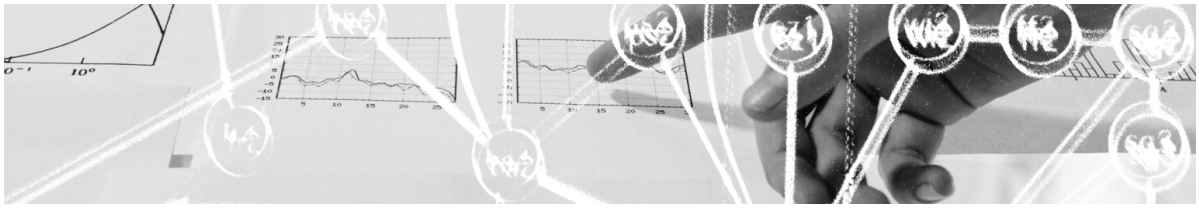
SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

DNSSEC Key Management Practice Statement



Version:	V1.4
Created:	23.08.18
Last changes:	23.08.18

Introduction

1.1 Document scope, document updates

This document describes the practices of SWITCH when managing cryptographic key material for securing the *.ch* and *.li* top-level domains by means of the domain name system security extensions (DNSSEC). Specifically, it covers the management of the key signing and zone signing keys for these TLDs.
SWITCH reserves the right to amend this practice statement as it sees fit, e. g. when required by updated technical recommendations on key sizes, hashing algorithms or other implementation properties. New versions of this document become effective by the date of their publication on the www.nic.ch website.

1.2 Glossary

DNSSEC: domain name system security extensions, as specified in RFCs 4033 to 4035. DNSSEC adds data origin authentication and data integrity to the domain name system.
DS record: a record in the domain name system which is used to uniquely identify a specific key. A DS record consists of a key tag, an algorithm number, and a digest (hash) of that key.
Key Signing Key (KSK): a cryptographic key used to sign one or more zone signing keys. Key signing keys are “long-lived” in the sense that they typically have an effectivity period of one or more years.
Key Rollover: the replacement of an existing key signing key or zone signing key by a new cryptographic key.
Zone Signing Key (ZSK): a cryptographic key used to sign a DNS zone, such as *.ch* or *.li*. Zone signing keys are “short-lived” and have a typical effectivity period of one or two months.

1.3 References

[FIPS140-2] National Institute of Standards and Technology (NIST): *Security requirements for cryptographic modules.* May 2001.
[FIPS180-3] National Institute of Standards and Technology (NIST): *Secure hash standard (SHS).* October 2008.
[RFC3447] Jonsson, Jakob / Kaliski, Burt: *Public-key cryptography standards (PKCS) #1: RSA cryptography specifications version 2.1.* February 2003.
[RFC4033] Arends, Roy / Austein, Rob / Larson, Matt / Massey, Dan / Rose, Scott: *DNS security introduction and requirements.* March 2005.
[RFC4034] Arends, Roy / Austein, Rob / Larson, Matt / Massey, Dan / Rose, Scott: *Resource records for the DNS security extensions.* March 2005.
[RFC4035] Arends, Roy / Austein, Rob / Larson, Matt / Massey, Dan / Rose, Scott: *Protocol modifications for the DNS security extensions.* March 2005.
[RFC4641] Kolkman, Olaf / Gieben, Miek: *DNSSEC operational practices.* September 2006.
[RFC4641bis] Kolkman, Olaf / Mekking, Matthijs: *DNSSEC operational practices, version 2* (draft-ietf-dnsop-rfc4641bis-12). July 16, 2012, work in progress.

2 Key generation and storage

For all cryptographic key material generated by SWITCH for its DNSSEC implementation, the following stipulations apply:

- Key generation takes advantage of a hardware-based random number generator whose output is compliant with [FIPS140-2].
- Keys are generated on a standalone offline system, which is never connected to any network. Only the minimum set of software packages required for DNSSEC key management operations is installed on this system.
- All key pairs are based on the ECDSA algorithm and its specified usage in DNSSEC [RFC6605].
- The Key Signing Key (KSK) and Zone Signing Key (ZSK) function is split into separate keys. KSKs have a key size of 256 bits and ZSK of 256 bits which has an approximate equivalent strength to RSA with 3072-bit keys.
- Distinct sets of keys are used to secure the *.ch* zone on the one hand and the *.li* zone on the other hand.
- For hashing, the SHA-256 standard is used, as specified in [FIPS180-3].

2.1 Key Signing Keys

When stored in non-volatile memory, key signing keys are always encrypted. The key for their protection is split into five shares, which are assigned to five different persons. By this form of secret sharing, a 3-out-of-5 access control mechanism is implemented for the key signing keys. For the TLD .ch the shares are assigned to permanently employed SWITCH staff as well as the BAKOM. For the TLD .li all shares are assigned to permanently employed SWITCH staff.
KSKs are stored on at least two different types of media, and are kept in a fire and burglar resistant, strictly access controlled safe. The five key share holders are obliged to keep their shares safe as well. The keys are only loaded into the primary memory of the offline system when needed for DNSSEC signing operations.

2.2 Zone Signing Keys

When stored on a permanent file system, zone signing keys are always encrypted. The current ZSK which is used for signing the *.ch* and *.li* zones is kept on the hidden primary DNS server for these zones, and needs to be unlocked on this system at boot time. The ZSK is encrypted and only accessible to the system administrators from SWITCH staff who are in charge of operating the hidden primary DNS server for the *.ch* and *.li* zones.
Zone signing keys are transferred from the offline system to the primary DNS server on removable media, in encrypted form only.

3 Key Use

3.1 Key Signing Keys

Key signing keys for the *.ch* and *.li* TLDs have an effectivity period of 396 days, and are rolled over on a yearly basis. For the rollover, the “double signature” mechanism defined in [RFC4641], section 4.2.1.2., is used, with a period of 30 days between the “new DNSKEY” and the “DNSKEY removal” stage.
The DS records of the key signing keys are published on the www.nic.ch website, in addition to being included in the root zone (which has been signed since 15 July 2010).
The validity period of RRSIG records signed by SWITCH’s key signing keys are linked to the zone’s SOA expire time. As of now, the validity period is 46 days.

3.2 Zone Signing Keys

Zone signing keys for the *.ch* and *.li* zones have an effectivity period of 37 days, and are rolled over on a monthly basis. For the rollover, the “pre-publish” mechanism defined in [RFC4641], section 4.2.1.1., is used, with a period of 60 days between the “new DNSKEY” and the “DNSKEY removal” stage.
RRSIG records signed by SWITCH’s zone signing keys have a validity of at most 30 days.

3.3 Emergency Rollover

An emergency replacement of either key signing keys or zone signing keys can be required (but is not necessarily limited to) the following situations:

- The key pair has been compromised, i. e. becomes/is known to unauthorized parties due to theft, exhaustive search or other forms of attack.
- SWITCH loses access to the private key, e. g. as a result of a hardware failure, human errors or other events.
- Weaknesses in the public-key and/or hashing algorithms used for the SWITCH DNSSEC implementation are identified through new research and require immediate replacement.

If the need for an emergency rollover has been determined, SWITCH will discontinue the use of the relevant private key(s) as soon as possible, and use the rollover mechanism which is most suitable to that particular situation. SWITCH will take all possible measures to keep the chain of trust intact at all times, while at the same time trying to minimize the window of vulnerability.