Security

Documentation

DNSSEC
Practice Statement (DPS) .nu

Document control

Document information & 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-NU.DOCX

Approved by

DATUM	NAME	FUNCTION
	TORBJÖRN CARLSSON	OWNER OF SERVICE
2015-02-25		

Revisions

DATUM	VERSION	NAME	DESCRIPTION
APR 22, 2013	PA1	AMEL	FIRST VERSION OF DPS FOR .NU.
MAY 7, 2013	PA2	AMEL	ADJUSTMENTS AFTER MEETING WITH REGISTRY AND IT OPERATIONS.
MAY 20, 2013	PA3	AMEL	SUPPLEMENTATION FOR UNANSWERED QUESTIONS.
JULY 19, 2013	PA4	AMEL	SUPPLEMENTATION AFTER REFERRAL.
SEPTEMBER 2, 2013	A	AMEL	FINAL VERSION
OCTOBER 7, 2013	B	AMEL	UPDATED
2015-01-07	PC1	AMEL	REVISION, CHANGING RFC REFERENCE
2015-01-08	PC2	AMEL	REVISED, COMMENTS FROM REGISTRY
2015-02-24	PC3	AMEL	COMMENTS FROM OPERATIONS
2015-02-24	C	AMEL	FINAL VERSION
2015-06-10	D	AMEL	UPDATING 3.5.2, NAME CHANGE .SE->IIS
2018-05-23	PE1	AMEL	UPDATED DUE TO GDPR
2018-05-25	E	AMEL	PUBLISHED
2018-10-17	PF1	ROGER MURRAY	CHANGES DUE TO ALGORITHM ROLL
2018-10-22	F	AMEL	PUBLISHED

Contents

1 Introduction

This document is .IIS statement of security practices and provisions that are applied in relation to the operation of DNS Security Extensions (DNSSEC) in the top-level domain .nu. 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 .nu zone. Other relevant documents are IIS baseline security standard, IIS information security policy and IIS business contingency plan, which are for internal use only, and 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: .nu DNSSEC Practice Statement (DPS)
Version: F
Created: August 15, 2013
Updated: 2018-10-22

1.3 Target group and applicability

The following parties to which this document has applicability have been identified. The relation between the Registry and a Registrar is regulated in the Registry-Registrar Agreement, which can be found in its entirety at:
https://registrar.iis.nu/97

1.3.1 Registry

SE (The Internet Infrastructure Foundation) is responsible for the top-level domain .nu and the management of the .nu registry, and consequently the registration of domain names that identify underlying zones in the .nu zone. This also means that IIS manages supplements, changes and the removal of all data that is associated with a .nu domain name.

Additionally, the IIS is responsible for:

- generating cryptographic key material,
- protecting the confidentiality of the private component of the key material, and
- securely signing all authoritative DNS resource records in the .nu zone using DNSSEC and the keys attached to it.

Finally, the registry 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 .nu zone and enables validation of DNS records in .nu 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 considered as a IIS partner.

The Registrar is responsible for securely identifying the Registrant of a domain and for adding, removing 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 through a Registrar.

It is also the Registrants 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 providers of validating resolvers and parties offering other corresponding applications. The relying party is responsible for the configuration and maintaining of the appropriate Trust Anchors (TAs, according to RFC 4033). The relying party should stay informed of any relevant DNSSEC-related events in the .nu 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 .nu top-level domain and describes the procedures, security controls and practices employed in the management of DNSSEC in the .nu zone.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC in the .nu domain 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 IIS Chief Information Security Officer. The outermost responsibility for the approval and publishing lies on the PMA function within IIS.

1.4.1 Specification administration organization

IIS (The Internet Foundation in Sweden).

1.4.2 Contact information

DNSSEC PMA (Policy Management Authority):
IIS (The Internet Foundation in Sweden)
Box 92073
SE-120 07 Stockholm
SWEDEN
Telephone: +46 8 452 35 00
Fax: + 46 8 452 35 02
Corp. Reg. No.: 802405-0190
https://www.iis.se
dnssec-pma@iis.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. This DPS and any amendments to it are published at: https://www.iis.se/docs/DNSSEC-Practice-Statement-DPS-nu.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.

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

2 Publication and repositories

2.1 Repositories

IIS publishes DNSSEC-relevant information on IIS website at:

https://www.iis.se/english/domains/tech/dnssec/

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

nu-dnssec-announce@lists.iis.se

Information on how to subscribe or manage subscriptions is published at http://lists.iis.se/mailman/listinfo/nu-dnssec-announce

2.2 Publication of key signing keys (KSK)

IIS uses a split-key signing scheme (refer to section 6.1) and publishes the relevant Key Signing Keys (KSKs) for the .nu zone as follows:

- Directly in the root zone (only DS).

IIS use the tools for secure electronic updating of data in the root zone as the IANA, 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 top-level .nu 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 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 .nu, meaning that domain names are allocated in the order in which applications are received by the IIS registry. Terms and conditions for registering .nu domains are published at https://www.iis.se/english/domains/nu/terms-and-conditions/

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 IIS and the Registrar.

3.3 Registration of delegation signer records (DS records)

DNSSEC is activated by publishing at least one DS record for the child zone in the .nu top-level domain. Publishing the DS record establishes the chain of trust to the child zones referred keys. The Registry presumes that any syntactically correct DS record 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 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 can be registered.

3.4 Method to prove possession of private key

IIS 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.

3.5 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 Authority of removal request

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 removal of DS records.

3.5.2 Procedure for removal request

Only 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. When a removal request is received by IIS via EPP, it takes no longer than until the next zone generation until the amendment is introduced into the zone file.

In cases where the Registrar is the name server operator for the Registrant's domain(s) the Registrar has the right, without a request from the Registrant, to add, remove or change DS records for these domains.

Under normal circumstances, the zone is currently updated every two hours. 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 five hours to complete, before being fully deployed. Registrants will have to account for this timing when determining their signing scheme and when performing key rollovers.

3.5.3 Emergency removal request

If a Registrant finds himself in a situation where it is not possible to perform the removal request through its current Registrar, IIS urges the Registrant to change Registrar and are thereby sending an authorization code which can be used for such change.

IIS has according to the Registry-Registrar agreement the right to change, remove or reject the publishing of DS records if they, according to the judgment of IIS, causes or might cause severe operational damages or disturbances to IIS.

4 Facility, management and operational controls

4.1 Physical controls

Based on continuous risk analysis and reevaluation of threats, IIS 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

IIS has established two fully operational redundant and geographically dispersed operation centers, at least 5 kilometers apart. The redundant facility contains a complete set of the Registry's critical systems. 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 IIS.

4.1.2 Physical access

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

4.1.3 Power and air conditioning

The data centers provide a controlled, regulated and monitored operating environment. Each facility is dual-powered with underground transmission from two separate transformer stations. In addition, the facilities provide backup power from generators, which are capable of powering the data center 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

IIS 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 IIS 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 IIS other operational facilities. The storage facility has at least the same level of physical protection as the data centers.

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 .nu zone. The trusted roles are:

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

At any given time, there must be at least 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 is 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 confidentiality agreement and an agreement to acknowledge their responsibilities with the IIS Registry 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 any of the operations facility. Duties are segregated by the Security Officer not having exclusive physical access to the operational facilities, while the System Administrators 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 the authority to register key material, while only the SA has the authority to initiate key generation (see section 5.1.2).

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

The aforementioned 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

[1] HSM – hardware security module

assessment is made by the chief information security officer before such a person assigned the powers 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 IIS. This process includes verifying:

- the candidate's resume,
- employment history,
- references (proclaimed and others), and
- documents 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

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:

- IIS 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 – SOs),
- advanced technical proficiency in DNS and DNSSEC (for System Administrators - SAs),
- 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 operations 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 confidentiality agreements. Severe negligence may lead to termination of employment and damage liability.

4.3.6 Contracting personnel requirements

In certain circumstances, IIS may need to use contractors as a supplement to full-time employees. These contractors sign the same type of responsibility and confidentiality 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

IIS supply 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 online in log collecting systems for at least 90 days. Thereafter, the log information is archived for a minimum of ten years.

4.4.4 Protection of audit log

All electronic log information is stored at both operations 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.

IIS 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 IIS 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 is required to prevent the event from reoccurring (or to limit its consequences). The procedures also include means of escalation and reporting of incidents to the appropriate authority within IIS.

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 IIS detects corruption of information systems or resources, the incident management procedures shall be initiated and appropriate measures be taken. If required, the disaster recovery procedures and/or the emergency key rollover procedures are also enacted.

4.5.3 Entity private key compromise procedures

If the confidentiality of a private key is suspected to have 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, IIS 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, taking into account 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 .nu zone will be unsigned until all the systems are recovered and new DNS 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

IIS has implemented a contingency plan ensuring that mission-critical operations can be relocated between the operational facilities within four hours. Spare components for critical hardware are stored onsite in each operations center.

The contingency plan also includes capability to resume mission-critical functions at an alternative location. The plans are regularly tested and the results are recorded and subsequently evaluated.

The contingency plan includes:

- roles and responsibilities in the activation of emergency recovery 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 Entity termination

If IIS must discontinue DNSSEC for the .nu 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 .nu zone is transferred to another party, IIS will take part 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

All keys required for the continued operation of the .nu zone (in the foreseeable future) are pre-generated in advance through a formal key ceremony. The generation of the keying 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 operation facilities. Keys will then automatically be distributed to the backup-module (refer to section 5.2.4).

Key generation requires the presence by two individuals, one each from two different trusted roles 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 export it is verified by 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 secondary checking that the keys published are the same as those that were being 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 validated hardware security devices, HSM's (refer to section 5.2.1) provides reasonable assurance that 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 DNSSEC signature has a maximum validity period of 14 days for both the ZSK and KSK, with an inception time of one hour from 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, or 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

IIS 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 Registry does not escrow private keys.

5.2.4 Private key backup

During the key ceremony, the pre-generated application keys are copied to a backup-module with characteristics similar to the HSM itself. The backup module is stored in a safe 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 role.

5.2.5 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.

5.2.6 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 using a set of hardware token devices. 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 role. Henceforth, this HSM Master Key is used to protect application keys during key distribution between the devices via IIS 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 is 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 role.

5.2.9 Method of deactivating private key

The HSM is locked if it is turned off, rebooted or lose 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 pair 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 into the expired state and becomes invalid. 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

The activation data is stored on a hardware security module 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 security module used to activate the HSM. Installation of activation data is done through physical interconnection between the HSM and the hardware security module.

5.4.2 Activation data protection

Each SO is responsible for maintaining the chain of custody of the hardware security module while in use in accordance with current rules and procedures. When the hardware security module is not in use it is stored in a safe accessible only by the SO role. 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 replaced.

5.4.3 Other aspects of activation data

In the event of an emergency, there exists one set of activation data in a sealed, tamper evident package at a secure location (refer to section 4.1.8). The activation data enables the assigning of an Emergency Security Officer (ESO). IIS DNSSEC contingency plan procedures state the conditions in which this procedure shall be enacted.

5.5 Computer security controls

IIS 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 sub system.

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 managing the communication between the different network segments and to critical components of the registry system.

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

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

5.7 Time stamping

The Registry retrieves time traceable to timeservers from the SP, the Technical Research Institute of Sweden. Time stamps are in UTC(SP), and are standardized within the organization for all log information, as well as validity time for DNSSEC signatures.

5.8 Lifecycle technical controls

5.8.1 System development controls

.nu's 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.

IIS 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 of complexity,
- systematic and automated testing and regression tests,
- issuing of distinct software versions,
- continuous improvement of quality and accuracy of produced software through tight integration with the quality management system (conforming to ISO 9001:2008).

5.8.2 Security management controls

IIS Registry Information Security Management System has been assessed and certified as compliant with the requirements of ISO/IEC 27001:2013.

IIS has established and maintains a system security plan for the Registry. The plan 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 plan follows the PDCA (Plan - Do - Check - Act) method as outlined in ISO/IEC 27001, and forms together with IIS Information Security Policy and the Baseline Security Standard, the basis for the information security management of the registry system.

5.8.3 Change management security controls

The Registry has implemented a formal IT Service Management (ITSM) Change Management process conforming to the principles of ISO/IEC 20000, in order to manage and control alterations to the IT environment.

6 Zone signing

6.1 Key lengths, key types and algorithms

IIS uses a split-key signing scheme in signing of the .nu 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.

Algorithms shall be standardized by the IETF, available to the public and resource efficient for all parties involved.

Currently, the ECDSA algorithm with a modulus size (key length) of 256 bits is used for both the KSK and ZSK.

6.2 Authenticated denial of existence

IIS uses NSEC3 with five (5) iterations to provide authenticated denial of existence, as specified in RFC 5155. IIS does not use opt-out. The salt used for NSEC3 is changed on a regular basis.

6.3 Signature format

Signatures are generated by encrypting ECDSAP256SHA256 hashes (ECDSAP256SHA256, 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 resigning frequency

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

6.6 Verification of resource records

To ensure valid signatures and the 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	3,600
DS	3,600
NSEC3[2]	as SOA minimum (7,200)
RRSIG	as RR (varies)

[2] The NSEC3 RR must have the same TTL value as the SOA minimum TTL field according to RFC 5155.

7 Compliance audit

To verify that the controls are working and are efficient IIS 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 IIS. 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 IIS attention,
- if significant changes are made at the management, organizational or processes that supports the IIS Registry operations.

7.2 Qualifications of 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 audit may engage technical experts with background experiences from IIS, or organizations affiliated with IIS.

7.4 Topics covered by audit

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

These documents are primarily IIS Information Security Policy, the Baseline Security Standard and the IIS Registry System Security Plan for the registry system 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 IIS. The severity of each discrepancy will be determined with input from the auditor. An appropriate correction plan will be developed 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 IIS within 30 days following the completion of the audit. The auditing reports are not made public.

8 Legal matters

8.1 Fees

Any fees associated with DNSSEC must be regulated by the agreement between registry and registrar.
https://registrar.iis.nu/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 IIS has entered into which regulates the protection and use of PII. IIS policy on privacy is available at
https://www.iis.se/docs/PrivacyPolicy_iis.pdf

8.3 Limitations of liability

The liability for damages between Registry and Registrar is regulated by the Registrar Registry Agreement.
https://registrar.iis.nu/97

IIS liability for damages to Registrants is regulated by IIS current General Terms and Conditions, pertaining to the top-level domain .nu, which are available at
https://www.iis.se/english/domains/nu/terms-and-conditions/