SCA6000 and Bind 9.6

CZ.NIC z.s.p.o.
Ondřej Surý
ondrej.sury@nic.cz
02.02.2009

cz nic
cz domain registry

Hardware

- Sun Fire T2000
  - 8 Core 1.0GHz UltraSPARC T1
- Sun Crypto Accelerator 6000
  - 13.000 RSA ops per sec

Software

- Solaris 10
- Bind 9.6 (CVS tag **rt18033a**)
- OpenSSL 0.9.8i/j
  - Patch from bind/contrib/pkcs11
  - openssl.conf with HSM PIN
- OpenSC
  - pkcs11-tool

Quick Howto – HSM

- Configure HSM
  - Create token store
  - Configure default KS
    - # cryptoadm enable metaslot token=<STORE_NAME>
  - Disable automatic key migration
    - # cryptoadm disable auto-key-migrate
    - CKR_TEMPLATE_INCONSISTENT
- Configure OpenSSL
  - See bind9/README.pkcs11

Quick Howto – OpenSSL

- Configure OpenSSL (openssl.cnf)

```
openssl_conf = openssl_def

[ openssl_def ]
engines = engine_section

[ engine_section ]
pkcs11 = pkcs11_section

[ pkcs11_section ]
PIN = xx:12345
```

```
# export OPENSSL_CONF=path_to_openssl.cnf
```

Quick Howto - OpenSC

- Prepare

```
# export PIN=xx:12345
```

- Generate key:

```
# pkcs11-tool --module /usr/lib/libpkcs11.so
--login --pin $PIN --keypairgen --key-type
rsa:1024 --label cz,zsk,9999
```

- List key(s):

```
# pkcs11-tool --module /usr/lib/libpkcs11.so
--slot 0 --login --pin $PIN --list-objects
```

Quick Howto – Bind 9.6 (rt18033a)

- Create the .key/.private pair

```
# dnssec-keyfromlabel -a RSASHA1
-l 'pkcs11:cz,zsk,9999' cz

Kcz.+005+61016
```

- Sign the zone

```
# cat Kcz.+005+61016 >> cz

# dnssec-signzone -n 8 -r /dev/urandom cz

cz.signed
```

- That's it!

Some timings

- 1xRSASHA1 2048b KSK
- 2xRSASHA2 1024b ZSK
- `dnssec-signzone`

  `-e +86400`

  `-j 86400 (randomize end for resigning)`

  `-r /dev/urandom (could Solaris use HSM?)`

  `-n 8 (match the number of cores)`

Some timings (T2000, Solaris 10)

- Clear zone, HSM

```
real     4:44.7
user     7:08.2
sys      1:25.5
```

- Reuse sigs, HSM

```
real     9:18.2
user    14:29.7
sys      2:10.0
```

- Clear zone, SW

```
real    42:43.3
user  5:31:54.4
sys           6.9
```

- Reuse sigs, SW

```
real     9:33.0
user    29:21.0
sys          11.0
```

Some timings (vs. commodity)

- Sparc T1 8-core, Solaris 10, Bind 9.6
- Clear zone, SW

```
real     42:43.3
user   5:31:54.4
sys           6.9
```

- Reuse sigs, SW

```
real      9:33.0
user     29:21.0
sys         11.0
```

- 2xAMD 2356 4-core, Linux, Bind 9.5.0-P2
- Clear zone, SW

```
real      2:26.2
user     16:44.5
sys       0:12.6
```

- Reuse sigs, SW

```
real      1:48.1
user      7:16.7
sys         33.0
```

Some timings (vs. my notebook)

- Sparc T1 8-core, Solaris 10, Bind 9.6
- Clear zone, SW

```
real      42:43.3
user    5:31:54.4
sys           6.9
```

- Reuse sigs, SW

```
real       9:33.0
user      29:21.0
sys          11.0
```

- Centrino Duo (3y old), Linux, Bind 9.5.0-P2
- Clear zone, SW

```
real      52:41.0
user   1:33:05.0
sys          56.0
```

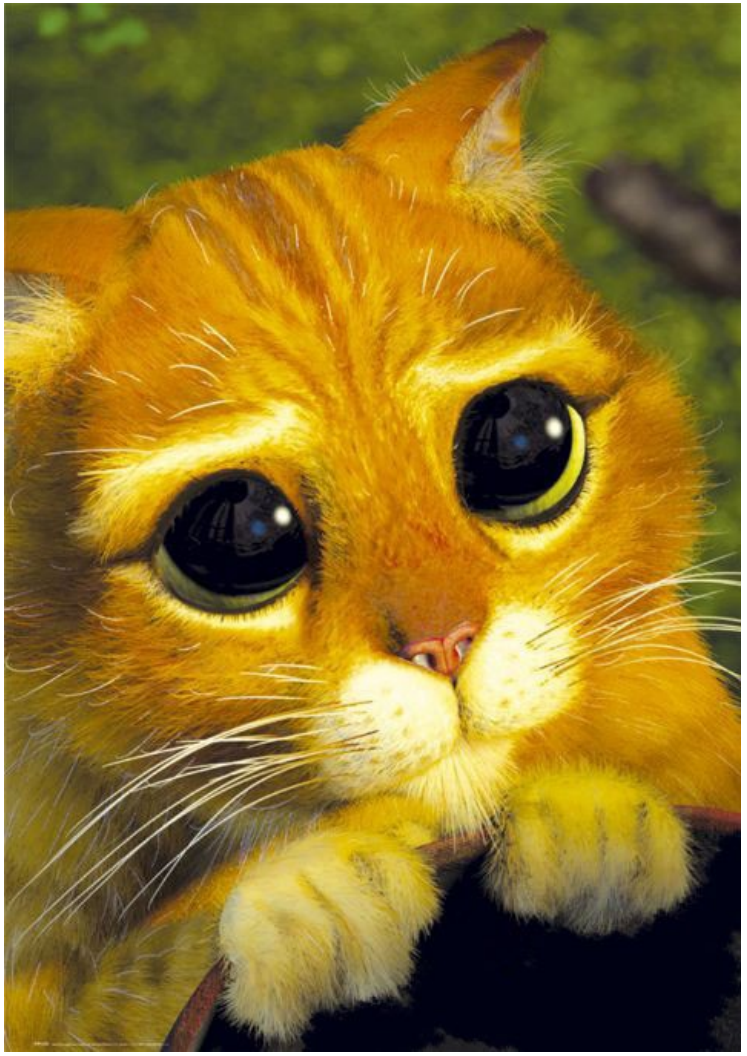
- Reuse sigs, SW

```
real      21:58.0
user      37:33.6
sys          26.2
```

Where to go next?

- Write a real HOWTO
- Tool to separate KSK and ZSK process
- Update patch to 0.9.8j (DSA bug)
- Improve man page of dnssec-keygen
  - Mention pkcs11: prefix

Bind 9.6



- Please review and merge rt18033a
- Please make Solaris faster (if doable :-)

Real usefulness of HSM