register.si

DNSSEC

Policy and Practice Statement

Academic and Research Network of Slovenia

Contents

1. Introduction

This document is **Arnes'** statement on security actions and practices that are applied in conjunction with DNS Security Extensions (DNSSEC) in **.si**, the Slovenian top-level domain. This document conforms with the draft RFC-draft DNSSEC Policy & Practice Statement Framework. The DPS is one of several documents relevant to the operation of the **.si** zone.

1.1 Overview

DNSSEC is a set of records and protocol modifications that enable the identification of DNS sources and also make it possible to ensure that content has not been modified during transfer, including mechanisms to verify the authentication of denial of existence. Resource records secured with DNSSEC are cryptographically signed and incorporate asymmetric cryptography in the DNS hierarchy, whereby trust follows the same chain as the DNS tree, meaning that trust originates from the root and is delegated in the same way as the ownership of a domain.

The purpose of this document is to enable local internet community to determine the level of trust they wish to grant to Arnes DNSSEC management. It details the procedures and policies employed by Arnes in operating DNSSEC services for the .si zone.

1.2 Document name and identification

Document title: DNSSEC Policy and Practice Statement (DPS)

Version: 1.0

Created: November 25, 2011

Updated: November 25, 2011

Published: December 1, 2011

1.3 Community and Applicability

This DPS is exclusively applicable to the top-level .si domain and describes the procedures and security controls and practices applicable for managing and employing keys and signatures involved in Arnes signing of the .si zone.

Currently Arnes does not accept the public keys of child zones in the form of Delegation Signer (DS) Resource Records for inclusion in the .si zone.

The following roles and delegation of liability have been identified.

1.3.1 Registry

Arnes manages the .si top-level domain and is responsible for the performance of the .si zone on the Internet.

Arnes is the single registry for .si. It is the responsibility of the registry to sign the .si zone and make its public keys (KSK and ZSK) available to the general public, while protecting the confidentiality of the private component of the keys.

1.3.2 Relying Party

Public key material published by the registry as a trust anchor can be used by anybody interested in using the zones as secure entry points for DNSSEC (e.g. validating resolvers). The relying party is responsible for configuring and updating the appropriate trust anchors. The relying party must also stay informed of any relevant DNSSEC-related events in the .si domain.

1.4 Specification Administration

This DPS will be periodically reviewed and updated, as appropriate.

1.4.1 Specification administration organization

Arnes (Academic and Research Network of Slovenia)

1.4.2 Contact Information

Arnes

Postal address

Jamova 39
1000 Ljubljana
Slovenia

Visiting address:

Tehnološki park 18
1000 Ljubljana
Slovenia

Phone: (+386) (0)1 4798800
Fax: (+386) (0)1 47998899
E-mail: register@register.si
Web: http://www.registry.si

1.4.3 Specification change procedures

Amendments to this DPS are either made in the form of amendments to the existing document or the publication of a new version of the

document. This DPS and amendments to it are published at http://www.registry.si/dnssec/.

Only the most recent version of this DPS is applicable.

2 Publication and repositories

2.1 Publication site

Arnes publishes DNSSEC-relevant information on http://www.registry.si/dnssec/.

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

2.2 Publication of key signing keys (KSK)

Arnes publishes KSK for the .si zone only directly in the root zone (DS). No other trust anchors or repositories are used.

3 Operational requirements

Currently Arnes does not accept the public keys of child zones for inclusion in the parent zone.

4 Facility, management and operational controls

4.1 Physical Controls

4.1.1 Site location and construction

Arnes operates two sites in Slovenia. These include server-rooms and cabinets in the Arnes offices in Ljubljana.

4.1.2 Physical access

All of our facilities have restricted access, limited to authorised personnel.

4.1.3 Power and air conditioning

All facilities have Uninterruptible Power Supply (UPS) capabilities and air conditioning. All sites have redundant systems in place in the event of a power failure, including the data centre at the Arnes office.

4.1.4 Water exposures

To avoid the risk of water exposure, all of our facilities are on elevated floors several meters above ground level.

4.1.5 Fire prevention and protection

All facilities have fire detectors and gas extinguishers.

4.1.6 Media storage

DNSSEC KSK key material is stored in a FIPS 140-2 Level 3 compliant HSM.

Access to the private part of the keys is only done as part of a backup.

Exporting private keys without encryption protection is not possible.

Backups of key material are stored encrypted on removable media stored inside of safe in a secure location.

4.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information is rendered unreadable before disposal.

4.1.8 Off-site backup

Backups of key material are stored encrypted on a USB token on a secure location. Backups of System Administrator and Security Officers tokens are stored in a safe in a secure location.

4.2 Procedural Controls

4.2.1 Roles

4.2.1.1 Trusted roles

Arnes has two different DNSSEC related roles:

- System administrator (SA)
- Security officer (SO)

4.2.1.2 Other roles

Witness may be present. Witness does not have access to the keys and does not have physical access or logical access to the operational facilities.

4.2.2 Number of persons required per task

For each DNSSEC ceremony at least 2 Security officers are physically required to be present.

Configuration changes and other administrative tasks on the HSM can only take place in the presence of 2 Security officers.

Configuration changes and other administrative tasks on the signer can only take place in the presence of 2 Security officers.

4.2.3 Identification and authentication for each role

Each person that is assigned to a role in the DNSSEC ceremony is added to the list of ceremony members.

4.2.4 Tasks requiring separation of duties

System administrators are trained technical staff and have no management function in Arnes. Without System Administrator no DNSSEC ceremony is possible. However, they cannot decide to start a DNSSEC ceremony without authorization from Security officers. Only emergency key-rollovers can be done by System Administrator.

Security officers fulfill a non technical role in Arnes (but do have technical knowledge on DNS and DNSSEC) and some of them have a senior management function in Arnes. They can authorize DNSSEC ceremonies but cannot execute them. For authorization at least one Security officer needs to be physically present and another Security officer (from senior management) needs to approve in writing.

4.3 Personnel Controls

4.3.1 Qualifications, experience, and clearance requirements

Every person that fulfills a role in the DNSSEC ceremony must

- have a permanent contract with Arnes
- work for Arnes for at least 3 months.

4.3.2 Background check procedures

For the trusted roles in Section 4.3.1, the following background checks are included:

- Candidate resume
- Previous employments
- Reference check
- Criminal convictions check

4.3.3 Training requirements

Every person that fulfills a role in the DNSSEC ceremony must be trained in the DNSSEC ceremony and have taken part in a DNSSEC training ceremony.

4.3.4 Contracting personnel requirements

No person outside of the specified Trusted Roles (4.2.1) can get 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.

4.3.5 Documentation supplied to personnel

The regular procedures for backup and restore are available to all personnel involved. If major alterations to those procedures are made, the personell will be informed accordingly.

4.4 Audit Logging Procedures

4.4.1 Types of events recorded

All DNSSEC ceremonies will be logged in a handwritten logbook, stored in a safe location.

All access to the signers and the signing software is logged in the syslog of these systems and systematically checked for anomalies.

4.4.2 Retention period for audit log information

Logs will be kept for the duration of at least two KSK rollovers.

4.5 Compromise and Disaster Recovery

4.5.1 Incident and compromise handling procedures

If an event leads to, or could lead to, a detected security compromise, an investigation is performed to determine the nature of the incident. If it is suspected that the incident has compromised the private component of an KSK, an emergency KSK roll-over procedure will be performed.

4.5.2 Corrupted computing resources, software, and/or data

In the event of corruption, the incident management procedures shall be initiated and appropriate measures shall be taken.

4.5.3 Entity private key compromise procedures

Upon the suspected or known compromise of a KSK follows assesment of the situation, development of an action plan and implementation of the action plan with approval from the Security Officer and the System Administrator.

An emergency roll-over of a compromised key will be communicated through the channels indicated in 2.1

4.6 Entity termination

If the registry must discontinue DNSSEC for the .SI zone for any reason and return to an unsigned position, this will take place in an orderly manner in which the general public will be informed. If operations are to be transferred to another party, the registry will participate in the transition so as to make it as smooth as possible.

5 Technical security controls

5.1 Key Pair Generation and Installation

5.1.1 Key pair generation

Key generation takes place in a hardware security module (HSM) that is managed by trained and specifically appointed personnel in trusted roles. These people are present during the entire operation.

In the first KSK/ZSK key generation keys for duration of 5 years will be generated. Key generation procedures are described in the 'Ceremony Guidebook'.

The entire key-generation procedure is logged, part of which is done electronically and part of which is done manually on paper by a Security officer.

5.1.2 Public key delivery

The public key is securely retrieved from the signer system and then published as detailed in section 2.2.

5.1.3 Key usage purposes

A key must only be used for one zone and cannot be reused.

5.2 Private key protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed in the hardware module and no private keys are ever found unprotected outside the secure DNS signing infrastructure.

5.2.1 Cryptographic module standards and controls

Arnes stores the DNSSEC keys in a FIPS 140-2 Level 3 compliant HSM.

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

No access to unencrypted keys is available in the entire system. Access to the signer system is specified in the Trusted Roles section.

5.2.3 Private key escrow

Not applicable.

5.2.4 Private key backup

Private keys are backed up on an encrypted media and stored in a secured location. Both the Security officer and System Administrator need to be present to make or restore a backup.

5.2.5 Method of activating private key

Private keys are activated by the signer software. ZSKs are activated automatically. KSKs are activated manually through the DNSSEC KSK rollover procedure.

5.2.6 Method of deactivating private key

Private keys are deactivated by the signer software. ZSKs are deactivated automatically. KSKs are deactivated manually through the DNSSEC KSK rollover procedure.

5.2.7 Method of destroying private key

Private keys are destroyed automatically by the HSM upon a command from the signer software which is generated automatically when keys are no longer needed.

5.3 Other Aspects of Key Pair Management

5.3.1 Key usage periods

KSKs are used for 1-3 years. ZSKs are used for 30 days

5.4 Activation data

The activation data consists of a set of PINs for the various safes and PGP-keys and passphrases. All activation data is personally used.

5.4.1 Activation data generation and installation

Each Security Officer and System Administrator is responsible for creating their own activation data conform the procedures described in the 'Ceremony Guidebook'.

5.4.2 Activation data protection

Each Security Officer and System Administrator is responsible for protecting their activation data as described in the 'Ceremony Guidebook' or otherwise in the best possible way. On the suspicion of compromised activation data, the operator must immediately change it.

5.5 Computer Security Controls

All critical components of the registry systems are placed in the organizations secure facilities in accordance with 4.1. Access to the servers operating systems is limited to individuals that require this for their work, meaning system administrators. All access is logged and is traceable at the individual level.

5.6 Network Security Controls

The registry has logically sectioned networks that are divided into various security zones with secured communications in-between. Logging is conducted in the firewalls. All sensitive information that is transferred over the communications network is always protected by strong encryption.

5.7 Timestamping

The registry utilizes its default NTP-policy for timestamping. Time stamps are conducted using UTC and are standardized for all log information and validity time for signatures.

5.8 Life Cycle Technical Controls

5.8.1 System development controls

The signing system is based on OpenDNSSEC and BIND. The Registry controls additional system development required for DNSSEC operation and evaluates the system prior to deploying it, in order to maintain the quality and security of .si DNSSEC Signing Service.

5.8.2 Security management controls

As security controls of .si DNSSEC Signing Service, the registry undertakes countermeasures such as entering/leaving controls, staff controls including training, operation controls including authority control and system controls including intrusion protection and virus protection.

5.8.3 Life cycle security controls

The Registry evaluates periodically whether the development of .si DNSSEC Signing Service is controlled under prescribed manner. Moreover, the Registry gathers information related to security, surveys technical trends, and evaluates/improves the system as necessary.

6 Zone signing

6.1 Key lengths and algorithms

RSA algorithms with a key length of 2048 bits are currently used for KSK and 1024 bits for ZSK.

6.2 Authenticated denial of existence

The registry uses NSEC3 opt out records as specified by RFC 5155.

6.3 Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA256.

6.4 Zone signing key roll-over

ZSK roll over is carried out every 30 days.

6.5 Key signing key roll-over

KSK roll-over is carried out on an annual basis by the double signature method described in RFC 4641.

6.6 Signature life-time and re-signing frequency

RR sets are signed with ZSKs with a validity period of fourteen days and are resigned every 3 days. Zone file generation and signing new records takes place every other hour.

6.7 Verification of zone signing key set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. This is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the .si SOA. The registry verifies that submited DS records have a corresponding DNSKEY records in the child zone prior adding it to the .si zone.

6.8 Verification of resource records

The registry verifies that all resource records are valid in accordance with the current standards prior to distribution.

6.9 Resource records time-to-live

DNSKEY: 3600 seconds
NSEC3: equal to minumum field of SOA record (RFC5155)
RRSIG: equal to TTL of RRset covered, 7200 in practice
DS: 7200 seconds
NSEC3PARAM: 3600 seconds