Lab: Zone signing

```
Created by: Yazid AKANHO
Modified by: -
Current version: 2024020400
Previous version:-
```

To sign the zone we first need two pairs of keys: a ZSK and a KSK. It can be signed with a single key pair but that's not a recommended configuration.

Position yourself in BIND configuration folder and then backup your zone file:

```
# cp zones/db.grpX zones/db.grpX.backup
```

Create a directory to hold your DNSSEC keys

```
# mkdir -p /etc/bind/keys
# cd /etc/bind/keys
```

Generate **ZSK**

```
# dnssec-keygen -a RSASHA256 -b 2048 -n ZONE grpX.<lab_domain>.te-labs.training
```

Generate **KSK**

```
# dnssec-keygen -f KSK -a RSASHA256 -b 2048 -n ZONE grpX.<lab_domain>.te-labs.training
```

Change ownership to the zones and keys folders

```
# chown -R bind:bind /etc/bind/keys
# chown -R bind:bind /etc/bind/zones
```

Then, sign the zone. Here we have two options:

1. Sign the zone manually, or
2. Tell BIND to sign.

There is even a third option and more... Which one to use is up to you. As we are in lab environment, why not testing manual zone signing, and then BIND inline-signing, one after the other ?

Manual zone signing.

```
# cd /etc/bind/
# dnssec-signzone -S -K keys/ -o grpX.<lab_domain>.te-labs.training zones/db.grpX
```

You should get an output similar to the follwing:

```
Fetching grpX.<lab_domain>.te-labs.training/ECDSAP256SHA256/5515 (KSK) from key
repository.Fetching grpX.<lab_domain>.te-labs.training/ECDSAP256SHA256/47091 (ZSK) from
key repository.Verifying the zone using the following algorithms: ECDSAP256SHA256.
Zone fully signed:
Algorithm: ECDSAP256SHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                            ZSKs: 1 active, 0 stand-by, 0 revoked
zones/db.grpX.signed
```

Then, replace the *db.grpX* file in `named.conf.local` with the *db.grpX.signed* and restart the server using `rndc reload`.

Use command line tools to query the signed zone and verify if the signing is effective.

We can now use *dig* utility to confirm that the zone is signed and play with the new DNSSEC RRs.

> ⚠ **Warning**
>
> remember that at this stage, you have only signed the zone and have not yet established the chain of trust.

QUESTION: Will you get the "ad" flag ? Why ?

```
root@soa:/etc/bind# dig @localhost soa grpX.<lab_domain>.te-labs.training. +dnssec
; <<>> DiG 9.16.1-Ubuntu <<>> @localhost soa grpX.<lab_domain>.te-labs.training. +dnssec

; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9591
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: 69a0c61239afd9a201000000609c5df711d4eb3a39f90d89 (good)
;; QUESTION SECTION:
;grpX.<lab_domain>.te-labs.training.        IN      SOA

;; ANSWER SECTION:
grpX.<lab_domain>.te-labs.training. 30 IN   SOA     grpX.<lab_domain>.te-labs.training.
dnsadmin.grpX.<lab_domain>.te-labs.training.grpX.<lab_domain>.te-labs.training. 1 604800
86400 2419200 86400
grpX.<lab_domain>.te-labs.training. 30 IN   RRSIG   SOA 8 4 30 20210611215606
20210512215606 41110 grpX.lacnic35.te-labs.training. RmUbjShh4jX
fw384miz1G1703ObV9WrYQOOJVSbzDNchCsLayuW/UQRR
w3X6eTXHOCSVOcG2Bamkbals48LYUA9Y/l2tmuaGxKkeQVT5xcy0wY/rbeaN4NgUG+N13BFodOPQumsBERQ+NUDAw8
98IfkcwcZ3pZFgIAsXplA1 MY4=
```

More tests:

1. dig DNSKEY *grpX.<lab_domain>*.te-labs.training @100.100.X.130
2. dig DNSKEY *grpX.<lab_domain>*.te-labs.training @100.100.X.130 +dnssec +multi
3. dig SOA *grpX.<lab_domain>*.te-labs.training @100.100.X.130 +dnssec +multi

QUESTIONS: did you get the answers ? Did you receive the signatures ? Did you get the "ad" flag ? Why ?

> **Important**
>
> When you are done with the manual signing and confirm that your public nameservers are serving the signed zone, you should:

1. revert back `named.conf.local` to its previous configuration, i.e. configure BIND to serve the unsigned zone file as before the manual signing configuration which was: `file "/etc/bind/zones/db.grpX";`
2. backup the signed zone file (.signed) and delete all the files created by the manual signing process except the unsigned zone file only (BIND will create its own signed zone file in the next step)
3. increase the serial in the unsigned zone file and reload BIND.

Configure BIND to sign the zone.

Edit config file.

Update your zone configuration statement in `/etc/bind/named.conf.local`, to look like the below :

```
zone "grpX.<lab_domain>.te-labs.training" {
  type primary;
  file "/etc/bind/zones/db.grpX";
  allow-transfer { any; };
  also-notify {100.100.X.130; 100.100.X.131; };
  key-directory "/etc/bind/keys";
  auto-dnssec maintain;
  inline-signing yes;
};
```

Then, reconfigure or restart BIND: using `rndc reconfig` or `systemctl restart bind9`. Always check status after such operation.

Some new files should appear in the *zones* directory.

Verify that your zone is signed.

We use the command `rndc signing -list` to confirm that the zone is signed. You should get an output like:

```
$ sudo rndc signing -list grpX.<lab_domain>.te-labs.training
Done signing with key 52159/RSASHA256
Done signing with key 51333/RSASHA256
```

Use command line tools to query the signed zone.

We can now use *dig* utility to confirm that the zone is signed and play with the new DNSSEC RRs.

> ⚠ **Warning**
>
> remember that at this stage, you have only signed the zone and have not yet established the chain of trust.

QUESTION: Will you get the "ad" flag ? Why ?

1. dig DNSKEY *grpX.<lab_domain>*.te-labs.training @100.100.X.130
2. dig DNSKEY *grpX.<lab_domain>*.te-labs.training @100.100.X.130 +dnssec +multi
3. dig SOA *grpX.<lab_domain>*.te-labs.training @100.100.X.130 +dnssec +multi

QUESTIONS: did you get the answers ? Did you receive the signatures ? Did you get the "ad" flag ? Why ?