Document control

Document information and security

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

Approved by

DATE	NAME	FUNCTION
		SECURITY OFFICER

Audits

DATE	VERSION	NAME	DESCRIPTION

Table of Content

Table of Content 2

1. Introduction 6

1.1. Overview 6

1.2. Document name and identification 6

1.3. Community and Applicability 6

1.3.1. Registry 6

1.3.2. Registrar 7

1.3.3. Registrant 7

1.3.4. Applicability 7

1.4. Specification Administration 7

1.4.1. Specification administration organisation 7

1.4.2. Contact Information 7

1.4.3. Specification Change Procedures 8

2. Publication and Repositories 9

2.1. Repositories 9

2.2. Publication of Key Signing Keys (KSK) 9

2.3. Access control 9

3. Operational Requirements 10

3.1. Meaning of domain names 10

3.2. Activation of DNSSEC for child zone 10

3.3. Identification and authentication of child-zone manager 10

3.4. Registration of delegation signer (DS) resource records 10

3.5. Method to prove possession of private key 10

3.6. Removal of DS resource record 10

3.6.1. Authority to request deregistration 10

3.6.2. Deregistration procedure 11

4. Facility, Management, and Operational Controls 11

4.1. Physical Controls 11

4.1.1. Site location and construction 11

4.1.2. Physical access 11

4.1.3. Power and Air Conditioning 11

4.1.4. Water Exposure 11

4.1.5. Fire Prevention and Protection 11

4.1.6. Media Storage 11
4.1.7. Waste Disposal 11
4.2. Procedural Controls 12
4.2.1. Trusted Roles 12
4.2.2. Number of persons required per task 12
4.2.3. Identification and authorization of people in trusted roles 12
4.2.4. Separation of Duties 12
4.3. Personnel Controls 12
4.3.1. Qualifications, experience and clearance requirements 12
4.3.2. Background checks 12
4.3.3. Training Requirements 12
4.3.4. Job Rotation Frequency and Sequence 13
4.3.5. Contracting Personnel Requirements 13
4.3.6. Documentation Supplied to Personnel 13
4.4. Audit Logging Procedures 13
4.4.1. Types of Events Recorded 13
4.4.2. Frequency of control of log information 13
4.4.3. Retention period for log information 13
4.4.4. Protection of Audit Log 14
4.4.5. Security backups of log information 14
4.4.6. Log-information collection system 14
4.4.7. Notification to event-causing subject 14
4.4.8. Vulnerability assessments 14
4.5. Compromise and Disaster Recovery 14
4.5.1. Incident management 14
4.5.2. Corrupted equipment, software or information 14
4.5.3. Entity Private Key Compromise Procedures 14
4.5.4. Contingency plan 15
4.5.5. Entity termination 15
5. Technical Security Controls 16
5.1. Key Pair Generation and Installation 16
5.1.1. Key Pair Generation 16
5.1.2. Public Key Delivery 16
5.1.3. Quality control of key parameters 16

5.1.4. Key Usage Purposes 16
5.2. Private Key Protection and Cryptographic Module Engineering Controls 16
5.2.1. Cryptographic Module Standards and Controls 16
5.2.2. Private Key (m-of-n) Multi-person Control 16
5.2.3. Key escrow 16
5.2.4. Private Key Backup 17
5.2.5. Private Key Archival 17
5.2.6. Private Key Transfer Into or From a Cryptographic Module 17
5.2.7. Storage in a cryptographic security module 17
5.2.8. Method for activating private keys 17
5.2.9. Method for deactivation of private keys 17
5.2.10. Destruction of private keys 17
5.3. Other Aspects of Key Pair Management 17
5.3.1. Public Key Archival 17
5.3.2. Key Usage Period 17
5.3.3. Activation data 17
5.3.4. Generation and installation of activation data 17
5.3.5. Protection of activation data 18
5.3.6. Other aspects of activation data 18
5.4. Computer Security Controls 18
5.5. Network Security Controls 18
5.6. Timestamping 18
5.7. Life Cycle Technical Controls 18
5.7.1. System development controls 18
5.7.2. System management controls 19
6. Zone Signing 20
6.1. Key Lengths and Algorithms 20
6.2. Authenticated Denial of Existence 20
6.3. Signature Format 20
6.4. Zone Signing Key Roll-over (ZSK) 20
6.5. Key Signing Key Roll-over (KSK) 20
6.6. Signature Life-time and Re-signing Frequency 20
6.7. Verification of zone signing key set 20
6.8. Verification of resource records 20

6.9. Resource Records Time-to-live (TTL) 20
7. Compliance Audit 21
7.1. Frequency of entity compliance audit 21
7.2. Qualifications of auditor 21
7.3. Auditor's relationship to the audited party 21
7.4. Topics covered by audit 21
7.5. Actions taken as result of deficiency 21
7.6. Communication of results 21
8. Legal Matters 22
8.1. Fees 22
8.2. Privacy of personal information 22
8.2.1. Responsibility to protect personal information 22
8.2.2. Disclosure of personal information to judicial authorities 22
8.3. Limitations of liability 22
8.4. Term and termination 22
8.4.1. Validity period 22
8.4.2. Expiration of validity 22
8.4.3. Dispute resolution 22
8.4.4. Governing law 22

1. Introduction

This document is the Registry Operator's statement of security practices and provision that are applied in conjunction with DNS Security Extensions (DNSSEC) in the gTLD top-level domain. This document conforms to the RFC-draft DNSSEC Policy & Practice Statement Framework (current draft: http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework-05). The DPS is one of several documents relevant to the operation of the Registry zone. Another relevant document is the business contingency plan.

1.1. Overview

The purpose of this document is to enable stakeholders to determine the level of trust they wish to grant to the Registry's DNSSEC management. It details the procedures and policies employed by the Registry Operator in operating the Registry zone.

DNSSEC is a set of records and protocol modifications that enable the authentication of DNS data and also make it possible to ensure that content has not been modified during transfer, including mechanisms for authenticated denial of existence. Resource records 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.

1.2. Document name and identification

DNSSEC Policy and Practice Statement or short DPS.

1.3. Community and Applicability

The Registry follows a Registry – Registrar – Registrant model. In this model, the owner of a zone (Registrant) and the operator of the parent zone (Registry Operator) are connected through an intermediary (Registrar).

1.3.1. Registry Operator

The Registry Operator is responsible for the administration of the domain names in the Registry zone. This means that the Registry Operator manages addition, changes and removal of all data that is related to a domain name in the Registry.

For DNSSEC, the Registry Operator is responsible for generating key pairs and protecting the confidentiality of the private component of the Key Signing Keys (KSK) and Zone Signing Keys (ZSK) and for making its public keys available to the general public. The Registry Operator is also responsible for signing all authoritative DNS resource records in the Registry zone in a secure manner.

Finally the Registry Operator is responsible for the registration and maintenance of DS resource records in the root zone.

1.3.2. Registrar

A Registrar is the party that is responsible for the administration and management of domain names of behalf of the Registrant. The Registrar handles the registration, maintenance and management of a Registrants domain name and is an accredited ICANN registrar.

The Registrar is responsible for securely identifying the Registrant of a domain. The Registrar is responsible for adding, removing or updating specified DNSKEY records for each domain at the request of the Registrant.

1.3.3. Registrant

A Registrant is the physical or legal entity that controls a domain name. Registrants are responsible for generating and protecting their own keys, and registering and maintaining the DNSKEY 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. Applicability

Each Registrant is responsible for determining the relevant level of security for their domain. This DPS is exclusively applicable to the top-level Registry domain and describes the procedures and security controls and practices applicable when managing and employing keys and signatures for Registry's signing of the Registry zone.

1.4. Specification Administration

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

1.4.1. Specification administration organisation

The administrator of .epost DPS is Deutsche Post AG

1.4.2. Contact Information

Deutsche Post AG
Charles-de-Gaulle-Straße 20
53113 Bonn
Germany

Phone +49 228 18296701
Fax +49 228 18296799
Email AdminContact.Domain@DeutschePost.de

1.4.3.Specification Change Procedures

Any change to this document needs to be signed off by a Senior Manager of the Registry Operator, and the Security Officer of the Registry Service Provider.

Only the most recent version of this DPS is applicable.

2. Publication and Repositories

2.1. Repositories

DNSSEC relevant information is published via the Registry Operator's secured website.

2.2. Publication of Key Signing Keys (KSK)

The Registry Operator will publish its Key Signing Keys (KSKs) in two formats:

- Directly in the root zone (only DS resource records)
- On the Registry's website, in the DNSKEY Format

2.3. Access control

Information published at the specific website is available to the general public and is protected against unauthorized adding, deletion or modification of the content on the website.

The public part of the registry's key Signing Key is signed with the Registry's official PGP-key, which may be found at the Registry Operator's secured website.

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 hosting or e-mail. Application for registry under the top-level Registry domain is limited to the Registry Operator.

3.2. Activation of DNSSEC for child zone

DNSSEC is activated by at least one Key Signing Key (KSK) DNSKEY record for the zone being sent from the Registrar to the Registry Operator and thus being published in the DNS, which established a chain of trust to the child zone. The Registry Operator will calculate and update the related DS resource records.

During the pre-delegation checks, we will ensure that the DNSKEY records provided are available as DNSKEY records at the apex of the child zone for all delegated name servers. We will also check if these DNSKEYs are properly signed.

3.3. 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, and in compliance with the stipulations in the contract between the Registry Operator and the Registrar.

3.4. Registration of delegation signer (DS) resource records

The Registry Operator accepts DNSKEY records through the EPP interface from the Registrar. The DNSKEY record must be valid and sent in the format indicated in RFC 5910 (EPP DNS Security Extensions Mapping).

The Registry Operator will calculate and insert the derived DS resource records.

3.5. Method to prove possession of private key

The Registry Operator does not conduct any controls with the aim of validating the Registrant as the manager of a private key. The Registrar is responsible for conducting the controls that are required and those deemed necessary.

3.6. Removal of DS resource record

A DS record is deregistered by sending a request from the Registrar to the Registry Operator. The deregistration of all DS records will deactivate the DNSSEC security mechanism for the zone in question.

3.6.1. Authority to request deregistration

Only the Registrant, or the party formally designated by the Registrant by assigning either the Tech C or Admin C role, has the authority to request deregistration of the DS records.

3.6.2. Deregistration procedure

The Registrant or the Registrant's representative in the form of Tech C or Admin C 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 the Registry Operator via EPP, it takes no longer than until the next zone generation for the change to be recorded in the zone file.

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 five hours to complete.

4. Facility, Management, and Operational Controls

4.1. Physical Controls

The Registry Operator has implemented physical security controls to meet the requirements specified in this DPS.

4.1.1. Site location and construction

The Registry Operator operates multiple sites in the Benelux, at least 25 kilometers apart. The redundant facility contains a complete set of the Registry's critical systems, whose information is continuously updated through automatic replication of the normal operations facility. All of the systems components are protected within a physical perimeter with an access control and alarm system.

The backup operations facility meets the minimum standards applied to the normal facility in terms of physical security, power supply, environment and fire and water protection.

4.1.2. Physical access

All of our facilities have restricted access, limited to authorized personnel.

4.1.3. Power and Air Conditioning

All facilities have Uninterruptible Power Supply (UPS) capabilities and air conditioning. The external data center sites have redundant systems in place in the event of a power failure.

4.1.4. Water Exposure

To avoid the risk of water exposure, all of our facilities are on elevated floors well above ground level.

4.1.5. Fire Prevention and Protection

All facilities have fire detectors and gas extinguishers.

4.1.6. Media Storage

Sensitive media is stored in a safe which is only accessible by the Registry Operator's Senior Management and specifically designated personnel.

4.1.7. Waste Disposal

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

4.1.8. Off-site Back-up

Signer backups are stored on our storage systems spread across all of our data centers.

4.2. Procedural Controls

4.2.1. Trusted Roles

Trusted roles are held by persons that are able to affect the zone file's content, or the generation or use of private keys. The trusted roles are:

- System & Network Administrator
- Security Officer, SO

4.2.2. Number of persons required per task

At any given time, there must be at least two individuals within the organization per trusted role indicated in 4.2.1.

Signer system activation requires two people to be present; one from each role.

Key generation requires two people to be present; one from each role.

The export and control of trust anchors requires two people to be present; one from each role.

None of the aforementioned operations may be performed in the presence of unauthorized people.

4.2.3. Identification and authorization of people in trusted roles

Only people who have signed a confidentiality agreement and an agreement to acknowledge their responsibilities with the Registry Operator may hold a trusted role. Before a person receives their credentials for system access, a valid form of identification must be presented. Refer to 4.3.2.

4.2.4. Separation of Duties

The trusted roles in 4.2.1 above may not be held simultaneously by one and the same person. The separation of duties is forced by the Security Officer not having exclusive physical access to the operational facilities, and the Network & System Administrator not having access to the activation material of the signer system.

4.3. Personnel Controls

4.3.1. Qualifications, experience and clearance requirements

Engineers taking part in the Trusted Roles have must have the qualifications necessary for the DNS engineer job role.

4.3.2. Background checks

The evaluation of background checks is conducted at the time of hiring the engineer.

4.3.3. Training Requirements

Should a new team be formed, this team will have to observe at least one regular key roll-over with an existing team.

4.3.4. Job Rotation Frequency and Sequence

The responsibility for conducting operations is rotated on each occasion between the people who hold a trusted role.

4.3.5. Contracting Personnel Requirements

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

4.3.6. 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 engineers of those teams will be informed accordingly.

4.4. Audit Logging Procedures

Logging is automatically carried out and involves the continuous collection of information regarding the activities that take place in an IT system. This log information is used in the monitoring of operations, for statistical purposes and for investigation purposes in suspected cases of violation of .SE's policies and regulations.

Logging information also includes the journals, checklists and other paper documents that are vital to security and that are required for auditing.

The purpose of the collected log information is to be able to reconstruct the case after-the-fact and analyze which people or applications/systems did what and at what time. Logging and the identification of users enables such features as traceability and the follow-up of unauthorized use.

4.4.1. Types of Events Recorded

Physical access to the facilities used for our signing systems is logged automatically on enter and exit. The main operation site requires personnel to be specifically granted permission to enter the suite in which the equipment is located and they will have to sign-in using a valid identification (passport, drivers license, etc.).

Log messages from the signer systems will be sent securely to a logging system and recorded for audit purposes.

4.4.2. Frequency of control of log information

Logs are continuously analyzed through automated and manual controls. Specific controls are conducted on processes including key generation, system reboots and detected anomalies.

4.4.3. Retention period for log information

Log information is stored in log systems for not less than 30 days. Thereafter, the log information is archived for not less than ten years.

4.4.4. Protection of Audit Log

Audit logs of our main operation site are stored at both operations facilities at the same time. The logging system is protected against unauthorized viewing and the manipulation of information.

4.4.5. Security backups of log information

All electronic log information is securely backed up on a monthly basis and is stored separately from the system in a secure location. All paper-based log information is scanned and electronically transferred to both facilities.

4.4.6. Log-information collection system

Electronic log information is transferred in real-time to the collection systems; one for each facility and external to the key generating system. Manual logs are recorded on paper, scanned, and manually transferred to the collection system on a monthly basis. The original documents are archived in a fireproof safe.

4.4.7. Notification to event-causing subject

Personnel causing an event to be logged will not be notified that such logging is taking place nor will they be entitled to review the log data.

4.4.8. Vulnerability assessments

All anomalies in the log information are investigated to analyze potential vulnerabilities.

4.5. Compromise and Disaster Recovery

4.5.1. Incident management

All real and perceived events of a security-critical nature that caused or could have caused an outage, damage to the IT system, disruptions and defects due to incorrect information or security breaches are defined as incidents.

All incidents are handled in accordance with the Registry's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, what effects the incident has had or may have had, measures to prevent the incident from recurring and forms to further report this information.

An incident that involves suspicion that a private key has been compromised leads to the immediate rollover of keys pursuant to the procedures indicated in chapter 4.5.3.

4.5.2. Corrupted equipment, software or information

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

4.5.3. Entity Private Key Compromise Procedures

Upon the suspected or known compromise of a key, we will assess the situation, develop and implement an action plan with approval from the Security Officer and Senior Management.

- If a zone signing key is suspected of having been compromised, it will immediately be removed from production and stopped being used. 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 timed out.
- If a 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 key sets until such time as it can be considered sufficiently safe to remove the key taking into account the risk for system disruptions in relation to the risk that the compromised key presents.

4.5.4.Contingency plan

The Registry Operator has a contingency plan that ensures that operation-critical production can be relocated between the two operation facilities within four hours. The facilities are equivalent in terms of physical and logistical protection. Information is replicated between the facilities. Frequently used spare components and critical hardware components are stored onsite in each operations facility.

The contingency plan and routines are regularly tested. The completed tests and trials are recorded and subsequently evaluated.

The contingency plan includes:

- Who decides on the activation of an emergency recovery procedure;
- How and where the crisis management shall convene;
- Activation of backup operations;
- Appointment of a Task Manager;
- Criteria for restoring normal operations.

4.5.5.Entity termination

If the Registry Operator must discontinue DNSSEC for the Registry zone for any reason and return to an unsigned position, 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.

5. Technical Security Controls

5.1. Key Pair Generation and Installation

5.1.1. Key Pair Generation

Key generation takes place on a signing system that is managed by trained and specifically appointed personnel in trusted roles.

Key generation takes place when necessary and must be performed by two people working in unison. These people are present during the entire operation.

The entire key-generation procedure is logged, part of which is done electronically and part of which is done manually on paper by the Security Officer.

5.1.2. Public Key Delivery

The public component of each generated KSK is exported from the signing system and verified by the Security Officer and Network & System Administrator. The Security Officer is responsible for publishing the public component of the KSK in a secure manner as per 2.1. The Network & System Administrator is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3. Quality control of key parameters

Key parameters are regularly reviewed and quality control includes checking the key length.

5.1.4. Key Usage Purposes

Keys generated for DNSSEC are never used for any other purpose or outside the signing system. A signature created by a DNSSEC key has a maximum validity period of 90 days for the ZSK and of 1 year for the KSK, starting from the time the signature is produced.

5.2. Private Key Protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed on the signing system and no private keys are ever found unprotected outside it.

5.2.1. Cryptographic Module Standards and Controls

The signing system used for signing the zones is using FIPS 140-2 Level 2-certified flash drives for start-up and private key backup.

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. Key escrow

The Registry does not apply a key escrow.

5.2.4. Private Key Backup

The key archive is encrypted with a Storage Master Key (SMK). The key archive and the SMK are stored on a portable storage medium (FIPS 140-2 Level 2-certified flash drives) in a bank vault, which can only be accessed by a Security Officer.

Keys are stored in an encrypted format on the signing module's hard drive. The encrypted key archive is securely backed up and synchronized between the operations facilities immediately after key generation.

5.2.5. Private Key Archival

Private keys can be restored from the back-ups specified above. Private keys are not archived on the signer system once they have been revoked.

5.2.6. Private Key Transfer Into or From a Cryptographic Module

Private keys can only be transferred off the system in encrypted form and restored onto the back-up system by the teams described in the Trusted Roles section.

5.2.7. Storage in a cryptographic security module

The Storage Master Key (SMK) is shared by all security modules in the system. This master key is used to decrypt the key archive that is stored outside the security module while deactivated.

5.2.8. Method for activating private keys

Private keys are activated by unlocking the signing system. An SA provides an SO with access to the facility. The Security Officer states a personal passphrase for the signing system through a console.

5.2.9. Method for deactivation of private keys

The signing system is locked after the system is either turned off or rebooted.

5.2.10. Destruction of private keys

Private keys are not destructed. After their useful life, they are removed from the signing system.

5.3. Other Aspects of Key Pair Management

5.3.1. Public Key Archival

Public keys are archived in accordance with the archiving of other information relevant to traceability in the system, such as log data.

5.3.2. Key Usage Period

Keys become invalid as they are taken out of production. Old keys are not reused.

5.3.3. Activation data

The activation data is the personal passphrase for each Security Officer that is used to activate the signing system.

5.3.4. Generation and installation of activation data

Each Security Officer is responsible for creating their own activation data pursuant to the applicable requirements of at least nine characters of varying nature.

5.3.5. Protection of activation data

Each Security Officer is responsible for protecting their activation data in the best possible way. On the suspicion of compromised activation data, the Security Officer must immediately change it.

5.3.6. Other aspects of activation data

In the event of an emergency, there is a sealed and tamper evident envelope in a secure location that contains activation information with instructions on appointing an Emergency Security Officer (ESO). The DNSSEC contingency plan procedures state the conditions in which this shall be applied.

5.4. Computer Security Controls

All critical components of the Registry's systems are placed in the organizations 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 Network & System Administrators. All access is logged and is traceable at the individual level.

5.5. Network Security Controls

Systems holding the signing infrastructure are inside a dedicated VLAN inside our network infrastructure. The only communications channel to those systems is through our firewall, which is limited to the minimal capabilities necessary for the operation of the system. All sensitive information that is transferred over the communications network is always protected by strong encryption.

5.6. Timestamping

The signer systems securely synchronize their system clocks with a trusted time source inside our network.

5.7. Life Cycle Technical Controls

5.7.1. System development controls

All source code is stored in a version control system. The source code archive is regularly backed up and copies are stored separately in a fireproof safe.

The 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 pursuit of minimizing complexity;
- Systematic and automated testing and regression tests;
- Issuing of distinct software versions;
- Constant quality follow-ups of detected defects.

5.7.2.System management controls

Authorization registers are kept and followed up regularly. The Registry Operator also conducts regular security audits of the system. The Registry prepares and maintains a system security plan that is based on recurring risk analysis.

6. Zone Signing

6.1. Key Lengths and Algorithms

Key lengths and algorithms are to be of sufficient length for their designated purpose during each key's useful life.

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

The RSA algorithm with a key length of 2048 bits is currently used for KSK and 1024 bits for ZSK.

6.2. Authenticated Denial of Existence

Authenticated denial of existence will be provided through the use of NSEC3 records as specified in RFC 5155.

6.3. Signature Format

Signatures are created with the RSASHA1-NSEC3-SHA1 algorithm.

6.4. Zone Signing Key Roll-over (ZSK)

The Registry will roll the ZSK with a pre-publishing scheme as described in RFC 4641, section 4.2.1.1.

6.5. Key Signing Key Roll-over (KSK)

The Registry will roll the KSK with a double-signing scheme as described in RFC 4641, section 4.2.1.2.

6.6. Signature Life-time and Re-signing Frequency

RR sets are signed with ZSKs with a signature lifetime of 90 days. Resigning takes place every day.

6.7. Verification of zone signing key set

To ensure signatures and the validity period of keys, security controls are conducted against the DNSKEY prior to publishing zone information on the Internet. This is done by verifying the chain from DS in the parent zone to KSK, ZSK and the signature over the Registry's SOA.

6.8. Verification of resource records

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

6.9. Resource Records Time-to-live (TTL)

- DNSKEY : Equal to the TTL used for the SOA record
- NSEC3 : Equal to the minimum field of the SOA record
- RRSIG : Equal to the lowest TTL of the record set covered
- DS : Equal to the TTL of the NS RRset

7. Compliance Audit

Audited documents (policy, procedures, requirements), information regarding facts or other information that is relevant in consideration of the audit criteria and that is verifiable are used as documentation when conducting audits.

7.1. Frequency of entity compliance audit

The need of audits is decided by the Registry Operator. Circumstances which may entail an audit requirement are:

- Recurring anomalies;
- Significant changes that are made at the management level, in the organization or in processes;
- Other circumstances, such as the competence among personnel, new equipment or other major changes;

7.2. Qualifications of auditor

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

7.3. Auditor's relationship to the audited party

An external auditing manager shall be appointed for the audit. When necessary, the auditing manager shall be able to recruit specific expert knowledge. The auditing manager is responsible for implementation during the entire audit.

7.4. Topics covered by audit

The auditing manager’s assignment includes ensuring that:

- The right competence represents the Registry;
- The auditee is informed and prepared prior to the audit;
- The auditee is informed of the topic of the audit in advance;
- Follow-up procedures of the audit results are in place;

7.5. Actions taken as result of deficiency

The auditing manager shall immediately verbally inform the Registry Operator’s management of any anomalies.

7.6. Communication of results

The auditing manager shall submit a written report of the audit results to the Registry Operator not later than 30 calendar days after the audit.

8. Legal Matters

8.1. Fees

The Registry does not charge any fees for DNSSEC from Registrars.

8.2. Privacy of personal information

8.2.1. Responsibility to protect personal information

This is regulated by the Registry Operator's Registration terms and conditions and by agreement between the Registry Operator and the Registrar.

8.2.2. Disclosure of personal information to judicial authorities

Considering the fact that the gTLD in question is subject to Specification 13, where any and all domain names are registered in the name of the Registry Operator or its Affiliates. Reference is made to the terms and conditions for registering domain names in the TLD, as provided to ICANN in the context of Registry Operator's request for Specification 13.

8.3. Limitations of liability

As the TLD is operated in accordance with Specification 13, Deutsche Post AG (and its affiliates) as registrant(s) are unlikely to incur damages as the result of issues with domain names it has registered itself in the TLD.

8.4. Term and termination

8.4.1. Validity period

This DPS applies until further notice.

8.4.2. Expiration of validity

This DPS is valid until it is replaced with an updated or new version as stated in section 1.4.3.

8.4.3. Dispute resolution

Reference is made to the terms and conditions for registering domain names in the TLD, as provided to ICANN in the context of Registry Operator's request for Specification 13.

8.4.4. Governing law

The operation of this Registry is governed by the laws of Germany.