DNSSEC Policy and Practice Statement .amsterdam

Contact
T +31 26 352 55 00
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem

Mailing address
Postbus 5022
6802 EA Arnhem

Inhoudsopgave

1 INTRODUCTION

This document is SIDN's statement of security practices that are applied in conjunction with DNS Security Extensions (DNSSEC) in the .amsterdam top level domain. This document conforms with RFC6841 "A Framework for DNSSEC Policies and DNSSEC Practice Statements". The DNSSEC Policy and Practice Statement .amsterdam (DPS) is one of several documents relevant to the operation of the .amsterdam zone.

1.1 Overview

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

The purpose of this document is to enable stakeholders to determine the level of trust they wish to grant to SIDN DNSSEC management. It details the procedures and policies employed by SIDN in operating DNSSEC services for the .amsterdam zone.

1.2 Document name and identification

Document title:	DNSSEC Policy and Practice Statement .amsterdam
Version:	2.0
Created:	March 1, 2012
Updated:	May 24, 2016

1.3 Community and Applicability

This DPS is exclusively applicable to the top-level .amsterdam domain and describes the procedures and security controls and practices applicable for managing and employing keys and signatures involved in SIDN's signing of the .amsterdam zone.
The relation between the registry and a registrar is subject to the "Registry-Registrar Agreement (RRA)" for .amsterdam.

The following roles and delegation of liability have been identified.

1.3.1 Registry

SIDN (the Foundation for Internet Domain Registration in the Netherlands) manages the .amsterdam top-level domain and is responsible for the .amsterdam zone on the Internet.
SIDN is the single registry for .amsterdam. It is the responsibility of the registry to sign the .amsterdam zone and make its public keys (KSK and ZSK) available to the general public, while protecting the confidentiality of the private component of the keys.

1.3.2 Registrar

A registrar is a party who, based on an agreement with ICANN and .amsterdam, has access to SIDN's registration system and provides registration and administrative services with regard to domain names to registrants. Under the agreement with ICANN and .amsterdam, a registrar is obliged to act on behalf of the registrant. The registrar is responsible for maintaining DNS records for each domain via SIDN's registration system on behalf of the registrant.

1.3.3 Registrant

A registrant is the physical or legal entity that has an agreement with a .amsterdam accredited registrar under which the registrant has the right to control a domain name. Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DS records through the registrar. The registrant is responsible for issuing an emergency key rollover if keys are suspected of being compromised or have been lost.

1.3.4 Relying Party

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

1.4 Specification Administration

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

1.4.1 Specification administration organization

SIDN (the Foundation for Internet Domain Registration in the Netherlands) provides all DNS and DNSSEC services for .amsterdam.

1.4.2 Contact Information

SIDN, Department of Registration & Service
Postal address
PO Box 5022
6802 EA Arnhem
The Netherlands

Visiting address
Meander 501
6825 MD Arnhem
The Netherlands

Phone: (+31) (0)26 352 55 00
Fax: (+31) (0)26 352 55 05
E-mail: support@sidn.amsterdam
Web: https://www.sidn.amsterdam
Dutch Chamber of Commerce number: 41215724

1.4.3 Specification change procedures

Amendments to this DPS are either made in the form of amendments to the existing document or the publication of a new version of the document. This DPS and amendments to it are published at https://nic.amsterdam/policy/.

Only the most recent version of this DPS is applicable.

2 PUBLICATION AND REPOSITORIES

2.1 Repositories

SIDN publishes DNSSEC relevant information on https:// nic.amsterdam/policy/.
The electronic version of the DPS at this specific address is the official version.

2.2 Publication of key signing keys (KSK)

SIDN publishes KSK's for the .amsterdam zone only directly in the root zone (DS). No other trust anchors or repositories are used.

3 OPERATIONAL REQUIREMENTS

3.1 Meaning of domain names

The DPS applies to .amsterdam domain names. The process of registration is governed by the "Registry-Registrar Agreement (RRA)" for .amsterdam.

3.2 Identification and Authentication of Child Zone Manager

DNSSEC is activated by at least one DNSKEY for the zone being sent from the registrar to the registry and are thereby published as a DS record in the DNS, which establishes a chain of trust to the child zone. The registry presumes that the DNSKEY is correct and will not perform any specific checks to establish whether that is the case or not.

3.3 Registration of delegation signer (DS) resource records

The registry accepts DNSKEY records through the Shared Registration System (SRS) from each Registrar. The DNSKEY record must be valid and sent in the format specified in RFC5910 (EPP DNS Security Extensions Mapping). Up to four DS records can be registered per domain name.

3.4 Method to prove possession of private key

The registry does not conduct any checks with the aim of validating the registrant as the manager of a private key.

3.5 Removal of DS resource records

A DS record is removed by the registry upon the reception of a request thereto from the registrar to the registry through the SRS. The removal of all DS records will deactivate the DNSSEC security mechanism for the zone in question.

3.5.1 Who can request removal

Only the registrant has the authority to request deregistration of the DS records via a registrar.

3.5.2 Procedure for removal request

The registrant tasks the registrar with implementing the deregistration. The registrar may only do this on behalf of the registrant. From the time the deregistration request has been received by SIDN via SRS, it takes no longer than until the next zone file generation for the change to be realised. Subsequently, it takes up to two times the TTL plus the distribution time before the changes have been deployed. The whole procedure may take a maximum of two hours to complete.

3.5.3 Emergency removal request

No emergency removal procedures are implemented.

4 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

SIDN is an ISO27001 certified organization. Procedures and processes related to facility, management and operational controls are based on the principles of this standard.

4.1 Physical Controls

4.1.1 Site location and construction

SIDN operates multiple geographically dispersed sites in the Netherlands. These include a command and control centre in the SIDN office, cabinets in multiple geographically dispersed data centres and a backup site outside of Arnhem.

4.1.2 Physical access

Access to all of our facilities is restricted to authorised personnel.

4.1.3 Power and air conditioning

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

4.1.4 Water exposure

To avoid the risk of water exposure, all of our facilities are on elevated floors several meters above ground level. Additionally, all sites have a water detection system that monitors possible water leaks in the data centre. Several sites are located above sea level.

4.1.5 Fire prevention and protection

All facilities have fire detectors and gas extinguishers.

4.1.6 Media storage

DNSSEC key material is stored in a FIPS 140-2 Level 3 compliant HSM (hardware security module). There are 2 different roles with respect to the HSM: the Crypto Officer and the HSM Operator, each with a different token. These tokens are stored in two different safes and in a secured backup location. At least two Crypto Officers and one trusted role are needed to gain access to the Crypto Officer safe. The HSM Operator safe can only be opened by two HSM Operators.

4.1.7 Waste disposal

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

4.1.8 Off-site backup

Backups of the key material is stored on a FIPS 140-2 Level 3 small factor HSM, which is stored in a safe in a secure location during the DNSSEC ceremony.

Backups of HSM Operator and Crypto Officer tokens are stored in a safe in a secure location. Access to the backup tokens in the secure backup location is only possible through identification with an authorized ID card and the possession of a secret key to open the safe in the secure backup location. Backup Crypto Officer tokens and HSM Operator tokens are kept in different backup safes with different keys.

4.2 Procedural Controls

4.2.1 Trusted roles

SIDN has two different DNSSEC related roles: Crypto Officers and HSM Operators. These distinct roles cannot be fulfilled by one and the same individual.
HSM Operators are allowed to maintain and administer a HSM. Crypto Officers are allowed to assign a HSM as containing official .amsterdam key material.

4.2.2 Number of persons required per task

For each DNSSEC ceremony at least 2 HSM Operators and 1 Crypto Officer are physically required to be present. Furthermore another Crypto Officer with a senior management position needs to approve each DNSSEC ceremony in writing.

Configuration changes and other administrative tasks on the HSM can only take place in the presence of 2 HSM Operators and 1 Crypto Officer. This is enforced by physical means.

Configuration changes and other administrative tasks on the signer will only take place in the presence of 2 HSM operators. This is enforced by procedure.

4.2.3 Identification and authentication for each role

Each person that is assigned to a role in the DNSSEC ceremony is added to the list of ceremony members, which is maintained in the latest version of the ceremony guidebook. A copy of an identity card, passport or driver’s license is added to the ceremony logbook. The assigned role is added as an addendum to the job description of the person.

4.2.4 Tasks requiring separation of duties

HSM Operators are trained System Administrators and have no management role at SIDN. Without HSM Operators no DNSSEC ceremony is possible. However, they cannot decide to start a DNSSEC ceremony without authorisation from Crypto officers. Only emergency key-rollovers can be done by HSM Operators. For regular rollovers that involve new HSMs Crypto Officers are required to generate trust in the new hardware.
Crypto Officers fulfil a non-technical role at SIDN (but they do have technical knowledge on the subject of DNS and DNSSEC) and some of them have a senior management function in SIDN. They can authorise DNSSEC ceremonies but cannot execute them. For authorisation at least one Crypto Officer needs to be physically present and another Crypto Officer (from senior management) needs to approve in writing.

4.3 Personnel Controls

4.3.1 Qualifications, experience, and clearance requirements

Every person that fulfils a role in the DNSSEC ceremony must

- have a permanent contract with SIDN
- work for SIDN for at least 6 months.

4.3.2 Background check procedures

All persons that fulfil a role in the DNSSEC ceremony must have a “Certificate of Conduct” (“Verklaring omtrent Gedrag”) issued by the Dutch government (https://www.justis.nl/producten/vog/certificate-of-conduct/index.aspx).

4.3.3 Training requirements

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

4.3.4 Contracting personnel requirements

No person outside of the specified Trusted Roles (4.2.1) can get access to the signer systems. If necessary, tasks can be performed with the guidance of an external contractor. At no time is the contractor allowed to be the person performing the tasks on the system.

4.3.5 Documentation supplied to personnel

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

4.4 Audit Logging Procedures

4.4.1 Types of events recorded

All DNSSEC ceremonies will be logged in a handwritten logbook, stored in a safe location.
All access and changes to the safes are logged in the safe-logbook, which is stored in the safe.
All access to the signers and the signing software is logged in the syslog of these systems and systematically checked for anomalies.

4.4.2 Retention period for audit log information

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

4.5 Compromise and Disaster Recovery

4.5.1 Incident and compromise handling procedures

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

4.5.2 Corrupted computing resources, software, and/or data

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

4.5.3 Entity private key compromise procedures

In the case of a suspected or established compromise of a KSK, an assessment of the situation will follow as well as the development and implementation of an action plan with the approval from the Information Security Officer and the Chief Technical Officer.

An emergency rollover of a compromised key will be communicated through the channels indicated in 2.2.

4.6 Entity termination

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

SIDN has provided ICANN with a transition plan for .amsterdam's registry services, providing for transition of DNS and DNSSEC to another registry operator.

5 TECHNICAL SECURITY CONTROLS

5.1 Key Pair Generation and Installation

5.1.1 Key pair generation

Key generation takes place in a hardware security module (HSM) that is managed by trained and specifically appointed personnel in trusted roles.

KSK key generation takes place when necessary and must be performed by three people working in unison. These people are present during the entire operation. Key generation procedures are described in the “Ceremony Guidebook”. ZSK keys are generated automatically by the signer system. The entire key generation procedure is logged, part of which is done electronically and part of which is done manually on paper by a Crypto Officer.

5.1.2 Public key delivery

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

5.1.3 Key usage purposes

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

5.2 Private key protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed in the hardware module and private keys will remain in the protected and secure DNS signing infrastructure.

5.2.1 Cryptographic module standards and controls

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

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

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

5.2.3 Private key escrow

Private keys are not placed in ESCROW.

5.2.4 Private key backup

Private keys are backed up on a FIPS 140-2 Level 3 small factor HSM and stored in a secured location outside the data centres. Both the Crypto Officer and two HSM Operators need to be present with their tokens to create or restore a backup.

5.2.5 Private key archive

Private keys are not archived.

5.2.6 Transferring of a private key into or from a cryptographic module

It is not possible to transfer a private key into or from a cryptographic module.

5.2.7 Storage of private key in the module

The private keys are stored encrypted in the module.

5.2.8 Method of activating private key

Private keys are activated by the signer software. ZSKs are activated automatically. KSKs are activated manually through the DNSSEC ceremony.

5.2.9 Method of deactivating private key

Private keys are deactivated by the signer software. ZSKs are deactivated automatically. KSKs are deactivated manually through the DNSSEC ceremony.

5.2.10 Method of destroying private key

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

5.3 Other Aspects of Key Pair Management

5.3.1 Key usage periods

KSKs are used for 3 to 5 years. ZSKs are used for 90 days.

5.4 Activation data

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

5.4.1 Activation data generation and installation

Each Crypto Officer and HSM Operator is responsible for creating their own activation data conform the procedures described in the “Ceremony Guidebook”.

5.4.2 Activation data protection

Each Crypto Officer and HSM Operator is responsible for protecting their activation data as described in the “Ceremony Guidebook”, SIDN’s security guidelines or otherwise in the best possible way. In any event of suspicion of compromise of activation data, the operator must immediately report the incident and change it.

5.5 Computer Security Controls

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

5.6 Network Security Controls

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

5.7 Timestamping

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

5.8 Life Cycle Technical Controls

5.8.1 System development controls

The signing system is based on OpenDNSSEC and BIND. SIDNs development model is based on industry standards and includes systematic and automated testing and regression tests and the issuing of distinct software versions. All source code is stored in a version control system.

5.8.2 Security 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 analyses.

5.8.3 Life cycle security controls

The registry complies with ITIL Change Management.

6 ZONE SIGNING

6.1 Key lengths, key types and algorithms

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

6.2 Authenticated denial of existence

The registry uses NSEC3 opt out records as specified by RFC5155.

6.3 Signature format

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

6.4 Key rollover

ZSK rollovers are carried out every 90 days. The KSK will only be scheduled to be rolled over through a key ceremony as required.

6.5 Signature lifetime and re-signing frequency

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

6.6 Verification of resource records

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

6.7 Resource records time-to-live

DNSKEY:	1800 seconds
NSEC:	equal to minimum field of SOA record (RFC4034)
RRSIG:	equal tot TTL of RRset covered, 1800 seconds in practice
DS:	1800 seconds

7 Compliance Audit

SIDN is an ISO27001 certified organization. Procedures and processes related to facility, management and operational controls regarding DNSSEC are based on the principles of this standard including the Annex A.

7.1 Frequency of entity compliance audit

An ISO27001 audit and all underlying audits are conducted every year.

7.2 Identity/qualifications of auditor

The audit is conducted by an external and independent certified auditor.

7.3 Auditor's relationship to audited party

There is no other relation to the audited party than that of a client and contractor.

7.4 Topics covered by audit

The yearly ISO27001 audits cover all procedures and processes of SIDN, including DNSSEC procedures and processes in a random way.

7.5 Actions taken as a result of deficiency

All finding are followed up. The time for resolving of a finding depends on its importance.

7.6 Communication of result

The results of the audit are not communicated publicly. The ISO27001 statement of applicability, however, is publicly available.

8 Legal Matters

8.1 Governing Law

This DPS shall be governed by the laws of the Netherlands.