface between Registrant and Registries, the Registrar plays a pivotal role in the chain of trust by:

- Ensuring the accuracy of Registrant contact and technical data.
- Protecting the integrity of Registrant data.
- Providing secure, authenticated paths for communication to Registrant and Registry.
- And supporting the propagation of DNSSEC parameters (e.g., DS records) from Registrant to Registry

a conscientious Registrar can set the level of trust in DNSSEC and associated applications while accelerating DNSSEC deployment.

The direct relationship between Registrars and Registrants also places them in a unique trusted position of giving Registrars the opportunity to offer a wide range of services from traditional DNS, Web, and email hosting to DNSSEC key management/signing, SSL CA services and enterprise SMIME PKI management.

As the basis for most of the practices used to build trust in DNSSEC deployment are the same as those for CAs, there are cost savings in the form of shared facilities, personnel and third party audit requirements.

Finally, by promoting DNSSEC and its associated applications, there is an opportunity for the Registrar to build loyalty programs and to offer differentiated services within its product line as well as with respect to its competitors.

4.5 For DNS Operators (Registries, Registrants and Registrars)

Whether DNSSEC operations are carried out by the Registry, Registrant, Registrar or by a third party DNS operator we believe the shortest path to deploying a trustworthy operation is to build on practices that have been honed over the past few decades by CAs. This has the advantage of not only capturing the best physical, access, logical, and crypto (engineering) practices but also allows bootstrapping many of the audit and legal practices used in the CA industry.

Based on our experience in developing practices and procedures for deploying DNSSEC at the root and DNSSEC deployment discussions with large Registries, the following key concepts make up a trustworthy deployment:

Transparency Often assumed but tedious to implement, transparent operations is the key to gaining the trust of your relying parties or public.

One of the first steps towards transparent operations is to set clear expectations and predictability by publishing a practices statement describing how your operations are implemented and contingency plans.

For DNSSEC we borrow directly from the established framework that the CA industry has had in place for creating Certificate Practice Statements (CPS). This framework was developed in cooperation with international accounting organizations which perform audits and provide certifications for CAs and related IT operations.

For DNSSEC this is called a DNSSEC Practices Statement (DPS) and specific frameworks for the same have been developed in the IETF [Fredrik].

The development of a DPS serves many purposes. It not only provides an opportunity to set reasonable expectations (e.g. response time, physical security,

response to incidents and disaster recovery) but also helps limit liability. Most importantly it forces the DNS operator to decide the level of risks it is willing to accept which will be a primary factor in determining cost. For example: it might be reasonable to forgo the cost of dedicated armed guards protecting your private keys if you have a well documented approach (that is also outlined in the DPS) for detecting and recovering from the unlikely event of compromise.

For the relying party, the DPS allows them to evaluate their own environment and their associated threats and vulnerabilities to determine the level of trust they may assign to DNSSEC in the given domain and the level of risk they are willing to accept.

Finally, as has been demonstrated in business [JNJ tylenol] and more recently in DNSSEC deployments [UK, FR], regular communication with the public via established channels (e.g., Web site), even if to describe a problem, are critical to building trust. The publication of incident reports describing a problem and the corresponding response [UK, FR] have not only garnered praise from other operators but has raised the bar by sharing lessons learned and increasing transparency expectations.

Now that we have said what we will do with the DPS, we need to prove that we did what we said.

Continuing along the same CA track we can provide this proof combining multiple elements. One is audit. This may be performed by a certifying third party (e.g. SysTrust, WebTrust certifications) or even internally depending on your administrative structure. Such audits can be expensive but can provide comfort to a wider range of industries that may not have a sufficient understanding of DNS operations.

Another element borrowed from the CA world is the key ceremony. A key ceremony is a recorded (and sometimes broadcast) event where those responsible for key generation and use follow a script with witnesses to ensure documented procedures are being followed. Such an event also provides the opportunity to involve those outside of normal DNS operations and therefore help broaden trust.

Security Securing any operation can become an impossibly expensive task if limits are not set based on acceptable levels of risk. Therefore, before embarking on deployment, a DNS operator should do a risk assessment based on the level of service they will be providing.

CAs typically break security into physical, logical, and cryptographic elements. Each one of these seek to protect content and key material from theft, loss, modification, and compromise.

Physical security is usually described in terms of concentric tiers with access to lower tiers required before gaining access to higher tiers. Progressively more restrictive physical access controls to each tier are applied. This could be, for example, tier 1 - a data center requiring authorized personnel to sign-in at a guard desk; tier 2 smart card access on to the data center floor through a mantrap; tier 3 a cage or rack area only accessible by DNS operator personnel; tier 4 a safe whose combination is only known by limited DNS operator personnel

authorized to access key storage devices. To deter collusion, access to the different tiers may be split across different personnel.

Although recovery procedures may be in place to deal with loss or compromise, an undetected compromise could lead to much greater damage due to its duration. A common approach to address this is to make use of motion detectors and video facilities (that may be part of the data center) and to rely on notifications and logs kept on the output of these systems. These logs along with entry and exit logs become part of any audit material.

Finally, the use of inexpensive tamper evident packaging to protect key material and associated devices goes a long way to proving that critical components have not been unknowingly compromised.

Logical security in the form of passwords and PIN codes are used to protect access to sensitive components. This includes off-net as well as off-line systems that must rely on configuration access to firewalls. Logs for such access would also fall under the category of audit material.

Logical security may also be used to further limit possible collusion. In the tier example above, activating the key storage device in tier 4 may require a PIN controlled by yet another person. This separation of roles is a key concept borrowed from CA operations and visible in most CA certificate practice statements.

Cryptographic security is central to CAs and DNSSEC operation. It includes ensuring that suitable algorithms and parameters are chosen and are implemented correctly; random number sources are trusted and have sufficient entropy; and keys are securely backed up and maintained.

Although this can be implemented in off the shelf software, the assurances certification brings has CAs generally using certified specialized hardware in the form of Hardware Security Modules (HSM) to implement key generation, use and maintenance.

Certification usually comes in the form of the US/Canadian based FIPS 140 standards [FIPS] although other national standards exist. These devices vary widely in features, level of protection (including erasure on tamper attempt), and cost. In some cases instead of the 20000USD high speed networked HSM, a 5USD smartcard validated to FIPS 140-2 level 3 might serve as an HSM for a domain name with very few entries.

Hence, modeling DNSSEC security on CA security methods need not cost much more than existing DNS operations in a typical data center. However, increased documentation, separation of roles requirements and greater involvement of staff to conduct key ceremonies will indirectly add to costs.

For Registrars, added requirements for secure exchange of information between Registries such as NS and DS records (as defined by the Registries) and authenticated secure auditable mechanisms between Registrants are necessary to fortify the trust in these links.

Availability The final key concept is service availability. Although ensuring the availability of DNS services is nothing new (e.g. with backup sites), with

DNSSEC and its dependence on signatures and absolute time, failures have shown that operations need to improve.

Providing this increased level of service is further made difficult with DNSSECs added key management complexity.

Monitoring DNSSEC operations to provide early warning notifications of eminent signature expirations has helped avoid some failures.

A balanced application of automation to key management reduces the possibility of signature expiry and administrative burden. Some Registries have done this by pre-generating signature and key material so as to allow automated processes to take over for extended periods of time.

Experience has shown that the complexities associated with key management that cannot be handled with automation can be tamed with documented procedures, checklists and sufficient coverage by personnel.

Overview Although these principles are not foreign concepts to most IT centric organizations, the implementation of the various controls necessary to adhere to them often are. This is understandable given the difference in cultures between CAs (and some of the industries that rely on them) and Internet engineering departments.

Controls consist of documented and published processes and procedures, extensive logging, physical intrusion detection (motion and video), key ceremonies, separation of duties through multi-person access control physical as well as logical, specialized cryptographic hardware to protect keying material, and audit.

Applying these basic but sometimes new practices to DNSSEC deployment brings the trusted framework established for the CA environment to DNSSEC and along with it the hope that it will fulfill the goal of a global PKI/trusted platform for innovative security solutions for the Internet.

5 Summary

With awareness building, setting reasonable expectations, and building on decades of CA practices we believe DNSSEC can be cost effectively supported by all entities in the DNS ecosystem thus creating an infrastructure that critical applications can rely on with opportunities that drive a race to the top benefiting all.

6 Footnotes

[ICANN root] - DNSSEC was deployed on the root on 15 July 2010 after two key ceremonies with the participation and presence of 21 Trusted Community Representatives from around the world. http://dns.icann.org/ksk/ds19036/

[VCandDK] - More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and repurposed in a number of different ways. .. Vint Cerf 16 June 2010

root key ceremony http://www.youtube.com/watch?v=b9j-sfP9GUU https://freedom-to-tinker.com/tags/security?page=2

"DNSSEC is the key to fixing the persistent authentication problems plaguing real-world, cross-organizational business for years, Dan Kaminsky 2009 http://www.darkreading.com/security/vulnerabilities/214501924/kaminsky-calls-for-dnssec-adoption.html

[Schlyter Cert] - DNS as X.509 PKIX Certificate Storage http://tools.ietf.org/html/draft-schlyter-pkix-dns

[IPSEC] - A Method for Storing IPsec Keying Material in DNS http://www.faqs.org/rfcs/rfc4025.html

[DKIM] - Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys) http://www.ietf.org/rfc/rfc4870.txt

[SSL obs] EFF SSL Observatory http://www.eff.org/observatory https://www.eff.org/files/DefconSSLiv 1482 CAs, 4M valid SSL sites, 200M websites

[comodo] Potentially Hundreds of Bogus Digital Certificates Issued https://infosecisland.com/blogview/ Potentially-Hundreds-of-Bogus-Digital-Certificates-Issued.html

Comodo http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/

Comodo compromise demonstrates need for DNSSec migration http://www.digitalsociety.org/2011/03/c compromise-demonstrates-need-for-dnssec-migration/

[DV SSL] Note: a popular mechanism used by many CAs to validate the identity of a domain name holder for Domain Validated (DV) certificates relies on the unsecured DNS as part of email exchanges.

[DANE SSL] Using Secure DNS to Associate Certificates with Domain Names For TLS http://tools.ietf.org/html/draft-ietf-dane-protocol

[DANK BH] Introducing the Domain Key Infrastructure http://www.slideshare.net/dakami/domain-key-infrastructure-from-black-hat-usa

[CHROME] DNSSEC authenticated HTTPS in Chrome http://www.imperialviolet.org/2011/06/16/dns

[DANE SMIME] Using Secure DNS to Associate Certificates with Domain Names For S/MIME http://tools.ietf.org/id/draft-hoffman-dane-smime

[ccnso survey] DNSSEC Survey Report of ccTLDs http://ccnso.icann.org/surveys/dnssec-survey-report-2009.pdf

[ccTLD PCH] Free DNSSEC signing service http://www.aptld.org/APTLDworkshopNoumea/DNSSEC

[pingdom] Internet 2010 in numbers http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/

[Comcast] DNSSEC Rollout by large ISP (18M Internet customers) http://www.dnssec.comcast.net/

[VRSN DNSSEC] VeriSign's DNSSEC signing service http://svsf40.icann.org/meetings/siliconvalley201 verisign-16mar11-en.pdf

[GoDaddy] Premium DNS 2.99USD/mo http://www.godaddy.com/domains/dns-hosting.aspx

Enabling DNSSEC in Your Premium DNS Account http://help.godaddy.com/article/6420?locale=en

[DNSSEC Koch] Changing DNS Operators for DNSSEC signed Zones http://tools.ietf.org/html/draft-koch-dnsop-dnssec-operator-change

[Fredrik] DNSSEC Policy and Practice Statement Framework http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework

[JNJ tylenol] Tylenol Crisis, 1982 http://iml.jou.ufl.edu/projects/fall02/susi/tylenol.htm

[UK, FR] Nominet (.UK Registry) Incident Report http://blog.nominet.org.uk/tech/wp-content/uploads/2010/09/dnssec-incident-report.pdf

AFNIC (.FR Registry) issues incident report on DNSSEC https://www.dnssec-deployment.org/index.php/2011/02/afnic-issues-incident-report-on-dnssec/

[FIPS] http://en.wikipedia.org/wiki/FIPS_140

[WebTrust] Certification required by some OS vendors to include a CA root key http://www.webtrust.org/ http://www.webtrust.org/principles-and-criteria/item27818.pdf

[SysTrust] SysTrust is what has been used for DNSSEC audit thus far though it is certainly not required. Same links as WebTrust. DNSSEC Root SysTrust Certification https://www.iana.org/dnssec/systrust

[SE DPS] .SE DPS http://www.iis.se/dl/DPS-PA9-ENG.pdf

[Root DPS] Root DPS https://www.iana.org/dnssec/icann-dps.txt

7 Acknowledgements

The author would like to thank Fredrik Ljunggren, Jakob Schlyter, Tomofumi Okubo, and Roy Arends as experts in their respective fields for their time and patience in enlightening the author.

8 Biography

Dr. Richard Lamb Rick has over 25 years of engineering, business, and policy experience in the Internet arena. Currently responsible for DNSSEC efforts at ICANN, Rick was the technical and policy architect for ICANN's root DNSSEC deployment. Prior to this he was director of global IT policy at US Department of State where he worked to bridge technology and policy. He has founded a number of computer networking startups the last acquired by Microsoft. Rick received his doctorate from MIT in 1987.