Internet Council of Registrars

DNSSEC Practice Statement for the .swiss TLD

CORE Internet Council of Registrars

Internet Council of Registrars

Table of Contents

1. INTRODUCTION..... 1
1.1. Overview..... 1
1.2. Document name and identification..... 1
1.3. Community and Applicability..... 1
1.4. Specification Administration..... 2
1.4.1. Specification administration organisation..... 2
1.4.2. Contact Information..... 2
1.4.3. Specification change procedures..... 2

2. PUBLICATION AND REPOSITORIES..... 3
2.1. Repositories..... 3
2.2. Publication of key signing keys..... 3
2.3. Access controls on repositories..... 3

3. OPERATIONAL REQUIREMENTS..... 4
3.1. Meaning of domain names..... 4
3.2. Activation of DNSSEC for child zone..... 4
3.3. Identification and authentication of child zone manager..... 4
3.4. Registration of delegation signer (DS) resource records..... 4
3.4.1 Initial Provisioning of DNSKEY..... 5
3.4.2 Update of Existing DNSKEY..... 5
3.5. Method to prove possession of private key..... 6
3.6. Removal of DS record..... 6
3.6.1. Who can request removal..... 6
3.6.2. Procedure for removal request..... 6
3.6.3. Emergency removal request..... 6

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS..... 7
4.1. Physical Controls..... 7
4.1.1. Site location and construction..... 7
4.1.2. Physical access..... 7
4.1.3. Power and air conditioning..... 7
4.1.4. Water exposures..... 7
4.1.5. Fire prevention and protection..... 7
4.1.6. Media storage..... 8
4.1.7. Waste disposal..... 8
4.1.8. Off-site backup..... 8
4.2. Procedural Controls..... 8
4.2.1. Trusted roles..... 8
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..... 9
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 unauthorised actions..... 10
4.3.7. Contracting personnel requirements..... 10
4.3.8. Documentation supplied to personnel..... 10
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....12
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....14
5.1. Key Pair Generation and Installation....14
5.1.1. Key pair generation....14
5.1.2. Public key delivery....14
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....15
5.2.4. Private key backup....15
5.2.5. Private key storage on cryptographic module....15
5.2.6. Private key archival....15
5.2.7. Private key transfer into or from a cryptographic module....15
5.2.8. Method of activating private key....15
5.2.9. Method of deactivating private key....15
5.2.10. Method of destroying private key....15
5.3. Other Aspects of Key Pair Management....16
5.3.1. Public key archival....16
5.3.2. Key usage periods....16
5.4. Activation data....16
5.4.1. Activation data generation and installation....16
5.4.2. Activation data protection....16
5.4.3. Other aspects of activation data....16
5.5. Computer Security Controls....16
5.6. Network Security Controls....17
5.7. Timestamping....17
5.8. Life Cycle Technical Controls....17
5.8.1. System development controls....17
5.8.2. Security management controls....17
5.8.3. Life cycle security controls....18

6. ZONE SIGNING....19
6.1. Key lengths and algorithms....19
6.2. Authenticated denial of existence....19
6.3. Signature format....19

6.4. Zone signing key rollover..... 19
6.5. Key signing key rollover.....19
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.....20

7. COMPLIANCE AUDIT.....21
7.1. Frequency of entity compliance audit..... 21
7.2. Identity/qualifications of auditor.....21
7.3. Auditor's relationship to audited party..... 21
7.4. Topics covered by audit.....21
7.5. Actions taken as a result of deficiency..... 22
7.6. Communication of results.....22

8. LEGAL MATTERS.....23
8.1 Legal Status of this Document..... 23
8.2 Governing Law and Jurisdiction.....23
8.3 Personal Data Protection and Mandatory Disclosures..... 23

1. INTRODUCTION

This document describes the policies and practices of the DNSSEC operations of .swiss Registry.

1.1. Overview

As the security of the DNSSEC standard is based on a model of a "chain of trust", a user who wishes to assess the security and trustworthiness of a DNSSEC secured domain name has to investigate all links of the chain, starting from the root down to the domain itself, as the strength of the chain depends on its weakest link. Since this chain of trust is symmetric to the delegation model of the DNS, the .swiss TLD represents one link of this chain.

This document describes the technical and operational conditions, under which DNSSEC is implemented at .swiss Registry. Thus, this supplied information can be taken by a user as a source for the assessment for the part in the chain of trust which the registry represents.

This document follows the DNSSEC Policy & Practice Statement Framework proposed in the IETF DNSOP working group.

1.2. Document name and identification

Name: DNSSEC Practice Statement for the .swiss TLD
Version: 1.2
Date: 2023-02-14

1.3. Community and Applicability

This document refers to the following roles:

- **Registry:** entity managing the domain name register for the .swiss TLD, which is .swiss Registry
- **Zone Administrator:** entity that is responsible for the generation of cryptographic key pairs that are being used as key and zone signing keys, for maintaining confidentiality of the private component of these key pairs, for the signing of the zone and for the publication of the respective DS records in the parent zone. For the .swiss TLD, this is CORE Internet Council of Registrars.
- **Registrar:** ICANN and registry accredited entity which is able to submit requests to the registry.

- **Registrant:** entity registering child domains via the Registrar. For the registered domain, the registrant is responsible for the operation of the respective zone as a Zone Administrator. However, this responsibility can be delegated to the Registrar or another third party, who is then considered as the Zone Administrator for the child domain.

1.4. Specification Administration

1.4.1. Specification administration organisation

This document is administered by CORE Internet Council of Registrars.

1.4.2. Contact Information

For inquiries regarding this document, please contact

CORE Association
INTERNET COUNCIL OF REGISTRARS
World Trade Center II
29, route de Pré-Bois CH-1215
Geneva
Switzerland
secretariat@corenic.org

1.4.3. Specification change procedures

The DNSSEC Practice Statement (DPS) is revised at least once a year by the DNSSEC Policy Officer. The DPS is updated upon changes in the policy, for error correction and clarifications. If a policy change may affect users in a notable way, directly or indirectly, the updated DPS is published a reasonable time before the changes come into effect in addition to the current version of the DPS.

2. PUBLICATION AND REPOSITORIES

2.1. Repositories

This DNSSEC Policy statement is available on the .swiss Registry website. Its latest version may be downloaded from:

https://cp.nic.swiss/download/dps-swiss.pdf

Updates on the document will be announced both on a registrar e-mail notification distribution list and on a public list destined for any interested parties.

2.2. Publication of key signing keys

The public components of key signing keys are not explicitly published. However, they can be retrieved via suitable DNS queries to the apex of the .swiss zone. Also, the keys are available as part of the zone file, which is available to third party entities which have qualified themselves for accessing it.

The delegation signer (DS) records are not explicitly published either, but can retrieved via the DNS in a similar way as the key signing keys.

2.3. Access controls on repositories

The DPS is freely available to every interested party without any access control.

3. OPERATIONAL REQUIREMENTS

3.1. Meaning of domain names

The definition of domain names can be found in the registration policy.

3.2. Activation of DNSSEC for child zone

DNSSEC is activated for a child zone as soon as at least one DS record is associated with the respective registry domain object. DS records are signed and published with the following update of the .swiss zone.

3.3. Identification and authentication of child zone manager

The registry has no reliable way to verify the identity of an alleged child zone manager and to establish enough trust to him, especially if the registrant has delegated the management of the zone to a third party.

As the registrant already has a trusted relationship to the registrar, depicted by the delegation of the management of the contact and name server data of his domain to that registrar, the registry assumes the extension of this trust to the management of the DS record data as well, since the security impact of wrong or missing DS record data is similar to wrong or missing name server data. Therefore it accepts DS record data from the registrar who manages the respective domain.

If a third party zone manager is involved, it is either the responsibility of the registrant to establish trust between the registrar and this zone manager so that the zone manager can submit the DS record data directly, or the DS record data has to be fetched by the registrant and to be submitted to the registrar.

Alternatively, a published and signed CDNSKEY record in the child zone can be used to establish trust.

3.4. Registration of delegation signer (DS) resource records

The registry accepts DNSKEY data from the registrar in two ways: either via the EPP interface, using the EPP extension defined in RFC 5910; or via the publication of CDNSKEY record(s) in the child zone as defined in RFCs 7344/8078. The registry calculates the appropriate DS record data from this DNSKEY data for the publication in the zone. Up to six entries may be specified.

For the automatic CDNSKEY provisioning via CDNSKEY the following general requirements must be fulfilled.

- The domain must be active and not in an EPP update prohibited state.
- All name servers must be reachable and deliver the same CDNSKEY record set.
- The CDNSKEY record set must be valid.
- There may be at most six CDNSKEY entries.
- The zone must be correctly signed for the corresponding DNSKEY record(s).

Depending on the DNSSEC state (signed/unsigned) different approaches are taken to allow the provisioning of DNSKEY records via CDNSKEY.

3.4.1 Initial Provisioning of DNSKEY

In case the domain's zone is not yet signed, there are two possibilities to activate DNSSEC.

The first way is called Accept from Inception and specified in RFC 8078 Section 3.5. For this to work all of the domain's intended name servers must correctly publish CDNSKEY records before the domain is created. Within the first few minutes after the domain creation the CORE Registration System checks all name servers of the newly registered domain and uses a consistent CDNSKEY record set.

The second way to initially provision DNSKEY records is specified in https://www.ietf.org/id/draft-ietf-dnsop-dnssec-bootstrapping-02.html draft. This approach is also possible for existing domains and is not restricted to the first minutes of a domain's existence. For this approach to work all of the domain's name servers must correctly publish the CDNSKEY records and additionally all name servers that are not within the domain's zone itself (and a minimum of one name server) must publish the same CDNSKEY records set in a special bootstrap subdomain, whose DNSSEC signature can be validated up to the root zone.

3.4.2 Update of Existing DNSKEY

In the case that the domain has DNSSEC already activated, an update of its DNSKEY records can be achieved by publishing a new CDNSKEY record set in the zone according to RFC8078. If the CDNSKEY record set is correctly signed, the respective DNSKEY records will replace the existing DNSKEY records.

Alternatively, the DNSSEC data can still be updated using the EPP extension defined in RFC 5910. Whenever an EPP update occurs, it overwrites any DNSKEYs previously obtained via published CDNSKEYs. Furthermore, any currently published CDNSKEY records will be ignored until the zone's SOA serial version has been increased (i.e., until a new version of the zone has been published).

3.5. Method to prove possession of private key

The registry does not perform any tests to verify the possession of the private key by the submitter.

3.6. Removal of DS record

3.6.1. Who can request removal

The removal of all DS records, which turns the zone into the unsigned state, can be requested by the registrar who manages the respective domain.

Alternatively, the operator of the domain's authoritative name servers can initiate a deactivation via a CDNSKEY record.

3.6.2. Procedure for removal request

There is no verification on the side of the registry whether the removal is intended and authorised by the registrant.

The way to remove all DS records is the same as for the general management of the DS records of the domain. This means that the registrar sends an EPP domain update command for the domain, specifying that all DNSKEY data shall be removed by indicating this in the RFC 5910 EPP extension.

An alternative means to deactivate DNSSEC is the publication of a special CDNSKEY records as defined in Section 4 of RFC 8078. As with a regular update using CDNSKEY this special record must also be correctly signed. Once such a record is found DNSSEC is deactivated in the same way as if a corresponding EPP request had been sent.

3.6.3. Emergency removal request

Due to the high frequency of the name server updates of the .swiss zone, there are no special provisions for an emergency removal of the DS records. DS record removals, like any other change to the domain, will be reflected at the name servers by the following update.

4. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

4.1. Physical Controls

4.1.1. Site location and construction

The registry operates two physical sites, a primary and a secondary site, which are geographically distributed to limit the probability that a single natural disaster affects both sites. The sites provide reasonable protection against those natural phenomenons which can be expected at their locations, like lightning strikes, floods or earthquakes.

4.1.2. Physical access

The data centre rooms at the primary and secondary sites hosting the DNSSEC related infrastructure can only be accessed via a security turnstile. Only authorised personnel is allowed to enter. Visitors of the data centre rooms need to prove their identity with their data being recorded. They need to be accompanied by the authorised personnel during their presence in the data centre. The systems themselves are housed in locked racks, with the keys only accessible to authorised personnel.

4.1.3. Power and air conditioning

Both primary and secondary sites provide redundant power and air conditioning. Power is being filtered for spikes, brownouts, frequency shifts etc. and supplemented by batteries for short term outages and an emergency power generator for long term outages.

4.1.4. Water exposures

While the buildings of the two sites provide constructive means to prevent water from entering the data centres, sensors are placed in the data centres to detect ingression of water. Pumps are kept ready to exhaust the water in such cases.

4.1.5. Fire prevention and protection

The data centres of the two sites provide fire sensors and automatic nitrogen-based fire extinguishing equipments.

4.1.6. Media storage

Removable storage media that contain sensitive data related to the DNSSEC signing process are stored under the same security and safety constraints as the related computer and on-line storage systems. This applies both for on-site and off-site storage.

4.1.7. Waste disposal

Sensitive documents and materials are destroyed according to DIN 32757 level 4. Functional electronic storage devices (like hard disks and USB flash memory devices) are erased by erasure programs that suffice the commonly accepted best practices. Non-operational electronic storage devices are physically destroyed by a certified provider.

4.1.8. Off-site backup

The registry stores relevant DNSSEC related data at an external location operated by an escrow provider. The data is additionally encrypted before submission. Also, key data is replicated to the secondary site.

4.2. Procedural Controls

4.2.1. Trusted roles

The following roles appear in the context of the operation of DNSSEC at .swiss Registry:

- The **DNSSEC Policy Officer** is responsible for defining the policies and procedures, selecting and assigning personnel as DNSSEC Key Management Operators and DNSSEC Signing Operators, setting up training plans and conducting training.
- The **DNSSEC Key Management Operator** is responsible for key management related operations, including triggering zone and key signing key rollovers, performing the DS data submission to ICANN and executing emergency procedures.
- The **DNSSEC Signing Operator** is responsible for monitoring the signing process, monitoring the key synchronisation between the primary and secondary sites and activating the signing process after a restart of the signing software.

- The **DNSSEC System Administrator** is a System Administrator authorised by the DNSSEC Policy Officer to administer hardware and software that is used for the DNSSEC signing.

4.2.2. Number of persons required per task

The roles DNSSEC Key Management Operator and DNSSEC Signing Operator are staffed insofar that a 24x7 availability is guaranteed. The DNSSEC Policy Officer is represented by a single person; however, he may nominate one or more deputies for times where he is unavailable.

4.2.3. Identification and authentication for each role

Persons to be assigned to the mentioned roles need to prove their identity, need to be trained and instructed about their duties (in written form and signed by the candidate) before the required credentials (passwords, hardware tokens etc.) are issued to them.

4.2.4. Tasks requiring separation of duties

The role DNSSEC Policy Officer, including its deputies, is mutually exclusive with the DNSSEC Key Management Operator and DNSSEC Signing Operator roles.

4.3. Personnel Controls

4.3.1. Qualifications, experience, and clearance requirements

Candidates are required to have long-term experience in the domain business and to have in-depth knowledge and understanding of security and cryptography and related practices and procedures.

4.3.2. Background check procedures

Candidates are required to have a good reputation. This is verified by a set of background checks which are not disclosed in this document.

4.3.3. Training requirements

The personnel is instructed in the technical background of DNSSEC and its concrete implementation at the registry. This includes the following topics, but is not limited to them:

- the principles of signing and key management
- the principles of the chain of trust as implemented in DNSSEC
- the importance of expiration dates in signatures
- the key rollover processes
- the importance of the timing of rollover processes
- emergency rollover processes
- execution of procedures related to the registry's implementation
- monitoring of the DNSSEC signing operations

4.3.4. Retraining frequency and requirements

As the signing process is mostly automated, manual interaction is rather infrequent. Infrequent execution of procedures, however, causes regression of the skills. Therefore, retraining is executed every six months. The retraining is conducted by the DNSSEC Policy Officer. He also determines the level of the skills of the personnel at the beginning of the training and uses this data to determine whether the frequency needs to be adjusted.

4.3.5. Job rotation frequency and sequence

No requirements.

4.3.6. Sanctions for unauthorised actions

Not disclosed in this document.

4.3.7. Contracting personnel requirements

Not applicable.

4.3.8. Documentation supplied to personnel

Documentation is provided to the personnel in electronic form where it is guaranteed that always the latest version is provided. Copies, both electronic and paper, are augmented by creation and expiration dates so that the personnel can determine the validity and accuracy of the copies.

4.4. Audit Logging Procedures

4.4.1. Types of events recorded

At least, the following events are recorded:

- signing
  - number of created and reused signatures
  - validity interval of signed zone
  - used keys
  - validation report
- key management
  - creation or deletion of keys
  - current phases of KSK/ZSK rollover processes with schedule
  - synchronisation status with mirror site
- manual interaction
  - start and stop of signing software
  - manual trigger of key rollover processes

4.4.2. Frequency of processing log

Audit logs are not processed automatically for the purpose of alerting. Instead, events that need attention by technical personnel are directly injected into the monitoring system and trigger the respective alert mechanisms.

Audit logs are reviewed in the context of error analysis and before and after manual interaction.

4.4.3. Retention period for audit log information

Audit logs are retained at least to that extend that the complete life cycle of a key can be traced two years after the end of its use for the signing process.

4.4.4. Protection of audit log

While audit logs do not contain any cryptographically sensitive information, they are protected from being accessed by personnel that does not represent one of the roles mentioned in Section 4.2.1.

The audit log files are administered by the DNSSEC System Administrator.

4.4.5. Audit log backup procedures

The audit log files are backed up as part of the system backup of the systems assigned for the DNSSEC signing process, using the same security constraints as for other data stored on the systems.

4.4.6. Audit collection system

Audit data is collected locally on the systems where the log events are generated. No special collection system is applied.

4.4.7. Notification to event-causing subject

Does not apply, as event escalation is handled separately.

4.4.8. Vulnerability assessments

The audit logs are periodically reviewed by the DNSSEC Policy Officer or his delegate to detect potential vulnerabilities on the one hand and to reevaluate the level of logging for that purpose on the other hand.

4.5. Compromise and Disaster Recovery

4.5.1. Incident and compromise handling procedures

If the private components of the zone and key signing keys have been compromised, or there is evidence that the key(s) might have been compromised, an emergency key rollover is conducted according to the procedures defined by the DNSSEC Policy Officer.

4.5.2. Corrupted computing resources, software, and/or data

If a hardware or software component fails and cannot be brought back into a working state within reasonable time, a switch-over to the mirror infrastructure at the secondary site is initiated.

4.5.3. Entity private key compromise procedures

The emergency key rollover procedures comprise a risk and impact analysis, which covers the evaluation of the extent of the security breach, whether it is

still in effect and, if so, how fast it can be fixed, the impact of the status quo on the users of the TLD and the speed of the execution of the available options for the mitigation, which may be dependent on external entities (like ICANN for changes to the root zone). The primary choices include the options to abort an ongoing rollover process, to initiate an emergency rollover process or, as last resort, to transfer the zone into the unsigned state by removing the respective DS record from the root zone.

4.5.4. Business Continuity and IT Disaster Recovery Capabilities

The disaster recovery strategy of the registry allows the switch-over from the primary site to the secondary site (and vice versa) within a short time frame. For this switch-over, it is not required (but helpful) if the original site is still accessible. In respect to DNSSEC, key management operations are executed in coordination with the mirror site in order to minimise the risk of losing the private key by which the zone is being signed.

4.6. Entity termination

In case that CORE Internet Council of Registrars terminates the operation of the .swiss TLD for whatever reason, CORE will cooperate with the successor at best effort and technical capabilities. This includes a smooth transition of the DNSSEC signing process, with a secured delivery of the private keys that are being used at that point in time.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

5.1.1. Key pair generation

The public/private key pair generation takes place via software in a secured environment. The private key is always stored in encrypted form.

5.1.2. Public key delivery

The public components of the key and zone signing keys are only published in the zone itself via the respective DNSKEY resource records.

5.1.3. Public key parameters generation and quality checking

The registry follows technological innovation and risk analysis of cryptographic algorithms and their parameters, especially with respect to key lengths. The algorithms and parameters are adjusted if need be.

5.1.4. Key usage purposes

The key and zone signing keys are solely used for the signing of the .swiss TLD and not for any other purposes.

5.2. Private key protection and Cryptographic Module Engineering Controls

5.2.1. Cryptographic module standards and controls

Not applicable.

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

The private key requires to be activated for the signing process by the DNSSEC Signing Operator.

5.2.3. Private key escrow

The private keys are not escrowed.

5.2.4. Private key backup

Private keys are copied to the secondary site in a secure manner as part of the creation process. New key pairs are not used in the signing process until the creation of the copy has been confirmed. Emergency procedures may nullify this rule, however.

5.2.5. Private key storage on cryptographic module

Not applicable.

5.2.6. Private key archival

Key pairs used for DNSSEC are archived for least two years after the termination of their use. Mechanisms ensure that the keys are not accidentally reused by the system during that time.

5.2.7. Private key transfer into or from a cryptographic module

Not applicable.

5.2.8. Method of activating private key

New zone signing keys are activated during the automatically performed rollover process. Key signing keys are manually activated by the DNSSEC Key Management Operator.

5.2.9. Method of deactivating private key

Zone signing keys are deactivated during the automatically performed rollover process. Key signing keys are manually deactivated by the DNSSEC Key Management Operator.

5.2.10. Method of destroying private key

Not applicable.

5.3. Other Aspects of Key Pair Management

5.3.1. Public key archival

Public keys are internally archived along with their private counterparts, as described in Section 5.2.6.

5.3.2. Key usage periods

- the zone signing key is used for signing no longer than for a period of 30 days
- the key signing key is used for signing no longer than for a period of one year

The times do not include wait times required within the key rollover processes.

5.4. Activation data

5.4.1. Activation data generation and installation

Not published.

5.4.2. Activation data protection

Not published.

5.4.3. Other aspects of activation data

Not published.

5.5. Computer Security Controls

Various provisions are made to increase the security of the computer systems used for the DNSSEC signing process:

- The systems are entirely reserved for and dedicated to the DNSSEC signing process, they are not used for any other services.

- The systems are protected by an internal firewall. Attempts to access the system from unauthorised addresses or at disallowed ports are logged and escalated.
- Only personnel representing the roles defined in Section 4.2.1 are allowed to access the system. The system uses a two-factor RSA authentication.

5.6. Network Security Controls

- The computer systems reside in a special network zone not accessible from outside. Systems and networks use private addresses (IPv4).
- Firewalls are configured to allow no access from outside and only from those internal systems that are designated to communicate with the DNSSEC related computer systems. Violations are logged and escalated.

5.7. Timestamping

Multiple time sources are used to detect time deviations of the systems that perform the zone signing. The signing process is suspended if the correctness of the time cannot be assumed. In this case, the problem is escalated.

5.8. Life Cycle Technical Controls

5.8.1. System development controls

The registry uses established software development, testing and change management processes to ensure the reliability and quality of the DNSSEC signing software. This includes reviews of the functional specification for completeness, accuracy and security and of the software for the implementation of the specification as well as for security vulnerabilities. Prior to the deployment of the software on production systems, it is installed and operated on test systems for security, stability and interoperability.

5.8.2. Security management controls

Measures are taken to retain integrity of the operating system, the application software and configuration files on the designated computer systems. In addition of the observance of various sources of known vulnerabilities and exposures (mailing lists, CVE databases etc.), digital hashes are created periodically

from executable files and from static configuration files of installed software. These are compared with those of previous runs to detect changes and the unexpectedly appearance or disappearance of files, which are then further investigated for their nature.

5.8.3. Life cycle security controls

Periodically, the security requirements for hard- and software components are revisited and adjusted for the current needs, including, but not limited to used protocols, cryptographic algorithms and key lengths. Deployed hard- and software components are reevaluated based on the requirements and on the history of discovered vulnerabilities and exposures.

If it is foreseeable that a component will no longer suffice the requirements in medium to long term, if the support of the component is discontinued by the manufacturer/developer or if the component has gained a bad reputation regarding its security so that an inherent insecurity can be assumed which cannot be mitigated by software/firmware updates, a system redesign containing a replacement of the respective component(s) is initiated.

For hardware, also the endurance is taken into account. To avoid the increasing probability of failure near the end-of-life of components, they are proactively replaced well before their expected lifetime.

6. ZONE SIGNING

Zone signing and the key management of the zone signing keys, including generation and rollover, is a fully automated process conducted by the signing software. The key management of the key signing keys is a semi-automated process, as the key rollover process needs human interaction with the root zone manager to perform the replacement of the delegation signer record(s) in the root zone.

6.1. Key lengths and algorithms

For the key signing key, the RSA algorithm with a key length of 2048 bits is used. For the zone signing key, the RSA algorithm with a key length of 1280 bits is used.

6.2. Authenticated denial of existence

To prove the non-existence of DNS resource record, signed NSEC3 and NSEC3PARAM records are added to the zone, as defined in RFC 5155. The "Opt-Out" feature of NSEC3 is not used, i.e. the non-existence of unsigned child zones can be proved. For the generation of the hash of the domain name, 0 iterations are performed with a salt of 4 bytes.

6.3. Signature format

Authoritative resource records of the .swiss zone are signed using the RSA-WITH-SHA256 algorithm.

6.4. Zone signing key rollover

The rollover of the zone signing key is automatically performed using the "key pre-publish" process as documented in RFC 4641.

6.5. Key signing key rollover

The rollover of the key signing key is performed using the "double signature" process as documented in RFC 4641. As the rollover of the key signing key re-

quires interaction with the parent zone (i.e. the root zone), the rollover includes human interaction.

6.6. Signature life-time and re-signing frequency

The signatures are valid for 14 days. Existing signatures are not replaced on each signing run. A minimum remaining signature validity period of 5 days is maintained. The inception time of the signatures is antedated by 2 hours to allow deviations of the system time of validating resolvers.

6.7. Verification of zone signing key set

After signing, the DNSKEY resource records along with the signatures (RRSIG resource records) are verified for validity, especially that the chain of trust remains intact.

6.8. Verification of resource records

For each signed resource record set, it is tested that the validity periods of the signatures suffice the requirements defined in Section 6.6. and that the signatures can be validated against the DNSKEY resource records contained in the zone.

6.9. Resource records time-to-live

The registry uses the following TTL values:

- DNSKEY: 12 hours
- NSEC3: 12 hours
- NSEC3PARAM: 12 hours
- DS: 12 hours
- RRSIG: same as the covered resource record set, as mandated by RFC 4035

7. COMPLIANCE AUDIT

To ensure that DNSSEC operations for the .swiss TLD are performed in compliance with all security policies, technical and organizational requirements, as well as best practices, audits are performed on a regular basis.

7.1. Frequency of entity compliance audit

Compliance audits for the .swiss TLD will be performed once per year. Under certain circumstances, such as after unforeseen incidents or in case of major changes to the involved infrastructure and processes, additional audits may be conducted.

7.2. Identity/qualifications of auditor

The auditor must be able to demonstrate proficiency in DNS and DNSSEC, encryption technologies, IT security techniques/tools and security auditing.

7.3. Auditor's relationship to audited party

In order to achieve an independent and unbiased assessment of the DNSSEC infrastructure deployed for the .swiss TLD, the appointed auditor shall be employed by an organization or company that is external to CORE Internet Council of Registrars.

7.4. Topics covered by audit

The audit will cover all DNSSEC operations in place for the .swiss TLD, including (but not limited to):

- key management procedures
- KSK/ZSK signature life cycle
- compliance with DNS/DNSSEC standards
- infrastructure controls
- security measures
- monitoring procedures
- backup procedures
- disclosure of practices

7.5. Actions taken as a result of deficiency

If any issues or deficiencies are found during the audit, the auditor will notify CORE Internet Council of Registrars at once. Based on the auditor's findings and recommendations, CORE Internet Council of Registrars will immediately deploy a team of experts to further assess the significance of the found issues, determine the course of action and prepare and execute a corrective action plan.

7.6. Communication of results

A written report containing the audit results shall be provided to CORE Internet Council of Registrars by the auditor no later than 14 calendar days after completion of the audit. In order to ensure expedited countermeasures in the event that severe issues or deficiencies are found, such findings are supposed to be immediately communicated to CORE Internet Council of Registrars verbally, i.e. in advance of the written report.

8. LEGAL MATTERS

8.1 Legal Status of this Document

This Document is a Policy Statement specifying the DNSSEC services provided by .swiss Registry, and does not constitute a contractual arrangement with any third party.

When applicable, its provisions are applied as DNSSEC Terms and Conditions through the .swiss Registry-Registrar Agreement; the .swiss Policies and Dispute Resolution Procedures, and the Registration Agreement between .swiss Registrars and Registrants.

8.2 Governing Law and Jurisdiction

The .swiss Registry is located in Switzerland. This DNSSEC Policy Statement shall be governed by the laws of the Swiss Confederation.

8.3 Personal Data Protection and Mandatory Disclosures

The .swiss Registry complies with Swiss Data Protection Legislation.

The .swiss Registry will only, and shall be entitled to, disclose private information when such disclosure is necessary in response to competent judiciary or administrative requests.