DNSSEC Policy & Practice Statement for .NO (DPS)

The purpose of this DPS is to document the policies and procedures for operating DNSSEC in .NO.

List of contents:

1 INTRODUCTION

This document is UNINETT Norid AS (Norid)'s statement of security practices and provisions that are applied related to the operation of DNS Security Extensions (DNSEC) in the Norwegian top-level domain (.no). The purpose of this DNSSEC Policy and Practice Statement (DPS) is to document the policies and procedures for operating DNSSEC in .no.

This document conforms to the DPS framework defined in [1].

The DPS is one of several documents relevant to the operation of the .no zone.

1.1 Overview

DNSSEC is an extension to the existing DNS system that enables the authentication of DNS data and makes it possible to verify that the content of a DNS response has not been modified.

Resource record sets secured with DNSSEC are cryptographically signed and use asymmetric cryptography to establish a so-called “chain of trust” that traverses the public DNS tree. This trust originates at the root zone and follows the same delegation process as that of domain name registrations.

1.2 Document name and identification

Document title: DNSSEC Policy & Practice Statement for .NO

Version: 1e1

Created: May 24, 2013

Updated: December 16, 2014

1.3 Community and applicability

Norid supports the registry-registrar model, which means that registrants normally need to contact their registrar to register and update information related to their domains.

1.3.1 Registry

UNINETT Norid AS (Norid) is responsible for the .no top level domain. This means that this organization is responsible for the management of all data related to the 1st-level '.no'-zone, the approximately 790 2nd-level-zones administered by Norid itself and also for the registration, modification and deletion of (2nd-level)-domain names under .no.

The registry is also responsible for generating the relevant cryptographic keys, ensuring protection for those keys, signing the actual zone files and the registration and maintenance of DS records in the root zone.

1.3.2 Registrar

The registrars are responsible for the administration and management of (2nd-level) domain names on behalf of the registrants. They are also responsible for the registration and maintenance of the corresponding DS records within the registry.

Only a DNSSEC enabled registrar can maintain DNSSEC data. A registrar is DNSSEC enabled via a special configuration parameter on his registrar account. The registrar need to contact Norid to enable the parameter.

1.3.3 Registrant

The registrant is a physical or legal entity that administratively controls a domain name. Registrants are responsible for proper technical administration of their zones, including proper signing of child zones and the registration and maintenance of DS records through the registrar. If necessary the process of zone signing can be delegated to the registrar.

1.3.4 Dependent entities

Dependent entities are the users of the DNSSEC data, for example ISPs using validating resolvers or other applications. The dependent entities are responsible for maintaining the appropriate DNSSEC trust anchors and configurations.

1.3.5 Applicability

Each registrant is responsible for determining an appropriate level of security for their domain. This DPS applies exclusively to the .no top-level domain and describes the procedures, security controls and practices employed in the management of DNSSEC in the .no zone.

With the support of this DPS, the relying party can determine the level of trust they may assign to DNSSEC in the .no domain and assess their own risk.

The process of registration is governed by the Domain Name Policies of Norid, [6].

1.4 Specification administration

This DPS will be reviewed and updated as appropriate.

1.4.1 Specification administration organization

UNINETT Norid AS (the registry for Norwegian domain names).

1.4.2 Contact information

UNINETT Norid AS
NO-7465 TRONDHEIM
Norway

Phone : +47 07355
Fax : +47 73 55 79 99

E-mail : info@norid.no
Website: www.norid.no

1.4.3 Specification change procedures

Any changes to this document need to be signed off by the Chief Technical Officer of Norid.

The most recent version of this DPS will be published on the Norid website.

2 PUBLICATION AND REPOSITORIES

2.1 Repositories

NO publishes DNSSEC-relevant information on NO's website at:

http://www.norid.no/dns/teknisk/dnssec/index.en.html

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

Notifications relevant to DNSSEC in .no will be distributed using the following email list:

dnssec-announce@lists.norid.no

Information on how to subscribe and manage subscriptions to this email list is also published at the above web address.

2.2 Publication of Key Signing Keys (KSK)

The deployed KSKs are published in the form of DS records directly in the root zone.

2.3 Access control

DNSSEC relevant information published on the specific Norid website is accessible by the general public.

3 OPERATIONAL REQUIREMENTS

3.1 Meaning of domain names

A domain name is a unique identifier, which is often associated with services such as web sites or e-mail. Applying for registration under the top-level .no domain is available according to:

http://www.norid.no/domeneregistrering/registrere.en.html

3.2 Activation of DNSSEC for child zone

DNSSEC is enabled for the relevant child zone by publishing at least one DS record for the child zone in the .no top level domain (or in any of Norid's second level zones). This is done when a registrar provides a minimum of one DS record in the registry, which is subsequently published in DNS. The published DS record establishes the chain of trust to the child zone.

The registry assumes and requires that provisioned DS records are of the correct form. To ensure correctness, some basic syntax checking will be performed for DS records. If the optional key is also provided, the DS will be validated against the key.

Before a DS is accepted in an EPP domain-create or domain-update, the registry will perform a number of DNSSEC checks to verify that the child zone can be validated. A fundamental requirement in the check is that at least one of the DSs can be used for validation.

3.3 Identification and authentication of child zone manager

Responsibility for the identification and authentication of a child zone manager/registrant rests with the registrar.

3.4 Registration of Delegation Signer (DS) records

The registry accepts DS records through its EPP interface only from a DNSSEC enabled registrar. The registrar is identified and authenticated via EPP.

The DS record must be valid and sent in the format indicated in RFC5910, [7].

Up to 6 DS records can be registered per child zone. The registrar can also update or remove all or selection of DS records for a child domain.

As an option, the corresponding key can be sent in along with the DS. If so, the DS will be validated against the key.

3.5 Method to prove possession of private key

The registry does not perform any validation checks for authenticating the registrant as the manager or holder of a specific private key. The registrar is responsible for conducting both the checks that are required and other checks that are considered necessary.

3.6 Removal of DS record

DS records can be removed via the EPP interface by the respective registrar.

If all DS records of a child zone are removed, DNSSEC validation for that zone is disabled, and the zone will become unsigned.

3.6.1 Who can request removal

Only the registrant, or another representative appointed by the registrant, has the authority to request removal of the DS records via a registrar.

3.6.2 Procedure for removal request

The registrants ask their registrar to perform the removal of a DS record. The registrar may only do this on behalf of the registrant or the representative appointed by the registrant.

From the time the EPP removal request has been processed by the registry, it normally takes no longer than until the completion of the next zone generation for the change to be published in the .no zone file. The frequency and times for zonefile generations are published on the Norid website (www.norid.no).

Subsequently, taking 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 (see 6.9 Resource records Time-To-Live (TTL) .

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

3.6.3 Emergency removal request

No special emergency removal procedures are implemented.

4 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1 Physical controls

Based on continuous risk analysis and reevaluation of threats, Norid implements physical perimeter protection, monitoring and access controls, as well as appropriate compensating controls, to reasonably ensure that the registry and signer systems are not tampered with, stolen or sabotaged.

4.1.1 Site location and construction

The .no registry is operated from two operational and geographically dispersed data centers, where one site is active mode and the other is in standby mode with all relevant data replicated.

4.1.2 Physical access

Physical access to the data centers is limited to authorized personnel.

4.1.3 Power and air conditioning

Power is supplied via separate and independent feeds. In case of power failure, power is provided by UPS and also via backup power generator units.

Both data centers are equipped with air cooling systems.

4.1.4 Flood protection

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

4.1.5 Fire protection and prevention

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

4.1.6 Media storage

The registry has implemented and enforces an information classification system, which

defines the requirements imposed for storage of sensitive information.

4.1.7 Waste disposal

All confidential documents and media are shredded or destroyed in a secure manner before disposal.

4.1.8 Off-site backup

All systems are backed up to a separate and third backup data center.

Sensitive data are encrypted.

4.2 Procedural controls

4.2.1 Trusted roles

So-called “trusted roles” are staffed with highly trained and experienced personnel who will perform all relevant DNSSEC tasks such as the generation and deployment of keys, the management of trust anchors etc. These trusted roles are:

- System Administrator, SA
- 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 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 .no registry may hold a trusted role. The agreements are signed as part of the employment procedures, ref. 4.3.2 Background checks .

4.2.4 Tasks requiring separation of duties

Separation of duties is enforced for critical operations. A number of critical tasks will require one individual from each role to participate in the process.

All critical signer and HSM operations are required to be performed on the specially secured signer server.

Critical tasks are separated between the Security Officer and the System Administrator. The tasks are identified and the restrictions are documented in dedicated routine documents, which define the separation rules.

None of the critical tasks may be performed in the physical presence of unauthorized individuals.

4.3 Personnel controls

4.3.1 Qualification, experience and clearance requirements

Staff taking part in a trusted DNSSEC role must have all necessary qualifications and demonstrate trustworthiness.

4.3.2 Background checks

Background checks are performed as part of the hiring process for all personnel.

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

4.3.3 Training requirement

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:

- .no operations,
- the role's authority and areas of responsibility,
- general domain name administration,
- 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,
- incident handling,
- crisis management and disaster recovery.

4.3.4 Contracting personnel requirements

Contractors may be used to supplement full-time employees. These contractors sign the equivalent confidentiality and responsibility agreements as full-time employees. Contractors must be qualified for a trusted role per 4.2.3.

4.3.5 Documents supplied to personnel

The registry supplies the necessary documentation to employees to support their work in a secure and satisfactory manner.

4.4 Audit logging procedures

4.4.1 Types of events recorded

The following events are logged to detect illegal/incorrect operations:

- Access attempts (successful and unsuccessful) to all DNSSEC Systems
- Any type of DNSSEC operation (such as key generation, key roll-overs etc.)
- Privileged operations
- Manual logs are created for special operations, like KSK roll-overs.

4.4.2 Frequency of processing log

All logs are checked by a number of automatic and manual methods. The automated checks are performed frequently and many times each day.

4.4.3 Retention period for audit log information

Log files are stored for at least 30 days on the logging system. Thereafter, log files are archived on the backup system for at least 3 months.

4.4.4 Protection of audit log

Access to audit logs is permitted only for authorized personnel.

4.4.5 Audit log backup procedures

Audit logs are backed up on external media periodically. The media library is located in an external backup data center.

4.4.6 Audit collection system

Electronic log information is transferred in real-time to audit collection systems. Manual logs are recorded on paper and stored in a fireproof safe.

4.4.7 Notification to event-causing subject

No notice is required to be given to the individual, organization, device, or application causing a log event.

4.4.8 Vulnerability assessments

Anomalies in logging information are investigated to analyse potential vulnerabilities.

4.5 Compromise and disaster recovery

4.5.1 Incident and compromise 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 registry's incident handling procedures.

If the private part of an active KSK is (likely to be) compromised, an emergency key roll-over will be performed.

If the DNSSEC systems become unavailable due to accidents or disasters, the personnel will attempt to get systems back online as soon as possible.

4.5.2 Corrupted equipment, software or information

In the event of a hardware fault, the faulty element(s) will be replaced as soon as possible.

In the event of a software or data issue, the registry will perform recovery actions in accordance with predefined recovery plans.

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 roll-over procedures will be initiated:

- If a zone signing key (ZSK) is suspected of having been compromised, .NO will immediately stop using that key, and, if necessary, a new ZSK will be generated. The old key will be removed from the key set as soon as its signatures have expired or timed out, 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 roll-over is always announced through the channels indicated in section 2.1.

4.5.4 Business continuity and IT disaster recovery capabilities

The registry has implemented a contingency plan ensuring that mission-critical operations can be relocated between the two operational facilities. Spare components for critical hardware are stored on-site 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.

4.6 Entity termination

If the Registry must discontinue DNSSEC for the .no zone for any reason, and return to an unsigned position, this will take place in an orderly manner with public notification.

5 TECHNICAL SECURITY CONTROLS

5.1 Key pair generation and installation

5.1.1 Key pair generation

Norid uses the recommended KSK and ZSK key scheme [3]. See chapter 6 Zone Signing for details.

The generation of key pairs is performed by hardware security modules (HSM) which are managed by trained and specifically appointed personnel in trusted roles. See 5.2.1 Cryptographic module standards and controls for a description of the HSM solution for .no.

Key generation actions take place when necessary, e.g. before a planned key roll-over or if an emergency has occurred which requires new keys to be generated.

A key generation procedure must be performed by a minimum of two authorized personnel. These personnel must be present during the entire operation.

The entire key-generation procedure is performed according to the documented routines for Norid. As part of the routine, the procedure is logged electronically and documented manually by the security officer.

5.1.2 Public key delivery

The public part of the KSKs are exported and verified by the system administrator and security officer. The security officer is responsible for publishing the DS record in the root zone.

Newly generated keys will be synchronized with the standby registry/DNSSEC site systems.

The system administrator and the security officer are responsible for verifying both synchronization of the keys to the standby site and correct publication in the root zone.

5.1.3 Public key parameters generation and quality checking

Key parameters are defined in the Zone Signing Policy (see chapter 6 Zone Signing for details) and quality control measures include verification of the key lengths.

5.1.4 Key usage purposes

A key generated for DNSSEC purposes must only be used for DNSSEC activities and should never be used outside of the signing systems. A key will only be used for one zone and will not be reused.

5.2 Private key protection and cryptographic modules engineering controls

All cryptographic operations are performed on a specially protected signer server.

No private keys are ever stored unprotected, or outside HSM.

5.2.1 Cryptographic module standards and controls

The DNSSEC system for .no will initially use a SoftHSM. This may be subject to change.

The signer engine and the SoftHSM will run on the specially protected signer server, where all data is stored on an encrypted area.

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

The Registry 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

Private keys are not escrowed.

5.2.4 Private key backup

Private keys are stored on at least two SoftHSMs.

The private keys (always encrypted) are also included in the file system backup on the separate backup data center..

5.2.5 Private key storage on cryptographic module

The SoftHSMs store the keys in an encrypted database which is located on a dedicated file system of the signer server.

The dedicated and local file system which is used for storing of keys is encrypted at the file system level. When the signer machine is booted, the file system need to be manually mounted using a special unlock password. The unlock password is known only by authorized personnel.

5.2.6 Private key archival

Private keys which are no longer in use are not archived in any particular form except that of normal backup copies.

5.2.7 Private key transfer into or from a cryptographic module

All private keys will be generated directly on the SoftHSMs. They will be synchronized periodically and automatically to the standby system.

5.2.8 Method of activating private key

ZSKs are activated automatically by the signer software.

KSKs are activated manually according to the special key ceremony documentation for .no.

5.2.9 Method of deactivating private key

ZSKs are deactivated automatically by the signer software.

KSKs are deactivated manually according to the special key ceremony documentation for .no.

5.2.10 Method of destroying private key

No efforts are made to destroy private keys after their operational period has expired. 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 an 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. 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.

See ch. 6.5 for details on KSK rollover.

See ch. 6.4 for details on ZSK rollover.

5.4 Activation data

5.4.1 Activation data generation and installation

To get access to the signer server and the SoftHSM itself, several authentication steps are required.

The various authentication and unlock codes are known by authorized personnel only, and will be changed regularly according to administrative routines.

5.4.2 Activation data protection

Each security officer is responsible for protecting the various authentication codes.

If a compromise of any of the authentication codes is suspected, the responsibility rests with the security officer to immediately change it.

5.4.3 Other aspects of activation data

As part of emergency planning, a copy of all authentication codes is stored in sealed envelopes and stored in a secure location.

5.5 Computer security controls

Access to all computing components and registry systems is logged and traceable. Critical operations performed on these systems will also be logged. All personnel with access to these systems must use individual access credentials. The use of shared credentials is not permitted.

5.6 Network security controls

The registry systems are split into a number of different VLANs and security zones depending on security classification. All network traffic between these security zones is filtered by a number of firewall layers.

5.7 Time stamping

Registry system components synchronize all system clocks with trusted time sources from a default NTP policy for time stamping.

All timestamps generated by the signing system processes are in UTC.

5.8 Life cycle technical controls

5.8.1 System development controls

The signing system is based on the open source products OpenDNSSEC and SoftHSM. Norid's development model is based on industry standards and includes systematic and automated testing and regression tests and the issuing of distinct software versions. Only when all tests have completed successfully will the software be rolled out to production environments and in accordance with predefined procedures.

All source code is stored in a version control system.

5.8.2 System management controls

The registry conducts regular security audits of the system and prepares and maintains a system security plan that is based on recurring risk analysis.

6 ZONE SIGNING

6.1 Key lengths and algorithms

Norid uses a split-key signing scheme in signing of the .no zone. Key lengths and algorithms 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 RSA-SHA256 algorithm with a key length of 2048 bits is used for generating KSKs and a key length of 1024 bits used for generating ZSKs.

6.2 Authenticated denial of existence

The registry uses NSEC3 with Opt-Out as defined in RFC5155, [4].

6.3 Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA256, as defined in RFC5702 [5].

6.4 Zone signing key roll-over

The expected lifetime of the ZSK is 90 days. Roll-over of a ZSK is then carried out each 90 days by the pre-publish method described in RFC6781 [3].

6.5 Key signing key roll-over

A KSK roll-over will be performed as needed.

The key generation and roll-over will be manually initiated.

Roll-over of a KSK is carried out by the double signature method described in RFC6781 [3].

6.6 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 other hour.

6.7 Verification of zone signing key set

Before publishing a signed zone on the name server, the zone must pass a number of checks, examples are:

- Verification of the chain of trust from the DS record in the parent zone to the signature of the SOA record in the child zone
- Verification that the validity period of the signature of the SOA record is at least 2 days in the future

6.8 Verification of resource records

The registry verifies that all resource records conform with the current standards before publishing the zone.

6.9 Resource records Time-To-Live (TTL)

The time-to-live (TTL) for each DNSSEC Resource Record (RFC4034, [9]) is specified as follows, in seconds:

DNS record type	TTL/Description
DNSKEY	3600
DS	7200
NSEC3	7200 (as SOA minimum)
NSEC3PARAM	7200
RRSIG	Inherits TTL from the corresponding signed RR set.

7 COMPLIANCE AUDIT

Regular audits for DNSSEC systems and services will be performed.

Special audits will be scheduled if needed, for instance if an incident has occurred which revealed some weakness in the procedures.

Audit reports are subsequently provided to the registry and any operational recommendations will be applied as necessary.

8 LEGAL MATTERS

8.1 Fees

Currently the .NO registry does not charge any fees for DNSSEC from the registrars. Any possible fees are regulated in the Agreement between the Registrar and the Registry:

http://www.norid.no/registrar/ordning/avtale/index.en.html

8.2 Privacy of personal information

NO's privacy policy is regulated by chapter 16 and appendix G of Norid's current Domain Name Policy:

http://www.norid.no/navnepolitikk.en.html

8.3 Limitations of liability

Norid's liability for damages to the Registrar is regulated by chapter 4 of the Agreement between the Registrar and the Registry:

http://www.norid.no/registrar/ordning/avtale/index.en.html

Norid's liability for damages to the Registrant is regulated by chapter 15 of Norid’s current Domain Name Policy:

http://www.norid.no/navnepolitikk.en.html

9 DOCUMENT HISTORY, REFERENCES AND ACRONYMS

This section is not defined in the framework [1], but is added by Norid because of the need for the below information.

9.1 Document history

Date	Revision	Author	Comment
2014-09-18	1	Trond Haugen	First approved version
2014-12-16	1e1	Trond Haugen	Ch. 2.1: Changed repository location.

9.2 References

Ref	Title	Doc nr
[1]	Framework for DNSSEC Policies and DNSSEC Practice Statements	RFC6841 (http://tools.ietf.org/html/rfc6841)
[2]	DNSSEC (on Wikipedia, has also refs. to all relevant RFCs)	http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
[3]	DNSSEC Operational Practices, version 2	RFC6781 (http://tools.ietf.org/html/rfc6781)
[4]	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence	RFC5155 (http://tools.ietf.org/html/rfc5155)
[5]	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC	RFC5702 (http://tools.ietf.org/html/rfc5702)
[6]	Domain name Policy for .NO	http://www.norid.no/navnepolitikk.en.html
[7]	Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)	RFC5910 (http://tools.ietf.org/html/rfc5910)
[8]	DNSSEC Policy & Practice Statement (DPS) for various ccTLDs (especially those for AT, NL and SE)	http://www.internetsociety.org/deploy360/resources/dnssec-practice-statements/
[9]	Resource Records for the DNS Security Extensions	RFC4034 (http://tools.ietf.org/html/rfc4034)

9.3 Acronyms

Se [1,2,3] for more acronyms and terms.

Term	Description
EPP	Extensible Provisioning Protocol
DNS	Domain Name System
DNSSEC	DNS Security
DS	Delegation Signer record. The DNS record used to identify the DNSSEC signing key of a delegated zone.
HSM	Hardware Security Module
SoftHSM	A software based HSM which offers most aspects of a real HSM, except the physical HSM box and it's special tamper protection facilities. A SoftHSM which runs on a tamper-proof and separate machine is not much different from a dedicated HSM, but might be reasonably cheaper.

