DNSSEC

Policy & Practice Statement

1. Introduction

This DNSSEC Policy & Practice Statement (hereinafter: **"DPS"**) defines the security policy and practices of the Research and Academic Computer Network - National Research Institute (hereinafter: **"NASK"** or **"Registry"**) in relation to the national .pl domain secured by DNSSEC.

This document was formulated based on the recommendations stipulated in the document published by the Internet Engineering Task Force IETF: RFC-6841 A Framework for DNSSEC Policies and DNSSEC Practice Statements.

1.1. Introduction

DNSSEC (Domain Name System Security Extensions) constitutes a solution enhancing the security of the DNS (Domain Name System). DNSSEC introduces the elements of cryptography (the mechanism of asymmetrical keys) to the DNS, which offers the opportunity to authenticate data received as part of the process of translating internet domain names to IP addresses (Internet Protocol). The authentication process is based on a so-called "chain of trust", where all levels of domain zones are signed individually, in accordance with the hierarchic structure of the DNS. This means that in order to secure the domain name, one has to sign the zone of such domain and publish the DS record (it is a cryptographic digest of the public part of the key signing the zone) in the parent domain. Then, the DS record in the parent zone is signed with a private key, and the digest of the public part of the signing key is transferred to its' parent zone in an analogous manner. Thereby, a chain to the Root zone (the highest level in the DNS hierarchy) is built, where the "Trust Anchor" (commonly accepted as trusted) is located.

The DPS is the description of policies and practices applied by the registry of the .pl zone and the second level zones, for which NASK is the registry, e.g.: .gov.pl, .com.pl, .org.pl, .net.pl, .waw.pl (hereinafter jointly "**NASK zones**"). The complete list of NASK zones is available on the following website www.dns.pl.

The DPS is applicable solely to the NASK zones. Each zone located below the NASK zones in the chain of trust created by DNSSEC may have different requirements in terms of security and a different level of risk may be accepted for a given zone. The domain name subscriber should, within the scope of available resources, ensure an adequate security level of the managed zone.

1.2. Name and designation of the document

Document title: DNSSEC Policy & Practice Statement

Version: 2.0

Date of publication: 12-03-2020

Date of last modification: 12-03-2020

1.3. Websites and operating environment

1.3.1. Registry

NASK operates the .pl ccTLD registry and the registry of.gov.pl domain names for public and government institutions.

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

1.3.2. Registrar

The Registrar, an entity bound with NASK by *Agreement on the cooperation concerning internet domain names* ("Agreement"). NASK publishes the up-to-date list of registrars along with the services provided by them, including the DNSSEC service, at www.dns.pl.

The Registrar registers and maintains the names in NASK zones on behalf of the Subscriber, including introduction or deletion of DS records in the .pl registry, via the EPP protocol.

1.3.3. Subscriber

The Subscriber is an entity which concluded an agreement on the maintenance of the domain name from the NASK zone, based on the *Regulations of .pl domain names* or *Regulations of .gov.pl domain names*.

The Subscriber transfers modified entries regarding the DS records to NASK via the Registrar.

In the case of the .gov.pl zone the Subscriber transfers the aforementioned changes directly to NASK.

1.3.4. DNSSEC user

The DNSSEC user is an entity using the DNS responses secured by DNSSEC, which is individually responsible for the proper configuration of its own devices and making updates related to correct validation of the chain of trust up to the “Trust Anchor”.

1.4. Rules of document management

In the event of any changes associated with the handling of DNSSEC in the NASK zones, the DPS shall be updated within the scope of said changes.

1.4.1. Organization managing the document

The Research and Academic Computer Network - National Research Institute

1.4.2. Contact details

NASK - National Research Institute

Domain Department
ul. Kolska 12
01-045 Warszawa
Tel.: +48 22 380 82 00
Fax: +48 22 380 83 01
Email: info@dns.pl

1.4.3. Procedures for amending the document

Changes to the DPS are implemented in form of amendments and published as a new version of the document. A new version of the DPS makes all earlier versions obsolete.

2. Publication and repositories

2.1. Place of publication of the DPS

The current version of the DPS is published on the NASK website at www.dns.pl.

2.2. Publication of public keys

NASK publishes the digest of the KSK in form of a DS record:

- for the .pl zone in the Root zone,

- for the second level zones managed by NASK, including the .gov.pl zone in the .pl zone.

3. Operational requirements

3.1. Significance of the domain name

The system of translating Internet domain names into IP addresses (DNS) allows the users to connect to selected services, like websites, email or IP telephony in a comprehensible and simple manner. Domain name is a unique entry in the domain registry (a higher level zone). The Registry accepts entries regarding the .pl TLD, e.g. dns.pl and the second level, e.g. nask.com.pl, nask.waw.pl. Conditions regarding name registration in the NASK zones are specified on the NASK website. NASK performs registrations on the basis of the “first come, first served” rule.

DNSSEC provides mechanisms guaranteeing that the origin of data obtained via the DNS protocol complies with the information included in the registry. It does not, however, confirm information on the Subscriber or rights to use the domain name.

3.2. DNSSEC activation for the child zone in relation to the NASK zone

Activation of DNSSEC for a child zone takes place through introduction of the DS record to the NASK zone by the Registrar or NASK and its publication in the signed parent zone by NASK. NASK assumes that the received record is correct and does not verify it.

The .gov.pl zone is the exception. NASK verifies the correctness of the configuration on the authoritative DNS server for the domains in that zone.

3.3. Identification and authentication of the manager of the child zone

The Subscriber is the manager of the sub zone in relation to the NASK zones

In accordance with the Agreement, NASK assumes that the Registrar is in possession of the Subscriber’s consent for handling of the .pl domain name, including introduction, modification and deletion of the DS records associated with a zone of a given domain and thus identifies the Subscriber.

In the case of names in NASK zones handled directly by NASK the Subscriber shall be identified by NASK.

3.4. Registration of DS records

DS records are introduced to the parent zone by the Registry System, where information regarding the .pl domain names maintained by NASK are stored. The Registry System accepts DS records, from the Registrars and NASK via the EPP protocol. DS records should be compliant with the standard defined in the RFC 5910 document. The maximum number of DS records that can be assigned to one domain name is 6.

3.5. Methods of confirming the possession of a private key

The Registry does not conduct correctness checks regarding the child zone, and therefore does not require the Subscriber of the child zone to confirm whether it has a private key signing the zone. the Subscriber is responsible for ensuring an adequate security level .

3.6. Deletion of DS records

3.6.1. Entity authorized to delete DS records

The DS record of the domain name may be deleted from the NASK zone by an authorized Registrar or NASK.

3.6.2. Procedure of deleting DS records

Deletion of DS records from the Registry System prompts changes in the NASK zone at the latest with subsequent full and correct reloading of the zone file. Current information on hours of reloading the zones is published on the website of NASK at www.dns.pl

3.6.3. Emergencies

In the case of inability to contact the Registrar, the Subscriber can individually request for a DS record to be deleted. NASK will perform such deletion, provided that the applying entity confirms, in no uncertain terms and in writing, that it is the Subscriber.

4. Management and Operational Controls

4.1. Physical Controls

NASK ensures a proper physical security level compliant with the DPS requirements.

4.1.1. Location

The Registry uses two locations for the purposes of DNSSEC: a primary location and a backup centre. The facilities used for the purposes of DNSSEC have multi-stage system of physical security and access control.

4.1.2. Physical access

Entry points to the facilities are monitored 24 hours per day. The premises are protected by a CCTV system and other technological solutions blocking access for unauthorized persons. Access to devices, which take part in the DNSSEC procedures, is restricted for authorized persons.

4.1.3. Power supply and air conditioning

Power supply comprises of: two independent lines powered from two independent transformer substations, two UPS systems, an automatically launched power generator and remote monitoring of the energy supply.

The rooms have stable environment conditions ensuring continuous operation of the devices. The rooms are equipped with a redundant air conditioning system.

4.1.4. Flood hazard

Facilities equipped with devices used for DNSSEC are located in areas which are not at risk of flooding. The facilities and devices are securely kept in a proper technical condition..

4.1.5. Fire protection

Fire safety is ensured by a fire detection system and an automatic fire extinguisher.

4.1.6. Data storage and procedures regarding carriers

Data are classified, labelled and stored in accordance with the internal regulations applicable at NASK specifying the adequate security level of processing of said data.

4.1.7. Procedures regarding redundant data

Redundant carriers, documents and material containing data protected by NASK are deleted or destroyed in a manner making it impossible to recreate or reuse them.

4.1.8. Backup copy

The backup copy of the system and data is stored in a secure spot outside of the primary location of NASK. Access to the copy is restricted to authorized persons.

4.2. Procedural safeguards

4.2.1. Roles

In order to ensure correct compartmentalization of the permissions and responsibilities, the users of the DNSSEC system are granted specific roles. Roles are groups of individuals with a specific set of permissions. Such set of permissions allows to assign a concrete role to a given person in DNSSEC administrational procedures. The detailed scope of responsibilities of specific roles is described in the internal procedures of NASK.

4.2.2. The number of persons and roles required to perform particular tasks

A principle was adopted, stipulating that each role has a number of persons assigned to it ensuring high quality of redundancy of permissions.

Each of the implemented operational or administrative activities require persons authorizing the access and persons participating in the process of carrying out the DNSSEC procedures.

4.2.3. Identification and authentication of persons fulfilling specific roles

Roles in DNSSEC procedures may only be performed by persons who were appointed by NASK and meet the criteria referred to in point **Błąd! Nie można odnaleźć źródła odwołania.**.

4.2.4. Principle of segregation of duties

Segregation of duties is applied in the DNSSEC procedures. Restrictions were introduced in relation to the ability to combine roles. Additionally, selected roles may be assigned to persons who are a part of specific organizational units of NASK.

4.3. Personnel controls

4.3.1. Qualifications, experience, and clearance requirements

Each person who fulfils a role in the DNSSEC procedures should meet the following conditions:

- be employed at NASK for at least a year,
- be employed on the basis of an employment agreement for an unspecified period or employment agreement for a specified period, which expires no earlier than 12 months form the date of qualification to fulfil a specific role,
- not be in the notice period,
- have the consent of its immediate superior to perform activities resulting from the DNSSEC procedures,
- be trained within the scope of application of the DNSSEC procedures (see point 4.3.3).

4.3.2. Background check procedures

NASK does not conduct further verifications in respect of fulfilling roles in the DNSSEC operations during the recruitment process. In accordance with point 4.3.1, newly hired persons cannot play a role in the DNSSEC procedures.

4.3.3. Training requirements

Each person who fulfils a role in the DNSSEC procedures has to undergo training including:

- handling of specific devices,
- scope of tasks and responsibilities related with the role,
- how to proceed in the case of security breach incidents, compromise of the keys and disaster recovery.

4.3.4. Training frequency

Each person who fulfils one of the roles stipulated in point 4.2.1 has to undergo training specified in point 4.3.3 prior to being permitted to implement the DNSSEC procedures. Additional training has to be completed by all persons each time after a change of the DNSSEC procedures and by persons who have not carried out the DNSSEC procedures for a period longer than 18 months.

4.3.5. Sanctions for unauthorized actions

Sanctions towards persons fulfilling roles specified in point 4.2.1, who have carried out an unauthorized action, result from the employment relationship between NASK and said persons.

4.3.6. Contracting personnel requirements

Persons not bound by an employment agreement with NASK cannot be nominated for the DNSSEC roles.

In the case of emergencies and the need to consult with third parties (supplier of devices and software supporting DNSSEC) persons fulfilling DNSSEC roles shall undertake to ensure data confidentiality and respect these principles by third parties.

4.3.7. Documentation supplied to personnel

Persons fulfilling specific roles are ensured access to internal procedures regarding all of the operations carried out by said roles.

4.4. Audit logging procedures

4.4.1. Types of events recorded

All operations performed with the use of the devices which take part in signing of NASK zones are logged.

4.4.2. Frequency of processing log

The Registry Administrators monitor the logged operations and events and inspect them at least once a week. In the event of an identification of an anomaly the Administrators act without undue delay.

4.4.3. Log retention time

The Logs of the collected operations and events are archived and retained for a period of at least 6 months.

4.4.4. Log protection

Access to operations and event logs is restricted to authorized persons. Event logs are stored on two independent devices.

4.4.5. Informing users about event logging

Persons fulfilling specific roles in the DNSSEC system are informed about logging of events specified in point 4.4.1 during the training.

4.4.6. Vulnerability assessment

All records of non-standards operations and events are subjected to an analysis in the event of determining a potential attempt of a security breach.

4.5. Compromise and disaster recovery

4.5.1. Incident handling

Incidents which pose security threat related with the DNSSEC system are handled by a team specifically assigned within the organizational structure of NASK. Depending on the incident (loss or corruption of data, compromise of private keys, compromise of the server where the NASK zones are signed) appropriate actions, described in the internal procedures of NASK, are taken.

The decisions regarding execution of a specific action are made by the leader of the assigned team in the organizational structure of NASK who informs his or her superior about the actions taken.

4.5.2. Procedures in case of data and software corruption or damage to the devices

The cryptographic material in form of private keys is stored on more than one device.

In the event of a failure of all DNSSEC devices in the primary location there is an option to redirect traffic and use devices located in the backup location.

In the case of a failure of the DNSSEC devices resulting in:

- inability to sign new records in the NASK zone,

- inability to resign the records, the validity of which is expiring,

then the DS record shall be deleted from the parent zone without undue delay. The NASK zone will be published in an unsigned form.

NASK has put an internal procedure in place describing the deletion of a DS record from the parent zone.

4.5.3. Entity private key compromise procedures

Information indicating a compromise of the DNSSEC keys of the NASK zones results in launching of an emergency procedure.
Each suspicion of a compromise of devices used to sign NASK zones results in creation of a copy of the current state of the system for the purposes of further analysis, a new installation of the systems and emergency exchange of keys. NASK has put internal procedures in place describing in detail the course of action in the event of a suspicion of a compromise of the private key.

4.5.4. Continuity plan

In order to ensure continuity of operation of the DNSSEC service, NASK maintains a backup centre for the DNSSEC system infrastructure and has emergency plans in place which allow to restore the operation of the service within a planned timeframe. All instructions, the cryptographic material and other necessary information have backups and are stored in a manner minimizing the risk of their loss and compromise.

5. Technical security controls

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

Keys are generated in the security module managed by the roles specified in the internal procedures of NASK. All activities are implemented in the presence of a specified number of authorized persons in order to minimize the risk of human errors and abuses.
The key generation procedure is described in the internal documentation of NASK.

5.1.2. Publication of the public part of the KSK

The public part of the KSK is published in a secure manner, in accordance with information provided in point 2.2.

5.1.3. Public key parameters generation and quality checking

The parameters of the public key and the rules and manners of its control are defined in the internal document of NASK.

5.1.4. Key usage purposes

Keys generated in the DNSSEC procedures may be used only during their validity cycle and cannot be used for purposes other than signing of NASK zones.

5.2. Private key protection and cryptographic module engineering controls

All cryptographic operations regarding private keys are carried out by the DNSSEC devices, whereas it is forbidden to process private keys in an insecure form outside of said devices.

5.2.1. Private key multi-person control

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

5.2.2. Deposit of private keys

NASK does not deposit private keys.

5.2.3. Private key backup

The keys are archived in encrypted form and stored in a safe location. In the case of data corruption security procedures, identical as in case of the DNSSEC key generation procedure, are applied. .

5.2.4. Private key storage on cryptographic module

Private keys are stored on a DNSSEC device and encrypted with a special key.

5.2.5. Private key archival

An unused private key is archived only in form of a backup copy.

5.2.6. Transfer of a private key to and from the cryptographic module

Transfer of a private key to and from the DNSSEC device takes place only in form of a backup copy. Instructions on how to create and restore the backup copy are described in the internal procedures of NASK.

5.2.7. Method of activating private key

Private keys are activated automatically via signing software.

5.2.8. Method of deactivating private key

Private keys are automatically deactivated after their expiration.

5.2.9. Method of destroying private key

Unused private keys are manually deleted from the DNSSEC devices in accordance with the internal procedures of NASK.

5.3. Activation data

Each of the roles participating in the DNSSEC procedures has an access key.

5.3.1. Data activation

Each role in the DNSSEC has a generated and assigned access key.

5.3.2. Activation data protection

Each person fulfilling a role in the DNSSEC procedures is obliged to protect activation data. In the case of a loss of an access key, its user is obliged to immediately report that fact in accordance with the internal procedures of NASK.

5.3.3. Other aspects of activation data

The Registry does not store copies of *activation* data.

The assigned access keys do not have deactivation date. Exchange of access keys should take place at least once every 2 years.

In the event of a loss of an access key or change of the personnel in a specific role, the key is immediately revoked and a new access key is generated and assigned to a specific role.

5.4. Device security

Critical elements of the DNSSEC system are isolated and located in a secure location (point **Błąd! Nie można odnaleźć źródła odwołania.**). Access to the devices is restricted and their usage is registered and subjected to inspections (point 4.4).

5.5. Network security

The NASK network is constructed in a way ensuring a proper security level in its specific segments. All of the protected information are encrypted.

5.6. Registration of time stamps

The DNSSEC system is synchronized with the time server.

5.7. Security of the processes of software maintenance and development

5.7.1. System development control

The Registry uses a code versioning system in order to manage software development. Repositories are located on a dedicated server managed by the team assigned in the organizational structure of NASK.

5.7.2. Security management control

The Registry regularly conducts security controls, estimates risk and orders security audits of the DNSSEC system.

6. Zone signing

6.1. Key Length and Algorithms

In the case of the KSK, the RSA algorithm with the key length of 4096 bits is applied, and in the case of the ZSK a key with a length of 2048 bits is applied.

6.2. Authenticated Denial of Existance

The Registry uses the NSEC3 standard defined by RFC 5155. All of the NASK zones are signed in the OPT-OUT mode.

6.3. Signature Format

Signatures are generated by RSA cryptographic operations, usingSHA256 (RSA/SHA256, RFC 5702).

6.4. ZSK rollover

Exchange of the ZSK is conducted every 6 months.

6.5. KSK rollover

Exchange of the KSK is conducted every 12 months.

6.6. Signature Life-Time and Re-Signing Frequency

The sets of records are signed with the KSK for the period of 30 days (+/- 1 day). New records are signed on the ongoing basis via a dynamic updates mechanism. The total export of the NASK zone and generation of signatures takes place at least once every 7 days.

6.7. Verification of Zone Signing Key Set

Verification of keys signing the zone takes place through inspection of the chain of trust for the SOA record for each zone.

6.8. Verification of Resource Records

The Registry verifies the correctness of the signed records automatically via the available tools and own scripts in accordance with the existing standards.

6.9. Resource Records TTL

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

7. Audit

In order to ensure an adequate security level of the DNSSEC system security audits need to be carried out.

The goal of the audit is to verify the compliance of the operation of the Registry with the requirements specified in the DPS.

7.1. Audit frequency

The audit is carried out in accordance with the NASK audit plans, but at least once every 3 years. Partial audits outside of the audit plan should be conducted in the case of:

- significant changes in the processes, infrastructure or organization associated with DNSSEC,
- obeservation of significant irregularities in the operation of the system and procedures related with the NASK zones secured by DNSSEC.

7.2. Qualifications of the auditor

An auditor should have at least two-year experience in carrying out internal information security audits, has to be familiar with IT security standards and norms, script languages and possess knowledge within the sphere of security of the DNS protocol and usage of encrypting algorithms.

7.3. Auditor’s Relationship to Audited Party

The auditor cannot fulfil any of the roles specified in point 4.2.1. An auditor can be an expert employed by NASK in order to perform that task.

7.4. Scope of the audit

The audit includes compliance of the operation of the Registry with the procedures and requirements stipulated in the DPS, as well as with the internal procedures, which cannot be disclosed in this document due to security reasons.

In the event where a decision on an audit results from the introduction of changes in the processes, infrastructure or organization or from an observation of significant irregularities in operations and procedures related to the NASK zones secured by DNSSEC, the audit may concern only those issues/areas of the DPS, where changes were introduced or where the irregularities occurred. Such an audit is called a partial audit.

7.5. Elimination of irregularities

In the event of identification of irregularities, as a result of the audit, in the operation of the DNSSEC system, information regarding said issues are transferred to the management of the Registry. The management of the Registry will make a decision on further proceedings regarding the non-compliance. Such actions are documented.

7.6. Communication of results

The auditor shall undertake to communicate the audit results in written form within the timeframe agreed upon with the management of the Registry.

8. Legal matters

8.1. Personal data protection

Personal data are stored, processed and made available in accordance with the Polish law and in particular with the Personal Data Protection Act.

8.2. Responsibility and Non-Disclosure Agreements

The liability of Registrars and the confidentiality obligation towards NASK, as well as NASK's obligation towards the Registrars are specified in the Agreement.
NASK's liability towards the Subscribers and the Subscribers' liability towards NASK are specified in the *Regulations on .pl domain names* and *Regulations on .gov.pl domain names.*

8.3. DPS Validity Period

This DPS shall be valid from the moment or replacing it with a new version introduced in line with the procedure referred to in point 1.4 or until it is revoked by the Registry.

8.4. Applicable laws

To all matters not regulated by the DPS, the *Agreement concerning internet domain names* and the *.pl domain name Regulation* the provisions of the Polish law shall apply.