NAME

dnssec-zkt — Secure DNS zone key tool

SYNOPSYS

dnssec-zkt [**−V**|**--view** *view*] [**−c** *file*] [**−l** *list*] [**−adefhkLrptz**] [{*keyfile*|*dir*} ...]

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

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

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

dnssec-zkt −T [**−V**|**--view** *view*] [**−c** *file*] [**−l** *list*] [**−hr**] [{*keyfile*|*dir*} ...]
dnssec-zkt −−list-trustedkeys [**−V**|**--view** *view*] [**−c** *file*] [**−l** *list*] [**−hr**] [{*keyfile*|*dir*} ...]

dnssec-zkt −K [**−V**|**--view** *view*] [**−c** *file*] [**−l** *list*] [**−hkzr**] [{*keyfile*|*dir*} ...]
dnssec-zkt −−list-dnskeys [**−V**|**--view** *view*] [**−c** *file*] [**−l** *list*] [**−hkzr**] [{*keyfile*|*dir*} ...]

dnssec-zkt −Z [**−V**|**--view** *view*] [**−c** *file*]
dnssec-zkt −−zone-config [**−V**|**--view** *view*] [**−c** *file*]

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

DESCRIPTION

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

In the common usage the command prints out information about all dnssec (zone) keys found in the given (or predefined default) directory. It is also possible to specify keyfiles (K*.key) as arguments. With option **−r** subdirectories will be searched recursively, and all dnssec keys found will be listed sorted by domain name, key type and generation time. In that mode the use of the **−p** option may be helpful to find the location of the keyfile in the directory tree.

Other forms of the command print out keys in a format suitable for a trusted-key section or as a DNSKEY resource record.

The command is also useful in dns key management. It offers monitoring of key lifetime and 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 *dnssec-zkt-<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).

−l *list* Print out information solely about domains given in the comma or space separated list. Take care of, that every domain name has a trailing dot.

−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 "dnssec-zkt -d *" will print out a list of all keys only found in the current directory. Maybe it is easier to use "dnssec-zkt ." instead (without -r set). The option works similar to the −d option of *ls(1)*.

−L, **−−left-justify**
Print out the domain name left justified.

−k, **−−ksk**
Select and print key signing keys only (default depends on command mode).

−z, **−−zsk**
Select and print 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).

−p, **−−path**
Print pathname in listing mode. In -C mode, don't create the new key in the same directory as (already existing) keys with the same label.

−a, **−−age**
Print age of key in weeks, days, hours, minutes and seconds (default is off).
Also settable in the dnssec.conf file (Parameter: PrintAge).

−f, **−−lifetime**
Print the key lifetime.

−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.

−e, **−−exptime**
Print the key expiration time.

−t, **−−time**
Print the key generation time (default is on).
Also settable in the dnssec.conf file (Parameter: PrintTime).

−h No header or trusted-key section header and trailer in -T mode

COMMAND OPTIONS

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

−T, **−−list-trustedkeys**
List all key signing keys as a *named.conf* trusted-key section. Use **−h** to supress the section header/trailer.

−K, **−−list-dnskeys**
List the public part of all the keys in DNSKEY resource record format. Use **−h** to suppress comment lines.

−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 filed 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").

−Z, **−−zone-config**
Write all config parameters to stdout. The output is suitable as a template for the *dnssec.conf* file, so the easiest way to create a *dnssec.conf* file is to redirect the standard output of the above command. Pay attention not to overwrite an existing file.

−−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

`dnssec-zkt −r .`
Print out a list of all zone keys found below the current directory.

`dnssec-zkt −Z −c ""`
Print out the compiled in default parameters.

`dnssec-zkt −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 live.

`dnssec-zkt −T ./zonedir/example.net`
Print out a trusted-key section containing the key signing keys of "example.net".

`dnssec-zkt −D 123245 −r .`
Depreciate the key with tag "12345" below the current directory,

`dnssec-zkt --view intern`
Print out a list of all zone keys found below the directory where all the zones of view intern live. There should be a seperate dnssec config file *dnssec-intern.conf* with a directory option to take affect of this.

`dnssec-zkt-intern`
Same as above. The binary file *dnssec-zkt* has another link, named *dnssec-zkt-intern* made, and *dnssec-zkt* 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

Some of the general options will not be meaningful in all of the command modes.
The option **−l** and the ksk rollover options insist on domain names ending with a dot.

AUTHORS

Holger Zuleger, Mans Nilsson

COPYRIGHT

SEE ALSO

dnssec-keygen(8), dnssec-signzone(8), rndc(8), named.conf(5), dnssec-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/)