DNSSec Operation Manual for the .cz and 0.2.4.e164.arpa Registers

version 1.9., valid since 1 January 2010

Introduction

This material lays out operational rules that govern the work of the CZ.NIC association in administering the DNSSEC keys, namely procedures for their generation, rotation, physical security and publishing.
It lays out rules for signing a zone file and determines persons responsible for individual operations.
This material is public.

Communication

Data about keys of individual domains are entered into the register through registrars. Communication with registrars is governed by relevant documents, in particular by Business Terms and Conditions for Registrars, Rules of Domain Names Registration under ccTLD .cz a Communication Rules. All these documents are available on the website of the CZ.NIC association.

Registrar's requirements are entered into the registry by means of a standard EPP protocol (pursuant to RFC 3730-3734) with extensions and changes brought about by the specific characteristics of the register. Communication takes place by means of SSL-secured TCP connection.

Contact persons from the contact list who have enabled e-mail notifications (including those removed in the UPDATE task) will be informed per e-mail about operations (CREATE, UPDATE, TRANSFER and DELETE) on relevant data structures (KEYSET, DOMAIN).

Administration of DNSSEC keys

Key generation

Key Signing Key

A special HSM module with PKCS#11 support is dedicated to KSK administration.
The HSM module and service server are only used to generate KSKs and ZSKs and for signing the zone apex that contains all keys of the relevant zones that are KSK-signed.
In the current version of the system, the HSM module is not used (it is not compatible with the current BIND version). Dedicated disk storages are temporarily used for administration of keys. To protect all KSKs from

being compromised, one KSK will be stored on the USB flash disk that will be stored offline in a safe place (a safe deposit). This USB flash disk will only be used when all KSKs are compromised. The key stored on the USB flash disk will not be used in normal operation. A public part of the offline key will be displayed in the ITAR register and published in the .cz zone. The key will be rotated in a standard way like online KSKs. Persons authorized to access the safe deposit will make sure that the offline key is available when needed.

Key algorithm:	RSA 2048 bits
Number of keys:	3 (1 active)
Key storage:	dedicated server disk (in future HSM)

Zone Signing Key

After generating the ZSK and signing the zone apex, ZSK and zone apex are transferred to the server that is used for signing the zone.
The process of zone signing is automatic.

Key algorithm:	RSA 1024 bits
Number of keys:	2 (1 active)
Key storage:	dedicated server disk

Dedicated servers

Physical location of servers

For the sake of redundancy, there are two dedicated servers on which keys are stored. They are located in two telehouses, operated by two different companies.

The servers are placed in locked racks and, in the case of one of the telehouses, in a dedicated space separated by a cage. Physical access to servers is granted to technical administrators and, upon request, also to employees of both telehouses.

Both telehouses can be accessed through a lodge manned by a porter who verifies authorization for access. Furthermore, one of the telehouses is protected by a surveillance camera system, and the other is connected to the operator’s CCTV system. Contactless sensors are fitted on racks. They monitor unauthorized opening of rack doors.

Access to servers

Dedicated servers are connected to the Internet in a separated network (VLAN) and are available through SSH and DNS protocols. Servers are also interconnected with the application server of the central register. Technical administrators have accounts for access through the SSH protocol. Access to the administrator account takes place through the SUDO mechanism.

Server back-up

Servers are backed up on a back-up server using standard mechanisms. Access to the back-up server is subject to the same conditions as access to the dedicated servers for administration of DNSSEC keys.

Key rotation

Key Signing Key

A mechanism of double signature is used for KSK rotation. KSK replacement will be announced half a year in advance (see the section Key publishing).
After the implementation of the key rotation mechanism described in the RFC 5011 document into the tools of BIND9 DNS server, the key rotation will proceed this way:

Key validity:	2 years
Rotation method:	manual

Rotation in case of key compromising

When CZ.NIC loses control over private parts of keys, new DNSSEC need to be generated so they can replace existing keys. When keys are compromised, rotation has to proceed like in case of normal rotation, i.e. so that the operation of the .cz zone is not interrupted.
When KSKs are compromised, new KSKs will be generated and DS records in the root zone, in DLV and in ITAR register will be replaced.
When just one KSK is compromised, the removal from the parent zone and generation of new ZSK are sufficient.

Zone Signing Key

The validity of an active ZSK is 8 weeks. ZSK rotation takes place every two months using the mechanism of key publishing in advance (RFC 4641, 4.2.1.1). At least two ZSKs are published in the zone. One is active and the other is published in advance. During rotation, the active key is marked as deprecated and the published key is marked as active. When the necessary period expires (see RFC 4641), the deprecated key is removed from the zone and a new ZSK is generated and marked as published.

Key validity:	90 days
Rotation method:	automatic (ZKT)

Rotation in case of key compromising

When the ZSKs are compromised, a new ZSK set is generated, apex zones are signed and the ZSK set is replaced.
When just one ZSK is compromised, it has to be removed from the zone file.

An example of the key list:

Keyname	Tag	Type	Status	Algorithm	Valid
0.2.4.e164.arpa.	31,333	KSK	active	RSASHA1	12 years
0.2.4.e164.arpa.	7,834	KSK	active	RSASHA1	2 years
0.2.4.e164.arpa.	23,092	KSK	backup	RSASHA1	2 years
0.2.4.e164.arpa.	15,590	ZSK	active	RSASHA1	3 months
0.2.4.e164.arpa.	42,605	ZSK	publish	RSASHA1	3 months
cz.	7,978	KSK	active	RSASHA1	12 years
cz	1,234	KSK	publish	RSASHA1	2 years
cz	58,372	KSK	backup	RSASHA1	2 years
cz.	50,820	ZSK	active	RSASHA1	3 months
cz.	47,420	ZSK	publish	RSASHA1	3 months

Key publishing

Parent zone supports secure delegation

KSKs for zones administered by the central register that have a signed parent zone, which permits secure delegation, will be placed in the parent zone. Currently, this only applies to the 0.2.4.e164.arpa domain which is securely delegated in the e164.arpa zone.

The parent zone does not support secure delegation

KSKs for zones administered by the central register that do not have a signed parent zone have to be announced to users in another way.

Websites

KSK is published at https://www.nic.cz/dnssec/. Websites are protected by a commercial SSL certificate. The algorithm applied is PKCS #1 SHA-1 With RSA Encryption and the key length is 1024 bits. The KSK is signed by the assigned PGP/GPG key 1024D/7140F726, CZ.NIC DNSSEC KSK Signing Key <dnssec@nic.cz> so that validity is ensured even when websites are compromised.
The fingerprint of this key is 07AD 2796 36B0 40DA 6FA8 22FE A199 A19B 7140 F726.

Mailing list

The KSK is sent to the dnssec-announce@lists.nic.cz mailing list. The new KSK will be signed by the PGP/GPG key 1024D/7140F726.

Domain Look-aside Validation (DLV) register

Since the root zone is not signed, the DNSSEC Look-aside Validation (RFC 5074) mechanism is used for publishing of DS records.
The service provided by the ISC association at dlv.isc.org is used.

Temporary register of fixed points of confidence (ITAR)

DS records related to .cz are also published in a temporary storage of trustworthy ITAR keys operated by the IANA organization.

Signing the zone file

A dedicated set of keys is kept for every zone administered by the central register. Keys are divided into Key Signing Keys (KSK) and Zone Signing Keys (ZSK).

Process of signing the zone file

Generation of RRSIG signatures takes place on a dedicated server that also generates a zone file.
The .cz zone file is generated every 30 minutes and new as well as changed records are signed after every generation.
After generating the zone file, RRSIG records are extracted from the old signed zone file and they are subsequently merged with a newly generated zone file. The merged zone file is signed with the dnssec-signzone tool from the BIND9 package that can use valid signatures. Changes in signatures are thus limited to the inevitable ones.

Validity of RRSIG signatures

The validity of RRSIG signatures is 1 month. A new signature is generated 1 week before the expiration of the existing signature.

Appointment of responsible persons

The subsequent table lays out competences of individual persons in relation to specific critical activities connected (in particular) with generation of keys.

Task	Performed by
generation of a new KSK	always two out of the following: manager, operations manager, technical manager
signing ZSK by means of KSK	authorized member of the DNSSEC team
KSK rotation	one of the following: manager, operations manager, technical manager
SZK rotation	automatic tool
back-up of KSKs on external storage	one of the following: manager, operations manager, technical manager
Access to safe deposit	manager, operations manager

Glossary

Key Signing Key (KSK)
DNSSEC key used only to sign other keys (DNSKEY RRSet) in a specific zone.

Zone Signing Key (ZSK)
DNSSEC key used to sign the whole zone file.

Domain Lookaside Validation (DLV)
The way of online validation of DNSSEC signatures through special DLV records which contain authoritative data about KSK data used to sign the zone. The best known and most used DLV register is operated by the Internet Systems Consortium (ISC) organization at div.isc.org.

Interim Trust Anchor Repository (ITAR)
Temporary offline storage for keys used for top-level domains. This storage is operated by the IANA organization at http://itar.iana.org/.

Key compromising
DNSSEC keys use asymmetric cryptography. A key is compromised when its private part used for signing ends up in the hands of people who are not authorized to tamper with it or to sign the zone. It can be an internal security incident provoked by an employee of the association or an external security incident, i.e. when the security of private parts of the key or the cryptographic algorithms of the key are compromised.

Key rotation

For the sake of security of asymmetric cryptography, DNSSEC keys used to sign the zone need to be changed regularly so that the keys are not compromised. Key rotation is a process of changing a DNSSEC key (KSK or ZSK) for a new one. The process needs to be performed in such a way so that an interruption of validation of the signed zone is technically impossible.