Recovery of a single dnskey from SoftHSM backup

This document describes how to recover a single keypair from a backup.

Before you start

This is a rare procedure that should never be necessary in a production environment. Before you start you should also consider restoring the entire environment from backup (instead of a single key) and/or regenerating the key.

Please be careful if you use this, the document below is a draft and contains a lot of assumptions about our environment.

Most information came from:

- https://wiki.opendnssec.org/display/DOCS/Migrating+to+OpenDNSSEC
- https://svn.opendnssec.org/trunk/softHSM/README

Background

- The HSM is SoftHSM. Other HSMs will differ substantially.
    - backups are made with the sqlite 'dump' command
    - for this example the backup is in a file named dnssec-softhsm_12-11-17.bak
- OpenDNSSEC uses the MySQL backend. The general procedure should also work with other backends but you will need create the temporary database yourself.
    - backups are made with the mysqldump utillity
    - for this example the backup is in a file named dnssec-sql_12-11-17.bak
- The domain is example.com
- Only Key Signing Keys are restored
    - ZSK's tend to expire within days
    - the procedure should also work for ZSK's but it's easier to generate a new ZSK
- the OS is Debian GNU/Linux 6
    - Ubuntu and other Linux-distributions should work as well but this has not been tested.

Procedure

High level overview

First we need determine the id used to identify the keypair by inspecting the ODS-database backup. Next we extract this keypair from the SoftHSM backup. Finally the keypair is imported back into OpenDNSSEC

1. Create temporary mysql database from backup
   $ mysqladmin -u root -p create odstemp
   $ echo "GRANT ALL ON odstemp.* to 'opendnssec'@'localhost';" | mysql -u root -p odstemp
   $ mysql -u root -p odstemp < MYSQL_BACKUP
2. Search the key info
   mysql> SELECT HSMkey_id,active,retire
   FROM keypairs,dnsseckeys,zones
   WHERE keypairs.id=dnsseckeys.keypair_id AND dnsseckeys.zone_id=zones.id
   AND keytype=257 AND zones.name='YOUR ZONE';
3. Create a temporary SoftHSM

```
$ sqlite3 softhsm.db "PRAGMA user_version = 100;"

$ sqlite3 softhsm.db < SOFTHSM_BACKUP

$ echo 0:$PWD/softhsm.db > softhsm.conf

$ export SOFTHSM_CONF=$PWD/softhsm.conf
```

4. Export keypair from temporary SoftHSM
   $ softhsm --export YOURZONE.zsk.pem --slot 0 --pin <pincode> --id HSMKEY_ID
5. Import keypair into running softhsm with a _new_ ID
   # export SOFTHSM_CONF=/etc/softhsm/softhsm.conf
   # softhsm --import YOURZONE.zsk.pem --slot 0 --label "SOME COMMENT" --id NEW_UNIQUE_ID --pin <pincode>
6. Import keypair into OpenDNSSEC
   # ods-ksmutil key import --cka_id NEW_UNIQUE_ID --repository YOUR_HSM --zone YOUR_ZONE \
   --bits FROM_KASP --algorithm FROM_KASP --keystate ACTIVE --keytype ksk --time SEE_STEP4 --retire SEE_STEP4
7. Sign zone with imported key
   # ods-signer sign YOURZONE

Example

1. Create temporary mysql database from backup
   $ mysqladmin -u root -p create odstemp
   $ echo "GRANT ALL ON odstemp.* to 'opendnssec'@'localhost';" | mysql -u root -p odstemp
   $ mysql -u root -p odstemp < dnssec-sql_12-11-17.bak
2. Search the key info
   mysql> SELECT HSMkey_id,active,retire
   FROM keypairs,dnsseckeys,zones
   WHERE keypairs.id=dnsseckeys.keypair_id AND dnsseckeys.zone_id=zones.id
   AND keytype=257 AND zones.name='example.com';

HSMkey_id	active	retire
d4aeef65b2ce3b1c0f5192778ad40b0c	2012-02-22 14:49:44	2013-02-21 14:49:44

3. Create a temporary SoftHSM

```
$ sqlite3 softhsm.db "PRAGMA user_version = 100;"

$ sqlite3 softhsm.db < dnssec-softhsm_12-11-17.bak

$ echo 0:$PWD/softhsm.db > softhsm.conf

$ export SOFTHSM_CONF=$PWD/softhsm.conf
```

4. Export keypair from temporary SoftHSM
   $ softhsm --export example.com.zsk.pem --slot 0 --pin <pincode> --id d4aeef65b2ce3b1c0f5192778ad40b0c
5. Import keypair into running softhsm with a _new_ ID
   # export SOFTHSM_CONF=/etc/softhsm/softhsm.conf
   # softhsm --import example.com.zsk.pem --slot 0 --label "recovered example.com" --id 00000065b2ce3b1c0f5192778ad40b0c --pin <pincode>
6. Import keypair into OpenDNSSEC
   # ods-ksmutil key import --cka_id 00000065b2ce3b1c0f5192778ad40b0c --repository LocalHSM --zone example.com \
   --bits 2048 --algorithm 8 --keystate ACTIVE --keytype ksk --time "2012-02-22 14:49:44" --retire "2013-02-21 14:49:44"
7. Sign zone with imported key
   # ods-signer sign example.com