Provozní manuál DNSSec pro registr .cz a 0.2.4.e164.arpa

verze 1.9., platná od 1.1.2010

Úvod

Tento materiál určuje provozní pravidla, kterými se řídí sdružení CZ.NIC při správě DNSSEC klíčů, konkrétně postupy pro jejich generování, rotaci, fyzické zabezpečení a zveřejňování.
Stanovuje pravidla pro podepisování zónového souboru a určuje osoby, odpovědné za jednotlivé úkony.
Tento materiál je veřejný.

Komunikace

Údaje o klíčích jednotlivých domén jsou ukládány do registru prostřednictvím registrátorů. Komunikace s registrátory se řídí příslušnými dokumenty, zejména Obchodními podmínkami pro registrátory, Pravidly registrace doménových jmen a Pravidly technické komunikace. Všechny tyto dokumenty jsou k dispozici na stránkách sdružení CZ.NIC.

Požadavky registrátorů jsou do registru zasílány standardním EPP protokolem (dle RFC 3730-3734) s rozšířeními a změnami vynucenými specifickými vlastnostmi registru. Komunikace probíhá TCP spojením zabezpečeným pomocí SSL.

O provedených operacích (CREATE, UPDATE, TRANSFER a DELETE) nad příslušnými datovými strukturami (KEYSET, DOMAIN) jsou prostřednictvím e-mailu informovány kontaktní osoby ze seznamu kontaktních osob, které mají nastaven notify email a to i ty, které byly v operaci UPDATE odstraněny.

Správa DNSSEC klíčů

Generování klíčů

Key Signing Key

Pro správu KSK je vyhrazen speciální modul HSM s podporou PKCS#11.
Modul HSM a obslužný server je používán pouze pro potřeby vygenerování nových KSK a ZSK klíčů a podepsání tzv. zone apexu, který obsahuje všechny klíče příslušné zóně podepsané pomocí KSK.
V aktuální verzi systému není modul HSM použit (není kompatibilní se současnou verzí BIND). Pro správu klíčů se dočasně používají vyhrazená disková úložiště. Z důvodů ochrany před kompromitací všech KSK klíčů bude jeden z KSK klíčů uložen na USB flash disku, a tento USB disk bude uložen offline na bezpečném místě (trezor). Tento USB flash disk bude použit pouze v případě kompromitace všech KSK

klíčů, při normálním provozu nebude klíč uložený na USB flash disku využíván.

Algoritmus klíče:	RSA 2048 bitů
Počet klíčů:	3 (aktivní 1)
Úložiště klíčů:	disk dedikovaného serveru (v budoucnu HSM)

Zone Signing Key

Po vygenerování ZSK a podepsání zone apexu jsou ZSK a zone apex přeneseny na server, který je určen k podepisování zóny.
Samotný proces podepisování zóny probíhá automaticky.

Algoritmus klíče:	RSA 1024 bitů
Počet klíčů:	2 (aktivní 1)
Úložiště klíčů:	disk dedikovaného serveru

Dedikované servery

Fyzické umístění serverů

Dedikované servery, na kterých jsou uloženy klíče, jsou z důvodů redundance dva a jsou umístěny ve dvou telehousech, provozovaných dvěma různými společnostmi. Servery jsou umístěny v zamčených stojanových rozvaděčích (rack) a v případě jednoho z telehousů navíc ve vlastním prostoru odděleném klecí. Fyzický přístup k serverům mají techničtí správci a na vyžádání i zaměstnanci obou telehousů. Přístupy do obou telehousů jsou realizovány přes vrátnici s fyzickým vrátným, který kontroluje oprávnění k přístupu. Dále je jeden z telehousů chráněn interním kamerovým systémem, druhý je potom napojen na vnitřní kamerový systém provozovatele. Na jednotlivých stojanech jsou instalována bezkontaktní čidla, které monitorují neautorizované otevření dveří stojanů.

Přístup na servery

Dedikované servery jsou připojeny do sítě internet v oddělené síti (VLAN) a jsou přístupné pomocí protokolů: SSH a DNS. Servery mají také propojení na aplikační server centrálního registru. Přístup pomocí protokolu SSH mají techničtí správci přes přidělené účty. Přístup na účet administrátora je realizován pomocí mechanismu SUDO.

Zálohování serverů

Servery jsou zálohovány standardními mechanismy na zálohovací server. Přístup na zálohovací server podléhá stejným podmínkám jako přístup na dedikované servery pro správu DNSSEC klíčů.

Rotace klíčů

Key Signing Key

Pro rotaci klíčů KSK se používá mechanismus dvojitého podpisu. Výměna klíče KSK bude zveřejněna v předstihu půl roku (viz. oddíl zveřejňování klíčů).
Po implementaci mechanismu rotace klíčů popsaného v dokumentu RFC 5011 do nástrojů DNS serveru Bind 9, bude rotace klíčů prováděna tímto způsobem.

Platnost klíče:	2 roky
Metoda rotace:	ručně

Rotace v případě kompromitace klíče

Pokud CZ.NIC ztratí kontrolu nad privátními částmi klíčů, je zapotřebí vygenerovat nové DNSSEC klíče a nahradit jimi stávající klíče. Rotaci klíčů v případě kompromitace je zapotřebí provést stejnými postupy jako běžnou rotaci, tedy tak, aby nedošlo k výpadku chodu zóny .cz
V případě kompromitace KSK budou vygenerovány nové KSK klíče a nahrazeny DS záznamy v kořenové zóně, v DLV a ITAR registru.
Pro případ kompromitace jen jednoho z KSK klíčů stačí jen odstranění z nadřazené zóny a vygenerování nových ZSK.

Zone Signing Key

Platnost aktivního ZSK klíče je stanovena na 8 týdnů. Rotace klíčů ZSK tedy probíhá každé dva měsíce pomocí mechanismu zveřejnění klíče předem (RFC 4641, 4.2.1.1). V zóně jsou publikovány vždy minimálně dva ZSK klíče – jeden aktivní (active) a jeden předem publikovaný (published). Při rotaci se aktivní klíč označí jako prošlý (deprecated) a publikovaný klíč se označí jako aktivní. Po uplynutí potřebné doby (viz. RFC 4641) je ze zóny odstraněn prošlý klíč a je vygenerován nový ZSK klíč, který je označen jako publikovaný.

Platnost klíče:	90 dní
Metoda rotace:	automaticky (ZKT)

Rotace v případě kompromitace klíče

V případě kompromitace ZSK bude vygenerována nová sada ZSK, podepsány apex zóny a nahrazena sada ZSK.
V případě kompromitace jen jednoho ze ZSK je potřeba jeho vyřazení ze zónového souboru.

Příklad seznamu klíčů

Keyname	Tag	Type	Status	Algorithm	Valid
0.2.4.e164.arpa.	31333	KSK	active	RSASHA1	12 years
0.2.4.e164.arpa.	7834	KSK	active	RSASHA1	2 years
0.2.4.e164.arpa.	23092	KSK	backup	RSASHA1	2 years
0.2.4.e164.arpa.	15590	ZSK	active	RSASHA1	3 months
0.2.4.e164.arpa.	42605	ZSK	publish	RSASHA1	3 months
cz.	7978	KSK	active	RSASHA1	12 years
cz	1234	KSK	publish	RSASHA1	2 years
cz	58372	KSK	backup	RSASHA1	2 years
cz.	50820	ZSK	active	RSASHA1	3 months
cz.	47420	ZSK	publish	RSASHA1	3 months

Zveřejňování klíčů

Nadřazená zóna podporuje bezpečnou delegaci

KSK klíče pro zóny spravované centrálním registrem, které mají podepsanou nadřazenou zónu a ta umožňuje bezpečnou delegaci, budou umístěny v nadřazené zóně. V současné době se jedná pouze o doménu 0.2.4.e164.arpa, která je bezpečně delegována v zóně e164.arpa.

Nadřazená zóna nepodporuje bezpečnou delegaci

KSK klíče pro zóny spravované centrálním registrem, které nemají podepsanou nadřazenou zónu, musí být směrem k uživatelům komunikovány jiným způsobem.

Webové stránky

KSK klíč je zveřejněn na stránkách https://www.nic.cz/dnssec/. Webové stránky jsou chráněny komerčním SSL certifikátem. Použitý algoritmus je PKCS #1 SHA-1 With RSA Encryption, a délka klíče je 1024 bitů. KSK klíč je podepsán určeným PGP/GPG klíčem 1024D/7140F726, CZ.NIC DNSSEC KSK Signing Key <dnssec@nic.cz>, aby byla zajištěna validita i v případě kompromitace webových stránek. Fingerprint tohoto klíče je: 07AD 2796 36B0 40DA 6FA8 22FE A199 A19B 7140 F726.

Poštovní konference

KSK klíč je zaslán do poštovní konference dnssec-announce@lists.nic.cz. Nový KSK klíč bude podepsán PGP/GPG klíčem 1024D/7140F726.

Domain Look-aside Validation (DLV) registr

Vzhledem k tomu, že kořenová zóna není podepsaná, je pro publikování DS záznamů využit mechanismus DNSSEC Look-aside Validation (RFC 5074).
Použita je služba poskytovaná sdružením ISC na adrese dlv.isc.org.

Dočasný registr pevných bodů důvěry (ITAR)

DS záznamy k .cz jsou zároveň publikovány i v dočasném úložišti důvěryhodných klíčů ITAR, provozovaném organizací IANA.

Podepisování zónového souboru

Pro každou zónu spravovanou centrálním registrem je udržována vlastní sada klíčů. Klíče jsou rozděleny na klíč podepisující klíče – KSK (Key Signing Key) a zónu podepisující klíče – ZSK (Zone Signing Key).

Proces podepisování zónového souboru

Generování podpisů RRSIG probíhá na dedikovaném serveru, který zároveň generuje zónový soubor. Zónový soubor .cz je generován každých 30 minut a po každé generaci jsou podepsány nové a změněné záznamy.
Po vygenerování zónového souboru jsou ze starého podepsaného zónového souboru extrahovány záznamy RRSIG a tyto jsou sloučeny s nově vygenerovaným zónovým souborem. Pro podepsání sloučeného zónového souboru je používán nástroj dnssec-signzone z balíku Bind 9, který umí použít stále platné podpisy. Změny v podpisech jsou tímto způsobem omezeny na nutné minimum.

Doba platnosti podpisů RRSIG

Platnost podpisů RRSIG je stanovena na 1 měsíc. Nový podpis je vygenerován 1 týden před skončením platnosti stávajícího podpisu.

Stanovení odpovědných osob

Následující tabulka určuje pravomoci jednotlivých osob ve vztahu ke konkrétním kritickým činnostem, souvisejících (zejména) s generováním klíčů.

Akce	Provádí
vygenerování nového KSK	vždy dva z: ředitel, provozní ředitel, technický ředitel
podepsání ZSK pomocí KSK	pověřený člen DNSSEC týmu
rotace KSK	jeden z: ředitel, provozní ředitel, technický ředitel
rotace ZSK	automatický nástroj
záloha KSK klíčů na externí médium	jeden z: ředitel, provozní ředitel, technický ředitel
Přístup do trezoru	ředitel, provozní ředitel

Slovníček pojmů

Key Signing Key (KSK)
DNSSEC klíč používaný pouze k podpisu dalších klíčů (DNSKEY RRSet) v konkrétní zóně.

Zone Signing Key (ZSK)
DNSSEC klíč používaný k podpisu celého zónového souboru.

Domain Lookaside Validation (DLV)
Způsob online validace DNSSEC podpisů pomocí speciálních DLV záznamů, ve kterých jsou uloženy autoritativní záznamy o KSK klíčích použitých pro podpis zóny. Nejznámější a nejpoužívanější DLV registr je provozován organizací Internet Systems Consortium (ISC) na adrese dlv.isc.org.

Interim Trust Anchor Repository (ITAR)
Dočasné off-line úložiště klíčů používaných pro doménová jména nejvyšší úrovně. Toto úložiště je provozováno organizací IANA na adrese http://itar.iana.org/.

Kompromitace klíče
DNSSEC klíče používají asymetrickou kryptografii. Ke kompromitaci klíče dochází ve chvíli, kdy se soukromá část klíče používaná pro podpis dostane k osobám, které nejsou oprávněny k manipulaci s tímto

klíčem, nebo k podepisování zóny. Může se jednat o interní bezpečnostní incident vyvolaný zaměstnancem sdružení nebo externí bezpečnostní incident, tedy prolomení zabezpečení soukromé částí klíče, nebo prolomení kryptografických algoritmů klíče.

Rotace klíče

Z hlediska bezpečnosti asymetrické kryptografie je zapotřebí DNSSEC klíče používané pro podpis zóny pravidelně měnit, aby nemohlo dojít ke kompromitaci klíče. Rotace klíče je proces, kdy se mění DNSSEC klíč (KSK nebo ZSK) za nový. Tento proces je potřeba provádět tak, aby technicky nemohlo dojít k výpadku validace podepsané zóny.