Key Management

This sections describes common key management activities of OpenDNSSEC.

The details of the command utilities shown below can be found here.

On this Page

Marking keys as backed up

You can configure the system to only make keys active once they have been backed up. This is done by editing the conf.xml file. The user must do backups and then notify OpenDNSSEC about this, so that the key rollover process can continue. The keys must be backed up regulary, because OpenDNSSEC is generating new keys prior to a rollover.

1. First prepare the backup by telling the Enforcer that you want to do backup of the keys. This is so that keys generated after you have done your backup won't accidentally be marked as backed up.

   For all of the repositories:

   ```
   ods-ksmutil backup prepare
   ```

   or a single repository:

   ```
   ods-ksmutil backup prepare --repository <repository>
   ```

2. Then you can safely do your backups. **Please read the documentation of your HSM for instructions on how to do backups.** When you are done, then notify the Enforcer about this:

   For all of the repositories:

   ```
   ods-ksmutil backup commit
   ```

   or a single repository:

   ```
   ods-ksmutil backup commit --repository <repository>
   ```

   The command *ods-ksmutil backup done* will mark your keys as backed up in one step. This means that keys may have been generated between you doing the backup and giving the command. Thus accidentally marking them as backed up. This command is deprecated and should not be used, unless you make sure to stop the Enforcer when doing your backup.

Backups are specified by way of a repository option in conf.xml:

```
<RequireBackup/>
```

If you decide you want to change this facility, you should edit conf.xml accordingly, and run:

```
ods-ksmutil update conf
```

It will report something along the lines of:

```
RequireBackup set.
```

Export the public keys

You need to publish your key to the parent or to interested parties. If you are doing a key rollover, then only the ready KSK should be exported. The following command will extract the trust anchors:

```
ods-ksmutil key export --zone example.com [--keystate READY]
ods-ksmutil key export --zone example.com --ds [--keystate READY]
```

What you get in return is the DNSKEY or DS in BIND-format.

Key rollovers

First step

This step is not needed for a scheduled rollover.
The rollovers are done automatically according to the policy of the zone. But a **manual** keyrollover may be desired in cases of emergency, such as having lost a private key.

A manual rollover can be done using the *ods-ksmutil* command like this:

```
ods-ksmutil key rollover --zone example.com --keytype KSK
```

This will roll the KSK key in a timely manner following the policy used for the zone *example.com*. If you want to roll the Zone Signing Key use *--keytype ZSK* instead.

You can also roll all the keys for zones which have a certain policy. This can be useful if you want to move all keys from one key store to another.

```
ods-ksmutil key rollover --policy default --keytype KSK
```

Second step for KSKs - Publish the DS to the parent

Unlike ZSKs, a KSK rollover requires a second step involving manual intervention. This intervention is a multi-stage process. First, the DNSKEY record for the new key is added to the zone. Then, after a suitable interval, the new DS record is submitted to the parent; at this point the old DS record can be removed from the parent.

The stages are:

1. Extract the DNSKEY record for the new key and publish it in the parent zone. (The new record replace any existing records for the zone being signed.) When it is time for this to happen a message with log-level "info" will be sent to syslog looking something like:

   ```
   Mar 16 11:39:05 sion ods-enforcerd: DS Record set has changed, the current set looks like:
   Mar 16 11:39:05 sion ods-enforcerd: example.com. 3600 IN DNSKEY 257 3 7
   AwEAAbcTSmphJUMKvegvDgqGspRM8IHlKZqoU5pkPaTtRLkioxGyZ5iIh4bNnvqmx1zWIttuJ6erGUMOatMm3SXxiTr9OLaRPr86KV
   po6mzejTqFicGxSp3KsrbUvyIs/V84Ry7XZBKVKVjgppjmqeS8mRtXM4UynwTEJk0hKQfCcmkH0Q
   /fhZibwBVG+OcBfvTdsQbp8LZN4oVqn/vzhnuxFkE8biTr19jmKTdtgkhp524ML59v7prg7F/+Lb2OJLc8Gg6pastUeqXc
   /Iv2CdVyOvMWRW39VCzyLbKpmyqB8Hc4Kn1pT5Idqc3/N3qBvXVe3HyyiZbjHGxOT6RZNNT8= ;{id = 51994 (ksk), size =
   2048b}
   Mar 16 11:39:05 sion ods-enforcerd: Once the new DS records are seen in DNS please issue the ds-seen
   command for zone example.com with the following cka_ids, 04260cd6eac67280cd2dea94c6e38cb7
   ```

   The DNSKEY or DS RR can also be retrieved by using the commands in the section *Export the public keys*.

   This step can be automated or semi-automated by placing a command in the <DelegationSignerSubmitCommand> tag. This should point to a binary which will accept the required key(s) as DNSKEY RRs on STDIN.
2. When the records indicated have been seen in DNS then this can be communicated to OpenDNSSEC with the ds-seen command as indicated:

   ```
   ods-ksmutil key ds-seen --zone example.com --cka_id 04260cd6eac67280cd2dea94c6e38cb7
   ```

3. If the DS records were not swapped, i.e. the old DS was left in the parent when the new one was added, then the --no-retire flag can be added to the ds-seen command. Then, at some later time, the old key can be retired with the command:

```
ods-ksmutil key ksk-retire --zone example.com ---cka_id 87f1385b114f9f9b299e6b551d728bfb
```

or

```
ods-ksmutil key ksk-retire --zone example.com
```

The former command will retire the specific key (provided the key is active, and the action will not leave the zone without any active keys). The latter command will retire the oldest active key on the zone, again provided it will not leave the zone without any active keys.

If you wish to run like this and use the DelegationSignerSubmitCommand hook then you will need to add the current key back into the set yourself.

Key rollovers on exact dates

Some users want to have more control over their key rollovers and roll keys on exact dates, for example the first day of each month. To do this you need to specify that you want manual key rollovers in the kasp.xml configuration. Add the *<ManualRollover/>* tag to the type and key you want to roll manually.

When this is done you can add the rollover commands to a cron job, with a command like this:

```
ods-ksmutil key rollover --zone example.com --keytype ZSK
```