NAME

zkt−keyman — A DNSSEC key management tool

SYNOPSYS

zkt−keyman −C<label> [**−V**|**--view** *view*] [**−c** *file*] [**−krpz**] [{*keyfile*|*dir*} ...]
zkt−keyman −−create=<label> [**−V**|**--view** *view*] [**−c** *file*] [**−krpz**] [{*keyfile*|*dir*} ...]

zkt−keyman −{**P**|**A**|**D**|**R**}**<keytag>** [**−V**|**--view** *view*] [**−c** *file*] [**−r**] [{*keyfile*|*dir*} ...]
zkt−keyman −−published=<keytag> [**−V**|**--view** *view*] [**−c** *file*] [**−r**] [{*keyfile*|*dir*} ...]
zkt−keyman −−active=<keytag> [**−V**|**--view** *view*] [**−c** *file*] [**−r**] [{*keyfile*|*dir*} ...]
zkt−keyman −−depreciate=<keytag> [**−V**|**--view** *view*] [**−c** *file*] [**−r**] [{*keyfile*|*dir*} ...]
zkt−keyman −−rename=<keytag> [**−V**|**--view** *view*] [**−c** *file*] [**−r**] [{*keyfile*|*dir*} ...]

zkt−keyman −−destroy=<keytag> [**−V**|**--view** *view*] [**−c** *file*] [**−r**] [{*keyfile*|*dir*} ...]

zkt−keyman −9 | −−ksk-rollover
zkt−keyman −1 | −−ksk-roll-phase1 *do.ma.in.* [**−V**|**--view** *view*] [**−c** *file*]
zkt−keyman −2 | −−ksk-roll-phase2 *do.ma.in.* [**−V**|**--view** *view*] [**−c** *file*]
zkt−keyman −3 | −−ksk-roll-phase3 *do.ma.in.* [**−V**|**--view** *view*] [**−c** *file*]
zkt−keyman −0 | −−ksk-roll-stat *do.ma.in.* [**−V**|**--view** *view*] [**−c** *file*]

DESCRIPTION

The *zkt−keyman* command is a wrapper around *dnssec-keygen(8)* to assist in dnssec zone key management.

The command is useful in dns key management. It is suitable for modification of key status.

GENERAL OPTIONS

−V *view***, −−view=***view*

Try to read the default configuration out of a file named *dnssec-<view>.conf* . Instead of specifying the −V or --view option every time, it is also possible to create a hard or softlink to the executable file to give it an additional name like *zkt−keyman−<view>* .

−c *file***, −−config=** *file*

Read default values from the specified config file. Otherwise the default config file is read or build in defaults will be used.

−O *optstr***, −−config-option=***optstr*

Set any config file option via the commandline. Several config file options could be specified at the argument string but have to be delimited by semicolon (or newline).

−d, **−−directory**

Skip directory arguments. This will be useful in combination with wildcard arguments to prevent dnsssec-zkt to list all keys found in subdirectories. For example "zkt−keyman -d *" will print out a list of all keys only found in the current directory. Maybe it is easier to use "zkt−keyman ." instead (without -r set). The option works similar to the −d option of *ls(1)*.

−k, **−−ksk**

Select key signing keys only (default depends on command mode).

−z, **−−zsk**

Select zone signing keys only (default depends on command mode).

−r, **−−recursive**

Recursive mode (default is off).
Also settable in the dnssec.conf file (Parameter: Recursive).

−F, **−−setlifetime**
Set the key lifetime of all the selected keys. Use option -k, -z, -l or the file and dir argument for key selection.

COMMAND OPTIONS

−h, **−−help**
Print out the online help.

−C *zone*, **−−create=***zone*
Create a new zone signing key for the given zone. Add option **−k** to create a key signing key. The key algorithm and key length will be examined from built-in default values or from the parameter settings in the *dnssec.conf* file.
The keyfile will be created in the current directory if the **−p** option is specified.

−R *keyid***,** **−−revoke=***keyid*
Revoke the key signing key with the given keyid. A revoked key has bit 8 in the flags field set (see RFC5011). The keyid is the numeric keytag with an optionally added zone name separated by a colon.

−−rename="*keyid*
Rename the key files of the key with the given keyid (Look at key file names starting with an lower ’k’). The keyid is the numeric keytag with an optionally added zone name separated by a colon.

−−destroy=*keyid*
Deletes the key with the given keyid. The keyid is the numeric keytag with an optionally added zone name separated by a colon. Beware that this deletes both private and public keyfiles, thus the key is unrecoverable lost.

−P|A|D *keyid,* **−−published=***keyid,* **−−active=***keyid,* **−−depreciated=***keyid*
Change the status of the given dnssec key to published (**−P**), active (**−A**) or depreciated (**−D**). The *keyid* is the numeric keytag with an optionally added zone name separated by a colon. Setting the status to "published" or "depreciate" will change the filename of the private key file to ".published" or ".depreciated" respectivly. This prevents the usage of the key as a signing key by the use of *dnssec-signzone(8)*. The time of status change will be stored in the ’mtime’ field of the corresponding ".key" file. Key activation via option **−A** will restore the original timestamp and file name (".private").

−−ksk-roll-phase[123] *do.ma.in.*
Initiate a key signing key rollover of the specified domain. This feature is currently in experimental status and is mainly for the use in an hierachical environment. Use --ksk-rollover for a little more detailed description.

SAMPLE USAGE

```
zkt-keyman −C example.net −k −r ./zonedir
```

Create a new key signing key for the zone "example.net". Store the key in the same directory below "zonedir" where the other "example.net" keys life.

```
zkt-keyman −D 123245 −r .
```

Depreciate the key with tag "12345" below the current directory,

```
zkt-keyman --view intern −C example.net
```

Create a new zone key for the internal zone example.net.

```
zkt-keyman-intern
```

Same as above. The binary file *zkt−keyman* has another link, named *zkt-keyman-intern* made, and *zkt−keyman* examines argv[0] to find a view whose zones it proceeds to process.

ENVIRONMENT VARIABLES

ZKT_CONFFILE

Specifies the name of the default global configuration files.

FILES

/var/named/dnssec.conf

Built-in default global configuration file. The name of the default global config file is settable via the environment variable ZKT_CONFFILE.

/var/named/dnssec-<view>.conf

View specific global configuration file.

./dnssec.conf

Local configuration file (only used in **−C** mode).

BUGS

AUTHORS

Holger Zuleger

COPYRIGHT

SEE ALSO

dnssec-keygen(8), dnssec-signzone(8), rndc(8), named.conf(5), zkt-conf(8), zkt-ls(8), zkt-signer(8)
RFC4641 "DNSSEC Operational Practices" by Miek Gieben and Olaf Kolkman,
DNSSEC HOWTO Tutorial by Olaf Kolkman, RIPE NCC
(http://www.nlnetlabs.nl/dnssec_howto/)