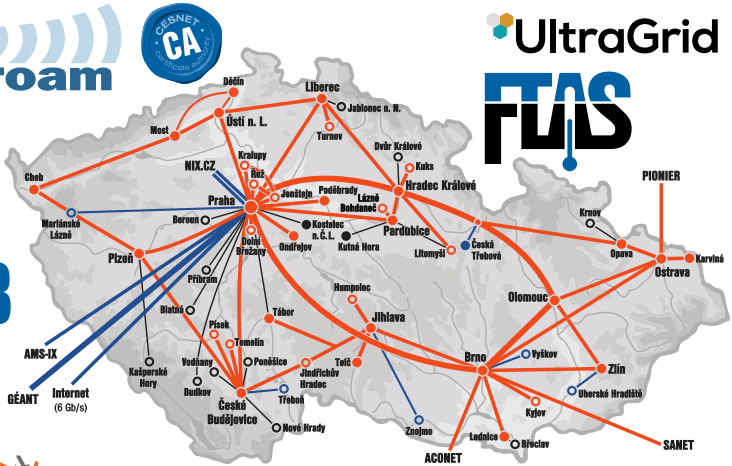
DNSSEC na vlastní doméně snadno a rychle

Ondřej Caletka

6. března 2016

O sdružení CESNET



Když se řekne DNSSEC

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

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 nebo Unbound
- 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

1996–2016 CESNET

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. vygenertovat 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 if.acad.cz.
$TTL 60
@     IN SOA  ns hostmaster 1 120 10 3600 60
@     IN NS   ns
ns    IN A    192.0.2.53
      IN AAAA 2001:db8::53
```

Konfigurace v named.conf.local

```
zone "if.acad.cz" {
        type master;
        file "/etc/bind/if.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 if.acad.cz
Generating key pair.
Kif.acad.cz.+013+24937
# chmod g+r K*.private
# ln -s /etc/bind/if.acad.cz /var/cache/bind/
```

Upravíme konfiguraci

Konfigurace zóny v named.conf.local

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

Po reloadu vzniknou v pracovním adresáři soubory:

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

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

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

Máme podepsáno

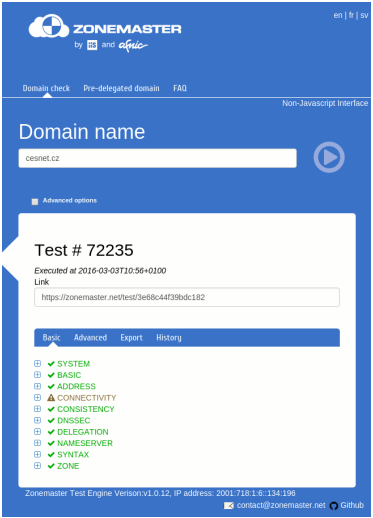
- případné změny jsou automaticky podepisovány
- podpisy jsou automaticky obnovovány
- zbývá o tom dát vědět nadřazené zóně

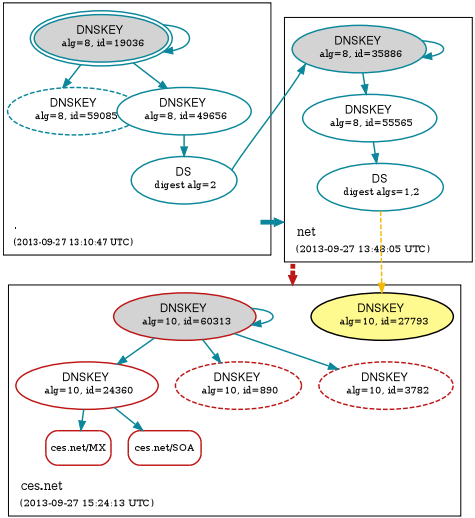
  .cz, .eu registrátorovi předáme přímo veřejný klíč

  ostatní registrátorovi předáme DS záznam vygenerovaný z veřejného klíče a doménového jména

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

On-line kontroly





1996–2016 CESNET

Výměna klíče

Publikace nového klíče

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

Závěrem

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

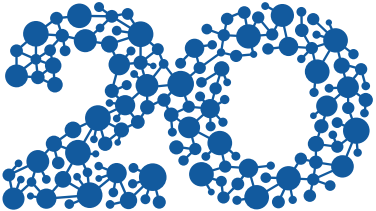
Přechod na NSEC3

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

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

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://Ondřej.Caletka.cz



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA