INTERNET
STIFTELSEN

DNSSEC Practice Statement (DPS)

Document type: Documentation
Creation date: 2010-04-19
Updated: 2021-10-18
Information owner: Nicklas Pousette, Head of DNS-Labs
Security class: Official
Approved by: Registry Services

Contents

1 Introduction

This document is the Swedish Internet Foundation's statement of security practices and provisions that are applied related to the operation of DNS Security Extensions (DNSSEC) for the top-level domains administered by the Swedish Internet Foundation.

This document conforms to RFC 6841: *A Framework for DNSSEC Policies and DNSSEC Practice Statements (DPS)*. This DPS is one of several documents relevant to the operation of the .se and .nu zones. One of the documents is the Swedish Internet Foundation's information security policy which may be found at https://internetstiftelsen.se/app/uploads/2019/02/iis-sak-0006-09-policy-informationssakerhet.pdf (Swedish)

Other relevant documents are the Swedish Internet Foundation's baseline security standards and the Swedish Internet Foundation's business contingency plan, which are not publicly available.

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 (DNS). DNSSEC provides a way for software to validate that DNS-data has not been tampered with or modified during transit. This is done by incorporating digital signatures and public key encryption into the DNS hierarchy. The trust follows the same distribution as the DNS tree, meaning that the chain of trust originates from the root zone, delegated in the same manner as the responsibility for a zone.

1.2 Document name and identification

Document title: DNSSEC Practice Statement (DPS)

Version: K

Created: April 19, 2010

Updated: 2020-11-11

1.3 Target group and applicability

The following parties, to which this document has applicability, have been identified.

1.3.1 **Registry**

The Swedish Internet Foundation is responsible for the administration and technical operation of the top-level domains .se and .nu and consequently the registration of domain names that identify underlying zones. This also implies that The Swedish Internet Foundation manages supplements, changes and removal of all data that is associated with a domain name.

The Swedish Internet Foundation is responsible for:

- generating the cryptographic key material used in DNSSEC
- protecting the confidentiality of the private component of the key pairs
- securely signing all authoritative DNS resource records in the applicable zone using DNSSEC with the designated keys.

Finally, the Swedish Internet Foundation is responsible for the secure export, registration and maintenance of DS resource records in the root zone, which establishes the chain of trust from the root zone to the applicable zone and enables validation of DNS records using the key for the root 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. The Registrar handles the registration, maintenance and management of the Registrants domain name and is a partner to The Swedish Internet Foundation. The Registrar is responsible for securely identifying the Registrant of a domain and for adding, removal or updating the specified DS records for each domain at the request of the domain's Registrant.

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.

It is also the Registrants responsibility to perform key rollovers when keys are suspected of having been compromised or lost.

1.3.4 Relying party

The relying party is the entity that relies on DNSSEC signatures, such as validating resolver operators and parties offering other corresponding applications. The relying party is responsible for the configuration and maintenance of the appropriate Trust Anchors. The relying party should stay informed of any relevant DNSSEC-related events 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 top-level domains administered by the Swedish Internet Foundation, and describes the procedures, security controls and practices employed in the management of DNSSEC in the applicable zone.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC for the applicable zone and based on this and other circumstances 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 significant effect on the content of this document. Such changes are announced through the sources indicated in section 2.1.

Responsible for the specification administration of the DPS is The Swedish Internet Foundations Chief Information Security Officer. The outermost responsibility for the approval and publishing lies with the PMA function within The Swedish Internet Foundation.

1.4.1 Specification administration organization

The Swedish Internet Foundation
Corp. Reg. No.: 802405-0190
https://internetstiftelsen.se

1.4.2 Contact information

DNSSEC PMA (Policy Management Authority):

The Swedish Internet Foundation
Box 90073
SE-120 07 Stockholm
SWEDEN

Telephone: +46 8 452 35 00

E-mail: dnssec-pma@internetstiftelsen.se

1.4.3 Specification change procedures

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

https://internetstiftelsen.se/app/uploads/2019/02/se-dnssec-dps-eng.pdf

Only the most recent version of this DPS is effective. Any changes will be approved by the PMA and may be effective immediately upon publication.

The Swedish Internet Foundation reserves the right to amend this DPS without notification for amendments that are not designated as significant from a security point of view. It is in the sole discretion of the PMA to designate changes as significant, in which case The Swedish Internet Foundation will provide notice. Such notices will be announced through the sources indicated in section 2.1.

2 Publication and repositories

2.1 Repositories

The Swedish Internet Foundation publishes DNSSEC-relevant information on the Swedish Internet Foundations website:

https://internetstiftelsen.se/en/tech-tools/recommendations-for-dnssec-deployment/

The DPS is published here:
https://internetstiftelsen.se/app/uploads/2019/02/se-dnssec-dps-eng.pdf

The electronic version of this DPS at this specific web address is the official version. Notifications relevant to DNSSEC in the applicable zone will be distributed using the following e-mail list service:

dnssec-announce@lists.iis.se (.se)

NU-dnssec-announce@lists.iis.se (.nu)

Information on how to subscribe or manage subscriptions is available at

https://lists.iis.se/mailman/listinfo/

2.2 Publication of key signing keys (KSK)

The Swedish Internet Foundation uses as split-key signing scheme (refer to section 6.1) and publishes the relevant Key Signing Keys (KSKs) for the applicable zones as follows:

- Directly in the root zone (only DS)

The Swedish Internet Foundation use the tools for secure electronic updating of data in the root zone as the IANA function within ICANN, from time to time provide for the purpose.

3 Operational requirements

3.1 Meaning of domain names

A domain name is a unique identifier, often associated with services such as web sites or e-mail. Applying for registration under the applicable top-level domains 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 organization with a designation similar to that of a public authority. Foreign applicants may use other methods of unique identification.

The “first come, first serve” approach applies to the registration of new domain names under applicable top-level domains, meaning that domain names are allocated in the order in which applications are received by the Swedish Internet Foundations registry services. Terms and conditions for registering domains are published for .se and .nu respectively at

.se: https://internetstiftelsen.se/app/uploads/2019/02/registreringsvillkor-se-eng.pdf

.nu: https://internetstiftelsen.se/app/uploads/2019/02/terms-and-conditions-nu.pdf

3.2 Identification and authentication of child zone manager

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

3.3 Registration of delegation signer (DS) records

To create a secure delegation for a child zone at least one DS record must be published in the parent zone. Publishing the DS records makes the signature chain to the child zone’s referred keys complete, thereby enabling DNSSEC validation.

There are two methods of provisioning DS records in the parent zone: via EPP from the registrar for the child zone or via publication of CDS record(s) in the child zone itself.

The Registry accepts DS records from the Registrars through the EPP interface, in the format specified in RFC 5910 (Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)). Up to six (6) DS records per domain name may be registered.

When using the EPP interface the Registry presumes that any syntactically correct DS record sent by the appropriate Registar (sponsoring client) is valid and will not perform any additional checking, such as making sure that the specified keys are part of the child zones keyset.

The Registry also implements automated DS record provisioning via CDS records in the child zone per RFC 8078/7344.

When using the CDS method several requirements must be fulfilled for the DS record to be provisioned. The following requirements will be independently verified from multiple locations:

- All name servers are reachable over TCP on all their IP addresses and deliver a consistent CDS RRset.
- The domain must have the state ACTIVE (control via whois).
- The domain must not be in Registry Lock (control via whois).
- The CDS RRset must not contain syntactic or semantic errors.
- If CDNSKEY records are published, they must match the published CDS records (RFC 7344 section 4).
- A child zone must have no more than 6 CDS records.

3.3.1 Initial DS Provisioning in a Child Zone

The Swedish Internet Foundation has implemented the RFC 8078 section 3.3. Accept after Delay policy with the following requirements:

- The CDS RRset must be consistently published for a minimum of 72 hours.
- All key algorithms and digest types in the CDS RRset must be supported by the Registry (see Section 8 Algorithms)
- DNSSEC validation would succeed using the CDS RRset as the DS RRset in the Parent zone.

3.3.2 Updates to DS records for a Child Zone

Subsequent changes to the DS may be achieved by use of CDS automation by the child according to RFC 8078 section 2.1 “Seeing” acceptance policy with the following requirements:

- DNSSEC validation would succeed using the CDS RRset as the new DS RRset in the Parent zone.
- DNSSEC validation of the CDS RRset must succeed.
- The inception time of the Resource Record Signature (RRSIG) for the CDS RRset is later than the last executed change of DS RRset.

3.3 Method to prove possession of private key

The Swedish Internet Foundation does not conduct any checks with the aim of validating the Registrant as the holder of a certain private key. The Registrar is responsible for conducting both the checks that are required and those that the Registrar furthermore considers necessary.

3.4 Removal of DS resource records

A DS record is removed by sending an EPP command from the Registrar to the Registry. The removal of all DS records will deactivate the DNSSEC security mechanisms for the child zone in question.

3.4.1 **Removal request**

The registrant has the authority to request removal of DS records. If the registrar serves as the name server provider for the registrant's domain name, the registrar has the right to, without the request of the registrant, remove these DS records. The Swedish Internet Foundation retains the right to remove DS records, if the Swedish Internet Foundation is of the view that they cause, or may cause, serious operational disruption. In cases where the name server operator publishes the necessary information for DNSSEC, the Swedish Internet Foundation may remove DS records for these domain names.

3.4.2 **Procedure for removal request**

The registrant or a representative designated by the registrant appoints the registrar to perform the task of carrying out the removal. A registrar that is not the name server operator of these domains may only do this on behalf of the registrant. When a removal command is received by the Swedish Internet Foundation via EPP it will be removed when the next version of the parent zone is published.

In cases where the registrar is the name server operator for the registrant's domain(s) the registrar has the right to, without a request from the registrant, add, remove or change DS records for these domains. Under normal circumstances, the zone is currently updated every hour. Subsequently, taking time-to-live (TTLs) and distribution time into account, the whole procedure of distributing new delegation information may take up to a maximum of 2,5 hours to complete, before being fully deployed. Registrants will have to account for this timing when calculating their signing scheme and when performing key rollovers.

3.4.3 **Removal via CDS**

It is possible to change the delegation for a child zone from secure to insecure by use of CDS automation according to RFC 8078 section 2.1 “seeing” acceptance policy with the following requirements:

- DNSSEC validation of the CDS RRset must succeed.

- The inception time of the Resource Record Signature (RRSIG) for the CDS RRset is later than the last executed change of DS RRset.

3.4.4 Emergency removal request

If a Registrant finds himself in a situation where it is impossible to perform the removal request through its current Registrar, the Swedish Internet Foundation urges the Registrant to change Registrar and are thereby sending an authorization code which can be used for such change.

The Swedish Internet Foundation has, according to the Registrar-Registry agreement the right to change, remove or reject the publishing of DS records if, and only if, they cause or might cause severe operational damages or disturbances to the applicable top-level domains administered by the Swedish Internet Foundation.

4 Facility management, administrative and personnel related controls

4.1 Physical controls

Based on continuous risk analysis and re-evaluation of threats, the Swedish Internet Foundation implements physical perimeter protection, monitoring and access controls, as well as appropriate compensating controls, to ensure that the registry and signer systems are not tampered with, stolen or sabotaged.

4.1.1 Site location and construction

The Swedish Internet Foundation has established two fully operational redundant and geographically dispersed operations facilities, at least 5 kilometers apart. All registry information is continuously updated through automatic replication between the facilities.

Both operations facilities implement comparable physical security controls in a multi-tiered structure, where the innermost tier is strictly controlled and monitored by the Swedish Internet Foundation.

4.1.2 Physical access

All critical components are available at both operational facilities. Physical access to the innermost tier is restricted to authorised personnel possessing the SA role (refer to section 4.2.1). Entry is logged, and the premises are continuously monitored.

4.1.3 Power supply and environment

The operational facilities provide a controlled, regulated and monitored operating environment. Each facility has redundant power with underground transmission from separate transformer stations. In addition, the facilities provide backup power from generators, capable of powering the facility for at least 24 hours.

4.1.4 Water exposures

The facilities are provided with detection mechanisms and protection for flooding.

4.1.5 Fire prevention and protection

The facilities are equipped with fire detection and automatic fire suppression mechanisms based on dry extinguishing agents. The facilities are provided with raised floor and each room in the facility constitutes an independent fire cell.

4.1.6 Media storage management

The Swedish Internet Foundation has implemented and enforces an information classification system, which defines the requirements imposed for storage of sensitive information. Storage devices carrying such information are stored in spaces with physical protection to the same level as the data centers.

4.1.7 Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner, either by the Swedish Internet Foundation or by a contracted party. This applies where appropriate for HSM's as well.

4.1.8 Off-site backup

Certain critical data is also securely stored using a third-party storage facility. Physical access to this storage facility is limited to authorized personnel possessing the SO role (refer to section 4.2.1). The storage facility is geographically and administratively separated from the Swedish Internet Foundation's other operational facilities. The storage facility has at a minimum the same level of physical protection as the operational facilities.

4.2 Procedural controls

4.2.1 Trusted roles

Trusted roles are held by individuals that are involved in the generation and use of private key material as well as the delivery and publication of the public key material of the applicable zones. The trusted roles are:

1. Systems Administrator, SA
2. Security Officer, SO

At any given time, there must be at minimum two individuals within the organization appointed per trusted role. A single individual may not hold more than one trusted role at a time.

4.2.2 Number of persons required per task

Separation of duties and roles are enforced for critical operations. These tasks require one individual from each role to participate in the process.

4.2.3 Identification and authorization for each role

Only people who have signed a non-disclosure agreement, and an agreement to acknowledge their responsibilities with the Swedish Internet Foundation may hold a trusted role.

4.2.4 Tasks requiring separation of duties

All critical HSM[1] operations are required to be performed on-location, in one of the operational facilities. Duties are segregated by the Security Officer not having exclusive physical access to the operational facilities, while the System Administrator are not allowed access to the information required to activate the HSM. Furthermore, the responsibility for export and publishing of the public key components of the KSK is distributed in such a way that only the SO has authority to register the key material, while only the SA has the authority to initiate key generation (see Section 5.1.2).

[1] HSM - Hardware security module

Critical operations therefore include activation of the HSM, key administration and export and publishing the public component of the KSK.

The operations may be carried out only in the presence of authorized individuals.

4.3 Personnel controls

4.3.1 Qualifications, experience, and clearance requirements

Candidates seeking to assume any of the trusted roles must be able to demonstrate trustworthiness and possession of appropriate qualifications. Such suitability assessment is made by the Chief Information Security Officer before such a person is assigned the responsibility conferred by each role.

4.3.2 Background check procedures

The evaluation of trustworthiness and background checking are carried out by both the security and the HR functions at the Swedish Internet Foundation. This process includes verifying:

- the candidate's résumé
- employment history
- references (proclaimed and others)
- documents confirming the most relevant and completed education.

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

4.3.3 Training requirements

The Registry provides the relevant and requisite training regarding processes, procedures and technical administration of the systems relevant for each trusted role. This training includes:

- the Swedish Internet Foundation operations in general
- the role's authority and areas of responsibility
- domain-name administration in general
- basic technical proficiency in DNS and DNSSEC (for Security officers – SO)
- advanced technical proficiency in DNS and DNSSEC (for System Administrators – SA)
- basic understanding of information security management
- administration, procedures and checklists
- procedures and exercises in incident handling

- procedures and exercises in crisis management and disaster recovery.

4.3.4 Job rotation frequency and sequence

The responsibility for conducting critical operations according to section 4.2.4 is rotated on each occasion between the individuals holding the trusted roles. In the daily operation all the designated system administrators are involved and responsibility for standby is rotated among them according to a predetermined schedule.

4.3.5 Sanctions for unauthorized actions

Sanctions resulting from unauthorized actions are regulated in the responsibility and non-disclosure agreements. Severe negligence may lead to termination of employment and damage liability.

4.3.6 Contracting personnel requirements

In certain circumstances, the Swedish Internet Foundation may need to use contractors as a supplement to full-time employees. These contractors sign the same type of responsibility and non-disclosure agreements as full-time employees.

Contractors who have not been subject to a background check and training, and thus are not qualified for a trusted role, may not participate in the activities indicated in section 4.2.4.

4.3.7 Documentation supplied to personnel

The Swedish Internet Foundation supplies the documentation necessary for the individual employee to perform their tasks in a secure and satisfactory manner. This includes systems documentation, manuals, operating procedures and checklists for all aspects of the operating environment.

4.4 Audit logging procedures

Logging is automatic and involves the continuous collection of audit information related to the activities in the registry system. This log information is used in the monitoring of operations, for statistical purposes and for root-cause analysis in the event of a suspected security compromise or incident.

Audit information, collected for the purpose of internal compliance audit, also includes the journals, checklists and other paper documents that are vital to security and that are required to verify an audit trail.

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 for remote access, successful and unsuccessful
- privileged operations

- entrance into a facility.

4.4.2 Frequency of processing log

Logs are continuously analyzed through automated and manual processes. Specific reviews are conducted on certain events, including key generation, privileged operations, system reboots and detected anomalies.

4.4.3 Retention period for audit log information

Log information is stored on-line in log collecting systems for at least 60 days. Thereafter, the log information is archived for a minimum of five years.

4.4.4 Protection of audit log

All electronic log information is stored at both operational facilities. The logging systems are protected against unauthorized viewing, manipulation and destruction of log data.

Audit information relating to the physical access control system is stored outside of the control of the SA role.

4.4.5 Audit log backup procedures

All electronic log information is backed up on a monthly basis and stored separately from the system in a secure location. All paper-based log information is stored in a fireproof safe adjacent to the facilities.

4.4.6 Audit log collection system

Electronic log information is transferred in real-time to the collection systems; one for each facility. Manual logs are recorded on paper and the original documents are archived in a fireproof safe.

4.4.7 Vulnerability assessments

All anomalies discovered in the audit log information are investigated and analyzed for potential vulnerabilities.

The Swedish Internet Foundation is also a member of several organizations and communities where security-related information is collected, analyzed and confidently shared among the stakeholders. This information is continuously evaluated for new threats.

4.5 Compromise and disaster recovery

4.5.1 Incident handling procedures

Any actual or perceived event of security-critical nature that has led to or could have led to a security compromise is defined as an incident.

All incidents are managed in accordance with the Swedish Internet Foundations incident handling procedures. The incident handling procedures includes conducting a root-cause analysis, to formally identify the nature and impact of the event, in order to identify what measures are required to prevent the event from reoccurring (or to limit its consequences). The procedures also provide means of escalation and reporting of incidents to the appropriate authority within the Swedish Internet Foundation.

An incident which involves the suspicion of a private key compromise, leads to the immediate rollover of keys in accordance with the procedures indicated in section 4.5.3.

4.5.2 Corrupted computing resources, software, and/or data

In the event the Swedish Internet Foundation detects corruption of information systems or resources, the incident handling procedures shall be initiated, and appropriate measures be taken. If required, the disaster recovery procedures are also enacted.

4.5.3 Entity private key compromise procedures

If the confidentiality of a private key is suspected of having been compromised, or if the key may have been misused, the following key rollover procedures will be initiated:

- If a zone signing key (ZSK) is suspected of having been compromised, the Swedish Internet Foundation will immediately stop using that key. If necessary, a new ZSK will be generated and the old key will be removed from the key set as soon as its signatures have expired or safely been discarded from the resolvers, whichever occurs first. If a ZSK is suspected of having been completely compromised and revealed to unauthorized parties, this will be notified through the appropriate channels as indicated in section 2.1.

- If a key signing key (KSK) is suspected of having been compromised, a new key will be generated and put into immediate use, in parallel with the old key. The old KSK will remain in place and be used to sign the key set until it can be considered sufficiently safe to remove the key, considering the risk for disruptions in relation to the risk presented by the compromised key. A KSK rollover is always announced through the channels indicated in section 2.1.

If the KSKs (and possibly also the ZSKs) are lost completely, new keys will be generated at the earliest convenient occasion and included in the key set. In the meantime, it may occur that the applicable zones will be unsigned until all the systems are recovered, and new DS records have been published in the root zone. During this time all the scheduled ZSK rollovers will be postponed.

4.5.4 Crisis management and Business continuity

The Swedish Internet Foundation has prepared a contingency plan ensuring that mission-critical operations can be relocated between the operational facilities within four hours. Spare components for critical hardware are available, if needed.

The contingency plan also includes capability to resume other mission-critical services and systems at any of the alternative locations. The plans are regularly tested, and the results are recorded and subsequently evaluated.

The contingency plan includes:

- roles and responsibilities in the activation of crisis management procedures

- how and where the crisis management shall convene
- activation of backup IT operations
- appointment of a Task Manager
- criteria and procedures for resuming normal operations.

4.6 Discontinuation of DNSSEC

If the Swedish Internet Foundation must discontinue DNSSEC for the applicable zones for any reason, and go to an unsigned zone, this will take place in an orderly manner with public notification.

4.7 Transfer of operational responsibility

If the operation of the applicable zone is transferred to another party, the Swedish Internet Foundation will assist in the transition 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 applicable zone (in the foreseeable future) are pre-generated in advance through a formal key ceremony. The generation of the key material includes KSKs, ZSKs and all internal keys used for access control, key distribution and backup.

During the initial key ceremony, the HSM master keys are first generated. After they have been safely and securely installed in each device designated for production, the application keys (KSKs and ZSKs) are generated and securely distributed using the master key.

When new keys are required to be generated, this will take place through a scheduled key ceremony on-location at one of the operational facilities. Keys will be generated and backed-up to the backup-module (refer to section 5.2.4).

Key generation and distribution require at the minimum one SA and one SO working in unison throughout the whole process.

The entire key-generation procedure is logged to produce an audit-trail of the events, part of which is recorded electronically and part of which is recorded manually on paper by the SO and verified by the SA.

5.1.2 Public key delivery

The public component of a KSK is exported from the signing system as part of the key ceremony. After exporting it is verified by both SO and SA. The SO is responsible for publishing the public component of the KSK in a secure manner as per section 2.2. The SA is responsible for checking that the published keys are the same as those exported and scheduled for production and that they are working as expected.

5.1.3 Public key parameters generation and quality checking

The usage of a validated hardware devices, HSM's (refer to section 5.2.1), provides reasonable assurance that the key generation is being performed in a secure manner with respect to among other things pseudo-random number generation and 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. The signing system and HSMs are not used for any other purpose than DNSSEC.

A signature made by a DNSSEC key has a maximum validity period of 14 days for both the ZSK and KSK, with an inception time of one hour from the time when the signatures are produced.

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 outside the HSMs.

5.2.1 Cryptographic module standards and controls

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

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

The Swedish Internet Foundation does not enforce multi-person control for private key operations. Refer to section 4.2.4 for compensating controls through separation of duties in the HSM activation process.

5.2.3 Private key escrow

The Swedish Internet Foundation does not escrow private keys.

5.2.4 Private key backup

During the key ceremony, the pre-generated application keys are copied to two separate backup-modules with characteristics similar to the HSM itself. The backup modules are stored separately in safes accessible by the SAs, while the activation data for the backup module is stored in the secure storage facility (refer to section 4.1.8), only accessible by the SO.

5.2.5 Private key storage on cryptographic module

Private keys, while stored in 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.

5.2.6 Private key archival

Private keys that are no longer used are not archived.

5.2.7 Private key transfer into or from a cryptographic security module

During the initial key ceremony, an HSM master key is generated and distributed to the designated devices set up for production. The distribution is performed physically using a separate set of hardware token devices with necessary activation keys. After this key distribution has been completed, the tokens are stored in a safe accessible only by the SO. Henceforth, this HSM Master Key is used to protect application keys during key distribution between the devices via the Swedish Internet Foundation’s internal communication infrastructure.

5.2.8 Method of activating private key

To activate the HSM and its private keys a SA is giving a SO access to the equipment. The HSM and its private keys are activated by the SO demonstrating possession of the activation data. This data is stored on a hardware token device stored in a safe accessible only by the SO.

5.2.9 Method of deactivating private key

The HSM is locked if it is turned off, rebooted or loses power for more than two hours.

5.2.10 Method of destroying private key

No efforts are made to destroy private keys after their operational period has expired and they have become invalid. After their usage period they are removed from the signing system to avoid accidental reuse but may still be available in the private key backup module.

5.3 Other aspects of key management

5.3.1 Public key archival

Public keys are archived in the same manner as other information relevant to the audit trail, such as log data.

5.3.2 Key usage period

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

5.4 Activation data

The activation data is stored on a hardware token device which is connected to the HSM during activation.

5.4.1 Activation data generation and installation

The activation data is created by machine and then stored in the hardware token device used to activate the HSM. Installation of activation data is done through physical interconnection between the HSM and the hardware token device.

5.4.2 Activation data protection

Each SO is responsible for maintaining the chain of custody of the hardware token device while in use in accordance with current rules and procedures. When the hardware token device is not in use it is stored in a safe accessible only by the SO. If the activation data is suspected of having been compromised or lost, it is the SO's responsibility to take immediate action to have it revoked and replaced.

5.5 Computer security controls

The Swedish Internet Foundation has implemented a centralized role-based authorization and authentication system, which enables fine-grained discretionary access controls and automated reporting of assigned authorizations. Logging is being done at a level which enables individual accountability for all (privileged) operations in each subsystem.

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 Swedish Internet Foundations network infrastructure is logically divided into various security zones. Firewalls are used for managing the communication between the different network segments and to critical components of the registry system.

All communication which is routed through the firewall systems is logged.

All information which may be of sensitive nature, and is being transferred over the communications network, is always protected using strong encryption mechanisms.

5.7 Time stamping

The Swedish Internet Foundation uses a combination of time sources, which is Rise[2] and Amazon Time Sync Service.

5.8 Life cycle technical controls

5.8.1 **System development controls**

The Swedish Internet Foundation registry system is developed in-house. All source code is stored in a protected version control system. The source code archive is regularly backed up and copies are stored separately in a fireproof safe.

The Swedish Internet Foundation's development model is based on industry standards and includes:

- fully functional specification and documented security requirements
- documented architectural design based on a natural modularization of the system
- continuous assessments for minimizing complexity
- systematic and automated testing and regression tests
- continuous improvement of quality and accuracy of produced software through tight integration with the quality management system (conforming to ISO 9001:2015).

5.8.2 **Security management controls**

The Swedish Internet Foundation's Information Security Management System has been assessed and certified as compliant with the requirements of SS-ISO/IEC 27001.

[2] https://www.sp.se/en/index/services/time_sync/ntp/sidor/default.aspx

The Swedish Internet Foundation has established a Baseline Security Standard, which forms the basis of the minimum level of security mitigations for the Registry Services. The Baseline Security Standard is revisited and updated regularly based on security incident reports, conducted security audits (refer to section 7) and recurring risk analysis and threat modeling workshops. The maintenance of the Baseline Security Standard follows the PDCA (Plan-Do-Check-Act) method as outlined in ISO/IEC 27001, and forms together with the Swedish Internet Foundations Information Security Policy the basis for the information security management.

5.8.3 Change management security controls

The Swedish Internet Foundation is using work models that include selected parts from adequate standards like ISO/IEC 20000 and parts from modern work models for continuous integration and continuous delivery in order to manage and control changes in the IT environment.

6 Zone signing

6.1 Key lengths, key types and algorithms

The Swedish Internet Foundation uses a split-key signing scheme in signing of the applicable zone. The splitting is made through key signing key (KSK) and zone signing key (ZSK). Key lengths and algorithms for each key shall be of sufficient strength for their designated purpose and operational period.

Only IETF standardized algorithms shall be used by the applicable top-level domains.

6.1.1 **Current configuration .se top level domain**

For the .se top level domain the RSA algorithm with a modulus size (key length) of 2048 bits is used for both KSK and ZSK.

6.1.2 **Current configuration .nu top level domain**

For the .nu top level domain the ECDSA curve P-256 with a modulus size of 256 bits is used for both KSK and ZSK.

6.2 Authenticated denial of existence

NSEC is used to provide authenticated denial of existence, as specified in RFC 4034.

6.3 Signature format

6.3.1 **Signature format: .se top level domain**

Signatures are generated by encrypting SHA256 hashes (RSA/SHA256 as specified in RFC 6594).

6.3.2 **Signature format: .nu top level domain**

Signatures are generated over a cryptographic condensate by ECDSA Curve P-256 with SHA-256, mnemonic ECDSAP256SHA256 (as specified in RFC 6605).

6.4 Key roll-over

ZSK rollover is carried out every 84th day.

KSK rollover is carried out as required.

6.5 Signature lifetime and re-signing frequency

Resource Records (RR Sets) are signed with a random validity period of between 12 and 14 days. Signatures which expire within 10 days will be refreshed once an hour (UTC(SP)).

6.6 Verification of resource records

To ensure valid signatures and integrity of the DNSKEY record, a set of checks are automatically run at each signing occasion. These controls include verification of signatures using the Delegation Signer (DS) records registered with IANA for the Root Zone, as well as verification of time and date. Zone information which does not pass the automatic checks will put the production of a new zone file on hold and become flagged for manual intervention and troubleshooting. The production of a new zone file is on hold until the troubleshooting and error-handling is completed.

Furthermore, verification of the validity of all resource records are made in accordance with the current standards prior to distribution.

6.7 Resource records time-to-live

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

RR type	**TTL**
DNSKEY	3600
DS	3600
NSEC/NSEC 3	as SOA minimum (7200)
RRSIG	same as TTL for RR (varies)

7 Compliance audit

To verify that the controls are working and are efficient the Swedish Internet Foundation conducts both internal and external audits of the registry system.

7.1 Frequency of entity compliance audit

Audits are conducted both regularly and when needed as deemed required by the Swedish Internet Foundation. Circumstances which may require an audit include among other things:

- if more than 24 months have elapsed since the last audit
- if recurring discrepancies or incidents are brought to the Swedish Internet Foundations attention
- if significant changes are made at the management, organizational or processes that supports the Swedish Internet Foundation's registry operations.

7.2 Qualifications of the auditor

The auditor shall be able to demonstrate proficiency in information security auditing, IT security, DNS and DNSSEC.

7.3 Auditor's relationship to the audited party

For external audits, an independent auditor shall be appointed to conduct and lead the audit. If necessary, the auditor may engage technical experts with background experiences from the Swedish Internet Foundation, or organizations affiliated with the Swedish Internet Foundation.

7.4 Topics covered by audit

Audits of the Registry System are conducted using the governing documentation.

These documents are primarily the Swedish Internet Foundation's Information Security Policy and Baseline Security Standard together with documented directions and procedures for the operations.

7.5 Actions taken as result of deficiency

Any deficiencies discovered during the audit will be directly communicated by the auditor to the top management of the Swedish Internet Foundation. The severity of each discrepancy will be determined with input from the auditor. An appropriate correction plan will be prepared and implemented with the urgency deemed necessary.

7.6 Communication of results

The auditor shall submit the results of the audit as a written report to the Swedish Internet Foundation within 30 days following the completion of the audit. The auditing reports are not made public.

8 Algorithms Supported by the Registry

The following algorithms are accepted by the Registry when validating CDS records provided by a child zone.

Key Algorithms

Algorithm	
5	RSASHA1
7	RSASHA1-NSEC3-SHA1
8	RSASHA256
10	RSASHA512
13	ECDSAP256SHA256
14	ECDSAP384SHA384
15	ED25519
16	ED448

Digest Algorithms

Algorithm	
2	SHA-256
4	SHA-384

Legal matters

8.1 Fees

Any fees associated with DNSSEC must be regulated by the agreement between registry and registrar.
https://registrar.iis.se/97

8.2 Privacy of personal information

Personally identifiable information (PII) are treated in accordance with the EU General Data Protection Regulation and any agreements the Swedish Internet Foundation has entered into which regulates the protection and use of PII. The Swedish Internet Foundation's policy on privacy is available at

https://internetstiftelsen.se/app/uploads/2019/02/dataskyddspolicy-internetstiftelsen.pdf

8.3 Limitations of liability

The Swedish Internet Foundation's liability for damages to the Registrar is regulated by the Registrar Registry agreement.

https://registrar.iis.se/97

The Swedish Internet Foundations liability for damages to Registrants is regulated by the Swedish Internet Foundations current General Terms and Conditions that are found at

https://internetstiftelsen.se/en/how-to-register-a-domain-name/terms-and-conditions-for-se-and-nu-domains/

Document control

Document information and security

CONDUCTED BY	RESPONSIBLE FOR FACTS	RESPONSIBLE FOR DOCUMENT
CHIEF SECURITY OFFICER	CHIEF SECURITY OFFICER	CHIEF SECURITY OFFICER

SECURITY CLASSIFICATION	FILE NAME
OPEN	DNSSEC PRACTICE STATEMENT.DOCX

Approved by

DATE	NAME	FUNCTION
APRIL 19, 2020	ANNE-MARIE EKLUND LÖWINDER	CHIEF SECURITY OFFICER

Revisions

DATE	VERSION	NAME	DESCRIPTION
APRIL, 19	A	AMEL	FINAL VERSION
NOVEMBER, 19	A	AMEL	UPDATED, ITAR REFERENCE REMOVED
MAY 20, 2011	B	AMEL	UPDATED 6.6 DUE TO CHANGES IN .SE'S SIGNING POLICY.
SEPTEMBER 8, 2011	C	AMEL	CLARIFICATION 4.4.7 AND 5.1.4
APRIL 12, 2012	PD1	AMEL	CORRECTION OF GRAMMAR AND BASED ON DPS FRAMEWORK DRAFT
MAY 21, 2012	PD2	AMEL	COMMENTS FROM .SE REGISTRY
AUGUST 17, 2012	D	AMEL	FINAL VERSION
FEBRUARY 14, 2013	E	AMEL	UPDATED DUE TO REVISED KASP AND COMMENTS FROM IT OPERATIONS.FE
FEBRUARY 1, 2015	FA1	AMEL	UPDATED TO HARMONIZE DPS .NU, CHANGED INFORMATION ON EMERGENCY KEY, CORRECTION OF RFC REFERENCE AND OTHER DETAILS.
FEBRUARY 25, 2015	F	AMEL	FINAL VERSION
JUNE 10, 2015	G	AMEL	UPDATING 3.5.2+ NAME CHANGE .SE -> IIS
NOVEMBER 22, 2017	PH1	AMEL	UPDATING DUE TO EXTENDED KEY LENGTH AND ALGORITHM ROLLOVER
DECEMBER 12, 2017	H	AMEL	ACCEPTED BY THE DNS TEAM (ULRICH) APPROVED
MAY 23, 2018	PI	AMEL	REVISION DUE TO GDPR
MAY 25, 2018	I	AMEL	NEW VERSION PUBLISHED

JULY 11, 2019	PJ1	AMEL	UPDATE WITH CURRENT ALGORITHMS IN SECTION 6. UPDATES DUE TO NEW DOMAIN NAME FOR INTERNETSTIFTELSEN AND CHANGED URL:S
OCTOBER 2019	PJ2	TC	FEEDBACK AND UPDATES
MARCH 2020	PJ3	AMEL/ROG	MERGING .SE AND .NU DPS INTO ONE SINGLE DOCUMENT, ENGLISH ONLY
MARCH 2020	PJ4	AMEL	UPDATED WITH COMMENTS FROM REGISTRY SERVICES
APRIL 2020	J	AMEL	ACCEPTED BY THE DNS TEAM. APPROVED BY REGISTRY SERVICES. NEW VERSION PUBLISHED.
NOVEMBER 2020	K	AMEL	ROLLOVER FROM NSEC3 TO NSEC IN .NU
OCTOBER 2022	L	ROG/JOHAN STENSTAM	NEW FUNCTIONALITY FOR CDS/CDNSKEY