SERBIAN JOURNAL OF ELECTRICAL ENGINEERING
Vol. 13, No. 3, October 2016, 369-380

UDC: 004.738.5:342.51(497.11Niš) **DOI: 10.2298/SJEE1603369A**

Implementation of DNSSEC-Secured Name Servers for ni.rs Zone and Best Practices

Đorđe Antić[1], Mladen Veinović[1]

Abstract: As a backbone of all communications over the Internet, DNS (Domain Name System) is crucial for all entities that need to be visible and provide services outside their internal networks. Public administration is a prime example for various services that have to be provided to citizens. This manuscript presents one possible approach, implemented in the administration of the City of Niš, for improving the robustness and resilience of external domain space, as well as securing it with DNSSEC (DNS Security Extensions).

Keywords: DNS, DNSSEC, Security, Cryptography.

1 Introduction

Domain Name System (DNS) is a hierarchical decentralized system for converting domain or host names into equivalent IP addresses. It is crucial and indispensable for all services running on the Internet. It has been improved substantially since its invention, with security remaining an important issue. The most serious problems come from DNS client flooding (a DoS attack) [1] and cache poisoning, allowing insertion of fake data into DNS client resolver cache, which was released in 2008 [2].

Driven by a desire to enhance the security of the system, the Domain Name System Security Extensions (DNSSEC) were proposed. They represent a set of protocols utilizing public-key cryptography to create digital signatures of data in DNS [3]. Three distinct benefits for resolvers are achieved using this technology: origin authentication, data integrity and authenticated denial of existence. Digital signatures are part of the hierarchical architecture of DNS, building a chain of trust from the root zone down to all signed subdomains.

Administration of the city of Niš relies on DNS to provide different online services to citizens over the Internet. Name-to-address mapping, while not apparent to users, is a crucial process. Interruptions in the functioning of the system can make the services unavailable or can, through misuse, present fake or deceptive information to citizens, which can lead to potential legal

[1] Singidunum University, Danijelova 32, 11000 Belgrade, Serbia;
E-mails: djordje.antic@gmail.com; mveinovic@singidunum.ac.rs

repercussions or cause material damage. Therefore, a stable and safe DNS system is absolutely necessary.

2 Background and Objectives

2.1 About DNS

Domain Name System is a global and hierarchical database. Maintained on name servers, the system links canonical names (used as domain names) with various data (most notably IP addresses). As a whole, the system can be represented in a form of a tree with root zone on top (as in Fig. 1). The branches of the tree are called domains (everything under .com, .rs, .edu, etc.), while the individual nodes are called zones. Zones are parts of the system delegated to a single administrative authority. Several authoritative DNS servers for resolution of names must be present under each zone.

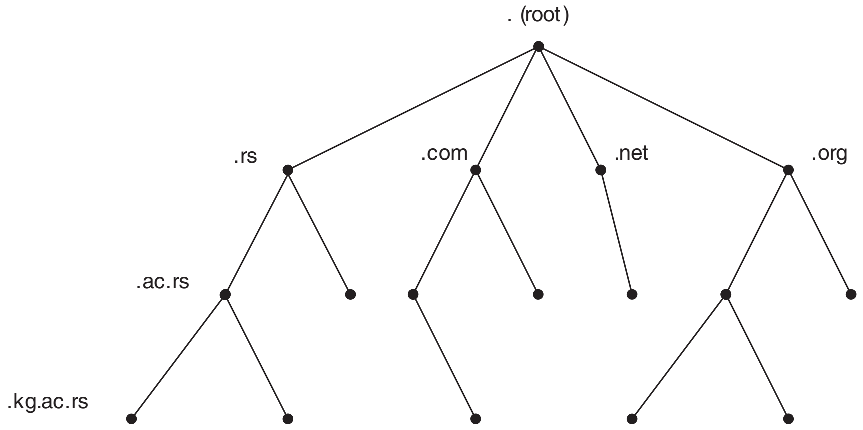

Fig. 1 – *DNS tree.*

2.2 Name resolution for ni.rs

Upon reviewing the network infrastructure of the public administration of the city of Niš, the conclusion was drawn that it should be upgraded.The assignment was divided into determining the current status, deficiencies and vulnerabilities, setting objectives and implementing the desired solutions.

Foremost, the current state of the name server infrastructure was thoroughly examined. It was found that the ni.rs zone was maintained on two hardware appliances (Networks Defender ND410), dating from 2007. Their DNS software was actually BIND 8, which was deprecated from the same year. The devices were not fully supported and were beyond the period of warranty, while one of them was permanently disconnected due to hardware problem. The other operational one struggled with intermittent software issues resulting in no responses for the queries sent (making ni.rs zone unreachable, as it was authoritative for that zone). The ni.rs zone was thus unreliable to reach. This issue was made even more complicated by the fact that ni.rs zone is the location of different online services provided by local administration. The conclusion could be made that the appliances had to be replaced and specific project goals were defined.

2.2 Objectives

1. Financial factor must be taken into account for any proposed solution. Cost-efficiency should be achieved and unnecessary compromises should be avoided.
2. Best industry practices should be implemented in any chosen solution. Name servers should be appropriately configured and maintained.
3. Special attention should be devoted to security issues. Implementation of DNSSEC is of crucial importance for achieving such goal.

3 Planning and Practice

Cost-efficiency was achieved by making use of the existing capacities on servers in city administration infrastructure, running VMware hypervisors. Thus, it was decided to create name servers as virtual machines.

Software chosen for such virtual servers was selected according to stability, security, system requirements and total cost of ownership. The operating system used was Linux. In order to provide diversity, two different Linux distributions were selected, namely CentOS and Ubuntu.

The actual DNS software was selected for its mainstream adoption in industry. The servers chosen have only authoritative functions and operate with high performances. Versions installed were the latest stable ones, supporting all major DNS functions, including zone transfers (full and incremental), dynamic updates, DNSSEC, response rate limiting, EDNS0 [4], NSEC3 [5] and NSID.

As can be seen in Fig. 2, the envisioned design was to place a hidden master server for preparation and validation of zone data. This server, after loading the prepared and validated data, sends a notification message to a machine configured to perform DNSSEC signing. Upon detecting the notification, it initiates the transfer of zone data from the hidden master server with encrypted mechanism (AXFR/IXFR). The transferred zone data is then signed using pre-generated cryptographic keys. The keys for signing are kept in a cryptographic store inside the software emulated HSM (Hardware Security Module). This concept is known as “bump-in-the-wire”, as it is positioned between a hidden preparation part and publicly available part of the system. After the signatures have been applied to the zone data, notification messages are sent to the public slave servers, informing them that new data is available. Slaves would then begin encrypted zone transfer from the signing machine and acquire zone data ready for public use.

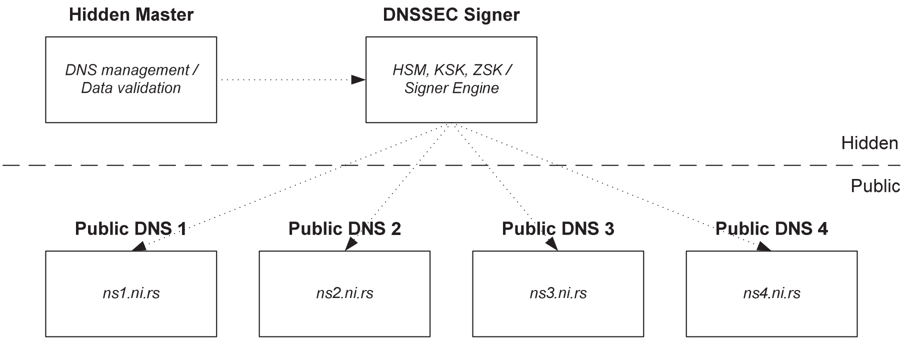

Fig. 2 – *DNSSEC design with hidden master and signer.*

3.1 Essential practices for DNS servers

Several recommendations for running public DNS servers were followed:

- The machines DNS servers are running on have no other role. The purpose is to avoid illegitimate access or negative effect of other software. Monitoring of the machine's performance is also simplified with this practice as well as troubleshooting.
- User name under which DNS software runs is a limited privilege.
- Mechanisms for access control are configured to allow transfers only where explicitly defined. They are encrypted with HMAC-SHA256 TSIG.
- Being authoritative-only servers, recursive queries have been forbidden.
- Specific TTL values were set for NS records and their A and AAAA records. Those values are set as recommended in [8] in order to reduce the effect of a potential DDoS attack.
- Response Rate Limiting (RRL) as a DDoS protection mechanism is configured and activated.

3.2 DDoS countermeasures - RRL

Response rate limiting (RRL) is a function that serves the purpose of reducing the effect of a DNS amplification attack. It is a category of reflection attacks, performed by sending traffic towards the victim via third parties, hiding behind them. Amplification is achieved by placing the attack so that the volume of traffic received by the victim is substantially bigger than the volume initially sent by the attacker.

The protocol used is what makes DNS a favorable ground for such types of attacks. Due to the lack of source validation, it is relatively easy for the attacker to spoof his IP address over UDP (User Datagram Protocol). Since DNS responses are much larger than queries, the attacker spoofing identity behind small queries can anonymously send large replies to the desired address. Many queries sent by abusing this mechanism to a large number of "open" DNS resolvers on the Internet can generate huge traffic towards the victim. Destination can be flooded with a large number of unwanted DNS replies, thus exhausting its network resources and making it unavailable.

Response rate limiting provides protection against this attack with limitations that are set on the rate at which DNS servers respond to an increasing number of queries. After the desired parameters are set, the patterns of queries defined as abusive can be detected and the rate at which the responses are sent is reduced. This results in reduction of bandwidth for the attack and makes the system less useful (to be used as an amplifier) for a potential abuser.

3.2 Security extensions

With the introduction of DNSSEC, four new resource records became part of DNS: RRSIG (Resource Record Signature), DS (Delegation Signer), DNSKEY (DNS Public Key) and NSEC (Next Secure). RRSIG contains digital signatures generated from an RRset, after it has been hashed and encrypted with private key designated for the zone it belongs to. The matching public key from the cryptographic key pair is published as DNSKEY RR. The hash of this DNSKEY is sent to the parent zone and published there, in a form of DS record, representing a delegation point between the parent and the child zone. This resource record performs like a certificate, securely connecting the zones in a chain of trust. Resolvers that are aware of DNSSEC can use this chain throughout the DNS tree (represented in Fig. 3).

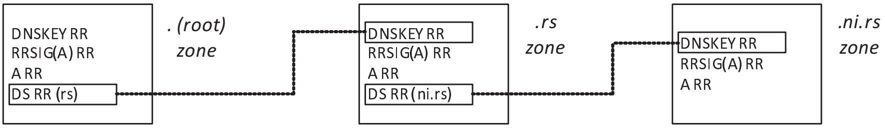

Fig. 3 – *Chain of trust in DNSSEC.*

Since DNSSEC is too complex to implement, the "bump-in-the-wire" approach (inserting a signer machine between the master and public slave servers) allowed the setup to be rolled out gradually, and to be put into service only after the non-secure DNS system (without DNSSEC) has been put online and working normally.

The software solution for a DNSSEC signer machine has been chosen according to several main criteria:

- Good integration into non-secure DNS environment already in place without interruptions or significant modifications.
- As much automation as possible. After the signer has been configured, very little or no manual intervention is necessary, but it can be done if required (in clearly defined cases of emergency). Also, strict timeframes for certain specific procedures in DNSSEC make it sensitive to human error. Higher level of automation reduces the risk of unintentional mistakes.
- High level of security. This is reflected as support for HSM. The configuration is using a software emulation of an HSM (to be budget friendly, which was one of the initial goals), but hardware HSM appliances can also be connected if they become available for use.

DNSSEC setup was performed in line with the practices outlined in [9]:

- The roles of keys are separated to Key Signing Keys (KSK) and Zone Signing Keys (ZSK).
- Size of Zone Signing Key is set to 1024 bits while the size of Key Signing Key is set to 2048 bits.
- RSA/SHA-256 algorithm is used for both KSK and ZSK, as defined in [13] (registered as algorithm 8 in IANA registry)
- Longest period of signature validity is 14 days (KSK and ZSK). Inception time is set to one hour.
- Periods of resigning (when engine for singing runs) is set to 2 hours. Refresh interval is set to 3 days (refresh of existing signatures).
- Time-to-live values of RRSIG records are the same as TTL of the resource record sets they are generated for, in line with the recommendations in [14].

Rollover of DNSSEC keys is foreseen in case keys become compromised or the policy requires it. There are two methods for rollover of keys:

- In case of Zone Singing Keys (ZSK), the method used is Pre-Publication, as recommended in [10]. Firstly, a new key is added to the DNSKEY RRset. The set is then resigned and allowed time to propagate to other caching name servers on the Internet. After that, signatures made using old key are deleted. Another time period is then allowed, this time for signatures made with old key to expire from caches on other Internet name servers. Upon this final period, old signing key can be safely deleted.

- In case of Key Signing Keys (KSK), the method used is Double-Signature. The first step to be taken is generation of new key and its corresponding DNSKEY record is included in the zone. Then, a new Delegation Signer (DS) record is sent to the parent zone, where it is installed instead of the old one. A time period is then allowed, during which all caching name servers record a new DS. Only after that can the DNSKEY (corresponding to old KSK) be removed from the zone. It is worth noting that it is recommended in [10] that the most efficient method for KSK rollover is Double-RRset, for the capability of new DS records and DNSKEY RRsets propagating alongside each other.

3.3 Authenticated denial of existence

Authenticated denial of existence is one of the distinct benefits for resolvers using DNSSEC. It is used as a proof that the queried domain name or resource records do not exist on the name server. This functionality is provided by making a list of all domain names and resource records present and making them secure with NSEC. However, this created an issue called ‘zone enumeration’, which can be used by an attacker to make a list of all domain names in a zone. NSEC3 was created to resolve this issue.

With NSEC3, a hash of every name in the zone is created and all those hashed names are linked. When any of those hashed names are queried, a response is sent stating that the name in question does not exist. Those queries will always be given the same response, with the ability to prove the non-existence of the requested domain names by including the hashes of the closest domain names in the reply.

NSEC3 uses three important configuration parameters:

- Opt-Out mechanism: With ni.rs being a small zone and containing no insecure delegations, opt-out mechanism is not used.
- Iterations: A parameter that has a purpose of countering brute-force cracking. The value is set in line with the recommendations in [5]. Limits that are set are 150 for key size of 1024 bits and 500 for key size of 2048 bits.
- Salt: Parameter preventing the creation of rainbow tables. The values are configured in line with the recommendations in [5], being at least 64 bits long. It should be noted here that a study [12] claims NSEC3 as ineffectual and inadequate, since “the value of the salt is publicly accessible via DNSSEC RR lookup…any attacker may obtain the salt to use as input into its dictionary computation, effectively negating the required increasing in dictionary size.”

Time to Live value of NSEC3 is set the same as SOA minimum value, in line with the recommendations in [5].

4 Testing

Measurement of the DNS serves performance is valuable for their uninterrupted operation. It also helps with the deployment of adequate infrastructure to ensure continuity of services.

Testing was performed on a signing machine (OpenDNSSEC, Ubuntu Server) and four public DNS servers:

- NS1, running NSD on CentOS,
- NS2, running BIND on Ubuntu Server,
- NS3, running BIND on Fedora Server and
- NS4, running Knot on Ubuntu Server

Servers are identical virtual machines with 1GB RAM and 2 vCPUs (2×4GHz). Response rate limiting was disabled during all tests.

4.1 Signing speed

Performance of RSA signing with an HSM was measured herein. This is a typical usage with DNSSEC. The signer machine was relatively modest (2 vCPUs), having to deal with a small number of zones. For the parameters, 1 and 2 threads were requesting signatures and RSA1024, RSA2048 and RSA4096 were algorithms tested.

Total signatures were 5000 for each test. Trials with low number of signatures (1-100) showed a disproportionately stronger impact of test setup on processing performance.

As benchmark software, *ods-hsmspeed* was used (part of OpenDNSSEC project).

Table 1
Speed test of DNSSEC signer.

	Average signatures per second	
Algorithm	**1 thread**	**2 threads**
RSA 1024	1336.57	2616.84
RSA 2048	379.52	751.42
RSA 4096	64.61	130.33

Increase of performance with additional threads confirms that SoftHSM (software implementation of HSM, used with OpenDNSSEC), as well as most HSMs, can be utilized better with multiple threads.

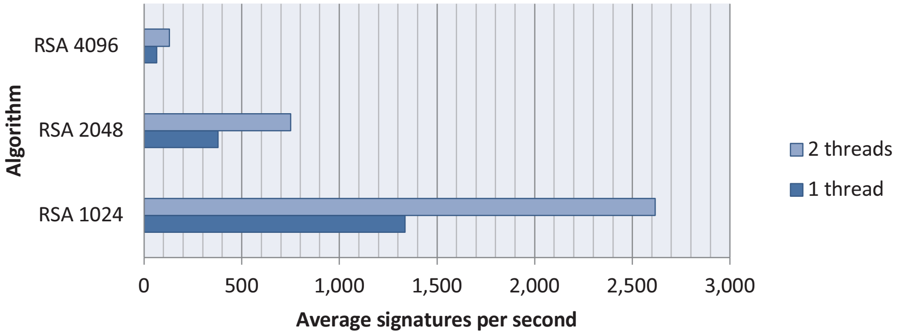

Fig. 4 – *Signing speed test.*

4.1 Packet size

Packet size comparison was performed with four different types of queries:

- [www.ni.rs A], non-DNSSEC query for a single A record.
- [www.ni.rs A +DNSSEC], DNSSEC query for a single A record
- [ni.rs ANY +DNSSEC], DNSSEC query for testing maximum response size
- [nx.ni.rs A +DNSSEC], DNSSEC query for testing NSEC3 responses

Table 2
Packet sizes.

	Packet sizes, bytes (request/response)			
Query	**NS1 (NSD)**	**NS2 (BIND)**	**NS3 (BIND)**	**NS4 (Knot)**
www.ni.rs A	27/179	27/179	27/179	27/43
www.ni.rs A +D	38/1180	38/1180	38/1180	38/219
ni.rs ANY +D (DNSSEC)	34/1821	34/2907	34/2907	34/2911
nx.ni.rs A +D	37/1003	37/1003	37/1003	37/1003

The non-DNSSEC test showed a significant difference in response size between Knot and the rest of the servers. NSD and BIND are sending NS records in AUTHORITY/ADDITIONAL sections for all NOERROR responses, while Knot does not, implementing a “minimal responses” policy, for security and performance purposes. This difference is lost in ANY and NSEC3 queries.

It is worth noting that the highest amplification factor (difference between request and response size) noted was 85,6 (for 34/2911 result), with ANY queries. This illustrates the potential for abuse if the servers are not configured properly, as shown in previous research [15].

4.1 Response rate

Response rate test was performed using *dnsperf* tool [16]. Each test was run for 1 hour and included four different types of queries described in the packet size test.

Table 3
Test of response rate.

	Average queries per second			
Query	**NS1 (NSD)**	**NS2 (BIND)**	**NS3 (BIND)**	**NS4 (Knot)**
www.ni.rs A	121.587,95	48.011,34	19.354,23	137.325,95
www.ni.rs A +D	97.099,41	38.087,76	15.283,68	126.560,55
ni.rs ANY +D (DNSSEC)	61.479,32	26.569,49	10.757,72	39.933,38
nx.ni.rs A +D	101.343,01	30.166,28	12.745,09	61.238,42

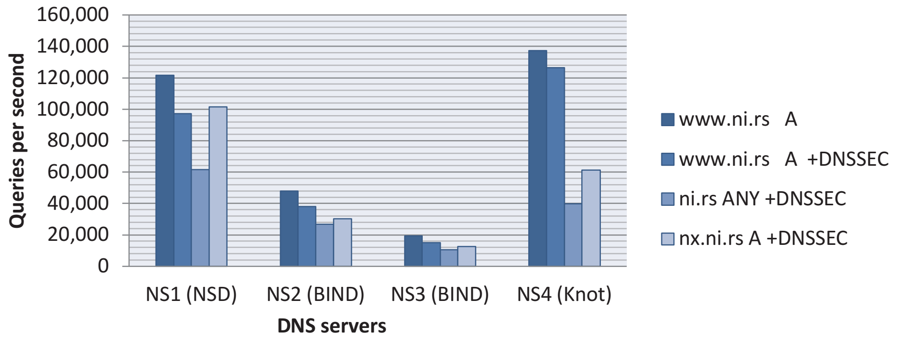

Fig. 5 – *Response rate comparison.*

The results point to a significant difference in performance between BIND and other name servers. This was expected, as NSD and Knot are optimized as high performance authoritative-only DNS servers, while BIND is multi-purpose. The inconsistency of performance between NS2 and NS3 remains to be investigated for possible impact of operating systems and their configuration.

Another significant factor observed is the impact of DNSSEC signatures in responses. Increased size of responses produced a noticeable drop in performance, as anticipated.

Being aware of the maximum traffic volume that can be endured should help with the evaluation of new infrastructure and plan for future demands.

5 Future Work

5.1 Dispersing the servers

Anycast is a technology for routing network traffic from a single source to several topologically scattered locations with the same IP address. Packets are sent using layer 3 routing to the closest server in the anycast group.

Anycast servers are planned for some future upgrade of the system presented herein. The advantages for using anycast servers are increased reliability, better performance, load balancing, stronger DDoS protection as well as improved availability. On the other hand, it is characterized by complexity, cost and greater difficulty in monitoring and troubleshooting. NSID support on all server software should help with anycast deployments.

5.2 Public documentation

DPS (*DNSSEC Policy and practice Statement*) represents a document, made in line with the recommendations in [11], describing the implemented policies and procedures that are important for DNSSEC. The aim of the document is to "provide a means for stakeholders to evaluate the strength and security of the DNSSEC chain of trust...comprising statements describing critical security controls and procedures relevant for scrutinizing the trustworthiness of the system" [11].

Preparation and publication of this document should help with recognizing the measures in place to secure the ni.rs zone. It should be important to all stakeholders, including regulatory authorities. Also, it will assist in determining the level of security implemented in our zone and conclude whether they can trust it. The benefits for other implementers are in planning of all important aspects of DNSSEC usage.

5.3 Certificates in DNS

DANE (DNS-based Authentication of Named Entities) is a protocol that can bind X.509 certificates with DNSSEC domain names, using the DNS to "store and sign keys and certificates that are used by TLS (Transport Layer Security)" [7].

This is another component planned for testing and implementation in our zone, providing an alternative to trust traditionally placed in commercial Certificate Authorities and providing a standard for email encryption, in line with the specification in [6].

6 Conclusion

DNSSEC still being in test status for ni.rs zone and the parent .rs zone still not been signed, it was not possible to verify DNSSEC operation in settings with established trust chain. This is the main reason why this DNS setup and configuration cannot be considered final or completely optimized. Industry standards have been followed in all relevant areas as well as best practices that are recommended. The project and the data presented herein have provided a valuable experience that will be useful for future work and may be beneficial to other implementers.

7 Acknowledgement

The authors would like to thank Mr. Žarko Kecić, CTO of Serbian National Internet Domain Registry (RNIDS) for his help and guidance.

8 References

[1] C. Rossow: Amplification Hell: Revisiting Network Protocols for DDoS Abuse, Network and Distributed System Security Symposium, San Diego, CA, USA, 23-26 Feb. 2014.

[2] Z. Wang: A Revisit of DNS Kaminsky Cache Poisoning Attacks, IEEE Global Communications Conference, San Diego, CA, USA, 06-10 Dec. 2015.

[3] Dj. Antic: DNSSEC Deployment and Challenges, International Scientific Conference of ICT and E-Business-related Research - SINTEZA, Belgrade, Serbia, 25-26 April 2014, pp. 678 – 682.

[4] P. Vixie: Extension Mechanisms for DNS (EDNS0), Aug. 1999.
Available at: https://tools.ietf.org/html/rfc2671.

[5] B. Laurie, G. Sissons, R. Arends, D. Blacka: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence, March 2008.
Available at: https://tools.ietf.org/html/rfc5155

[6] V. Dukhovni, W. Hardaker: SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS), Oct. 2015.
Available at: https://tools.ietf.org/html/rfc7672.

[7] P. Hoffman, J. Schlyter: The DNS-based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, Aug. 2012.
Available at: https://tools.ietf.org/html/rfc6698.

[8] V. Pappas, B. Zhang, E. Osterweil, D. Massey, L. Zhang: Improving DNS Service Availability by using Long TTLs, June 2006.
Available at: https://tools.ietf.org/html/draft-pappas-dnsop-long-ttl-02.

[9] O. Kolkman, W. Mekking, R. Gieben: DNSSEC Operational Practices, Version 2, Dec. 2012.
Available at: https://tools.ietf.org/html/rfc6781.

[10] S. Morris, J. Ihren, J. Dickinson, W. Mekking: DNSSEC Key Rollover Timing Considerations, Oct. 2015.
Available at: https://tools.ietf.org/html/rfc7583.

[11] F. Ljunggren, A.M. Eklund Lowinder, T. Okubo: A Framework for DNSSEC Policies and DNSSEC Practice Statements, Jan. 2013.
Available at: https://tools.ietf.org/html/rfc6841.

[12] J. Bau, J.C. Mitchell: A Security Evaluation of DNSSEC with NSEC3, International Association for Cryptologic Research - Cryptology ePrint Archive: Report 2010/115.

[13] J. Jansen: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC, Oct. 2009.
Available at: https://tools.ietf.org/html/rfc5702.

[14] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose: Resource Records for the DNS Security Extensions, March 2005.
Available at: https://tools.ietf.org/html/rfc4034.

[15] R. van Rijswijk-Deij, A. Sperotto, A. Pras: DNSSEC and its Potential for DDoS Attacks: A Comprehensive Measurement Study, Internet Measurement Conference, Vancouver, Canada, 05-07 Nov. 2014, pp. 449 – 460.

[16] http://nominum.com/measurement-tools.