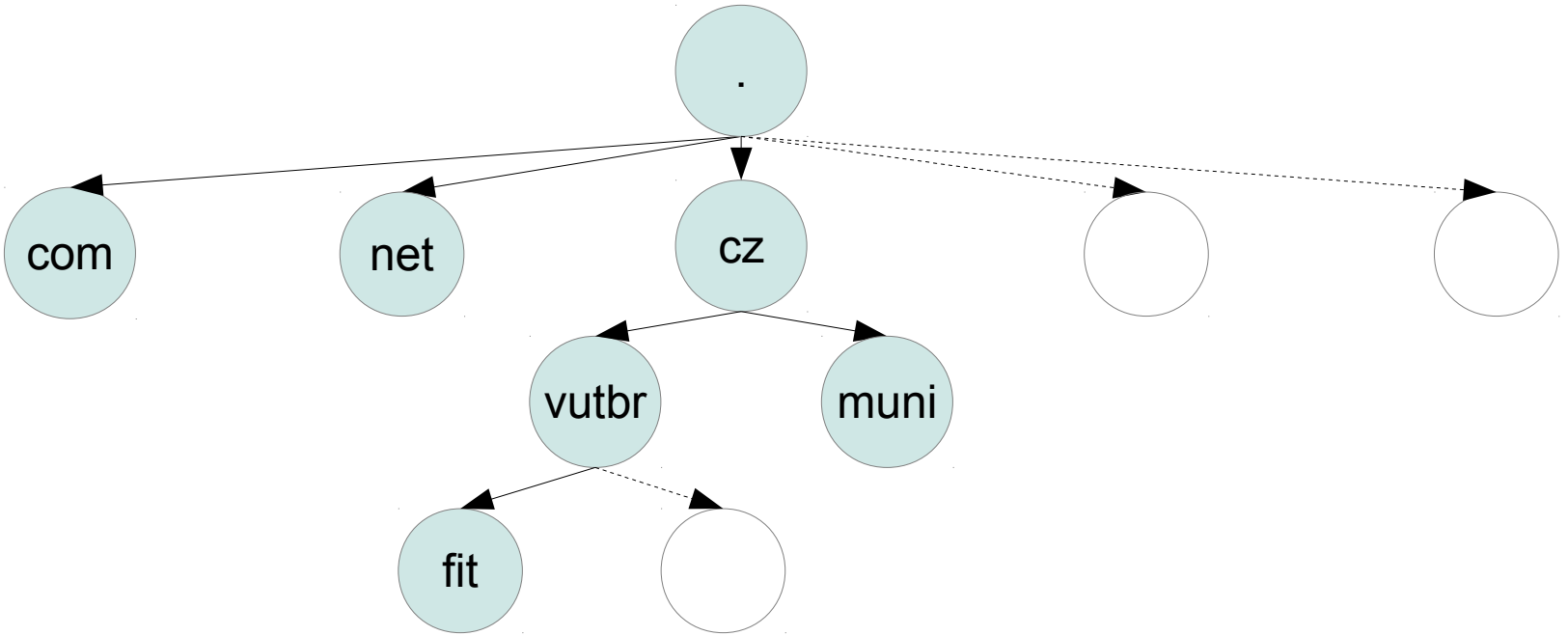
Snadné nasazení DNSSEC s Knot DNS

Jan Včelák • jan.vcelak@nic.cz • 02.11.2013

DNS (Domain Name System)

- RFC 1034 (listopad 1987)
- hierarchická, distribuovaná „databáze“
- doménové jméno, typ záznamu, data
- autoritativní servery, delegace autority

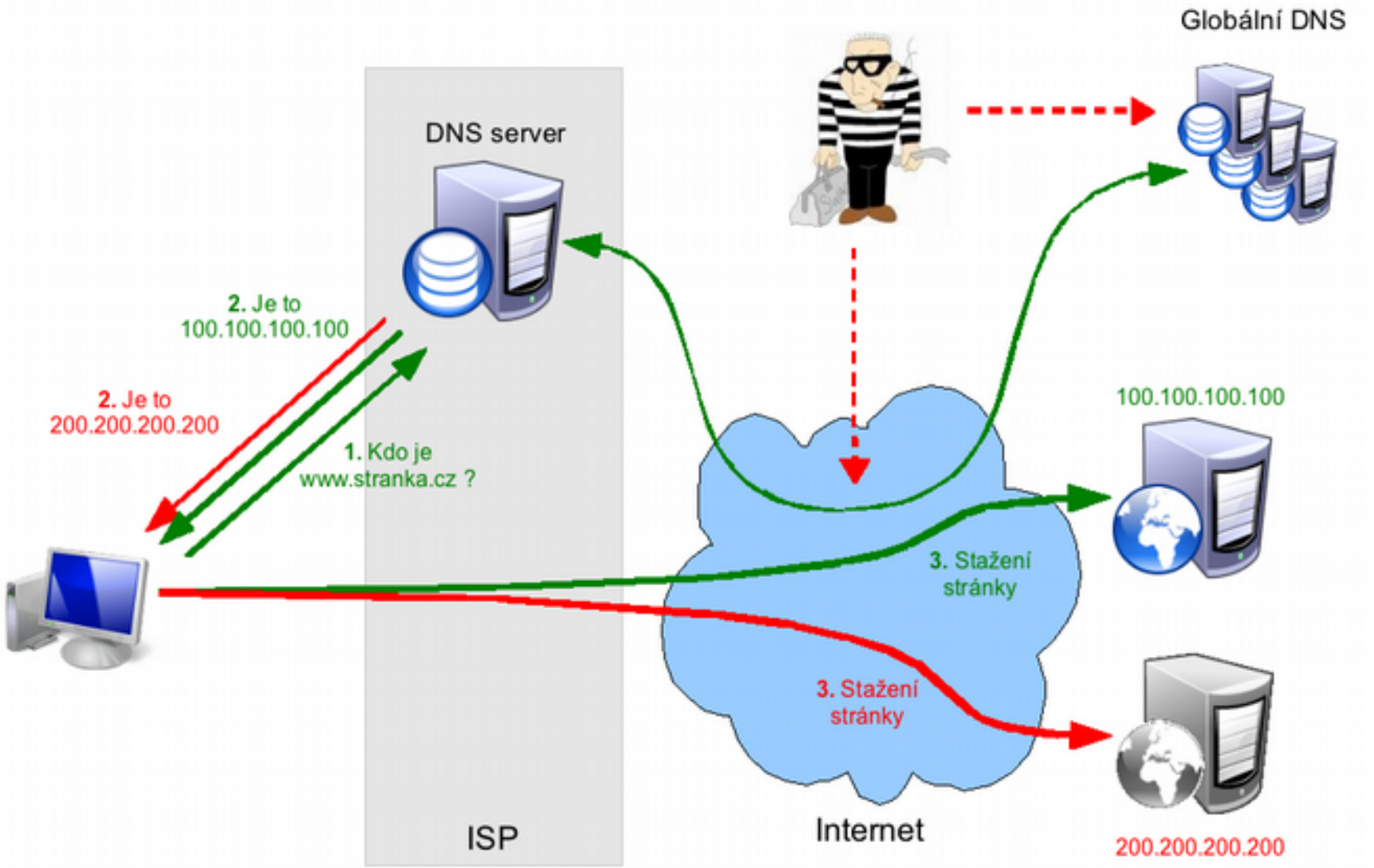
DNS (Domain Name System)



DNSSEC (DNS Security Extensions)

- RFC 4033, 4034, 4035 (březen 2005)
- ochrana proti DNS Spoofing
  (zajišťuje autentizaci a integritu dat)
- princip kryptografie s veřejným klíčem
- umí zabezpečit „cokoli“ v zóně
- předpoklad pro použití DKIM, DANE, SSHFP, ...

DNS Spoofing



http://dnssec.cz

Typy záznamů pro DNSSEC

- DNSKEY
- DS
- RRSIG
- NSEC
- NSEC3PARAM + NSEC3

Výhody a nevýhody DNSSEC

- ☺ bezpečnost
- ? výčet zóny
- ? kořen důvěry
- ? musí být podporováno resolverem
- ☹ velikost zóny
- ☹ amplifikační útoky
- ☹ správa klíčů (generování, rotace, publikace DS)

Přístupy pro nasazení DNSSEC

- ruční podepisování
- automatické podepisování
- podepisování v odděleném procesu

Ruční podepisování

- první řešení, průkopník Bind (ISC)
- server dostane podepsanou zónu

- dnssec-keygen
- dnssec-settime
- dnssec-signzone

```
zone "example.com" IN {
        type master;
        file "example.com.signed";
};
```

Automatické podepisování

- server dostane nepodepsanou zónu a klíče
- Bind, PowerDNS, Knot DNS 1.4

- dnssec-keygen
- dnssec-settime
- ~~dnssec-signzone~~

```
zone "example.com" IN {
        type master;
        file "dynamic/example.com";
        update-policy local;
        auto-dnssec maintain; # allow
        key-directory "keys";
};
```

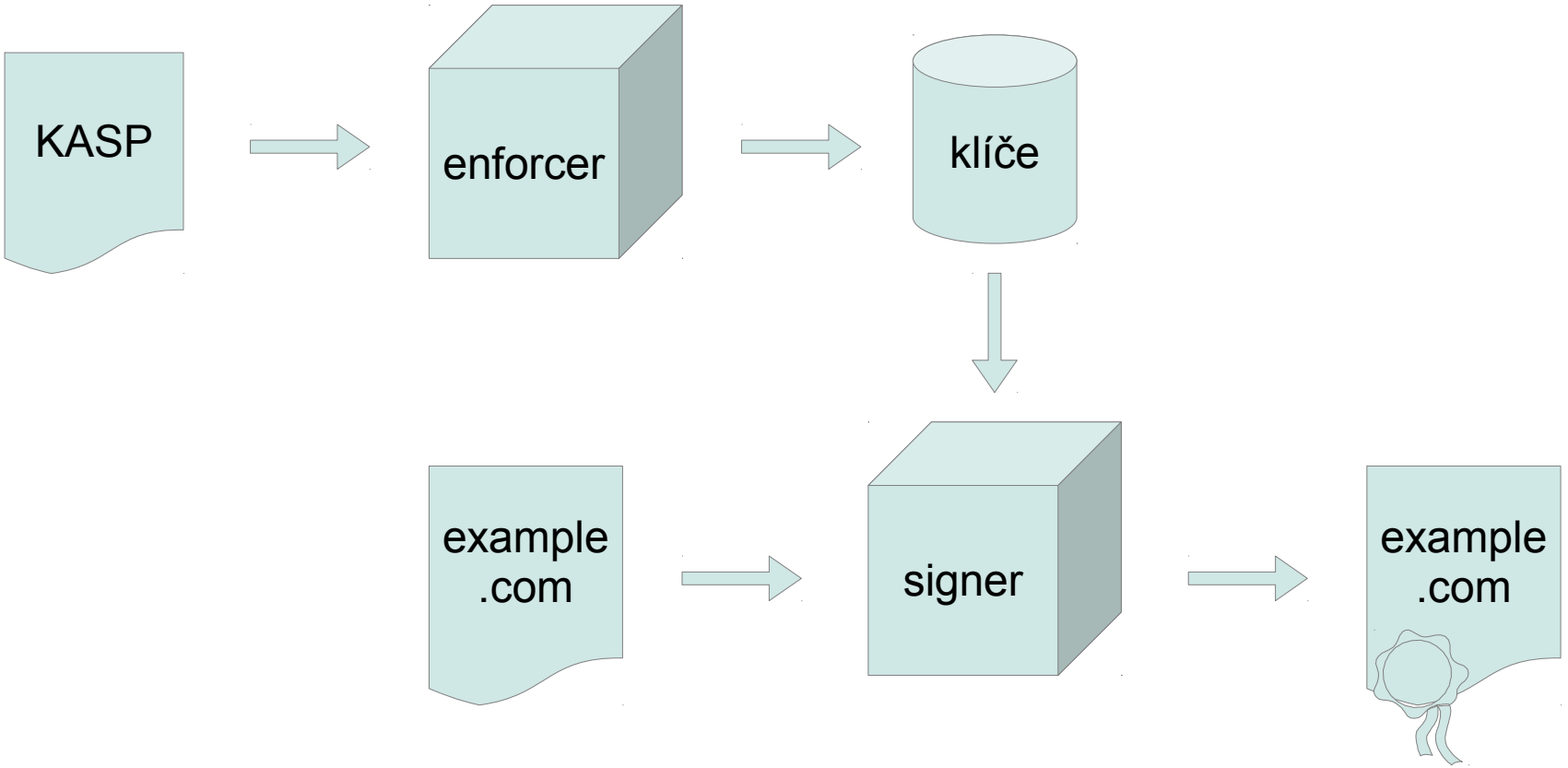
Za podpory skriptů v Perlu, Bashi, ...

http://dnsreactions.tumblr.com/post/49249889635

Podepisování v odděleném procesu

- přístup, který používá OpenDNSSEC
- čte nepodepsanou zónu ze souboru nebo ji získává pomocí AXFR
- výstup do souboru, který čte DNS server
- robustní řešení
- problém s DDNS

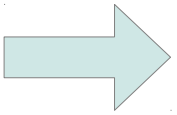
OpenDNSSEC



Knot DNS 1.4

- první beta verze – vyšla v pondělí (28.10.2013)
- umí automatické podepisování s klíči v souborech ve formátu dnssec-keygen

```
zones {
    example.com {
        file "example.com";
    }
};
```



```
zones {
    dnssec-enable on;
    dnssec-keydir "keys";

    example.com {
        file "example.com";
    }
};
```

Knot DNS 1.5

- alternativa k OpenDNSSEC
- nezávislost na nástrojích od ISC
- automatické správa klíčů na základě politiky
- podpora pro HSM přes PKCS#11
- oddělená DNSSEC knihovna

Děkuji za pozornost

Jan Včelák • jan.vcelak@nic.cz