



Agentúra

Ministerstva školstva, vedy, výskumu a športu SR
pre štrukturálne fondy EÚ



UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

PRÍPRAVA ŠTÚDIA MATEMATIKY A INFORMATIKY NA FMFI UK V
ANGLICKOM JAZYKU

ITMS: 26140230008

DOPYTOVO – ORIENTOVANÝ PROJEKT

Moderné vzdelávanie pre vedomostnú spoločnosť/Projekt je
spolufinancovaný zo zdrojov EÚ

DNSSEC – demo

Martin Stanek

Department of Computer Science
Comenius University
`stanek@dcsc.fmph.uniba.sk`

Security of IT infrastructure (2013/14)

Setup

- ▶ DNS server (bind9 (9.8.1-P1), Ubuntu 12.04): 192.168.56.103
- ▶ DNSSEC validating resolver:
 - ▶ import KSK for the root zone (include “/etc/bind/bind.keys”):

```
managed-keys {  
    . initial-key 257 3 8 "AwEAAg...ihz0=";  
};
```
 - ▶ configure DNSSEC validation and support in options section of the configuration file (dnssec-validation yes; dnssec-enable yes;)
these are default, not necessary to take any action
 - ▶ ...and test, e.g.:

```
dig @192.168.56.103 www.verisign.com +dnssec
```

Flags for dig

AA = Authoritative Answer

TC = Truncation

RD = Recursion Desired

RA = Recursion Available

AD = Authenticated Data (DNSSEC only: authenticated data)

dig @192.168.56.103 www.verisign.com +dnssec

```
; <<>> DiG 9.7.3 <<>> @192.168.56.103 www.verisign.com +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63367
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 12, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.verisign.com. IN A

;; ANSWER SECTION:
www.verisign.com. 60 IN CNAME www-ilg.verisign.net.
www.verisign.com. 60 IN RRSIG CNAME 8 3 60 20120422180859 20120408180859 19358 verisign.com. bCedmOyMdYeQLpF.....XZc:
www-ilg.verisign.net. 60 IN A 69.58.181.89
www-ilg.verisign.net. 60 IN RRSIG A 8 3 60 20120422183859 20120408183859 13433 verisign.net. ccSSAIfqrok9T/K.....Nz8:

;; AUTHORITY SECTION:
verisign.net. 391 IN NS e2.nstld.net.
verisign.net. 391 IN NS m2.nstld.net.
verisign.net. 391 IN NS k2.nstld.net.
verisign.net. 391 IN NS a2.nstld.com.
...
verisign.net. 391 IN NS c2.nstld.net.
verisign.net. 391 IN NS g2.nstld.com.
verisign.net. 391 IN RRSIG NS 8 2 900 20120422183859 20120408183859 13433 verisign.net. dHlKFzjRskt/HbW.....Swc=

;; Query time: 1108 msec
;; SERVER: 192.168.56.103#53(192.168.56.103)
;; WHEN: Tue Apr 10 20:45:15 2012
;; MSG SIZE rcvd: 810
```

Authoritative server for TLD zone biti

- ▶ `/etc/bind/named.conf.local:`

```
zone "biti" {  
    type master;  
    file "/etc/bind/db.bit";  
};
```

- ▶ ...and test, e.g.:

```
dig @192.68.56.103 biti. MX  
dig @192.68.56.103 tango.bit.
```

```
; Zona bitl.  
$TTL 604800  
$ORIGIN bitl.
```

```
@      IN      SOA      ns1.bitl.   admin.bitl. (  
                                2 ; Serial  
                                28800 ; Refresh  
                                7200  ; Retry  
                                864000 ; Expire  
                                86400 ) ; Negative Cache TTL
```

```
;
```

```
        NS      ns1.bitl.  
        NS      ns2.bitl.  
        MX      10 mail.bitl.  
        MX      20 mail2.bitl.  
ns1      IN      A      192.168.56.103  
ns2      IN      A      192.168.56.103  
  
mail      IN      A      192.168.56.200  
mail2     IN      A      192.168.56.201  
  
tango     IN      A      192.168.56.210  
waltz     IN      A      192.168.56.211  
samba     IN      A      192.168.56.212  
rumba     IN      A      192.168.56.213
```

DNSSEC in zone biti

- ▶ generate KSK a ZSK:

```
dnssec-keygen
```

```
-a RSASHA256 -3 -b 2200 -r /dev/urandom -fk biti
```

```
dnssec-keygen
```

```
-a RSASHA256 -3 -b 1200 -r /dev/urandom biti
```

- ▶ public keys: .key
- ▶ private keys: .private

- ▶ signing the zone (incl. NSEC3):

```
dnssec-signzone -3 abcdef00 -S -o biti db.biti
```

- ▶ signed zone: db.biti.signed

DNSSEC in zone biti (2)

- ▶ replacing zone file with the signed one in `/etc/bind/named.conf.local`:

```
zone "biti" {  
    type master;  
    file "/etc/bind/db.bit_i.signed";  
};
```

- ▶ ...and we can test, e.g.:

```
dig @192.168.56.103 biti. MX +dnssec  
dig @192.168.56.103 tango.bit_i. +dnssec  
dig @192.168.56.103 tangooo.bit_i. +dnssec  
...
```

notice the missing ad flag in responses (authoritative server do not set ad flag)

Other necessary actions

- ▶ regular signing of zone (the signatures have limited validity)
- ▶ managing the serial number of zone file
- ▶ inclusion of DS record for KSK into parent zone
 - ▶ file (`dsset-bit1.`) is generated automatically
- ▶ regular change of cryptographic keys
- ...