Good practices guide for deploying DNSSEC

enisa
European Network and Information Security Agency

About ENISA: *The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors. Internet: http://www.enisa.europa.eu/*

Contact details:

This report has been edited by: Panagiotis Saragiotis, Panagiotis.Saragiotis@enisa.europa.eu

Acknowledgements:

We would like to thank the following members of the ENISA's expert group on DNS resilience for their input and advice:

- Anne-Marie Eklund Lowinder (.SE)
- Dimitris Zacharopoulos (AUTH-NOC)
- Fredrik Ljunggren (Kirei)
- Lutz Donnerhacke (IKS-JENA)
- Olaf Kolkman (NLnet Labs)
- Patrik Faltstrom (Cisco Systems)
- Patrik Wallström (.SE)

Table of Contents

Good practices guide for deploying DNSSEC

The Domain Name System (DNS) is the protocol and worldwide system that supports communication networks by associating digital identifiers to Internet Protocol addresses and services[1]. While DNS is used in almost every interaction with the networks, its design was focused on data availability and did not address any resilience or security issues.

The European Network and Information Security Agency (ENISA) is executing a Multiannual Thematic Programme (MTP1) with the ultimate objective to collectively evaluate and improve the resiliency of public eCommunications[2] in the EU. As part of this programme, innovative technologies that had the potential to increase the resilience of such communications were investigated[3]. DNS Security Extensions (DNSSEC) has been identified as a technology that could improve the trustworthiness and quality of the DNS. It is complementary to other technologies such as Secure Sockets Layer that secure the delivery of content by increasing the security of online services.

DNSSEC addresses the critical security shortcomings of DNS by defining a process whereby a suitably configured resolver can verify the authenticity and integrity of query results from a signed zone. DNSSEC uses public key cryptography and digital signatures to enable a security-aware validating resolver to: (i) authenticate that the data received could only have originated from the requested zone, (ii) verify the integrity of the data, ie, that the data has not been modified in transit, and (iii) verify that, should a negative response (NXDOMAIN) be received to a query, the target record does not exist (denial of existence). However, it should be noted that DNSSEC does not offer confidentiality by means of encryption.

Deploying DNSSEC requires a number of security details and procedures to be defined and followed with specific requirements as to timing. This guide addresses these issues from the point of view of information security managers responsible for defining a policy and procedures to secure the DNS services of a company or an organisation, and from the point of view of competent authorities defining or regulating requirements for deployment.

The cases elaborated are:

---

[1] *Protecting the Domain Name System,* ENISA Quarterly Review, Vol. 4, No. 4, Oct-Dec 2008
http://www.enisa.europa.eu/publications/eqr/issues/eqr-q4-2008-vol.-4-no.-4

[2] http://www.enisa.europa.eu/act/res

[3] http://www.enisa.europa.eu/act/it/library/deliverables/stock-tech-res
http://www.enisa.europa.eu/act/it/library/deliverables/res-feat

- signing of a domain's zone;
- providing validating recursive resolver services;
- writing a DNSSEC practices statement;
- selecting products or outsourcing services.

Scope of this document

A company or an organisation that holds a domain name would want to deploy DNSSEC in its authoritative name-servers by signing the zone. Offering DNSSEC signed zones ensures that DNSSEC enabled resolvers will be able to verify replies received for the domain, securing the lookup process and subsequently having 'clients' connecting to the right source for services.

On the opposite side of the lookup process, a company or an organisation would want to deploy DNSSEC validation on its recursive resolver. Such deployment will ensure that the 'users' of the network will be offered validated replies for the lookups they request and will be subsequently connecting to the right source for services. However, the validation will only occur on domains that have deployed DNSSEC and a chain of trust originating from the resolver's trust anchors to that domain can be constructed.

This document lists the considerations that have to be made and provides recommendations for the security details and procedures to be defined and followed with specific timing requirements in order to deploy DNSSEC:

- by domain holders, signing their domain zones;
- in validating recursive resolvers.

These considerations have to be addressed when specifications are compiled:

- to deploy DNSSEC using internal resources;
- for buying a DNSSEC enabled commercial-of-the-shelf (COTS) DNS product;
- to outsource all or part of the DNS service and sign a service level agreement (SLA).

The technical details required to deploy DNSSEC can be found in the documents (RFC 4033, *DNS Security Introduction and Requirements*), (RFC 4034, *Resource Records for the DNS Security Extensions)*, (RFC 4035, *Protocol Modifications for the DNS Security Extensions*), and (Internet-Draft, *DNSSEC Operational Practices, Version 2*), and several others included in the Reference section. In addition, current best practices in operating DNS services are applicable but are not included in this document.

All of the recommendations given come from referenced technical documents and the current experience of ENISA's expert group. These recommendations are applicable for the near future.

This document assumes that the reader is familiar with the general concepts of DNS, DNSSEC and Public Key Infrastructure (PKI).

DNSSEC practices statement

Deploying DNSSEC will introduce procedures such as key management that will be either automatic or manual and will have to be repeated at specific time intervals. Additionally, trusted roles will be introduced which will be given specific tasks to perform and defined responsibilities. These roles must be assigned to individuals. All the procedures, the tasks, and their assignment should be specified and documented in a practices statement.

Most of the considerations that are discussed in this document should be included in the practices statement. Additional topics that could be covered include personnel controls, technical controls, etc. An extensive list of contents for a practices document is presented in the (Internet-Draft, *DNSSEC Signing Policy & Practice Statement Framework*). However, this Internet draft addresses the practices statements that should be made by a registry to provide parties relying on them with the means to evaluate the trust and strength of the security chain. As the goal of this practices documentation differs, a lot of provisions might be filled with 'no stipulation'.

If a company or organisation is using auditing services, the DNSSEC practices statement should be provided to the auditors so they can certify compliance with the defined procedures.

While a practices statement applies only to a single domain holder, a regulatory authority might define requirements in a signing policy for DNSSEC operations for one or more top level domains (TLD). The signing policy would be a broad statement of the general requirements for the domain holders under the TLD.

Signing your zone

Before the deployment of DNSSEC, the management of the DNS was something that could be handled on demand. The data entered in a domain zone could stay there without needing to be updated unless a change was required. When a zone is signed with DNSSEC, the signatures and the keys have a validity period which requires that a procedure is put in place for the signatures to be updated in a timely manner (Internet- Draft, DNSSEC Key Timing Considerations).

'Relative timing: before DNSSEC time was relative, now it is absolute.'

Many zones exist in the DNS that include mistakes in their definitions. However, these zones seem to work due to assumptions in the systems and the flexibility allowed by existing resolver implementations. Deploying DNSSEC enhances the focus of an organisation to the DNS and the domain

zones. The zones should be tested for correctness using available tools (IIS) enhancing the quality of the DNS.

Value of a signed zone

Domain holders might use DNSSEC as a differentiator that offers a competitive advantage over other domain holders offering competing services. By providing signed zones the odds that your domain records are successfully modified by an unauthorized party is reduced; this may prevent losses in terms of customers or reputation. Other than that, there is no expected return from signing a domain zone.

The legal value of a signed DNS record and its possible implications should be considered. The domain holder of a signed zone can prove that he used all available technology to ensure that lookups to that zone were protected.

Designing a signing system

The first consideration to be made when designing the signing system is its integration into the existing DNS architecture and infrastructure. In addition, the changes the system will bring into the existing procedures of DNS management will have to be considered.

The architectures of most existing DNS implementations have an internal repository for the zone data and a delivery mechanism to the external authoritative name-servers. The delivery protocol is the DNS protocol itself through an exchange of NOTIFY (RFC 1996, *A Mechanism for Prompt Notification of Zone Changes* (DNS NOTIFY)) and AXFR (RFC 1034, *Domain Names - Concepts and Facilities*) possibly in combination with IXFR (RFC 1995, *Incremental Zone Transfer in DNS*) messages. Alternative ways of transferring for the zones can be used.

The signing system would ideally be placed in between these two components, in the internal side of the network, so it would receive data from the repository and deliver signed data to the external authoritative servers (Figure 1).

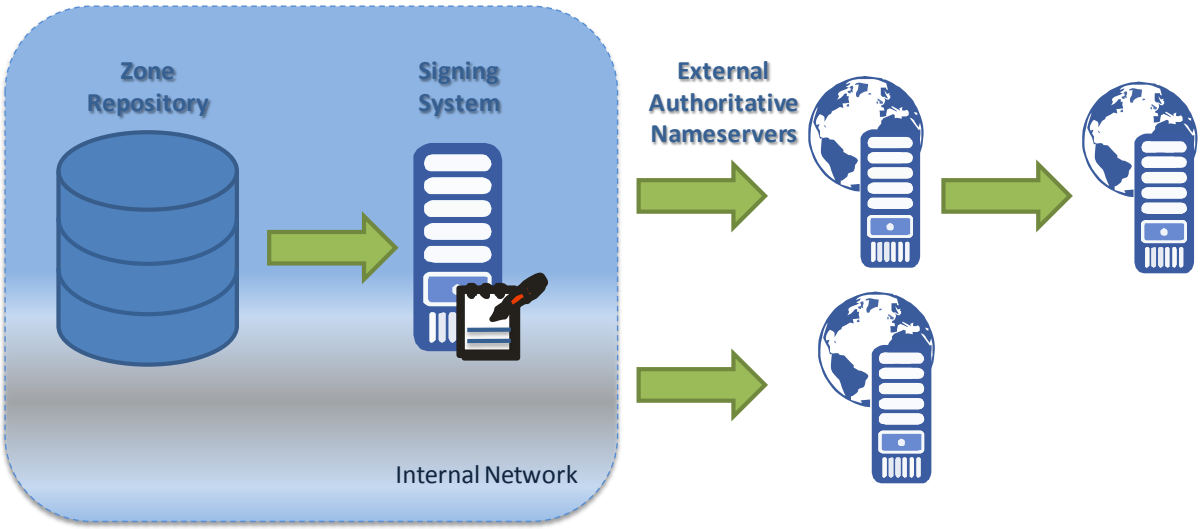

Figure 1: Signing system architecture

Issues regarding the specifications of the signing system need to be considered. In particular, the configurability of the system, the automation process, key management and security, and the performance of the system have to be examined. In addition, the number of supported zones should be considered.

The parameters of the signing system should be configurable. Support must be provided for several signing algorithms including RSA/SHA-1 and DSA with variable key lengths ranging from 1024 bits to 4096 bits. RSA/SHA-256 should be supported (RFC 5702, *Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC*) or provided as a future upgrade. Depending on the view of the domain holder on the possibility to enumerate the zone content the use of NSEC3 (RFC 5155, *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*) should be considered. Its parameters must be configurable. The NSEC3 OPT out feature should only be applied over delegation points.

In addition, the validity period of the signatures and the keys must be configurable. The handling of the start of authority record (SOA) must be configurable or match the requirements of the system architecture. All those parameters must be configurable per zone.

As a general principal, all functions of the system should operate fully automatically. Specifically, the signing and resigning of the zone should be automatic and the key generation procedure must be able to be automatic, but be configurable. Manual signing and resigning should be possible at all times. The operators of the system should be notified when manual actions need to be performed.

A side effect of the time relevance is the changes that must provisioned in the backup procedures. A backup of the signed zone at a given time in the past may not be valid when it is restored. The DNS

architecture should take this assumption into account. The signing system must not release, for delivery to the authoritative name–servers, a signed zone unless its validity has been checked specifically when such zone has been retrieved from a backup.

A means for creating a secure backup of the keys used by the system must be provided, together with the option for key generation in a separate environment. Depending on the security requirements of the domain holder, a hardware security module (HSM) could be required for the signing system. In addition, requirements might be set to conform to the specified Security Requirements for Cryptographic Modules, Federal Information Processing Standards 140 (FIPS) level[4]. The random number generator for the system should pass the NIST SP 800-22rev1[5] test.

It might be required that the signing system uses a common criteria for Information technology security evaluation (CC) assurance level (EAL). The protection profiles (PP) that can be used for the target of evaluation (ToE) are CMCKG-PP for key generation and CMCSO-PP for signing operations.

Detailed logging of the operations must be performed. Additionally, it should be considered should an automated auditing procedure be present in the signing system. The auditing procedure will check the validity of the signed zone before it is allowed to be delivered to the external authoritative name-servers. The combination of outputs from the logging and the auditor must provide sufficient reliable evidence of the continuous security, accuracy and availability of the service.

Signing in a test environment

After the implementation of the signing system, the domain holder is advised to test the complete system in a test environment before releasing it to the external world. All the defined procedures must be tested during this period. For the purpose of accelerating the testing, the lifetime of the signatures and the lifetime of the keys could be shortened significantly. However, the constraints of the (Internet-Draft, DNSSEC Key Timing Considerations) must be honoured.

Following the initial testing phase, the domain holder could make the DNSSEC enabled zones available to the internal recursive resolvers and use DNSSEC validation for internal resolution. This could also mean that the signed zones are distributed to the external authoritative name-servers but the trust

[4] *Security Requirements for Cryptographic Modules*
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*
http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf

anchor is not passed to the parent zone or any repository. Taking this gradual approach would ensure the extensive testing of the system while limiting the possibility of service disruptions.

Checking the DNS servers

It must be verified that the external authoritative name-servers that are operating as masters or slaves are supporting DNSSEC and the deployed extensions. These servers must include all name-servers with an NS record included in the signed zone. If one of the name-servers does not implement the DNSSEC protocol, domain validation will fail causing loss of service.

The delivery mechanism of the signed zones to the external authoritative name-servers has to be considered. DNSSEC is not applicable in securing the zone transfers. However, the Transaction SIGnature (TSIG) protocol (RFC 2845, *Secret Key Transaction Authentication for DNS (TSIG)*) provides a cryptographically secure means of identifying each endpoint of a connection as being allowed to make a zone update. TSIG should be used to secure zone delivery to the external name-servers. If it is used it must be supported by the name-servers..

Provisions should be made for the restoration of a backup. Signed zones should be freshly fetched from the signer and should not be restored from backup if any of the signatures in the zone are expired, or close to expiration. Using invalid zones will mark the zones as ‘bogus’ in caches and make domains unreachable.

A list of the versions of the most commonly used name-servers, which support DNSSEC and specific features, is shown in ANNEX 2.

Key generation and management

The keys that are used in a signed zone are generally separated into two categories: *Zone signing keys* (ZSKs) which are used to sign the records of a zone, and *key signing keys* (KSKs) which are used to sign the key records in a zone.

Key signing keys are used to build the trust hierarchy and should have a longer lifetime than ZSKs. Also, KSKs can be strengthened without significant impact on the size of the zone and the cost to validate the signatures. The procedures used to generate and manage those keys, the algorithms used, and the size and the lifetime of the keys have to be considered.

Careful generation of all keys is a sometimes overlooked, but absolutely essential, element in any cryptographically secure system. Keys with a long life time are particularly sensitive as no revocation mechanism is available and they will represent a more valuable target and be subject to attack for a longer time than short-period keys. The keys could be stored in a software or hardware token that will be protected by a PIN.

The lifetime of a key is a function of the lifetime of the records in a zone and the key timing considerations for DNSSEC. The length of the key is a function of the algorithm used and the lifetime of the key. It is recommended that RSA/SHA-1 be used but be replaced by RSA/SHA-256 when it is broadly available. On the assumptions that the requirements of the domain holder accommodate a lifetime for the records of 1 day and that the RSA/SHA-1 algorithm is used, it is recommended (SPARTA) that the KSK length used is 1280 bits with a maximum lifetime of 4 years and the ZSK length used is 1024 bits with a maximum lifetime of 1 year.

The private key portions of the KSK and ZSK can be used in different zones. If the domain holder uses multiple zones, it should consider following this approach. In its consideration, it should take into account that the security of the keys is not compromised when they are used in different zones. However, using the same keys in a large number of zones makes the keys a larger target for attack and the compromise of a key will have a bigger impact. Moreover, the token used to store the keys may impose a constraint on the number of keys, if a large number of zones are present and a large number of keys are required.

Physical security

It is recommended that long-term key generation occurs off-line in a system isolated from the network via an air gap or, at a minimum, high-level secure hardware.

Site location and construction, physical access to the site and environmental control of the site must follow the same rules that the domain holder uses in securing its data and the services it provides.

Use of NSEC3

DNSSEC provides for authenticated denial of existence of a requested name in a zone. This is handled with NSEC records (RFC 4034, *Resource Records for the DNS Security Extensions*). However, an interested party, using trivial means, could obtain the full list of the names present in a zone through those records. Domain holders that do not want to disclose the content of their zones, should consider using the resource record NSEC3 (RFC 5155, *DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*), which similarly provides authenticated denial of existence but also provides measures against zone enumeration.

NSEC is simpler to implement and results in smaller packets when a negative answer is required. NSEC3 requires additional computation during zone signing, when responding to a NXDOMAIN query and when negative responses are validated by the recursive resolvers. It is recommended that domain holders with a small number of names in their domain zones and little or no non-disclosure requirements for these names or domain holders with only predictable names in their domain zones (such as www, ns, mail, etc) use NSEC.

Where NSEC3 is used, the following parameters are recommended (SPARTA); these are based on the assumptions made in the *Key generation and management* section of this report. One algorithm iteration should be used, with 64 bits cryptographic salt and a salt lifetime of two weeks (the same lifetime as the lifetime of the signatures). For large zones, re-salting may be challenging (especially if using IXFR for zone distribution), as the whole NSEC3-chain has to be replaced instantly.

Key rollovers

It is recommended that two KSKs and two ZSKs be present at all times in the ready state in a zone, while only one of them is used for signing. This is the minimum required for a smooth operation of the zone. The transition states for the key are presented in Figure 2.

The duration of the transition from one state to the next is a function of the lifetime of the records in a zone, the time required to deliver the zones to the external servers and clock jitter time (Internet-Draft, DNSSEC Key Timing Considerations).

It is recommended that the transition of a KSK from the published state to the ready state (introduction time) lasts for 45 days (RFC 5011, *Automated Updates of DNS Security (DNSSEC) Trust Anchors*). If the parent of the zone is signed, the recommended introduction time (SPARTA) is one week. The recommended period during which a KSK is retired before it is removed from the zone (retirement time) is four weeks. For the ZSK, the recommended introduction time is four days and the retirement time is two weeks.

Although the DNSSEC protocol does not make a distinction between ZSKs and KSKs and their rollovers, making this distinction is recommended as it provides a clear separation between the keys that can be rolled without external interaction (the ZSKs) and the keys that need external interaction (the KSKs).

All key rollovers should be planned and automatic. Planned rollovers occur to keys that are in the ready state. Unplanned rollovers occur when a key is lost or suspected to be compromised but another keys is present and in a ready state in the zone.

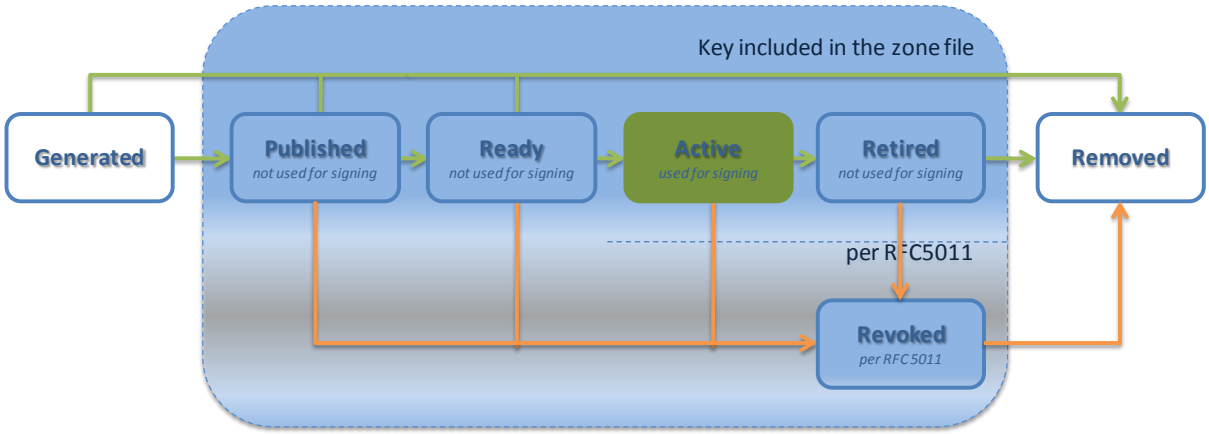

Figure 2: Key timing considerations

Emergency rollovers

Emergency key rollovers occur when any of the keys (KSK or ZSK) in a zone are lost or suspected to be compromised. These rollovers occur to a new key that was not present in the zone or was not in the ready state.

Emergency roll-overs should be conducted by introducing, by rolling, new keys in parallel to the compromised keys. This can be achieved either by publishing double trust anchors during the transition, or (if the private keys are not lost) by dual signing and updating the trust anchors in the parent zone or the repositories. In this way, the zone will not be invalidatable during emergency rollover, a state which is often unacceptable. The above process is also faster and is not less secure than transitioning though an unsigned zone.

Performance issues

Several issues have to be considered regarding the performance of DNSSEC deployment for domain holders. These issues include the performance of the signing system, the performance of the external authoritative name-servers, the bandwidth, and the time required to deliver the zone and the strain put on the validating recursive resolvers.

To improve the performance of the system for domain holders with a large number of names or zones, signatures that are not close to expiry should be reused and the signature expiration time should be scattered over time by introducing jitter time. This measure, when used in conjunction with incremental zone updates, will additionally allow for less bandwidth and time required to deliver the zones to the external authoritative name-servers.

Hardware acceleration can be used to fasten signing operations. When such devices are used, their support of the recommended key sizes should be considered.

The number of active keys in a zone and their key sizes, as well as the use of NSEC3, negatively influences the size of the zone, requiring more bandwidth and time to deliver the signed zone. Those parameters also influence the size of the replies the authoritative name-servers produce to queries coming from validating recursive resolvers. The anticipated increase in bandwidth is 50% (ENISA).

Generally the queries and responses use UDP packets as the transfer protocol. However, if network elements along the path, such as firewalls, do not support UDP (de)fragmentation[6] or drop DNS packets which they do not recognize (since DNSSEC has not been implemented on them), the query has to be repeated with a TCP connection. As a result, an increase in TCP connections is expected (Afilias) and should be monitored.

Publication of keys

When the parent of a zone is signed, delegation signer (DS) records (RFC 3658, *Delegation Signer (DS) Resource Record (RR)*) must be inserted at the zone cut (ie, a delegation point) for each of the KSK that are used to sign the zone or is planned to be used. These records indicate that the delegated zone is digitally signed. Zone owners that would expect the public part of their keys to be used as trust anchors should follow the provisions of *(RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors*). The DS record format will be the preferred way of distributing the TA in the future.

The repositories must be updated and the caches must expire before the key can enter into the active state. The retired keys must not be removed from a zone before they are removed from the repositories.

Parent zone

If the parent zone is signed, the trust anchors should only be published there. Support for (RFC 5011, *Automated Updates of DNS Security (DNSSEC) Trust Anchors*) should not be provided in this case.

The domain holder must update the parent zone (in most cases a top level domain registry) through its registrar. The procedure usually involves the use of the registrar's web interface, after the authentication of the domain holder. The registrar then updates the records in the registry. Depending

[6] Ethernet-based links that do not support fragmentation (often due to a firewall or similar device) can facilitate a maximum UDP size of 1500. 1492 bytes includes room for PPoE encapsulation. (SPARTA)

on the policy of the registry, these changes can be reflected in the parent zone immediately or at specific time intervals.

Trusted anchor repositories

A domain holder should consider the following options for publishing the zone's keys in trust anchor repositories (TARs): allowing TARs to harvest the keys from the zones themselves, or disallowing them from doing so. In order to make a decision, the domain holder should examine the policy and practices used by the repository. In ANNEX 1 the required information that should be presented in a DPS from a repository is listed and elaborated. The domain holder must decide whether to use the services of a repository based on its DPS. Disallowing TAR operators to harvest the keys of a zone cannot be performed automatically and involves the domain holder contacting those TAR operators.

DNSSEC Lookaside Validation (DLV) (RFC 5074, *DNSSEC Lookaside Validation (DLV)*) is a mechanism for publishing trust anchors, using the DNS protocol, outside the DNS delegation chain. It allows validating resolvers to validate DNSSEC-signed data from zones whose parents are not signed.

DLV is a specific type of TAR, and thus the same considerations apply for the utilisation of its services by a domain holder. However, DLV's clients (ie, validating recursive resolvers) are updated automatically in a timely and predictable way when a key is updated.

A trust anchor repository should only be used after verifying that the parent zone is not providing secure delegations. In this case it is also recommended contacting the parent zone and making them aware of your requirements.

Change of registrar

When changing a registrar, a domain holder whose parent zone is signed must require, from the new registrar, support to update the DS resource records in the registry. If the change of registrar happens as a result of changing the DNS provider, the considerations listed in the *Change of DNS provider* section must be made.

Change a zone from signed to unsigned

When changing a signed zone into an unsigned (and unsecured) zone, a domain holder must allow for a transition period. The delegation signer records in the parent zone or the trust anchors in the repositories must be removed and the caches must be allowed to expire before the signatures can be removed. It should be noted that the actual transition from signed to unsigned happens when the trust anchor is removed.

Change of domain holder (registrant)

When the domain holder changes, the delegation records in the registry remain the same. If the new holder does not have access to the private keys used in the zone, the migration strategies described in the *Change of DNS provider* section must be used.

Selecting a product

Based on a study conducted by (ENISA), most of the existing deployments of DNSSEC zone signing involve customised open-source solutions or signing solutions developed in-house. Early adaptors, before 2008, were obliged to invest significantly in in-house developments, which were afterwards released as open source. Those deploying at a later date benefit from these developments by using the the most recent open source solutions (at the moment this report is written several new Open Source products have been announced).

Several commercial-off-the-shelf (COTS) DNS products are currently available in the form of software products and appliances. These products include DNSSEC zone signing support and several DNS and IP address management features and capabilities. A domain holder, which is evaluating such products, should consider how these products integrate with the existing DNS architecture and the decisions made based on the considerations and the recommendations in this document.

Additionally, two important considerations affecting the operational expenditure (OPEX) and the trust the domain holder can put in the product have to be taken into account. The additional licence cost per zone, the support for the product and the auditability of the product should be considered.

Auditability is a central concept for any product whose results are relied upon. To provide assurance that the product has auditability, the product must provide proof that its results are reliable, and have features such that an independent, objective review of transactions processed, data stored, and output provided can identify sufficient reliable evidence of continuous security, accuracy, confidentiality, and availability of information.

.SE (The Internet Infrastructure Foundation) has, together with Certezza, produced a report (IIS (.SE) and Certezza) that shows the current state of administrative tools for DNSSEC. The report is a summary of the functionality of some leading DNSSEC management tools. The focus of the examination has been on COTS DNSSEC signing and key management functionality, Open Source products where not studied.

In addition, online repositories currently containing up to date information on available administrative tools for DNSSEC are:

- http://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources
- http://www.dnssec.net/software

Outsourcing

A domain holder that outsources the operation of the domain's zone to a DNS provider must check the DPS of the provider for the utilisation of the recommendations and considerations of this document that the holder endorsed. The DPS and any additional provisions must be included in a service level agreement that will be honoured be the provider. Moreover, the additional cost per zone charged by the DNS provider and affecting the OPEX should be considered. Finally the SLA should contain appropriate provisions that allow for timely and structured transfer of a secured zone to another DNS provider without the domain needing to go insecure (also see below).

Special consideration must be given in the use of the same keys for several zones handled by the same DNS operator. This makes the keys more valuable targets and the subject of attacks. This practice also makes it impossible for the provider to disclose the private keys of the zone for backup and contingency purposes or where the DNS provider changes.

DNS providers, in most cases, are also registrars. This dual role, in general, simplifies DNS operations, and does so specifically in the case of DNSSEC where updates of the parent zone are required repeatedly.

Change of DNS provider

A domain holder which wishes to change its DNS provider and has access to the private keys used in a zone can proceed without considering the procedures for the change. However, this is not the most usual case.

Two migration strategies are available when changing DNS provider without having access to the private keys in current use.

The first strategy is to transition the zone to unsigned, following the procedure in the section *Change a zone from signed to unsigned*, before leaving the original provider. This will make the zone unsecured. Then, change the provider and resign the zone with new keys and reinsert trust anchors.

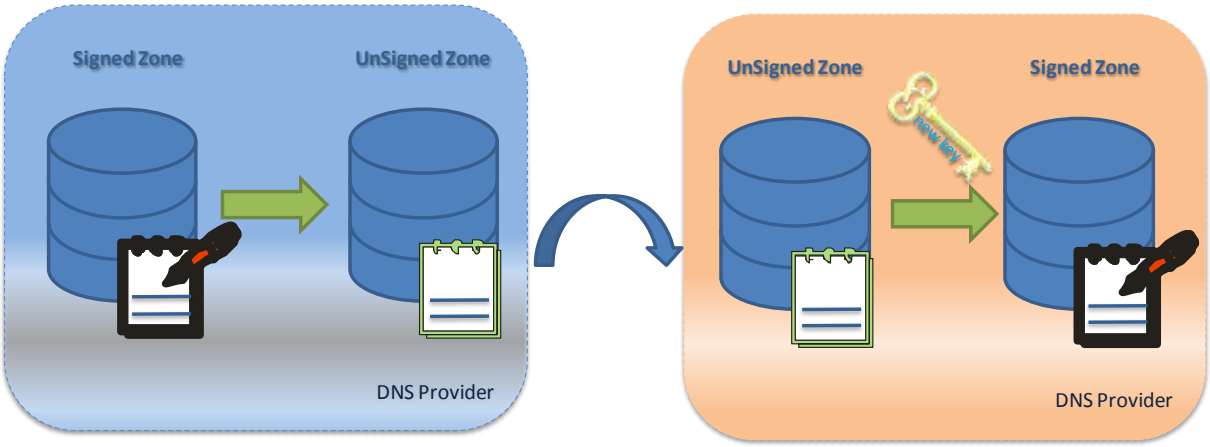

Figure 3: Change of DNS provider through unsigned zone transitioning

The second strategy involves the cooperation of the loosing DNS provider. The public parts of the new keys must be introduced in the zone, as they would have to be in a planned key rollover, and a second trust anchor should be introduced in the parent zone or the repositories. When the key transits in the ready state, the zone can move to the new DNS provider and be signed by the new key. The old key and the signatures created with it should stay in the zone for the duration of its transition from the retired state to the removed state.

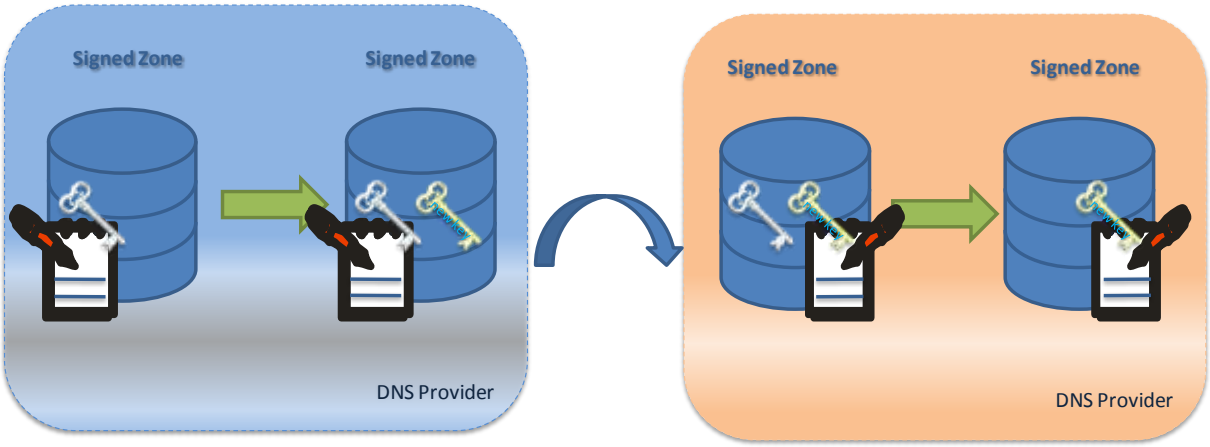

Figure 4: Change of DNS provider with prior introduction of new key

Validating DNS queries

Validating recursive resolvers are used by end systems that implement stub resolvers, to query the DNS hierarchy and provide name resolution (Figure 5). At the same time they provide validation of the DNSSEC signatures of records for which a trust path can be build from configured trust anchors.

Currently, the stub resolvers do not have to be aware of any trust anchors and do not have to be DNSSEC aware. When a validation error occurs and a zone is considered 'bogus', the stub resolver receives a DNS error. However, if the stub resolver is DNSSEC aware, the end user can be informed that the DNS validation has failed.

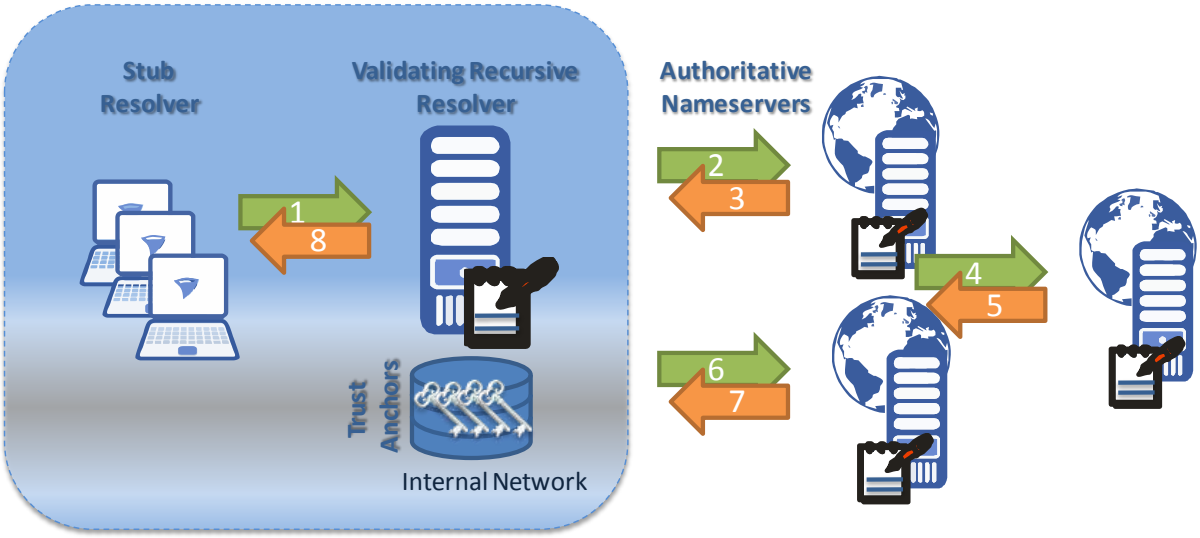

Figure 5: Validation steps

A company or an organisation would want to deploy DNSSEC to the recursive DNS resolvers that are used by their end systems. Providing a DNSSEC recursive resolver ensures that the replies received by authoritative name-servers are validated, securing the lookup process and subsequently having the internal end system connecting to the right source for services.

A list of the versions of the name-servers most commonly used as recursive resolvers that support DNSSEC and their specific features is presented in ANNEX 2. It should be expected that a validating recursive resolver will require more incoming bandwidth than a non-validating one, as the replies originating from the authoritative name-servers of a signed zone will be larger. It should also be expected that the processing capabilities of validating recursive resolver should be higher as they validate the cryptographic signatures.

The recursive resolver should provide auditability. However, the privacy concerns of the end-users should be addressed. Additionally, considerations concerning the configuration of trust anchors and the connectivity of the systems should be examined.

Several commercial-off-the-shelf (COTS) DNS products are available, in the form of software products and appliances that, among other capabilities, include DNSSEC recursive resolver support. A recursive resolver operator evaluating such a product should check, among other things, the considerations and the recommendations of this document.

Where the recursive resolver operation is being outsourced to a DNS provider, the practices followed by the provider must be checked on the basis of the recommendations and considerations in this document. The DPS and any additional provisions must be included in a service level agreement that will be honoured by the provider.

Configure trust anchors

Managing trust anchors is the only operational procedure imposed by the validating recursive resolver. When the DNS root zone is signed together with the majority of the TLDs, the only required external trust anchor would be that of the root zone. Until this happens, a recursive resolver operator should consider configuring and managing trust anchors, enabling (RFC 5011, *Automated Updates of DNS Security (DNSSEC) Trust Anchors*) and using a TAR. The (RFC 5011, *Automated Updates of DNS Security (DNSSEC) Trust Anchors*) can also be used to maintain the root trust anchors. The DPS of a TAR should be evaluated against the expectations of a recursive resolver operator. The required provisions of a TAR that should be included in a DPS are listed and elaborated in ANNEX 1.

In addition to any external trust anchors, trust anchors of the held and signed zones should be configured and managed. Providing local trust anchors for the held zones is a recommended practice.

The keys that can be used as trust anchors are the KSKs used in a zone. When trust anchors are manually configured, the keys validity period should be checked. When new keys are introduced they should also be added as trust anchors and their removal should also be followed by their removal from configured trust anchors. To achieve this operation, the publishing rules of the domain holder should be checked and followed.

The domain holder may publish the keys utilising different medium and formats, through websites, PGP signed, in newspapers, etc. When the keys in a zone are providing signalling *(*RFC 5011*, Automated Updates of DNS Security (DNSSEC) Trust Anchors*), the update of the keys, in planned and unplanned rollovers, can be performed automatically. Manual configuration of trust anchors should be discouraged.

Routers, firewalls and other network equipment

In general, the queries and responses in the DNS use UDP packets as transport protocol. The initial requirements for DNS messages over UDP were to have a data payload of 512 bytes or less. DNSSEC signatures are increasing the reply's size. The (RFC 3226, *DNSSEC and IPv6 A6 aware server/resolver message size requirements*) mandates the support of EDNS0 (Extension Mechanisms for DNS) for DNSSEC enabled servers. Such servers should support UDP messages of 4000 bytes before falling back to TCP connections which will have a negative impact on query latency and DNS server load.

It is recommended that the compatibility of the communications equipment in the configuration used is checked for the support of large UDP messages and TCP fallback. Most of the business routers can handle these requirements. However, customer premises equipment (CPE) routers and firewalls, targeting broadband consumers, can have a negative effect on a DNSSEC deployment (Core Competence & Nominet). While all of the tested devices could route DNSSEC queries addressed to validating recursive resolvers without size limitations, most of them imposed limitations when a validating recursive resolver was operating behind them.

Conclusions

Deploying DNSSEC requires a number of security details and procedures to be defined and followed with specific timing requirements. A number of decisions have to be made based on the considerations and requirements presented in this document. These decisions have to be documented in a DNSSEC policy and practices statement, which must be used for deployment, management and, in the case of outsourcing, to ensure a secure and successful deployment.

Deployment should balance the level of complexity with the security requirements they put forward and the risks of running an unsigned zone. The deployment can start in a small way by signing the zone using long expiration times on the signatures and not publishing trust anchors in the zone or repositories. In this way the risk of ending up with an invalidatable zone is mitigated and the risks related to a key's length and validity period can be handled by ad-hoc key rollovers.

Management of the system should be practiced in a test environment and then in the internal network until the required maturity level is reached to publish the key to the parent zone or repositories if the parent zone is not signed. Doing such a controlled rollout would result in incremental costs and benefits.

ANNEX 1: Contents of a TAR's policy and practices statement

This annex describes what a DNS operator should expect from a trusted anchor repository (TAR), how the DNSSEC public key material is transferred from its rightful holder to the repository and how the identity of the holder of a domain is ensured.

Such a TAR policy and practices statement could follow (RFC 3647, *Certificate Policy and Certification Practices Framework*) and the work performed in applying the same RFC on domain registries implementing DNSSEC (Internet-Draft, *DNSSEC Signing Policy & Practice Statement Framework*).

There are several examples of 'trusted repositories' such as TACAR (http://www.tacar.org/) and TI (http://www.trusted-introducer.nl/).

Note that the procedure for key acceptance/management should not necessarily be stronger than the procedure for changing the DNS records of a specific domain.

What is a TAR?

There has been a lot of discussion about the definition of a TAR and there are several definitions available. In this document, a *trusted anchor repository* is an entity that – similar to PKI – is governed by a policy practice statement and handles issues such as the:

- collection of DNSSEC keys from their rightful holders;
- publishing of DNSSEC keys;
- continuous validation of published keys;
- decommissioning and revocation of keys.

Which organizations can send keys to a specific TAR?

A TAR policy should state which organizations that run DNS+DNSSEC are allowed to become members of a particular TAR. Members are allowed to perform key management operations (list, de-list, etc) to the repository for their organization. For example, there could be a TAR for academic and research institutions, banks, government sites, etc. Of course, the scope of the TAR could be global, continent-wide, nationwide, etc.

Note that TARs should only collect keys from domains that do not have a signed parent domain.

Establishing procedures for key acceptance

This section describes the issues that should be considered by a TAR policy writer for establishing accreditation, registration, and/or validation procedures. These procedures eventually describe a

security model for DNSSEC key acceptance and management. This model should not necessarily be stronger than the procedure for changing the DNS records of a specific domain.

Registration process

A TAR entity should establish registration procedures for organizations (domain rightful holders) that would like their DNSSEC keys included in the trusted repository. The registration procedure is a secure entry point for the inclusion of a participant's key into the TAR. For the first time, it should follow the process of an initial DNS registration. Subsequent updates can be made electronically, by accredited administrators.

Accreditation process

A TAR entity should establish procedures for collecting keys from organizations. These procedures must ensure that keys are collected from official representatives of the organization. It is suggested that one or two DNS administrators may be accredited to perform key operations. PGP-key usage for data integrity and confidentiality is strongly recommended.

Key validation process

The TAR must have clear rules for key validation before any key is accepted and inserted into the trusted keys repository. In order to provide optimal security, it is strongly recommended that the crypto algorithms and key lengths must be periodically updated as technology improves. Currently, the DNSKEY format should be SHA1 or SHA256. The key format should be in either DNSKEY or DS presentation format. There is currently a broad consensus that the DS format is more appropriate for TARs.

Establishing procedures for key management

Trust keys can be managed with automatic operations that scale very well but there are some cases where manual operations apply as well, especially in cases where keys are compromised.

Automatic operations as described in RFC5011

RFC5011 describes specific ‘auto-procedures’ that can be used for:

1. key-rollovers
2. key revocations.

Manual operations in cases of key compromise or loss

In the – not so unlikely – event of a private key getting lost or in the case of a key being exposed, accredited persons from the zone-holder should be able to send 'authorized' requests via means other than DNS (using pgp, x509, etc) to remove keys from the TAR.

Procedures for modifying key-holder information

The policy should describe how the TAR verifies or confirms domain-specific changes (eg, changes in accredited staff, e-mails, postal address info, etc).

What are the obligations of a TAR?

'Keep alive' and integrity verification procedures

The policy should clearly state the specific key validation or verification procedures that are in place and the automatic measures taken when validation or verification fails.

'Keep alive' for registration and accreditation data

The TAR could establish a procedure to periodically check the validity of registration-accreditation information such as e-mail addresses, pgp keys for the registrants and their accredited staff. For example, a TAR could automatically send an e-mail every 6 or 12 months to the e-mail addresses of the registrants and the accredited staff, requesting them to access a specific page. Another example would be to have the registrants or accredited staff reply with a pgp or x509 signed e-mail to the TAR operators every 6 or 12 months.

Speed of operations

The TAR operators must state the minimum and maximum time it takes for specific tasks. These operations could be manual or automatic. Such a list might include the:

1. time for the registration/accreditation process after an application is received;
2. time for the key validation/verification process (between key reception and key publication);
3. time for the key revocation process.

Key-holder information disclosure or publication and restrictions

A TAR should state the information from the key-holders that is likely to be published (such as a list of participants in a specific TAR) or released in the case of a specific zone query (eg, contact details for somedomain.gr).

What are the obligations of the key-holders?

- *Domain change* (change of domain holder): the key-holder should notify the TAR and appropriate actions should take place. The TAR policy should state and describe these actions.
- *Change of accredited staff*: the person listed in the registration process as responsible should repeat the accreditation process.
- *Minimum security measures*: the policy should state the minimum security measures that key-holders should take in order to protect their DNS private keys.

Expected key distribution method

This section describes how the TAR distributes its collected keys to the DNS resolvers.

DLV operation

Large amounts of secure entry points (SEPs) cannot be maintained securely and efficiently by manual operation. The idea of DNSSEC Lookaside Validation is to use the DNSSEC secured DNS system itself as a scalable database.

Islands of trust are classes of signed zones connected by DS-DNSKEY chains, which miss a DS from the next higher parent zone. This missing DS record might be retrieved by securely looking up a DLV RR in the most appropriate lookaside zone. The DLV RRSet has the same RDATA content as the (missing) DS RRSet from the delegating parent zone. Multiple lookaside zones are permitted and subject to local resolver policy. Common approaches are: single match, use of the most specific match, and majority voting.

DLV registries can and do choose any validation and maintenance method as they like. So resolver operators need to check carefully if and which DLV they configure. For example, ISC as a cooperation-based registry is for operators of signed zones that like to be listed there. On the other hand, IKS, as a spidering registry, is for resolver operators that like to provide as much validation coverage as possible. Another common DLV scenario is to use an enterprise registry containing all the zones the enterprise operates or deals with.

Pgp signed tar.gz or zip file

The TAR should have a key published to the pgp key-servers. With this key, the TAR signs a file with a collection of keys (zipped) and publishes this file. It may choose to publish it over http or https (recommended). This file should be updated on a regular basis.

The DNS resolver administrators should download this file regularly, verify the pgp signature and then present the new keys to their DNS server.

Co-operation with other TARs

It is not uncommon for TARs to work together in order to extend their trust domain. For example, a national TAR that collects keys from academic institutions could merge with a similar TAR with a wider scope (continent-wide) but in the same sector (academic institutions). The policy could include a section that describes merging procedures with other TARs for future use.

Policy update procedures

Like every policy document, there should be a procedure for updating this document along with publication issues, version tracking, etc.

ANNEX 2: Support of DNSSEC on commonly used name-servers

Authoritative name servers

- BIND versions 9.6.0 and later support NSEC3.
- BIND Developmental Release 9.7.0b1 supports SHA-256.
- BIND Release 9.7.0 and later support for RFC 5011 automated trust anchor maintenance.
- NSD versions 3.1.0 and later support NSEC3 by default, NSD versions 3.0.0 and later support NSEC3 when turned on at compile time.
- NSD version 3.2.1 supports SHA-256.

Recursive Name Servers

- BIND versions 9.6.0 and later support NSEC3.
- BIND Developmental Release 9.7.0b1 supports SHA-256.
- BIND Developmental Release 9.7.0 supports for RFC 5011 automated trust anchor maintenance.
- Unbound versions 0.10 and later support NSEC3.
- Unbound versions 1.4.0 and later support SHA-256 by default, version 1.3.4 support SHA-256 when enabled at compile time.
- Unbound 1.4.0 also includes supports for RFC5011.
- Autotrust is a commandline tool to automatically update your DNSSEC trust anchors per RFC 5011. It is intended to run from a cron job and can run next to any validating resolver.

Reference

Afilias. “Deploying DNSSEC: Experiences From a Generic TLD Registry Operator.” <http://www.internetdagarna.se/wordpress/wp-content/uploads/JamesGalvin_Registry-Lessons.pdf>.

Core Competence & Nominet. “DNSSEC Impact on Broadband Routers and Firewalls.” <http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf>.

ENISA. “Study on the Costs of DNSSEC Deployment.” 2009. <http://www.enisa.europa.eu/act/res/technologies/tech/dnsseccosts>.

IIS (.SE) and Certezza. A Review of Administrative Tools for DNSSEC. <http://www.iis.se/docs/DNSSEC-Admin-tools-review-1.01.pdf>.

IIS. DNS Check. <http://dnscheck.iis.se/>.

“Internet- Draft, DNSSEC Key Timing Considerations.” <http://tools.ietf.org/html/draft-morris-dnsop-dnssec-key-timing-01>.

“Internet-Draft, DNSSEC Operational Practices, Version 2.” <http://tools.ietf.org/html/draft-ietf-dnsop-rfc4641bis-01>.

“Internet-Draft, DNSSEC Signing Policy & Practice Statement Framework.” <http://www.ietf.org/id/draft-ietf-dnsop-dnssec-dps-framework-00.txt>.

“RFC 1034, Domain Names - Concepts and Facilities.” <http://tools.ietf.org/html/rfc1034>.

“RFC 1995, Incremental Zone Transfer in DNS .” <http://tools.ietf.org/html/rfc1995>.

“RFC 1996, A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY).” <http://tools.ietf.org/html/rfc1996>.

“RFC 2845, Secret Key Transaction Authentication for DNS (TSIG).” <http://tools.ietf.org/html/rfc2845>.

“RFC 3226, DNSSEC and IPv6 A6 aware server/resolver message size requirements.” <http://tools.ietf.org/html/rfc3226>.

“RFC 3647, Certificate Policy and Certification Practices Framework.” <http://www.ietf.org/rfc/rfc3647.txt>.

“RFC 3658, Delegation Signer (DS) Resource Record (RR).” <http://tools.ietf.org/html/rfc3658>.

“RFC 4033, DNS Security Introduction and Requirements.” <http://tools.ietf.org/html/rfc4033>.

“RFC 4034, Resource Records for the DNS Security Extensions.” <http://www.ietf.org/rfc/rfc4034.txt>.

“RFC 4035, Protocol Modifications for the DNS Security Extensions.” <http://tools.ietf.org/html/rfc4034>.

“RFC 5011, Automated Updates of DNS Security (DNSSEC) Trust Anchors.” <http://www.ietf.org/rfc/rfc5011.txt>.

“RFC 5074, DNSSEC Lookaside Validation (DLV).” <http://tools.ietf.org/html/rfc5074>.

“RFC 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.” <http://tools.ietf.org/html/rfc5155>.

“RFC 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC.” <http://tools.ietf.org/html/rfc5702>.

SPARTA, Inc. and Shinkuro, Inc. “DNSSEC Operations: Setting the Parameters.” <http://www.dnssec-deployment.org/documents/SettingtheParameters.pdf >.