Security Documentation

DNSSEC Practice Statement (DPS)

Estonian Internet Foundation
Silikaltsiidi 3a, 11216 Tallinn, Estonia T +372 727 1000 E info@internet.ee www.internet.ee
Reg. nr 90010019 VAT nr EE101286464

Table of Contents

1. Introduction

This document is Estonian Internet Foundation's statement of security practices and provisions that are applied in relation to the operation of DNS Security Extensions (DNSSEC) in the Estonian top-level domain (.ee). This document conforms to RFC 6841, DNSSEC Policy & Practice Statement Framework. This DPS is one of several documents relevant to the operation of the .ee zone. Other relevant documents are for internal use only, and are not available to the public.

1.1. Overview

The Domain Name System Security Extensions (DNSSEC) is a set of IETF specifications for adding origin authentication and data integrity to the Domain Name System. DNSSEC provides a way for software to validate that Domain Name System (DNS) data has not been tampered with or modified during Internet transit. This is done by incorporating public key cryptography into the DNS hierarchy to form a chain of trust originating from the root zone.

1.2. Document name and identification

Document title: DNSSEC Practice Statement (DPS)

Version: 1.1

Created: February 21, 2014

Updated: March 7, 2014

1.3. Community and applicability

The following parties to which this document has applicability have been identified. In the rest of the paragraph, we shall identify the obligations of the named parties within the DNSSEC context. The relation between the Registry and a Registrar is regulated in the Registrar Contract.

1.3.1. Registry

Estonian Internet Foundation (the Registry) is responsible for the Internet's Estonian top-level domain (.ee) and the management of the .ee registry, and consequently it is responsible for the registration of domain names that identify underlying zones in the .ee zone. This also implies that the Registry manages supplements, changes and removals of all data that is associated with a domain name.

Additionally, the Registry is responsible for generating cryptographic key material, protecting the confidentiality of the private component of the key pairs, and securely signing all authoritative DNS resource records in the .ee zone using DNSSEC and the keys attached to it.

Finally, the Registry is responsible for the secure export, registration and maintenance of DS[1] resource records in the root zone, which establishes the chain of trust from the root zone to the .ee zone.

1.3.2. Registrars

A Registrar is the party that is responsible for the administration and management of a domain name on behalf of the Registrant and under the contract with the Registry. The Registrar handles the registration, maintenance and management of the Registrant's domain name and is an accredited .ee registrar.

The Registrar is responsible for identifying the Registrant of a domain name and for adding, removing or updating the specified DS records for each domain at the request of the domain's Registrant.

1 Delegation Signer (DS) record contains a fingerprint (shortened version) of a public key (DNSKEY). The DS record is used in the authentication of DNSKEYs in the lookup procedure using the chain of trust.

1.3.3. Registrants

A Registrant is the physical person or legal entity that has registered and holds a domain name. Registrants are responsible for generating and protecting their own DNSSEC keys, for signing the relevant data and for registering and maintaining corresponding DS records through a Registrar.

It is also the Registrant's responsibility to perform key rollover when keys are suspected of having been compromised or have been lost.

1.3.4. Relying party

The relying party is the entity that relies on DNSSEC signatures, such as DNSSEC validating resolvers and other applications. The relying party is responsible for maintaining the appropriate Trust Anchors. The relying party should stay informed of any relevant DNSSEC-related events in the .ee domain using the sources indicated in section 2.1.

1.3.5. Applicability

Each Registrant is responsible for determining an appropriate level of security for their domain. This DPS applies exclusively to the .ee top-level domain and describes the procedures, security controls and practices employed in the management of DNSSEC in the .ee zone.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC in the .ee domain and assess their own risk.

1.4. Specification administration

This DPS is updated as appropriate, such as in the event of significant modifications in systems or procedures that have a significant effect on the content of this document.

1.4.1. Specification change procedures

Changes to this DPS are either made in the form of amendments or with the publication of a new version. This DPS and any amendments to it are published at:

http://internet.ee/public/ee-dnssec-dps-eng.pdf

Only the most recent version of this DPS is effective.

The Registry reserves the right to amend this DPS without notification of amendments that are not designated as significant. It is in the sole discretion of the Registry to designate changes as significant, in which case notice will be provided. Any changes may be immediately effective upon publication.

2. Publication and repositories

2.1. Repositories

The Registry publishes DNSSEC-relevant information (in Estonian) on the Foundation's website at:

http://www.internet.ee/et/dnssec/

The electronic version of this DPS at this specific address is the official version.

Notifications relevant to DNSSEC in .ee are published on the Estonian Internet Foundation's webpage and additionally distributed using Twitter feed:

http://internet.ee/et/uudised/

https://twitter.com/Eesti_Internet

2.2. Publication of public keys

The Registry uses a split-key signing scheme and publishes the relevant Key Signing Keys (KSK[2]s), as follows:

- Directly in the root zone (only DS),

Estonian Interneti Foundation's website (DS and DNSKEY):
http://internet.ee/et/dnssec/dnssec-eisis/

2 KSK is a type of DNSSEC keys that are used for signing other keys in the zone. DS record contains a fingerprint (shortened version) of the KSK.

3. Operational requirements

3.1. Meaning of domain names

A domain name is a unique identifier, which is often associated with services such as web sites or e-mail. According to .ee Domain Regulation applying for registration under the top-level .ee domain is open to all private individuals and legal entities with a civil or corporate registration number, or who can be identified through the registry of a public authority, or an organisation with a designation similar to that of a public authority. The "first come, first serve" approach applies to the registration of new domain names under .ee, meaning that domain names are allocated in the order in which applications are received by the .ee registry.

3.2. Identification and authentication of child zone manager

It is the responsibility of the Registrar to identify and authenticate the Registrant through a suitable mechanism, as stipulated in the contract between the Registry and the Registrar.

3.3. Registration of delegation signer (DS) records

DNSSEC is activated by publishing at least one DS record for the child zone in the .ee top-level domain. Publishing the DS record establishes the chain of trust to the child zone.

The Registry accepts only DNSKEY records and the registry system generates and publishes DS records to the .ee zone. The Registry presumes that any syntactically correct DNSKEY record is valid and will not perform any additional verifications, such as making sure that the specified keys are part of the child's keyset.

The EPP interface is the only channel via which the Registry accepts DNSKEY records from the Registrars. Up to nine DNSKEY records per domain name can be registered. Estonian Internet Foundation's EPP specification is available on the Registry's webpage:

http://www.internet.ee/et/registripidajad/

http://www.internet.ee/en/registrars/

3.4. Method to prove possession of private key

The Registry does not conduct any verification checks with the aim of validating the Registrant as the holder of a certain private key.

3.5. Removal of DS resource records

A DS record is deregistered by sending an EPP request from the Registrar to the Registry. The removal of all DS records will deactivate the DNSSEC security mechanism for the zone in question.

3.5.1. Who can request removal of DS records

Only the Registrant, or the Registrant's representative as the Technical contact or the Administrative contact formally designated by the Registrant, has the authority to request the removal of DS records.

3.5.2. Procedure for removal request of DS records

The Registrant, or the Registrant's representative as the Technical contact or the Administrative contact formally designated by the Registrant, is assigned to perform the task of carrying out the removal. A Registrar may only do this on behalf of the Registrant.

Under normal circumstances, the zone is updated every ten minutes. According to the Registry's usual workload and procedures, the propagation delay is estimated in between 10 minutes and three hours.

Registrants will have to account for this timing when determining their signing scheme and when performing key rollovers.

3.5.3. Emergency removal request of DS records

If a Registrant is unable to perform the removal request through its Registrar, the Registry urges the Registrant to change Registrar and sends out a new authorisation code[3] that can be used to perform such a change of Registrar.

3 Authorisation code is defined in .EE Domain Regulations as the password used to identify the relationship between the registered Domain Name and the Registrant.

4. Facility, management and operational controls

4.1. Physical controls

The Registry is committed to implements physical perimeter protection, monitoring and access controls, as well as appropriate compensating controls, to reasonably ensure that the registry and signer systems are not tampered with, stolen or sabotaged.

4.1.1. Site location and construction

The Registry has established two geographically dispersed operation centres, at least 5 kilometres apart.

4.1.2. Physical access

All critical components are installed at both operation facilities. Entry is logged and the premises are continuously monitored.

4.1.3. Power and air conditioning

The datacentres provide a controlled, regulated and monitored operating environment. Each facility is dual-powered with underground transmission from at least two separate transformer stations. In addition, the facilities provide backup power from generators.

4.1.4. Water exposures

The equipment is reasonably protected from water exposures and the facilities provide detection mechanisms for flooding.

4.1.5. Fire prevention and protection

The facilities are equipped with fire detection and automatic fire extinguishers.

4.1.6. Media storage

All media containing production software and data, audit, archive, or backup information are stored within Estonian Internet Foundation facilities or in a secure off-site storage facility with appropriate physical and logical access controls.

4.1.7. Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner.

4.1.8. Off-site backup

Certain critical data is also securely stored using a third-party storage facility. The storage facility is geographically and administratively separate from the Registries' other operational facilities.

4.2. Procedural controls

4.2.1. Trusted roles

Trusted roles are held by individuals that are involved in the generation or use of private key material, delivery and publication of public keys, or able to affect the contents of the .ee zone. The trusted roles are:

- Systems Administrator, SA.
- User Manager, UM.
- Backup Manager, BM.
- Security Officer, SO.

Each role is associated with a specific task.

4.2.2. Number of persons required per task

The two-person rule is enforced for critical operations. Two individuals are required for user generation, key generation and HSM synchronisation and three individuals for HSM replacement operations.

4.2.3. Identification and authorization for each role

Only people who have a valid work contract with Estonian Internet Foundation or have signed a confidentiality agreement as well as an agreement to acknowledge their responsibilities with the .ee Registry may hold a trusted role.

4.2.4. Task requiring separation of duties

All critical operations including management of full life-cycle of the keys require separation of duties.

4.3. Personnel controls

4.3.1. Qualification, experience, and clearance requirements

Candidates seeking to assume any of the trusted roles must be able to demonstrate trustworthiness and appropriate qualifications.

4.3.2. Background check procedures

The evaluation of trustworthiness and background checking includes verifying:

- the candidates resume,
- employment history,
- references (proclaimed and others),
- documentation confirming the most relevant and completed education.

To qualify for any of the trusted roles, these controls must not reveal any significant discrepancies that indicate unsuitability.

4.3.3. Training requirements

For people acting in trusted roles relevant and requisite training regarding processes, procedures and technical administration of the systems is provided by the Registry.

4.3.4. Job rotation frequency and sequence

No regular job rotation is implemented. The roles change as the individuals holding them change their roles and positions within the Registry.

4.3.5. Sanctions for unauthorized actions

Severe negligence may lead to termination of employment and damage liability.

4.3.6. Contracting personnel requirements

Only persons that have been assigned to the specified Trusted Roles (4.2.1) can gain access to the signer systems. If necessary, tasks can be performed with the guidance of an external contractor. At no time is the contractor allowed to be the person performing the tasks on the system.

4.3.7. Documentation supplied to personnel

The .ee Registry and IT operations supply the documentation necessary for the individual employee to perform their tasks in a correct and secure manner.

4.4. Audit logging procedures

Logging is automatic and involves the continuous collection of audit information related to the activities in the registry system. Logs are replicated between two operation centres together with all the other data. Logs are backed up once a day.

This log information is primarily used in the monitoring of operations and for root-cause analysis in the event of a suspected security compromise or incident.

4.4.1. Types of events recorded

The following events are included in automatic logging:

- all types of operations involving an HSM, such as key generation, key activation, signing and exporting of keys,
- attempts of unauthorized operations,
- privileged operations.

4.4.2. Frequency of processing log

Logs are analysed through manual processes in case of alarms from monitoring system and in the events of suspected security compromise or incident.

4.4.3. Retention period for audit log information

Log information is stored on-line. Logs are kept in the system for at least 2 KSK rollover periods.

4.4.4. Protection of audit log

The logging systems are protected against unauthorised viewing.

4.5. Compromise and disaster recovery

4.5.1. Incident and compromise handling procedures

If an event leads to, or could lead to, a security compromise, an investigation is performed to determine the nature of the incident. If it is suspected that the incident has compromised a private key, the key rollover procedure will be performed.

4.5.2. Corrupted computing resources, software, and/or data

In the event that the Registry detects corruption of information systems or resources, the incident management procedures shall be put into operation. If required, the disaster recovery procedures and/or key rollover procedures are also enacted.

4.5.3. Entity private key compromise procedures

In the event of suspected or known compromise of private key material, an immediate rollover of keys shall be performed. The causes and effects of such event shall be analysed, which shall include the development and execution of a proper action plan with an aim to identify the cause, people responsible and changes necessary to avoid similar situations in the future.

4.6. Entity termination

If the Registry must discontinue DNSSEC for the .ee zone for any reason, and return to an unsigned position, this will take place in an orderly manner with public notification. If the operation of the .ee Registry is transferred to another party, Estonian Internet Foundation will take part in the transition in order to make it as smooth as possible.

5. Technical security controls

5.1. Key pair generation and installation

5.1.1. Key pair generation

All keys required for the continued operation of the .ee zone (in the foreseeable future) are pre-generated in advance once a year. The generation of the key material includes KSKs, ZSKs and all internal keys used for access control, key distribution and backup.

Key generation takes place in a hardware security module (HSM) that is managed by trained and specifically appointed personnel in trusted roles. The key generation process requires the presence of two System Administrators (SA).

5.1.2. Public key delivery

The public component of a KSK is exported from the signing system. Public keys are published as detailed in section 2.2.

5.1.3. Public key parameters generation and quality checking

Using a HSM provides reasonable assurance that key generation is being performed in a secure manner with respect to pseudo-random number generation and the quality checking of key parameters, such as exponent size and primality testing.

5.1.4. Key usage purposes

Keys generated for DNSSEC are never used for any other purpose or outside of the signing system.

5.2. Private Key protection and Cryptographic Module Engineering controls

All cryptographic operations involving the KSKs and ZSKs are performed in the protected memory of an HSM. No private keys are ever stored unprotected, or outside the HSMs.

5.2.1. Cryptographic module standards and controls

The signing system uses hardware security modules (HSMs) validated at FIPS 140-2 level 3.

5.2.2. Private key (m-of-n) multi-person control

Multi-person requirements to access key material is described in chapter 4.2

5.2.3. Private key backup

Private keys are only kept inside two HSMs located in separate geographical locations. Private keys are not otherwise backed up, escrowed, or archived.

5.2.4. Private key storage on cryptographic module

Private keys, while stored on persistent memory in the HSM, are always stored in encrypted form using a key, which resides in a tamper-proof and secure memory area of the HSM.

5.2.5. Private key archival

Private keys that are no longer used are not archived.

5.2.6. Private key transfer into or from a cryptographic security module

Synchronisation of key material between production HSM is done immediately after the key generation process over a secure and encrypted channel.

5.2.7. Method of activating private key

Private keys are activated with the help of signing software in the presence of persons with permission to generate keys as described in chapter 4.2.

5.2.8. Method of deactivating private key

Private keys are deactivated with the help of signing software.

5.2.9. Method of destroying private key

No efforts are made to destroy private keys after their operational period has expired. Keys are deleted by HSM Administrators.

5.3. Other aspects of key pair management

5.3.1. Public key archival

We only publish the public keys currently relevant to the operation of our zones. No archive of public keys past their revocation is available.

5.3.2. Key usage period

After the operational period of a key has elapsed and the key is superseded, the key enters into an expired state. Keys in the expired state will not be reused and are normally removed as part of the standard operating procedures for maintaining the signer system.

5.4. Activation data

Activation data consists of HSM access key cards, HSM access keys stored on these cards and associated PIN codes.

5.4.1. Activation data generation and installation

The access keys are generated and stored on the access key cards using the HSM.

5.4.2. Activation data protection

Every person performing a role in DNSSEC procedures is responsible for protection of activation data in their possession. On the suspicion of compromised activation data, it is revoked and replaced.

5.4.3. Other aspects of activation data

One set of activation data is kept in sealed, tamper evident package at a secure location geographically apart from both operation centers.

5.5. Computer security controls

All mission-critical systems are also continuously monitored for events relevant to the stability and security of the system.

5.6. Network security controls

The Registry's network infrastructure is logically divided into various security zones. Firewalls are used for limiting the source and nature of the communication between the different network segments and to critical components of the Registry system.

The firewall systems also implement the logging of communication, which is routed through them.

5.7. Time stamping

The Registry retrieves time from ee.pool.ntp.org. Time stamps are conducted using EET/EEST and are standardised for all log information and validity time for signatures.

5.8. Life cycle technical controls

5.8.1. System development controls

.ee's registry system is based on the FRED open source solution (http://fred.nic.cz/). The Registry has done some in-house modifications to the software to meet the needs of the Registry. All source code is stored in a version control system. The source code is regularly backed up.

6. Zone signing

6.1. Key lengths, key types and algorithms

The Registry uses a split-key signing scheme for signing the .ee zone. Key lengths and algorithms are of sufficient strength for their designated purpose and operational period.

Algorithms are standardised by the IETF, available to the public and resource efficient for all parties involved.

Currently, the RSA algorithm with a modulus size (key length) of 2048 bits is used for KSK and 1024 bits for ZSK.

6.2. Authenticated denial of existence

.ee uses NSEC3 to provide authenticated denial of existence, as specified in RFC 4034.

6.3. Signature format

Signatures are generated by encrypting SHA256 hashes (RSA/SHA256, RFC 3110).

6.4. Key rollover

ZSK rollover is carried out quarterly. KSK rollover is carried out as required.

6.5. Signature life-time and re-signing frequency

Resource Record Sets (RR Sets) are signed with a random validity period of between 14 and 28 days.

6.6. Resource records time-to-live

The time-to-live (TTL) for each DNSSEC Resource Record (RFC 4034) is specified as follows, in seconds:

RRtype	TTL
DNSKEY	3600
DS	3600
NSEC3	as SOA minimum (3600)
RRSIG	as RR (varies)

7. Legal matters

7.1. Fees

Currently .ee Registry does not charge any extra fees for DNSSEC from the Registrars. Any possible fees shall be regulated in the Registrar Contract concluded between the Registrar and the Registry.

7.2. Privacy of personal information

Personal data is treated in accordance with the Estonian Personal Data Protection Act (RT I, 30/12/2010, 11), section 8 of .ee Domain Regulation (Processing and Protection of Personal Data) and Annex 4 to the Registrar Contract (Personal Data Processing Guidelines).

7.3. Limitations of liability

Liability of the Registry for damages incurred by the Registrant is regulated by section 10 of .ee Domain Regulation (http://www.internet.ee/en/domains/).

Liability of the Registry for damages incurred by the Registrar is regulated by section 16 of the Registrar Contract concluded between the Registrar and the Registry (http://www.internet.ee/public/Registrar_contract_06.01.2014.pdf).