KS-Registry DNSSEC Policy Statement

1. INTRODUCTION....5
1.1 Overview....5
1.2 Document name and identification....5
1.3. Community and Applicability....5
1.3.1 Registry....5
1.3.2 Registrars....5
1.3.3 Registrants....6
1.3.4 Relying Party....6
1.4 Specification Administration....6
1.4.1. Specification administration organization....6
1.4.2. Contact Information....6
1.4.3. Specification change procedures....6
2. PUBLICATION AND REPOSITORIES....6
2.1. Repositories....6
2.2. Publication of key signing keys (KSKs)....6
2.3. Access controls on repositories....7
3. OPERATIONAL REQUIREMENTS....7
(3.1. Meaning of domain names)....7
3.2. Activation of DNSSEC for child zone....7
3.3. Identification and authentication of child zone manager....7
3.4. Registration of delegation signer (DS) resource records....7
3.5. Method to prove possession of private key....7
3.6. Removal of DS record....7
3.6.1. Who can request removal....7
3.6.2. Procedure for removal request....7
3.6.3. Emergency removal request....8
4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS....8
4.1. Physical Controls....8
4.1.1. Site location and construction....8
4.1.2. Physical access....8
4.1.3. Power and air conditioning....8
4.1.4. Water exposures....8
4.1.5. Fire prevention and protection....8
4.1.6. Media storage....8
4.1.7. Waste disposal....9
4.1.8. Off-site backup....9
4.2. Procedural Controls....9
4.2.1. Trusted roles....9
4.2.2. Number of persons required per task....9
4.2.3. Identification and authentication for each role....9
4.2.4. Tasks requiring separation of duties....9
4.3. Personnel Controls....9
4.3.1. Qualifications, experience, and clearance requirements....9
4.3.2. Background check procedures....10
4.3.3. Training requirements....10
4.3.4. Retraining frequency and requirements....10
4.3.5. Job rotation frequency and sequence....10
4.3.6. Sanctions for unauthorized actions....10
4.3.7. Contracting personnel requirements....11
4.3.8. Documentation supplied to personnel....11
4.4. Audit Logging Procedures....11

4.4.1. Types of events recorded....11
4.4.2. Frequency of processing log....11
4.4.3. Retention period for audit log information....11
4.4.4. Protection of audit log....11
4.4.5. Audit log backup procedures....11
4.4.6. Audit collection system....12
4.4.7. Notification to event-causing subject....12
4.4.8. Vulnerability assessments....12
4.5. Compromise and Disaster Recovery....12
4.5.1. Incident and compromise handling procedures....12
4.5.2. Corrupted computing resources, software, and/or data....12
4.5.3. Entity private key compromise procedures....12
4.5.4. Business Continuity and IT Disaster Recovery Capabilities....13
4.6. Entity termination....13
5. TECHNICAL SECURITY CONTROLS....13
5.1. Key Pair Generation and Installation....13
5.1.1. Key pair generation....13
5.1.2. Public key delivery....13
5.1.3. Public key parameters generation and quality checking....14
5.1.4. Key usage purposes....14
5.2. Private key protection and Cryptographic Module Engineering Controls....14
5.2.1. Cryptographic module standards and controls....14
5.2.2. Private key (m-of-n) multi-person control....14
5.2.3. Private key escrow....14
5.2.4. Private key backup....14
5.2.5. Private key storage on cryptographic module....14
5.2.6. Private key archival....14
5.2.7. Private key transfer into or from a cryptographic module....14
5.2.8. Method of activating private key....15
5.2.10. Method of destroying private key....15
5.3. Other Aspects of Key Pair Management....15
5.3.1. Public key archival....15
5.3.2. Key usage periods....15
5.4. Activation data....15
5.4.1. Activation data generation and installation....15
5.4.2. Activation data protection....15
5.4.3. Other aspects of activation data....15
5.5. Computer Security Controls....15
5.6. Network Security Controls....15
5.7. Timestamping....16
5.8. Life Cycle Technical Controls....16
5.8.1. System development controls....16
5.8.2. Security management controls....16
5.8.3. Life cycle security controls....16
6. ZONE SIGNING....16
6.1. Key lengths and algorithms....16
6.2. Authenticated denial of existence....16
6.3. Signature format....17
6.4. Zone signing key roll-over....17
6.5. Key signing key roll-over....17
6.6. Signature life-time and re-signing frequency....17
6.7. Verification of zone signing key set....17

6.8. Verification of resource records....17
6.9. Resource records time-to-live....17
7. COMPLIANCE AUDIT....17
7.1. Frequency of entity compliance audit....17
7.2. Identity/qualifications of auditor....18
7.3. Auditor's relationship to audited party....18
7.4. Topics covered by audit....18
7.5. Actions taken as a result of deficiency....18
7.6. Communication of results....18
8. LEGAL MATTERS....18
8.1. Fees....18
8.2. Privacy of personal information....18
8.2.1 RESPONSIBILITY TO PROTECT PERSONAL INFORMATION....18
8.2.2 DISCLOSURE OF PERSONAL INFORMATION TO JUDICIAL AUTHORITIES….18
8.3 Limitations of liability....19
8.4 Term and termination....19
8.4.1 VALIDITY PERIOD....19
8.4.2 EXPIRATION OF VALIDITY....19
8.4.3 DISPUTE RESOLUTION....19
8.4.4 GOVERNING LAW....19
Appendix....19
References....19

1. INTRODUCTION

This document is the *KSregistry DNSSEC Practice Statement* (DPS) for the .ALLFINANZ zone. It states the practices and provisions that KSregistry employs in providing zone signing and distribution services that include, but are not limited to, issuing, managing, changing and distributing DNS keys.

1.1 Overview

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

Title: KSregistry DNSSEC Practice Statement

Version: 0.1_alpha

Created: 2011-09-12

Updated: 2011-09-12

1.3. Community and Applicability

This DPS is exclusively applicable to the TLD mentioned above and describes the procedures and security controls and practices applicable for managing and employing keys and signatures involved in KSregistry's signing of the zone.

The following roles and delegation of liability have been identified.

1.3.1 Registry

On behalf of the applicant (registry operator), KSregistry (registry service provider) manages the top-level domain and is responsible for the performance of the zone on the Internet.

It is the responsibility of the registry service provider to sign the 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 Registrars

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 partner of the registry operator.

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

1.3.3 Registrants

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 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

The relying party is the entity relying on DNSSEC such as validating resolvers and other applications. The relying party is responsible for configuring and updating the appropriate trust anchors (TAs). The relying party must also stay informed of any relevant DNSSEC related events in the domain.

1.4 Specification Administration

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

1.4.1. Specification administration organization

KSregistry

1.4.2. Contact Information

KSregistry GmbH
Im Oberen Werk 1
St. Ingbert
Germany

Phone: +49 (0) 68 94 - 93 96 250

E-Mail: info@ksregistry.net
Web: https://www.ksregistry.net

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://www.ksregistry.net/dnssec.

Only the most recent version of this DPS is applicable.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

KSregistry publishes DNSSEC-relevant information on https://www.ksregistry.net/dnssec. The electronic version of the DPS at this specific address is the official current version.

2.2. Publication of key signing keys (KSKs)

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

2.3. Access controls on repositories

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.

3. OPERATIONAL REQUIREMENTS

(3.1. Meaning of domain names)

(This section describes the overall policy of child zone naming, if any.)

3.2. Activation of DNSSEC for child zone

DNSSEC is activated by at least one DS record for the zone being sent from the Registrar to KSregistry and thus being published in the DNS, which established a chain of trust to the child zone. KSregistry presumes that the DS record is correct and will not perform any specific controls.

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 Registry Operator and the Registrar.

3.4. Registration of delegation signer (DS) resource records

Registry Operator/ KSregistry accept DS records through the EPP interface from each Registrar. The DS record must be valid and sent in the format indicated in RFC 5910. Up to 10 DS records can be registered per domain name.

3.5. Method to prove possession of private key

KSregistry 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 record

3.6.1. Who can request removal

Only the Registrant has the authority to request the removal of the DS records.

3.6.2. Procedure for removal request

A DS record is removed by Registrars sending a EPP request to the SRS to remove the DS record. The removal of all DS records for a domain name will cancel the DNSSEC security mechanism for the zone in question.

The Registrant tasks the Registrar with implementing the removal. The Registrar may only do this on behalf of the Registrant. Upon receipt of the removal request by the SRS, it takes no longer than until the next zone generation for the change to be recorded in the zone file. Hence, 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.

3.6.3. Emergency removal request

If a Registrant finds himself in a situation in which he is unable to reach the Registrar, KSregistry can deregister the DS record, provided that is it possible to securely identify the Registrant.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

KSregistry has implemented physical security controls to meet the requirements specified in this DPS.

4.1.1. Site location and construction

KSregistry has established two fully operational and geographically dispersed operation centers, at 385 kilometers apart. The redundant facility contains a complete set of the critical registry functions. The information is continuously updated through automatic replication of the normal operations facility. All of the system components are protected within a physical perimeter with an access control and alarm system operated by Skyway DataCenter GmbH/M-net. Telekommunikation GmbH.

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

Physical access to the protected environment is limited to authorized personnel. Entry is logged and the environment is continuously monitored.

4.1.3. Power and air conditioning

Power is provided to the operational facilities through several separate sources. In the event of power outages, power is provided by UPS until the backup power systems have begun to generate electricity. The backup power systems have the capacity to supply critical resources with electricity for at least 48 hours.

4.1.4. Water exposures

The facilities implements flooding protection and detection mechanisms.

4.1.5. Fire prevention and protection

The facilities are equipped with fire detection and extinguishing systems. The facilities are equipped with automatic extinguishers with dry extinguishing, fireproof floors and each room constitutes an independent fire cell.

4.1.6. Media storage

All media containing production software and data, audit, archive, or backup information is stored within KSregistry facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

4.1.7. Waste disposal

Disposed storage media and other material that may contain sensitive information are destroyed in a secure manner, either by KSregistry or by a contracted party.

4.1.8. Off-site backup

Certain critical data is also securely stored using a third-party storage facility. Physical access to the storage facility is limited to authorized personnel. The storage facility is geographically and administratively separated from from the primary datacenter.

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, delivery of trust anchors or the generation or use of private keys. The trusted roles are:

- Security Administrators
- System administrators

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.

HSM modifications (e.g. HSM policy changes) 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 authentication for each role

Only people who have signed a confidentiality agreement and an agreement to acknowledge their responsibilities with KSregistry 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. Tasks requiring 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 Administrators not having exclusive physical access to the operational facilities, and the System Administrator not having access to the activation material of the HSM.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Candidates seeking to assume any of the trusted roles must be able to present proof of the requisite background and qualifications.

System administrators: basic DNSSEC knowledge

Security Adminstrators: deep system knowledge, track security mailing lists, encryption/signing, pkcs#11, ssl, hsm, roll-over

4.3.2. Background check procedures

The evaluation of background checks is conducted by the human resources (HR) function at KSregistry.

The control of backgrounds and qualifications includes reviewing

- Criminal Records Bureau check
- Verification of previous employment
- Check of professional references
- To qualify for any of the trusted roles, these controls cannot reveal any discrepancies that indicate unsuitability.

4.3.3. Training requirements

KSregistry provides the relevant and requisite training regarding procedures, administration and the technical systems that are associated with each trusted role.

These training courses include:

- KSregistry's operations (equivalent to the certification training program for Registrars).
- The role's scope, areas of responsibility and authority.
- General domain-name administration.
- Basic technical proficiency in DNS and DNSSEC (for System administrators)
- Advanced technical proficiency in DNS and DNSSEC (for Security Administrators)
- Basic knowledge of information security
- Administration, procedures and checklists.
- Procedures for incident management
- Procedures for crisis management.

4.3.4. Retraining frequency and requirements

People holding trusted roles must participate in new tests and possible supplementary training courses every third year and in the event of major changes.

4.3.5. Job rotation frequency and sequence

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

4.3.6. Sanctions for unauthorized actions

Sanctions resulting from unauthorized actions are regulated in the responsibility agreement. Severe negligence may lead to termination and damage liability.

4.3.7. Contracting personnel requirements

In certain circumstances, KSregistry may need to use contractors as a supplement to full-time employees. These contractors sign the same type of responsibility agreements as full-time employees. Contractors who have not been subject to a background check and training, and thus are not qualified for a trusted role, may not participate in the activities indicated in 4.2.2.

4.3.8. Documentation supplied to personnel

KSregistry supplies the documentation necessary for the individual employee to perform their work task in a secure and satisfactory manner.

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 KSregistry'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

The following events are included in logging:

- All types of activities that involve HSM, such as key generation, key activation, and signing and exporting keys.
- Remote access, successful and unsuccessful.
- Privileged operations.
- Entry to data centers.

4.4.2. Frequency of processing log

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 audit 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

All electronic log information is stored at both operations facilities. The logging system is protected against unauthorized viewing and the manipulation of information.

4.4.5. Audit log backup procedures

All electronic log information is securely backed up on a monthly basis and is stored separately from the system in a secure location.

4.4.6. Audit 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 and compromise handling procedures

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 KSregistry's incident handling procedures. The incident handling procedure includes investigating the cause of the incident, investigating what effects the incident has had or may have had, as well as implementing 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 computing resources, software, and/or data

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

Suspicion that a private key has been compromised or misused leads to a controlled key rollover as follows:

- 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 ZSK is suspected of having been compromised revealed to unauthorized parties, this will be notified through the channels indicated in 2.1.
- 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. A KSK rollover in progress is always notified through the channels indicated in 2.1.

If a KSK is lost, a key exchange will take place without an overlap between the lost and a pre-published emergency KSK. At such time, that will be announced through the channels indicated in 2.1. Relying parties with a static configuration of KSregistry's trust-anchor should add the emergency KSK as an extra trust-anchor, in advance. During the time until the rollover, the key set will remain static and any scheduled ZSK rollover will be postponed until after the KSK exchange.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

KSregistry has a contingency plan that ensures that operation-critical production can be relocated between the two operation facilities within 1 hour. 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.

4.6. Entity termination

If the Registry Operator must discontinue DNSSEC for the 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, KSregistry 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 in a hardware security module (HSM) that is managed by trained and specifically appointed personnel in trusted roles.

The entire key-generation procedure is logged, which is done electronically.

5.1.2. Public key delivery

The public component of each generated KSK is exported from the signing system and verified by the SO and SA. The SO is responsible for publishing the public component of the KSK in a secure

manner as per 2.1. The SA is responsible for ensuring that the keys that are published are the same as those that were generated.

5.1.3. Public key parameters generation and quality checking

Key parameters are regulated by KSregistry's KASP (Key and Signing Policy) 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 14 days for both the ZSK and KSK, starting from the time the signature is produced.

5.2. Private key protection and Cryptographic Module Engineering Controls

All cryptographic operations are performed in the hardware module and no private keys are ever found unprotected outside HSM.

5.2.1. Cryptographic module standards and controls

The system uses a hardware security module (HSM) which conforms to the requirements in FIPS 140-2 level 3.

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

KSregistry does not apply multi-person controls for HSM activation. A Security Administrator is required to activate the module, which in turn requires physical access, which can only be performed by the System administrator.

5.2.3. Private key escrow

KSregistry 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 in a bank vault, which can only be accessed by an SO.

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 storage on cryptographic 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.

5.2.6. Private key archival

Private keys that are no longer used are not archived in any other form than as backup copies.

5.2.7. Private key transfer into or from a cryptographic module

During the installation of the signing system, a joint HSM key (or Storage Master Key, SMK) is transferred via a portable USB media, after which the HSM is locked to prevent further export of keys. The USB media is subsequently stored in accordance with 5.2.4.

5.2.8. Method of activating private key

An System administrator provides an Security Administration with access to the facility. The Security Administrator states a personal passphrase for the HSM through a console.

5.2.9. Method of deactivating private key

5.2.10. Method of destroying private key

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 periods

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

5.4. Activation data

The activation data is the personal passphrase for each SO that is used to activate the HSM.

5.4.1. Activation data generation and installation

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

5.4.2. Activation data protection

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

5.4.3. 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). KSregistry's DNSSEC contingency plan procedures state the conditions in which this shall be applied.

5.5. Computer Security Controls

All critical components of the registry 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 system administrators. All access is logged and is traceable at the individual level.

5.6. Network Security Controls

KSregistry 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

KSregistry retrieves its time from reliable sources and synchronizes the system clocks with it. 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

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.

KSregistry's 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.

5.8.2. Security management controls

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

5.8.3. Life cycle security controls

The operations follow well-defined business and security processes which are based on the ITILv3 standard and are in accordance with ISO 27001.

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

KSregistry uses NSEC3 records as specified by RFC 5155.

6.3. Signature format

Signatures are generated using RSA operation over a cryptographic hash function using SHA-256 (RSA/SHA-256, RFC 5702).

6.4. Zone signing key roll-over

ZSK rollover is carried out every 28th day.

6.5. Key signing key roll-over

Each KSK will be scheduled to be rolled over through a key ceremony each year, and extraordinarily when needed as described in Section 4.6.3.

6.6. Signature life-time and re-signing frequency

RRsets are signed with the ZSKs with a validity period of 12 to 16 days. Resigning takes place every hour, but only signatures close to expiration will be regenerated. Signatures are recalculated when their expiration date is less than 3 days in the future.

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 SOA.

6.8. Verification of resource records

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

6.9. Resource records time-to-live

Controlled using the Key and Signing Policy (KASP). DNSKEY = 3,600 seconds. SOA = 172,800 seconds. RRSIG inherits TTL from the RR set that it signs.

7. COMPLIANCE AUDIT

Audited documents (policy, procedures, requirement), 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 / KSregistry. 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. Identity/qualifications of auditor

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

7.3. Auditor's relationship to 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 Registry Operator / KSregistry.
- 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 a result of deficiency

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

7.6. Communication of results

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

8. LEGAL MATTERS

8.1. Fees

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

8.2. Privacy of personal information

Personal information will be treated in accordance with German data privacy and data protection legislation and pursuant to the terms of the Registry-Registrar Agreements.

8.2.1 RESPONSIBILITY TO PROTECT PERSONAL INFORMATION

This is regulated by the Registry Operator's Registration terms and conditions and by the Registry-Registrar Agreements, in accordance with German data protection and data privacy legislation.

8.2.2 DISCLOSURE OF PERSONAL INFORMATION TO JUDICIAL AUTHORITIES

Requests regarding the disclosure of personal information to judicial authorities shall be reviewed and decided upon by KSregistry's legal role on a case-by-case in accordance with the German data protection and data privacy legislation.

8.3 Limitations of liability

Between the Registry Operator and the Registrar the liability for damages is regulated by the applicable term of the Registry-Registrar Agreement. The Registry-Registrar Agreement includes further terms regarding liability terms that are required as part of the Registrars' Registration Agreements with the Registrants.
KSregistry’s direct liability of damage toward Registrars and Registrants is excluded as KSregistry shall not be considered a party to any agreements between Registry Operator, Registrar or Registrant. KSregistry remains liable to Registry Operator according to the terms of the Registry Service Agreement.

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

Any dispute or conflict resulting from this Agreement shall be filed at Saarbrücken District Court.

8.4.4 GOVERNING LAW

This DPS shall be governed exclusively by German law.

Appendix

References

- http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework-05
- http://www.iis.se/docs/se-dnssec-dps-eng.pdf