# DNSSEC Policy & Practice Statement (DPS)

dnsbelgium

# Introduction

The purpose of this DPS is to document the policies and procedures for operating DNSSEC in .vlaanderen and .brussels. This document conforms to the Internet-Draft DNSSEC Policy & Practice Statement Framework (draft-ietf-dnsop-dnssec-dps-framework).

## 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.

**Document Name and Identification**

*Document title: DNSSEC policy statement for .vlaanderen and .brussels*

*Version: 1.1*

*Created: May 3, 2019*

# 1 Community and Applicability

The Registry supports the registry-registrar model. It deals only through registrars and registrants have no direct contact with the registry.

### 1.1 Registry

The Registry is responsible for the TLD .vlaanderen and .brussels. This means that this organization is responsible for the management of all data related to registration, modification and deletion of (2nd-level)-domain names under .vlaanderen and .brussels.

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

### 1.2 Registrar

The Registrar is responsible for the administration and management of domain names on behalf of the Registrant. They are also responsible for the registration and maintenance of the corresponding DS-Records within the Registry.

### 1.3 Registrant

The Registrant is a physical or legal entity that controls a domain name. They are responsible for the 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.

### 1.4 Dependent entities

Dependent entities are those users of that 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.

# 2 Specification Administration

This DPS will be periodically reviewed and updated as appropriate.

### 2.1 Specification Administration Organization

DNS Belgium vzw/asbl
Contact
DNS Belgium vzw/asbl
Philipssite 5 bus 13
3001 Leuven
Belgium
Phone: +32.16284970
Fax: +32.16284971
E-Mail: support@dnsbelgium.be
Website: http://www.dnsbelgium.be

### 2.2 Specification Change Procedures

Any changes to this document need to be signed off by the Engineering Manager of DNS Belgium vzw.

The most recent version of this DPS will be published on the website of DNS Belgium vzw.

## 3 Publication and Repositories

### 3.1 Publication Site

DNSSEC-relevant information will be published on the website of DNS Belgium vzw.

### 3.2 Publication of Key Signing Keys (KSK)

The public portion of the KSKs are published in the form of DS-Records directly in the root zone.

### 3.3 Access Control

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

# 4 Operational Requirements

## 4.1 Meaning of Domain Names

The purpose and meaning of domain names can be found in domain registration policies of DNS Belgium vzw.

## 4.2 Activation of DNSSEC for Child Zone

A minimum of one DS Record must be provisioned by a registrar in the registry and subsequently published in the DNS for DNSSEC to be enabled for the relevant child zone. The published DS Record establishes the chain of trust to the child zone.

The registry presumes that provisioned DS records are of the correct form and will not perform any specific validation checks on these records except some basic syntax checking This means, in essence, that the registry will not verify if a DNSSEC enabled child-zone can be validated by the relevant DS record.

## 4.3 Identification and Authentication of Child Zone Manager

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

## 4.4 Registration of Delegation Signer (DS) Records

The registry accepts DS records through its EPP interface from any registrar. The registrar is identified and authenticated on the EPP server. The DS record must be valid and sent in the format indicated in RFC 5910. Up to six DS records can be registered per child domain. The registrar can also remove all or selected DS records for a child domain.

## 4.5 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.

## 4.6 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.

# 5 Facility, Management and Operational Controls

## 5.1 Physical Controls

### Site Location and Construction

Our registry systems operate in a high availability configuration within our Cloud infrastructure (AWS), set up to be Fault-Tolerant as well as using Multi-AZ. By enabling Multi-AZ, our services physically run within different Availability Zones (AZs) or locations that are in separate geographic areas. All components of the SRS are redundant over at least 2 of the 3 geographical locations in a high-availability setup.

### Physical Access

The AWS cloud is ISO27001 and ISO27017 certified.

### Power and Air Conditioning

The AWS cloud is ISO27001 and ISO27017 certified.

### Flood protection

The AWS cloud is ISO27001 and ISO27017 certified.

### Fire Protection and Prevention

The AWS cloud is ISO27001 and ISO27017 certified.

### Media Storage

The AWS cloud is ISO27001 and ISO27017 certified.

### Waste Disposal

All confidential documents and media are shredded or destroyed before disposal.

### Off-site Backup

All key material is backed up to external locations outside of AWS.

KSK Backup: Stored in three offline and offsite locations

ZSK Backup: Stored in one offline and offsite location

## 5.2 Procedural Controls

### 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:

- Signing handler: has access to the DNSSEC-signer, but not the keys.
- Key handler: has acces to the DNSSEC keys.

### Task Requiring Separation of Duties

Any task performed on the zone-signer system requires at least one Signinghandler and one Keyhandler to be present.

## 5.3 Personnel Controls

### Qualification, Experience and Clearance Requirements

At least on of the trusted roles taking part in a trusted DNSSEC role must have been working for the company for more than one year and all must have all necessary qualifications.

### Background Checks

DNS Belgium performs the following pre-employment reference checks:

- DNS Belgium will conduct a reference review prior to extending an offer of employment.
- This process will apply to all candidates regardless of the position.
- This review is used to validate information on a candidate’s resume.
- The reference check will be conducted by the Human Resources manager.
- Information gathered will include the quality and quantity of work performed, attendance, education and other work-related information.

### Training Requirement

New trusted role members must be present for and observe at least two regular key roll-overs with existing trust role members.

### Contracting Personnel Requirements

Only personnel in specified trusted roles are permitted access to DNSSEC systems.

### Documents Supplied to Personnel

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

# 6 Audit Logging Procedures

## 6.1 Types of Events Recorded

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

Remote access attempts (successful and unsuccessful) to all DNSSEC Systems

Any type of DNSSEC operation (such as key generation, key rollovers, etc.)

## 6.2 Frequency of Log Processing

Logs are processed automatically and a monitoring system is configured to alert about the most common DNSSEC errors and audit violation.

## 6.3 Retention Period for Audit Log Information

Log files are stored for at least 6 months on the logging system. Thereafter, log files are archived on the backup system for at least 1 year.

## 6.4 Protection of Audit Log

Access to audit logs is permitted only for authorized personnel.

## 6.5 Audit Log Backup Procedures

All logs are collected and backed up to encrypted online storage (S3 on AWS).

## 6.6 Audit Collection System

Electronic log information is transferred in real-time to audit collection systems.

## 6.7 Notification to Event-causing Subject

Any persons who trigger an event to be logged are not also notified of this action or that such logging is taking place.

## 6.8 Vulnerability Assessments

Anomalies in logging information are investigated to analyze potential vulnerabilities.

# 7 Compromise and Disaster Recovery

### 7.1 Incident and Compromise Handling Procedures

If the private part of an active KSK is (likely to be) compromised, an emergency key rollover 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.

### 7.2 Corrupted Equipment, Software or Information

Replacement or repair of malfunctioning hardware is the responsibility of the infrastructure-provider (AWS). In the event of hardware malfunction, the system will be restarted on other hardware.

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

### 7.3 Business Continuity and IT Disaster Recovery Capabilities

In the event of a disruption to DNSSEC services due, for example, to a disaster at a data center facility, the registry will recover the service(s) as soon as possible at the backup data center.

# 8 Entity Termination

If it becomes necessary to discontinue DNSSEC services for any reason, the registry will invoke a pre-defined set of procedures. The general public will also be informed in such an event.

If operations are to be transferred to another party, the registry will participate in the transition to ensure it will take place as seamless as possible.

# 9 Technical Security Controls

### 9.1 Key Pair Generation and Installation

#### Key Pair Generation

The entropy needed for the generation of key pairs is generated by a mix of  hardware TPM and dedicated instruction sets in CPUs by dedicated hardware, which is managed by trained and specifically appointed personnel in trusted roles. Key generation actions take place when necessary and must be performed by a minimum of two authorised personnel. These personnel must be present during the entire operation.

The entire key-generation procedure is documented.

### Public Key Distribution

The public part of the KSKs are exported and verified by the signing handler and key handler. The signinghandler is responsible for publishing the DS record in the root zone.

Newly generated KSK keys will be synced manuallly with the offsite and offline backup. The signinghandler and the keyhandler are responsible for verifying synchronisation to the offsite and offline backup.

Newly generated ZSK keys will be synced automatically with the offsite and offline backup and with the onsite backup. The signinghandler and the keyhandler are responsible for verifying synchronisation to the offsite and offline backup.

### Public Key Parameters Generation and Quality Checking

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

### 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 must only be used for one zone and cannot be reused.

# 10 Private Key Protection and Cryptographic Modules Engineering Controls

Private keys are protected by software encryption.

## 10.1 Cryptographic Module Standards and Controls

All software we use, like for example the kernel crypto API version, are regularly updated for FIPS 140-2 validation by the vendor.

## 10.2 Private Key (m-of-n) Multi-person Control

A minimum of 2 persons is required to access any private part of a key.

## 10.3 Key Escrow

Private keys are not escrowed.

### 10.4 Private Key Backup

KSK Private keys are stored offline on 2 encrypted media in different locations and offline encrypted on the signer.

ESK Private keys are stored on 2 encrypted media in different locations.

ZSK Private keys are stored on 1 extra encrypted medium in different location and stored online encrypted on the signer.

### 10.5 Private Key Storage on Cryptographic Module

Only keyhandlers can decrypt the encrypted volumes with their high security personal password.

### 10.6 Private Key Archival

Private keys which are no longer in use are archived forever on above mentioned locations.

### 10.7 Private Key Transfer into or from a Cryptographic Module

All private keys will be generated directly on the HSMs. They will be synced periodically and automatically to the backup system, which is initialized with the same HSM master key.

### 10.8 Method of Activating a Private Key

A new private key is activated be a team consisting of a signinghandler and a keyhandler.

### 10.9 Method of Destroying a Private Key

Private keys will not be destroyed.

## 11 Other Aspects of Key Pair Management

### 11.1 Public Key Archival

Obsolete public keys are archived forever.

### 11.2 Key Usage Period

KSKs will be rolled over when needed; ZSKs will be rolled over every three months, on the third Thursday of the month.

# 12 Activation Data

### 12.1 Activation Data Generation and Installation

Each keyhandler is responsible for creating their own activation data.

### 12.2 Activation Data Protection

Each keyhandler is responsible for protecting their activation data. If a compromise of this activation data is suspected, the responsibility rests with the keyhandler to immediately change it.

### 12.3 Other Aspects of Activation Data

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

# 13 Computer Security Controls

Access to all computing components and registry systems is logged and traceable. All 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.

# 14 Network Security Controls

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

# 15 Time Stamping

Registry systems synchronise all system clocks with trusted time sources from Belnet (http://www.belnet.be) . All timestamps generated by the registry system are in UTC.

# 16 Life Cycle Technical Controls

### 16.1 System Development Controls

An in house developed key management tool is used. Any new versions of this software are tested in a lab environment and are subjected to a pre-defined testing framework. Only when all tests have completed successfully, the software can be rolled out to production environments and in accordance with pre-defined procedures.

### 16.2 System Management Controls

A security audit of the registry system was performed before initialising the service and will be repeated at regular intervals.

# 17 Zone Signing

### 17.1 Key Lengths and Algorithms

The RSA algorithm with a key length of 2048 bits is used for generating KSKs and a key length of 1024 bits used for generating ZSKs.

### 17.2 Authenticated Denial of Existence

The registry uses NSEC3 with Opt-OUT as defined in RFC 5155.

### 17.3 Signature Format

The digital signature algorithm used to sign the TLD zone file is RSA/SHA-2 as defined in RFC 5702.

### 17.4 Zone Signing Key Roll-over

The expected lifetime of the ZSK is maximum 35 days.

### 17.5 Key Signing Key Roll-over

A KSK roll-over will be performed as needed.

### 17.6 Signature Life-time and Resigning Frequency

The KSK signatures of the TLD zone DNSKEY RRset will have a validity period of 40 days.

The ZSK signatures of the TLD zone authoritative data will have a validity period of 10 days.

### 17.7 Verification of Zone Signing Key Set

- We are doing dynamic updates and live key rollovers
- We continuously monitor RRSIG expiration
- We continuously monitor the DNSSEC chain from the root server

### 17.8 Verification of Resource Records

The Registry verifies that all resource records are conformant with the current standards before publishing the zone.

### 17.9 Resource Records Time-to-live (TTL)

The TTL for DS records and the TTL for DNSKEY will be set to 86400 seconds and NSEC3 records to 600 seconds. RRSIG records inherit TTLs from the corresponding signed RRset.

## 18 Compliance Audit

A regular audit for DNSSEC systems and services will be performed. Audit reports will subsequently provided to the registry and any operational recommendations will be applied as necessary.

## 19 Legal Matters

Jurisdiction resides within the operators country of residence. Respective contracts such as Registrar contracts as well as the Terms and Conditions of end customer contracts (if applicable) will be closed.

The registry also complies with the national data protection acts and only releases customer data without consent if legally obliged.