RED NACIONAL ACADEMICA
DE TECNOLOGIA AVANZADA

DNSSEC for ENUM zone

This is a basic installation/configuration "how-to" to provide DNSSEC using OpenDNSSEC and BIND. ENUM is involved since it uses NAPTR records.

Install dependencies/packages

```
:~# apt-get update && apt-get upgrade
```

```
:~# apt-get install softhsm opendnssec opendnssec-enforcer opendnssec-enforcer-sqlite3
```

Copy your zone to your opendnssec unsigned zones directory

```
:~# cp /path/to/your/zone/file /var/lib/opendnssec/unsigned/
```

Initialize a token

```
:~# softhsm --init-token --slot 0 --label "OpenDNSSEC"
```

This is going to ask you for a PIN code and you must remember it.

Edit you conf file

```
:~# vim /etc/opendnssec/conf.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
  <RepositoryList>
    <Repository name="SoftHSM">
      <Module>/usr/lib/softhsm/libsofthsm.so</Module>
      <TokenLabel>OpenDNSSEC</TokenLabel>
      <PIN> ---> YOUR PIN CODE GOES HERE<---  </PIN>
      <SkipPublicKey/>
    </Repository>
    ...
```

Edit your zonelist file like this

```
:~# vim /etc/opendnssec/zonelist.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ZoneList>
  <Zone name="example.com">
    <Policy>default</Policy>
    <SignerConfiguration>
       /var/lib/opendnssec/signconf/example.com.xml
    </SignerConfiguration>
    <Adapters>
      <Input>
        <File>/var/lib/opendnssec/unsigned/db.example.com</File>
      </Input>
      <Output>
        <File>/var/lib/opendnssec/signed/db.example.com</File>
      </Output>
    </Adapters>
  </Zone>
</ZoneList>
```

Update your zonelist

```
:~# ods-ksmutil update zonelist
```

Add your zone to the zonelist

```
:~# ods-ksmutil zone add -zone example.com
```

Sign your zone

```
:~# ods-signer sign example.com
```

List your key states

```
:~# ods-ksmutil key list -v
```

You should see something like this

```
Keys:
Zone:         Keytype:  State:    Date of next transition:  CKA_ID:   Repository:     Keytag:
example.com   ZSK       active    2010-10-15 06:59:28       ...      OpenDNSSEC      XXXX
example.com   KSK       ready     waiting for ds-seen       ...      OpenDNSSEC      KEYTAG
```

Notify the Enforcer when you can see the DS RR in your parent zone

```
:~# ods-ksmutil key ds-seen --zone example.com --keytag KEYTAG
```

You should see this:

```
Result:
Found key with Keytag KEYTAG
Key KEYTAG made active
```

And then if you list your zones again now is active

```
:~# ods-ksmutil key list -v
```

```
Keys:
Zone:                           Keytype:      State:    Date of next transition:
example.com                     ZSK           active    2010-10-15 07:20:53
example.com                     KSK           active    2010-10-15 07:31:03
```

Ensure that your zone has been signed

```
:~# ls -lta /var/lib/opendnssec/signed/
```

You should see your zone file with a lot of RRSIG and DNSKEY records inside

Point to your new signed zone

```
:~# vim /etc/bind/named.conf.enum
```

```
  zone "example.com" {
    type master;
    file "/var/lib/opendnssec/signed/db.example.com";
  };
```

Now you can query your zone using dig tool

```
:~# dig @ -t NAPTR 3.2.1.example.com +dnssec
```

References links

1. OpenDNSSEC Documentation, Uploading a Trust Anchor (Publishing DS record to the parent). https://wiki.opendnssec.org/display/DOCS/Running+OpenDNSSEC#RunningOpenDNSSEC-UploadingaTrustAnchor%28PublishingDSrecordtotheparent%29
2. Github Gist – OpenDNSSEC Installation/Configuration. https://gist.github.com/hernandanielg/f854e085a29943848196