DNSSEC a Knot DNS

Minulost, současnost a budoucnost

Jan Včelák • jan.vcelak@nic.cz • 13.05.2014

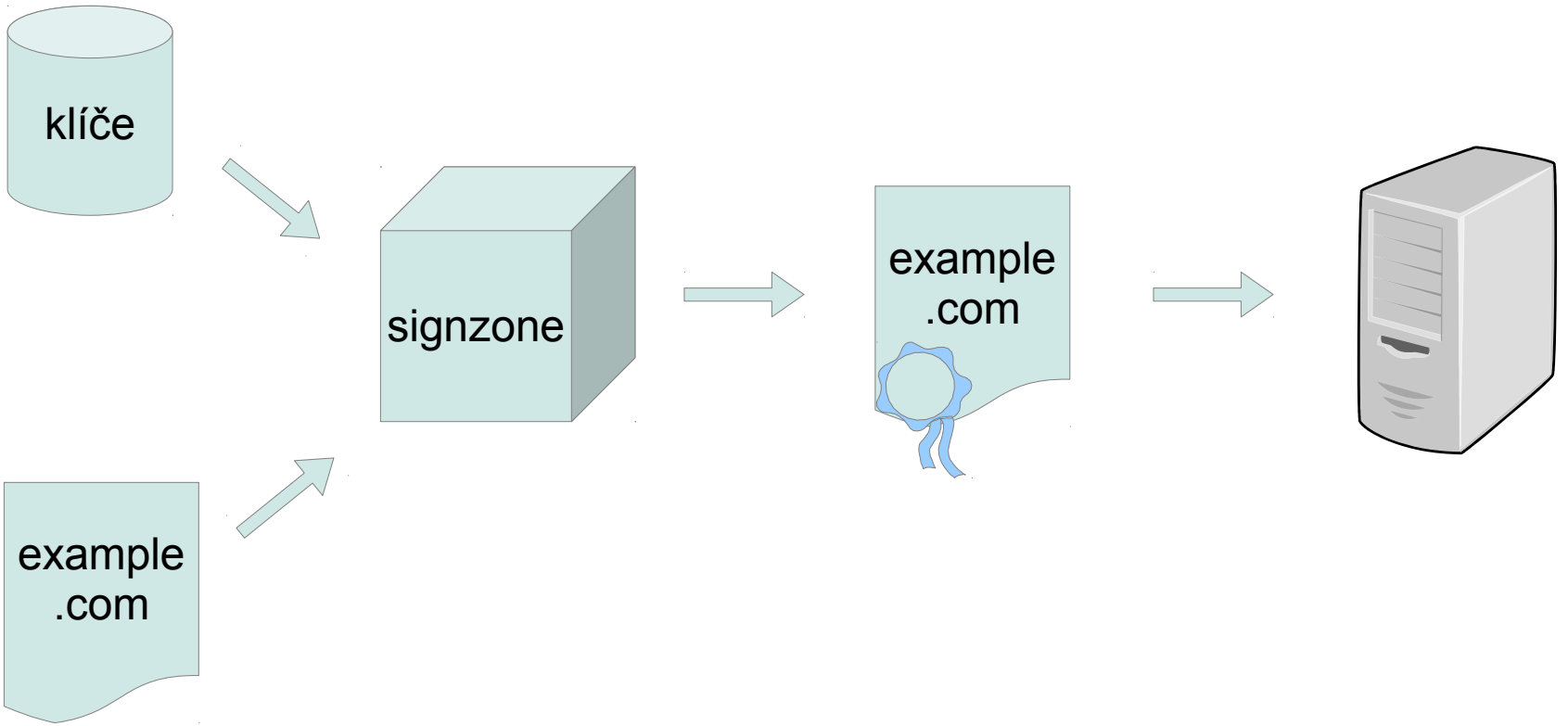
Obsah přednášky

- Metody podepisování DNSSEC
- Ukázka postupů pro jednotlivé metody
  - BIND, Knot DNS 1.4, PowerDNS, OpenDNSSEC
- Plany do budoucna
  - Knot DNS 1.5
  - Knot DNS 1.6 a libdnssec

Metody podepisování

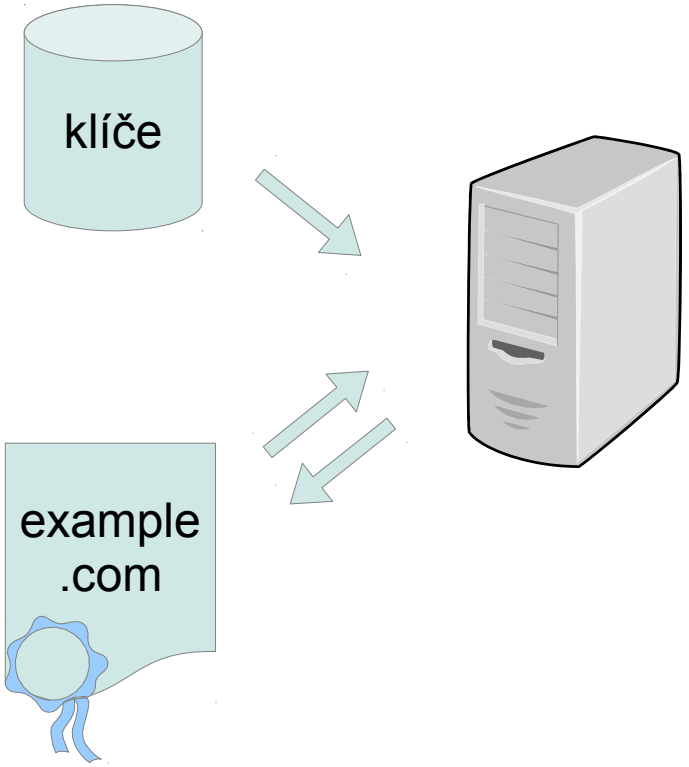
- pre-signing
- automatic signing
- on-line signing (také in-line, live, frontend, ...)
- bump-in-the-wire signing

Pre-signing



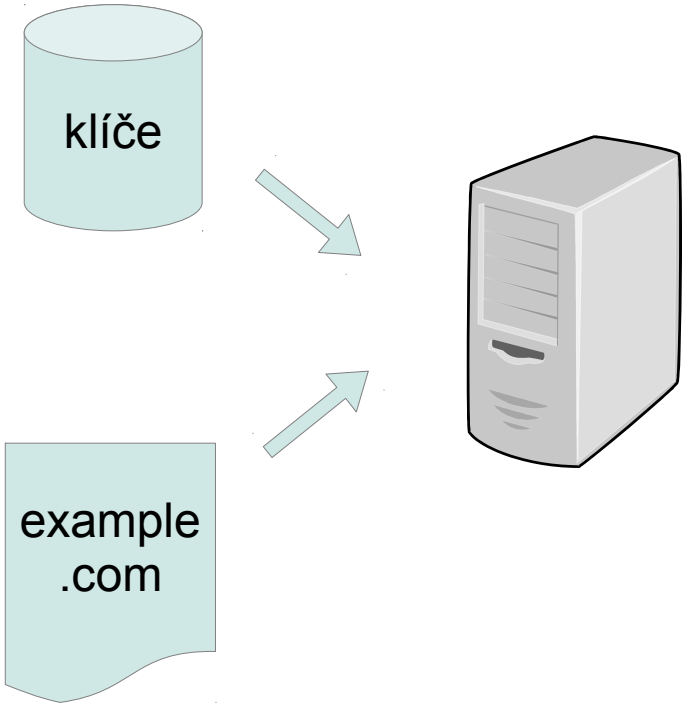
BIND, NSD, Knot DNS, PowerDNS, Yadifa

Automatic signing



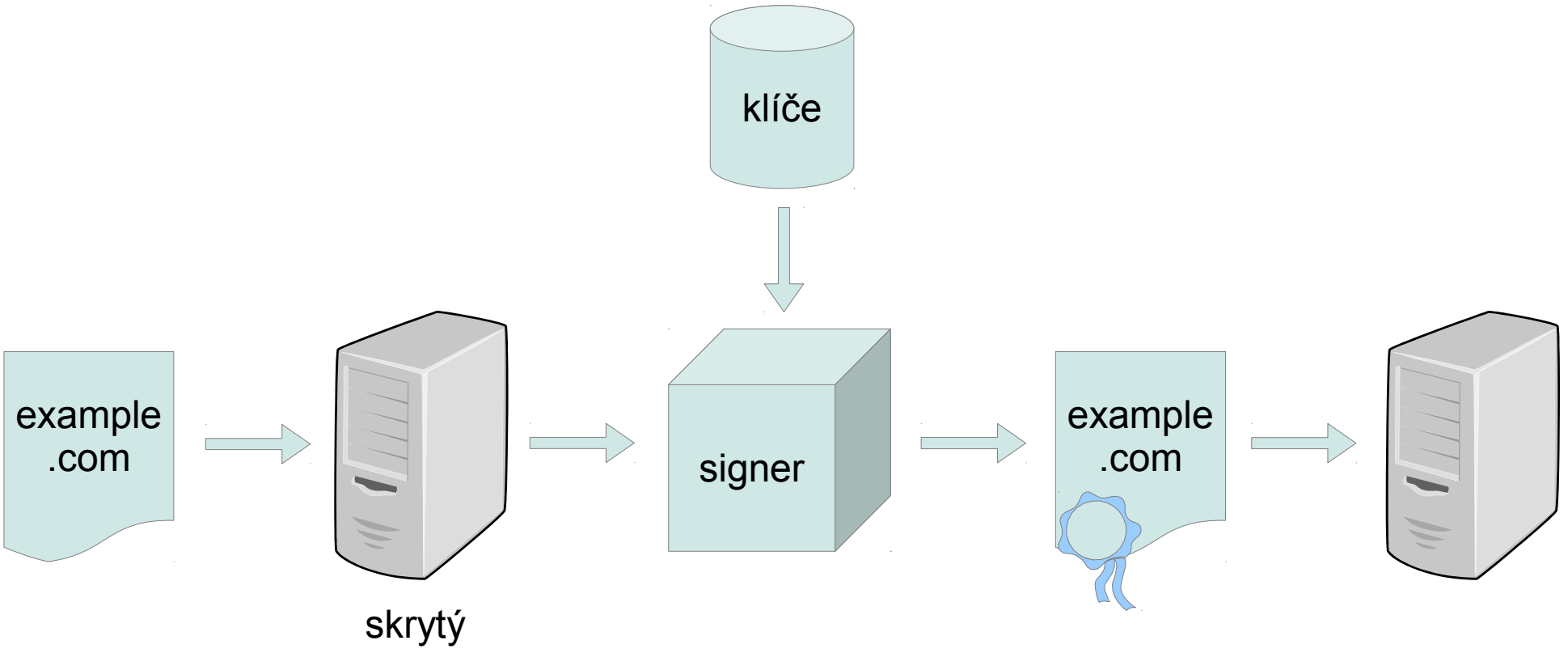
BIND, Knot DNS

On-line signing



PowerDNS

Bump-in-the-wire signing



OpenDNSSEC

Pre-signing

```
$ dnssec-keygen -a RSASHA1 -b 1024 example.com
Generating key pair.....................++++++ ....++++++
Kexample.com.+005+12966

$ dnssec-signzone -K keys -S example.com
Fetching KSK 50469/RSASHA1 from key repository.
Fetching ZSK 12966/RSASHA1 from key repository.
Verifying the zone using the following algorithms: RSASHA1
Zone fully signed:
Algorithm: RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
                    ZSKs: 1 active, 0 stand-by, 0 revoked
example.com.signed
```

NSD: ldns-keygen, ldns-signzone, ldns-revoke

Formát klíčů – BIND

```
$ cat Kexample.com.+005+49215.key
example.com. IN DNSKEY 256 3 5 AwEAAb9NUWaiG37w/N/Omyrn...

$ cat Kexample.com.+005+49215.private
Algorithm: 5 (RSASHA1)
Modulus: v01RZqIbfvD8386bKufQ4dadJoF3/AeB9tF8Us4UCYPNxQ...
PublicExponent: AQAB
PrivateExponent: nMX0S7PV7LX5xkA/EW5g1HNY3lGDztsoOul6hT...
...
Created: 20140512170707
Publish: 20140512170707
Activate: 20140512170707
```

Automatic signing

```
$ dnssec-settime -p all Kexample.com.+005+49215.private
Created: Mon May 12 19:07:07 2014
Publish: Mon May 12 19:07:07 2014
Activate: Mon May 12 19:07:07 2014
Revoke: UNSET
Inactive: UNSET
Delete: UNSET
```

- **DNSKEY** Publish, Delete, Revoke
- **RRSIG** Activate, Inactive

BIND vs. Knot DNS

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

    update-policy local;
    key-directory "keys";
    auto-dnssec maintain;
};
```

```
rndc sign
rndc signing
```

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

    dnssec-enable on;
    dnssec-keydir "keys";
  }
}
```

```
knotc signzone
```

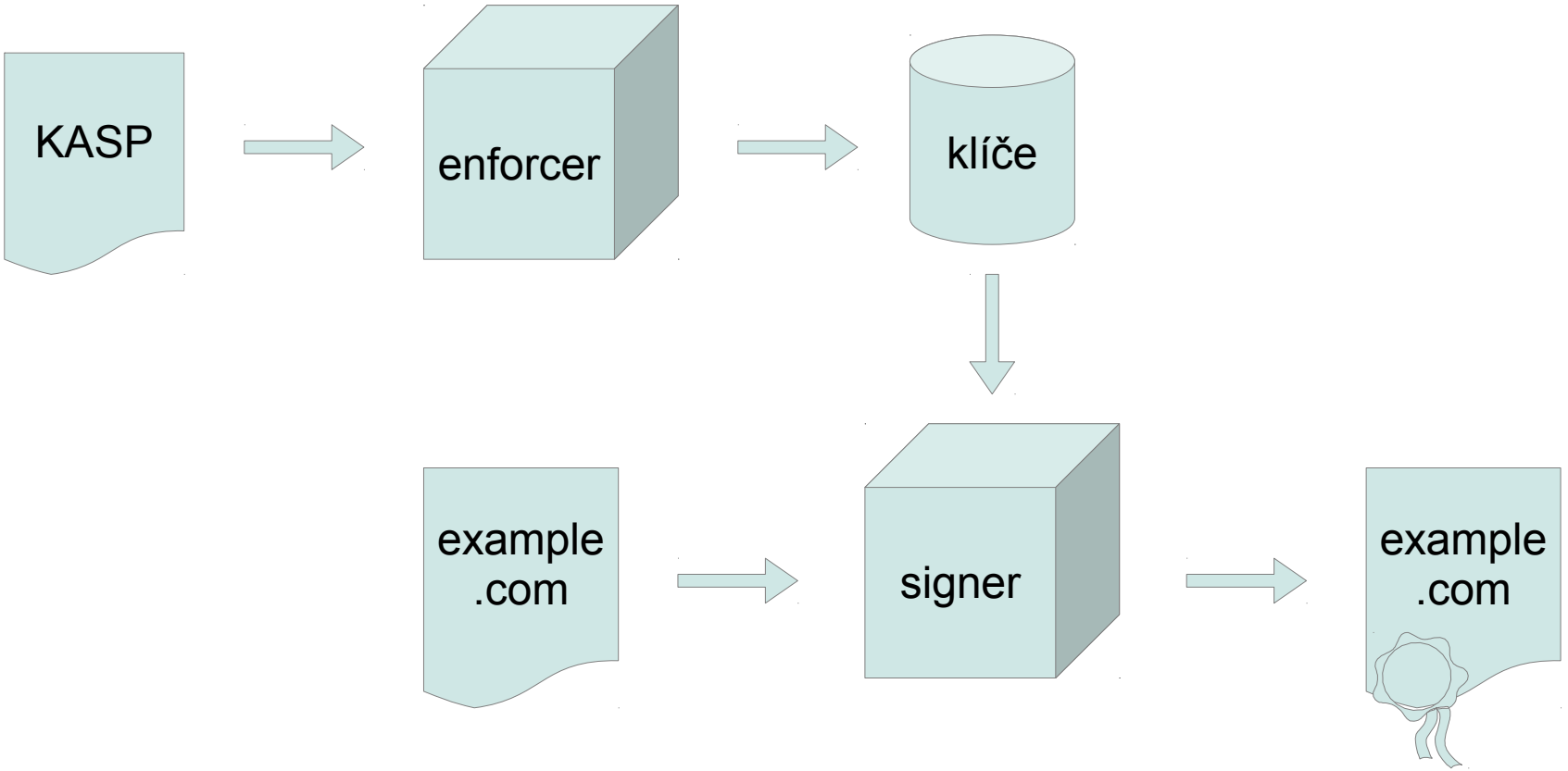
On-line signing: PowerDNS

```
$ pdnssec secure-zone example.com

$ pdnssec show-zone example.com
Zone is not presigned
Zone has NSEC semantics
keys:
ID = 1 (KSK), tag = 58474, algo = 8, bits = 2048
 Active: 1 ( RSASHA256 )
KSK DNSKEY = example.com IN DNSKEY 257 3 8 AwEAAcybi1SS...
DS = example.com IN DS 58474 8 1 ec5e... ; ( SHA1 digest )
...
ID = 2 (ZSK), tag = 12133, algo = 8, bits = 1024
 Active: 1 ( RSASHA256 )


$ pdnssec set-nsec example.com '1 0 10 C01DCAFE'
$ pdnssec rectify-zone
```

Bump-in-the-wire: OpenDNSSEC



Knot DNS 1.5 (brzy)

- žádné novinky týkající se DNSSEC
- pracuje se na oddělení *libknot* a *libzscanner*
- hodně změn pod kapotou (refactoring)
- vzniká knihovna *libdnssec*
- dynamické moduly pro odpovídání

Dynamické moduly

- split-horizon (GeoIP, ...)
- syntéza reverzních záznamů (Knot DNS 1.5):

```
$ khost 2a00:1028::1
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.2.0.1.0.0.a.2.ip6.arpa points to
dynamic-2a00-1028-0000-0000-0000-0000-0000-0001.ipv6.
broadband.iol.cz.

$ khost dynamic-2a00-1028-0000-0000-0000-0000-0000-0001...
dynamic-... has IPv6 address 2a00:1028::1

$ kdig +short @ipv6.iol.cz. version.bind. TXT CH
"Knot DNS 1.5.0-alpha"
```

Knot DNS 1.6

- bude používat *libdnssec*
  - přechod od OpenSSL ke GnuTLS
  - podpora pro hardwarová úložiště (PKCS #11)
  - politika klíčů a podepisování (vzor OpenDNSSEC)
  - řízení podepisování z pohledu cachujícího resolveru
- možnost on-line podepisování
- minimální NSEC3 důkazy

Knot DNS a libdnssec

- git repozitář Knot DNS, větev libdnssec
- základ funkční, ale chybějí utility

```
policy: default
keystore: default
keys:
  - id: 788e1e2d37ab359899735349e38442cc8d038795
    ksk: false
    algorithm: 3
    public_key: APwZQ3iOx0qCijjkzyjU8sVYApPzt+xj7V...
    publish: 2014-04-25 18:44:18
    active: 2014-04-25 18:44:18
```

Děkuji za pozornost

Jan Včelák • jan.vcelak@nic.cz