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

verze 2.0., platná od 1.3.2011

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.

Algoritmus klíče:	RSASHA512 2048 bitů
Počet klíčů:	**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:	RSASHA512 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.

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).

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.

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 je standardně publikován jeden ZSK klíč se který se kterým se podepisuje. 7 dní před uplynutím dvouměsíčního období je předem publikovaný nový klíč. Tímto novým klíčem se začne podepisovat se započetím dalšího dvouměsíčního období. Po uplynutí potřebné doby (viz. RFC 4641) je starý klíč se zóny odstraněn.

Platnost klíče:	56dní
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.

Zveřejňování klíčů

DS záznamy pro .CZ jsou publikovány v kořenové zóně spravované ICANN/IANA, DS záznamy pro 0.2.4.e164.arpa jsou umístěny v zóně e164.arpa spravované RIPE NC

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 14 dni. 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.

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.