DNSSEC

Policy and Practice Statement

1. Introduction

Present DNSSEC *Policy and Practice Statement* (later called:"DPS") document specifies the security policy and rules of proceeding of Naukowa and Akademicka Sieć Komputerowa - a research institute (later: "NASK" or "Registry") in respect to national .pl domain zone, secured by DNSSEC.
Present document is written in accordance with specifications defined in IETF organization project: RFC-draft DNSSEC *Policy & Practice Statement Framework.*

1.1. Intro

DNSSEC (Domain Name System Security Extensions) is a solution which increases DNS (Domain Name System) security. DNSSEC introduces cryptographic elements (asymmetric keys mechanism) to DNS, which gives a possibility to authenticate data received in the process of resolving internet domain name to IP (Internet Protocol) addresses. Authentication process is based on so called "trust chain", which requires proper signing of corresponding levels of domain zones, according to the hierarchic structure of DNS. This means that in order to secure a domain name, one must sign the zone of such domain and introduce a special cryptographic shortcut from the public part of the key which signs the zone (DS record, delegation signer) to the domain zone, parent in the DNS hierarchy, in which the protected domain name was registered. Here, in turn, the mentioned shortcut should be signed with a private key and its shortcut, transferred in the similar manner to the parent zone. Such chain is built up to Root zone (highest level in DNS hierarchy), where a key called "Trust Anchor" is located. It is commonly accepted that "Trust Anchor" is trusted.

DPS is a description of politics and rules used by the registry of the .pl domain zone secured by DNSSEC and other zones, for which NASK is the Registry, for example: .com.pl, .org.pl, .net.pl, .waw.pl (later together as "NASK zones"). Full list of NASK zones is available at the http://www.dns.pl web page.

1.2. Document Name and Identification

Title of the document: DNSSEC Policy and Practice Statement

Version: 1.3

Date of publication: 13-12-2011

Date of modification: 03-07-2018

1.3. Community and Applicability

1.3.1. Registry

NASK maintains highest level, national, .pl domain name registry, performs all entries: enters, modifies and removes data concerning .pl domain names and second level domain names like: .com.pl, .org.pl, net.pl, .waw.pl.

Registry is responsible for signing NASK zones and transferring the DS record from the .pl zone to Root zone. DS record from second level zones is transferred to .pl zone.

1.3.2. Partner

Partner (Registrar) is an entrepreneur, who signed *the Agreement on the cooperation concerning internet domain names* ("Agreement") with NASK and obtained a consent from the .pl domain name Subscriber (Registrant) for representation before NASK.

Partner, on behalf of the Subscriber, with use of EPP protocol, directly in .pl domain registry, performs registrations and services names in NASK zone, therein enters or removes DS records. Rules, according to which such entries are made, Partner's duties, rights and responsibilities are regulated by the Agreement.

1.3.3. Subscriber

Subscriber is an entity or an organizational unit, which does not possess any legal personality, who, basing on .pl domain names Regulations published on the internet webpage http://www.dns.pl, signed an agreement regarding maintenance of domain name belonging to NASK zone. If subject-matter of such agreement also covers administrational and technical service, the Subscriber submits changes regarding domain name entries, including DS records, directly to NASK.

In case the agreement is signed by Partner of NASK on behalf of the Subscriber, changes regarding DS record are done by the Partner of NASK.

1.3.4. DNSSEC User

DNSSEC user is an entity or an organizational unit, which does not possess any legal personality, that uses DNS responses protected by DNSSEC, which is fully responsible for the configuration of its devices, performing updates connected with correct validation of the trust chain up to "Trust Anchor".

1.3.5. Usage

DPS usage concerns only NASK zones.

Every zone below NASK zones in the trust chain created by DNSSEC may have different requirements concerning security and may allow for other levels of risk. Domain name subscriber, with use of available resources, should ensure an appropriate level of security to the maintained zone.

1.4. Specification Administration Rules

DPS should be updated in case there occurs a change NASK zones, connected with DNSSEC service, which have a direct influence on its content.

1.4.1. Organizacja zarządzająca dokumentem

Naukowa i Akademicka Sieć Komputerowa – research institute

1.4.2. Contact Data

Naukowa i Akademicka Sieć Komputerowa – research institute

Domain Department
ul. Kolska 12
01-145 Warszawa
Phone: +48 22 380 82 00
Fax: +48 22 380 83 01
Email: info@dns.pl

1.4.3. Change Introduction Procedures

Changes in the DPS are entered in a form of corrections and published as a new version of the document. New DPS version makes all earlier versions obsolete.

2. Publication and Repositories

2.1. Location of Publication

Current version of DPS is published on NASK webpage https://www.dns.pl.

2.2. KSK Publication

NASK publishes, in a form of DS record, a shortcut from KSK key which signs:

- .pl zone in Root zone,

- second level zones, managed by NASK in .pl zone.

2.3. Access Control

DPS is published on NASK webpage, secure from unauthorized deletion and modification, via HTTPS protocol.

3. Operational Requirements

3.1. Meaning of Domain Names

System resolving internet domain names on computer IP numbers (DNS) allows, in understandable and easy way, to connect the user with a chosen service like www, electronic mail, IP telephony. Domain name is a unique record in registry of this domain (parent zone). Registry of .pl domain name accepts records concerning first (dns.pl) or second (nask.com.pl, nask.waw.pl) level names, in respect to the .pl domain name. Conditions concerning registrations of names in NASK zones are specified at NASK internet webpage. NASK registers domain names using the "first come, first served" rule. DNSSEC delivers mechanism, which guarantees that the origin of data, obtained by DNS protocol, complies with information from the registry. However it does not confirm information about the Subscriber or permissions to use the domain name.

3.2. Activation of NASK DNSSEC Child Zone

Activation of the DNSSEC for child zone is done by entering a DS record, by Partner or NASK, with use of EPP protocol, to the NASK zone and publishing it in signed parent zone. NASK assumes that the obtained record is correct and no verification is required.

3.3. Identification and Authentication of Child Zone Manager

Subscriber of the domain name belonging to the NASK zone is the administrator of the child zone.

According to the Agreement, NASK assumes that Partner has the Subscribers consent to service .pl domain name of the Subscriber, including modifications and removals of DS records bound with the zone of the given .pl domain name and thus it identifies the Subscriber.

In case of names in NASK zones, serviced directly by NASK, identification of the Subscriber is also done directly by NASK.

3.4. Registration of DS Records

DS records are entered to the parent zone by the Registry - electronic system in which information about .pl domain names, serviced by NASK, are being kept. Registry accepts DS records, from Partners and NASK with use of EPP protocol, according to the standard described in RFC 5910 document. Maximum 6 DS records may be assigned to 1 domain name.

3.5. Methods to Prove Possession of Private Key

Registry does not control the correctness of child zone signing and so it also does not request any confirmation from the Subscriber that he/she is in possession of private key signing the zone. Subscriber is responsible for assuring appropriate security level.

3.6. Removal of DS Resource Records

3.6.1. Entities Authorized to Remove DS Records

Domain name DS record may be removed from NASK zone by an authorized Partner or by NASK.

3.6.2. DS Record Removal Procedure

After the DS record is removed from the Registry, changes in NASK zone will come up with the next, correct, full reload of the zone, that is with full export of the Registry data base to the form of zone files. Current information about zone reload hours is published at NASK webpage https://www.dns.pl.

3.6.3. Extraordinary Situation

In case of lack of contact with the Partner, the Subscriber may personally request for DS record removal. NASK will execute such removal if the requesting person will confirm in writing, in a form not raising any suspicions, that he/she is the Registrant of this .pl domain name.

4. Management and Operational Controls

4.1. Physical Controls

NASK provides appropriate level of physical security, accordant to the DPS requirements.

4.1.1. Localization

Registry of the .pl domain, for DNSSEC purposes, utilizes two localizations: main and backup center. Objects used for DNSSEC purposes have multistage system of physical protection and access control.

4.1.2. Physical Access

Entrances to the objects as well as the terrain around the objects are monitored around the clock. Terrain inside objects is protected by industrial television system and other technological solutions which prevent any trespassing. Access to the devices, which take part in DNSSEC procedures, is limited to authorized personnel.

4.1.3. Power Supply and Air Conditioning

Power supply consists of: two independent power lines from two independent transformer substations, two uninterruptible power supplies, generator activated automatically and a remote monitoring of energy supply. In case of malfunction of one of the stations there is an automatic switch of the power supplies.

Rooms are equipped with redundant, precise air conditioning system which keeps the temperature and humidity at constant level. All the devices, servers as well as the networking devices may work in continuous manner thanks to these stable environmental conditions.

4.1.4. Risk of Flood

Objects are kept at the appropriate technical condition and are safe from flooding. All the technical rooms with DNSSEC devices are placed at least at the 1st floor.

4.1.5. Protection from Fire

Protection from fire is ensured by fire detection and signalization system and an automatic fire extinguishing system.

4.1.6. Storage

Confidential data are kept according to NASK internal instructions and recommendations.

4.1.7. Dealing with „Waste"

Documents and materials, which include confidential data, are destroyed in a way which makes it impossible to recreate them.

4.1.8. Backup copy

System and data backup copy is kept in a safe place, outside of the main NASK localization. Access to the copy is limited to authorized personnel.

4.2. Procedural Controls

4.2.1. Roles

Roles are groups of people with an appropriate set of permissions.
Such set of permissions allows to assign a concrete role to a given person in DNSSEC administrational procedures.

NASK had specified following roles for DNSSEC purposes:

- *HSM Administrator*
- *MBK Key Administrator*
- *Administrator with rights to generate keys*

4.2.2. Number of people and roles required to perform particular tasks

Every role is performed by more than one person. A rule was accepted, that for every role the number of persons required has to be sufficient to ensure a fault-tolerant system with a high degree of redundancy.
It is required that always the same amount of persons are present, 3 at minimum ($n \geq 3$), to perform a task in DNSSEC procedures. Internal NASK procedures determine in detail the required number of people and roles in DNSSEC procedures.

4.2.3. Identification and authentication of persons to perform particular tasks

Roles in DNSSEC procedures may be performed only by persons which were chosen by NASK in writing and fulfill the criteria mentioned in point 4.3.

4.2.4. Tasks that require split of duties

HSM Administrators, as users with unlimited access capabilities, should not perform any other role.

4.3. Personnel Controls

4.3.1. Requirements Toward Personnel

Every person, which performs one of the roles from point 4.2.1 should fulfill the following requirements:

- be NASK's employee at least for a year,
- have a contract for an unspecified time or contract for a specified time, which expires not earlier than 24 months since the day the person was qualified to fulfill a given role,
- have a permission from supervisor to perform duties resulting from DNSSEC procedures.

4.3.2. Check up Actions

Supervisor of the person, which requests to take part or already takes part in DNSSEC procedures, every 2 years, assures the manager of the selected team in NASK organizational structure, that this person met all requirements from point 4.3.1.

4.3.3. Requirements Toward Trainings

Every person fulfilling a role in DNSSEC procedures must go through training process concerning:

- handling the hardware, which this person will use,
- scope of the tasks and responsibilities, which come with the performed role,
- persons share in procedures used in cases of security breach incidents, key compromise and disaster recovery.

4.3.4. Frequency of Trainings

Every person, which performs a role from point 4.2.1 must go through trainings presented in point 4.3.3 during a period of one month from the date of obtaining authorization data. Furthermore, persons performing roles of *HSM Administrators* and *Administrators with authority to generate keys*, should be present during the procedure of key generation, presented in point 5.1, at least once a year.

4.3.5. Sanctions in Case of Unauthorized Actions

Sanctions, toward persons fulfilling roles from point 4.2.1, which took unauthorized actions, result from the relationship between NASK and those persons.

4.3.6. Requirements toward Personnel

Nobody beside the persons fulfilling roles from point 4.2.1 can have access to devices of the key management system and may not perform any changes in it. In case of emergency a person fulfilling a given role may perform his/her duties after consulting the supplier of the devices or software but any confidential data exposure or any security breach situation like key exposure, may not take place.

4.3.7. Sharing the Documentation with Personnel

Persons performing particular roles have access to internal procedures, which involve change of key, creation and restoration of backup copy. These persons are immediately informed about any changes made in the procedures.

4.4. Audit Logging Procedures

4.4.1. Event Logging

All operations, which are performed with use of devices that take part in signing NASK zones, are recorded.

4.4.2. Frequency of gathered information checks.

Administrators of the Registry monitor recorded operations and events and check all of them at least once a day.

4.4.3. Storage Time

All recorded operations and events are archived and stored for at least 3 years.

4.4.4. Protection

Access to the operation and event records is limited to persons entitled.. Recorded operations and events are stored on two separate devices.

4.4.5. Informing users about event logging

Persons performing particular roles in the system are informed, during the training, about recording the actions described in point 4.4.1.

4.4.6. Evaluation of Suseptibility

All records of non-standard operations and actions are analyzed for security breach attempts.

4.5. Compromise and Disaster Recovery

4.5.1. Incident Handling

Security breach incidents, connected with DNSSEC system are being handled by a team specially selected among NASK's organizational structure. Depending on incident(data loss or damage, compromise of private keys, compromise of server on which NASK zone signing is done), appropriate actions, described in internal procedures, are undertaken.

Decision about execution of a particular action is made by the manager of the team selected among NASK's organizational structure. Manager also informs his superior about action undertaken.

4.5.2. Damage of Data, Software or Hardware

Cryptographic material in form of private keys is kept on more than one HSM (Hardware Security Module) device.

In case of malfunction of all HSM devices in the main localization there is a possibility to reroute the traffic and to use HSM devices from the backup localization without the necessity to switch whole Registry infrastructure.

In case of malfunction of all HSM devices it will become impossible to sign new records in NASK zone. It will also become impossible to re-sign existing records if their validity time expires. In such case, in an emergency mode, DS record will be deleted from the parent zone and an unsigned NASK zone will be published on DNS servers. NASK possesses an internal procedure which describes removal of DS record from parent zone.

4.5.3. Private Key Compromise

Information, which points to DNSSEC keys compromise for NASK zones, results in initiation of an emergency procedure. Every suspicion of compromise of devices used to sign NASK zones results in creation of backup of current state of systems for threat analysis purposes, new installation of the systems and emergency key exchange. NASK possesses internal procedures which, in detail, describe the way of proceeding in case such suspicion of private key compromise arises.

4.5.4. Contingency Plan

Constant readiness to switch the Registry system to the backup localization is maintained. Additionally, all instructions, procedures and cryptographic material is kept in safe place, outside of the main location. Decisions about switching to the backup location is made by the manager of the team selected among the NASK's organizational structure. Manager also informs his superior about action undertaken.

5. Technical Security Controls

5.1. Key Pair Generation and Installation

5.1.1. Key Pair Generation

Keys are generated in hardware security module (HSM), managed by persons performing roles of *HSM Administrators*. All activities, performed on HSM device, are done in the presence of at least three *HSM Administrators*. To generate keys, presence of additional three persons from the *Administrators with key generation rights* group is required. Key generation procedure is described in NASK internal documentation. Procedures, accepted by the Registry, force synchronization of the HSM devices immediately after the keys are generated.

5.1.2. Publication of KSK Public Key

Public key, in a secure manner, is downloaded by the *HSM Administrators* and published according to the information in point 2.2.

5.1.3. Parameters of Public Key and Quality Control

Public key parameters, rules and method of its control are described in NASK's internal document.

5.1.4. Key Usage

Keys, generated in DNSSEC procedures, may be used only during their validity period and may not be used in any other way than to sign NASK zones.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations, concerning private keys, are conducted in HSM device and private keys may not be found outside of the device, unprotected.

5.2.1. Norms and Cryptographic Module Control

Cryptographic hardware module, used by NASK, must possess an appropriate certificate.

5.2.2. Multi-personal Private Key Control

Multi-personal access to the keys is described in point 4.2.

5.2.3. Private Key Deposit

NASK does not deposit private keys.

5.2.4. Security Copy

Keys are archived in a form ciphered by Master Backup Key (MBK), which is stored in a safe place. To create copies, presence of *HSM Administrators* is required and in case when such copy must be created because of data damage on the HSM device, presence of *HSM Administrators* and *MBK key Administrators* is required.

5.2.5. Storage of the Private Key on HSM

Private keys are stored in HSM device in a form ciphered by a special key, which exists only in the HSM device. In case of device integrity breach due to physical attack, the key is permanently removed from the HSM device. This results in lack of possibility to decipher the cryptographic material.

5.2.6. Archivisation of Private Key

Private key, which is not used, is archived only in a form of backup copy.

5.2.7. Transfer of the Private Key from/to the Cryptographic Module

Transfer of the private key from/to the HSM device is done in a way of backup copy which is restored on a different HSM device. Instruction of creation and restoration of the backup copy is described in NASK's internal procedures.

5.2.8. Private Key Activation Method.

Private keys are activated with help of signing software, in presence of persons performing roles of *HSM Administrators* and *Administrators with permission to generate keys.*

5.2.9. Private Key Deactivation Method

Private keys are deactivated with help of signing software, in presence of people performing roles of *HSM Administrators*.

5.2.10. Private Key Destruction Method

Unused private keys are removed from the system connected with the protected NASK zone. Keys are deleted by *HSM Administrators*.

5.3. Other Aspects of Key Pair Management

5.3.1. Public Key Archivisation

Public keys are archived on a backup server, connected to the main backup system. Backup server stays under control of a team selected among NASK's organizational structure.

5.3.2. Key Usage Time

Keys cease to be valid with the moment their production utilization ends. Keys may not be reused.

5.4. Activation Data

Every person performing a role in DNSSEC procedures owns an individual access key. Every access key is assigned only to one person.

Login data do not repeat and are known to one person only.

5.4.1. Data Activation

Every person performing a role in DNSSEC process gets a generated and assigned individual access key. Access Keys generation is done in the presence of *HSM Administrators*.

5.4.2. Authorization Data Protection

Every person performing a role in DNSSEC procedures is obliged to protect the authorization data in form of access key. In case the access key is lost, its user is obliged to inform the persons performing *HSM Administrative* roles about this fact immediately.

5.4.3. Other Aspects of Authorization Data

Registry will not store copies of authorization data.

Assigned access keys do not have any deactivation date. Exchange of the access keys should take place at least once per 2 years.

In case the access key is lost, it is immediately deactivated, a new access key is generated and assigned to the person performing a particular role.

5.5. Hardware Security Controls

Critical elements of the Registry system are separated and are located in a appropriately secured location (point 4.1). Access to the devices is limited and the way, they are used, is recorded and controlled (point 4.4).

5.6. Network Security Controls

NASK's network is designed to ensure an appropriate level of security in its corresponding segments. All confidential information is ciphered.

5.7. Timestamping

Registry System is synchronized with time server, managed by NASK.

5.8. Life Cycle Technical Controls

5.8.1. System Development Control

To manage the system development, the Registry uses an appropriate code versionizing systems. Repositories are located on a separate server, managed by a team, selected among the NASK organizational structure.

5.8.2. Security Management Control

Registry conducts systematic security controls and risk estimations for the system and undergoes cyclic system security audits as well.

5.8.3. Modification Management

Registry uses a modification management system to manage the software responsible for DNSSEC operations.

6. Zone Signing

6.1. Key Length and Algorithms

In case of KSK keys, RSA algorithm of 2048 bit key length is used. In case of ZSK keys the key length is 1024 bits.

6.2. Authenticated Denial of Existance

Registry uses the NSEC3 standards, described by RFC 5155. All NASK zones are signed in OPT-OUT mode.

6.3. Signature Format

All signatures are generated with help of RSA cryptographic operations, using SHA256 (RSA/SHA256, RFC 5702).

6.4. ZSK Roll-Over

Change of ZSK keys is conducted every 3 months.

6.5. KSK Roll-Over

Change of KSK keys is conducted every 6 months.

6.6. Signature Life-Time and Re-Signing Frequency

Sets of records are signed with ZSK key for 30 days (+/- 1 day). New records are signed as they come, with use of dynamic actualizations. Whole export of NASK zone and generation of the signatures is done at least once per 7 days.

6.7. Verification of Zone Signing Key Set

Verification of keys, which sign the zone, is done by checking the trust chain for every SOA record of every zone.

6.8. Verification of Resource Records

Registry verifies the validity of signed records automatically with use of available tools and its own scripts, according to the existing standards.

6.9. Resource Records TTL

Global TTL for zones = 86400 seconds.
DNSKEY TTL = 3600 seconds.
TTL for RRSIG record specifies the TTL of the record the signature covers.

7. Audit

Audit is conducted in order to check the correspondence of functioning of the Registry according to the requirements described in DPS.

7.1. Frequency of Audit

NASK decides about the necessity of conducting an audit. Complete audit is conducted at least once per two years. Partial audit may be conducted more often. Basic prerequisites to conduct a partial audit for correspondence with DPS:

- meaningful changes introduced in processes, infrastructure or organization,
- relevant anomalies observed in the functioning of the system and procedures connected with NASK's DNSSEC secure zones.

7.2. Auditor's Qualifications

Auditor should have at least two-year experience in conducting internal security audits, possess knowledge of standards and IT security norms, BIND software, script languages and knowledge from the DNS protocol security domain and ciphering algorithms used in it.

7.3. Auditor's Relationship to Audited Party

Auditor may not take any of the roles defined in point 4.2.1. Auditor may be an expert, employed by NASK do partake of this task.

7.4. Topics Covered by Audit

Complete audit assumes correspondence of functioning of the Registry according to the procedures and requirements, described in DPS as well as with internal procedures, which, for security reasons, may not be disclosed in this document and existence of which results from DPS requirements.
In case the decision about audit results from introduction of changes in processes, infrastructure or organization or from detection of relevant anomalies in functioning of the Registry and in procedures connected with NASK's DNSSEC secure zones, audit may concern only those DPS areas/issues, in which changes were introduced or anomalies detected. Such audit is called a partial audit. Audited entity should be informed about the audit with an appropriate advance.
.

7.5. Actions Taken as a Result of Deficiency

If a fault in functioning of the Registry or in procedures connected with NASK's DNSSEC secure zones is detected, the auditor informs the audited persons and the management of the Registry about this fact, who in turn will initiate repair and prevention actions if necessary.

7.6. Communication of Results

Auditor is obliged to communicate the results of the audit in a written form in time limit adjusted with the management of the Registry.

8. Legal Matters

8.1. Personal Data Protection

Personal data are stored, processed and made available according to the Polish law, in particular with the personal data protection act.

8.2. Responsibility and Non-Disclosure Agreements

Partner's responsibility and the commitment to keep the confidentiality in respect to NASK as well as NASK in respect to Partners, are described in the Agreement. NASK's responsibility to its Subscribers and Subscribers to NASK is defined in the *.pl domain name Regulation*.

8.3. DPS Validity Period

This presented DPS is in force until the moment its replaced with a new version, introduced according to the procedure described in point 1.4 or until withdrawal.

8.4. Binding Law

In matters not regulated by the DPS, the *Agreement concerning internet domain names* and the *.pl domain name Regulation*, the letter of the Polish law is used.