

# DNSSEC na vlastní doméně snadno a rychle

Ondřej Caletka



1996–2016

**CESNET**

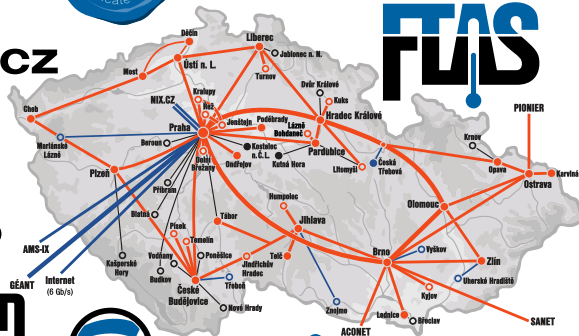
SPOLUPRÁCE  
VÝZKUM  
KOMUNITA

5. listopadu 2016



Uvedené dílo podléhá licenci Creative Commons Uvedte autora 3.0 Česko.

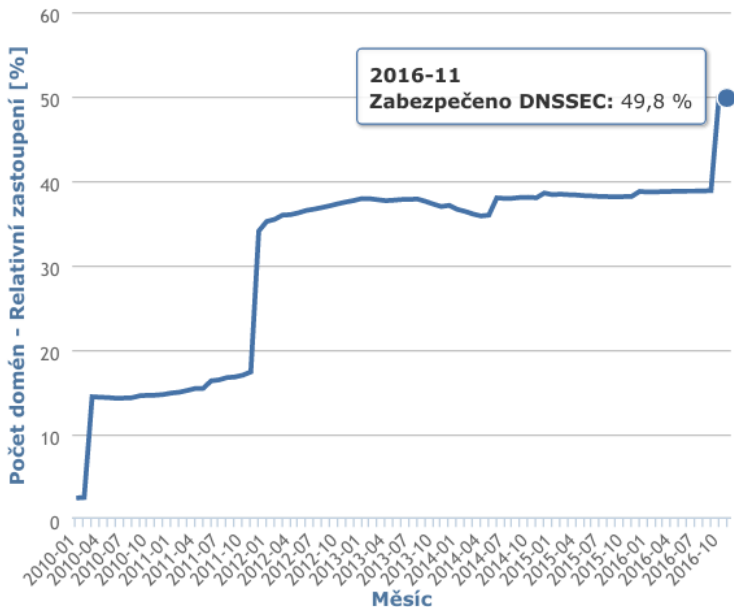
# 0 sdružení CESNET



# Když se řekne DNSSEC

- end-to-end zabezpečení autenticity DNS zpráv
- majitel domény podepisuje, kdokoli může validovat
- hierarchická delegace důvěry
  - v nadřazené zóně je umístěn otisk klíče (DS záznam)
  - otisk klíče kořenové zóny je součástí validátoru
- i u nepodepsané domény probíhá validace nadřazených zón
  - až po podepsanou informaci, že další zóny podepsány nejsou

## Zavádění DNSSEC



Ondřej

https://prod.eet.cz

← → ↻ https://prod.eet.cz/eet/serv **6**

This XML file d  
it. The document

**prod.eet.cz**  
**Zabezpečeno DNSSEC**

Doménové jméno prod.eet.cz je korektně zabezpečeno DNSSEC technologií.

Více info

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Body>
    <env:Fault type="soap:env:Receiver" faultcode="EETRequestProcessingError" faultstring="EET Request processing: Unrecognized resource requested in URI /eet/services/EETServiceSOAP/v3. Please, see EET service documentation."/>
  </env:Body>
</env:Envelope>
```

# Validace v prohlížeči

- rozšíření DNSSEC a TLSA validátor
- obsahuje kompletní DNSSEC resolver
- kontroluje, zda se prohlížeč připojuje na správnou adresu
- nezasahuje do validace TLS spojení v prohlížeči



# Validace na serveru / domácím routeru

- stačí aktuální BIND, Unbound, nebo Knot DNS Resolver
- konfigurace je obvykle připravena, stačí vložit klíč kořenové zóny
- režim plné rekurze nebo forwardování na nadřazený DNS server
  - problémy s chybami v nadřazených serverech znemožňující validaci některých jmen
  - režim plné rekurze špatně škáluje, vyžaduje nezasahování ISP do udp/53 provozu



# Problém poslední míle

- DNSSEC z principu nechrání před útokem na poslední míli mezi validátorem a konzumentem
- specifikace nařizuje bezpečný kanál
- jsou-li pochybnosti o bezpečnosti kanálu, je nutné kritická data znovu validovat
- validace na vzdáleném serveru hlavně chrání server před otrávením své vlastní cache



# DNSSEC detekuje, ale neopravuje

Součástí specifikace DNSSEC není **křišťálová koule**. Validátory manipulaci detekují, ale nejsou schopny zmanipulovaná data opravit.

Nejčastější příčiny nevalidních DNS dat:

- zastaralé verze rekurzivních DNS serverů
- nevhodné konfigurace firewallů
- captive portály
- **chyba na straně držitele domény**

# DNSSEC na vlastním serveru

- vyrobit klíč(-e)
- klíči *pravidelně* podepisovat všechny DNS záznamy
- umístit otisk klíče do nadřazené zóny
- klíče *pravidelně* vyměňovat

## Zjednodušení s eliptickými křivkami

- použití eliptických křivek generuje krátké a silné klíče
- takové není třeba měnit dříve než za několik let
- pro celou doménu nám stačí jediný klíč

# In-line signing v BIND 9.9

- automaticky pravidelně podepisuje zónu
- nemění původní zónové soubory
- vyžaduje ruční generování klíčů

Na nás tedy zbývá:

- 1 vygenerovat klíč
- 2 upravit konfiguraci
- 3 publikovat DS záznam v nadřazené zóně

# Základem je dostatek entropie

- generování klíčů i podpisů potřebuje náhodná čísla
- standardně se používá /dev/random
- není-li v systému dostatečná entropie, celý BIND vytuhává
- použití /dev/urandom není bezpečné
- správné řešení: instalace haveged

```
# apt-get install haveged
```

# Výchozí stav

## Zónový soubor v /etc/bind

```
$ORIGIN openalt.acad.cz.  
$TTL 60  
@      IN SOA  oans.acad.cz. adm 1 120 10 3600 60  
@      IN NS   oans.acad.cz.  
ww     IN A    192.0.2.53  
       IN AAAA 2001:db8::53
```

## Konfigurace v named.conf.local

```
zone "openalt.acad.cz" {  
    type master;  
    file "/etc/bind/openalt.acad.cz";  
};
```



# Vygenerujeme klíče

- nutno upravit práva, aby BIND mohl číst privátní klíče
- symlinkujeme zónový soubor do pracovního adresáře

```
# mkdir /etc/bind/keys
# cd /etc/bind/keys
# dnssec-keygen -a ECDSAP256SHA256 -fK openalt.acad.cz
Generating key pair.
Kopenalt.acad.cz.+013+24937
# chmod g+r K*.private
# ln -s /etc/bind/openalt.acad.cz /var/cache/bind/
```

# Upravíme konfiguraci

## Konfigurace zóny v `named.conf.local`

```
zone "openalt.acad.cz" {  
    type master;  
    file "openalt.acad.cz";  
    inline-signing yes;  
    auto-dnssec maintain;  
    key-directory "/etc/bind/keys";  
};
```

Po reloadu vzniknou v pracovním adresáři soubory:

`openalt.acad.cz.jnl` žurnál změn v originálním souboru

`openalt.acad.cz.signed` podepsaný zónový soubor

`openalt.acad.cz.signed.jnl` žurnál podepsaného souboru



# Máme podepsáno

- případné změny jsou automaticky podepisovány
- podpisy jsou automaticky obnovovány
- zbývá o tom dát vědět nadřazené zóně
  - **.cz, .eu** registrátorovi předáme přímo veřejný klíč
  - **ostatní** registrátorovi předáme DS záznam vygenerovaný z veřejného klíče a doménového jména

```
# dnssec-dsfromkey /etc/bind/keys/Kopenalt.acad.cz.+013+24937.key  
openalt.acad.cz. IN DS 24937 13 1 CC4BE...9F723C071F263  
openalt.acad.cz. IN DS 24937 13 2 C117A41CF0...100C416BFB6DB1B3D9189324
```



# On-line kontroly

ZONEMASTER  
by and

en | fr | sv

Domain check Pre-delegated domain FAQ

Non-Javascript Interface

Domain name  
cesnet.cz

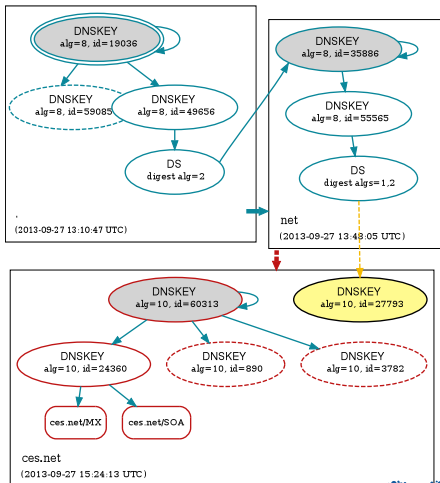
Advanced options

Test # 72235  
Executed at 2016-03-03T10:56+0200  
Link  
<https://zonemaster.net/teso3e68c44f39bdc1b2>

Basic Advanced Expert History

- SYSTEM
- BASIC
- ADDRESS
- CONNECTIVITY
- CONSISTENCY
- DNSSEC
- DELEGATION
- NAMESERVER
- SYNTAX
- ZONE

Zonemaster Test Engine Verzion.v1.0.12, IP address: 2001:718:1:6-134:196  
contact@zonemaster.net GitHub



## Publikace nového klíče

```
# cd /etc/bind/keys
# dnssec-keygen -a ECDSAP256SHA256 -fK openalt.acad.cz
Generating key pair.
Kopenalt.acad.cz.+013+26322
# chmod g+r K*.private
# rndc sign openalt.acad.cz
```

- stačí jednou za  $n$  let, kde  $n < 10$
- po publikaci jsou oba klíče aktivní, je možné změnit DS záznam (po určité době)

## Deaktivace a vymazání původního klíče

```
# cd /etc/bind/keys  
# dnssec-settime -I +1d -D +1W Kopenalt.acad.cz.+013+24937  
# chmod g+r K*.private
```

- v okamžiku deaktivace (-I) již klíč neslouží k podpisování, je ale přítomen pro účely ověření podpisů
- v okamžiku vymazání (-D) je klíč zcela odstraněn a všechny podpisy nahrazeny

- podepisování v BINDu představuje minimální nároky na úpravu stávajících nástrojů
- ve výchozím stavu se používá NSEC, možnost přepnout na NSEC3

## Přechod na NSEC3

```
# rndc signing -nsec3param 1 0 10 0deafbee openalt.acad.cz
```

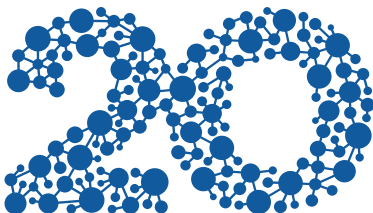
Potřebuje vůbec vaše doména DNSSEC?  
Pokud na ní přijímáte e-maily, pak bezpochyby ano.

Děkuji za pozornost

Ondřej Caletka

Ondrej.Caletka@cesnet.cz

<https://Ondrej.Caletka.cz>



1996–2016

**CESNET**

SPOUPRÁCE  
VÝZKUM  
KOMUNITA