

NAME

`dnssec-importkey` – import DNSKEY records from external systems so they can be managed

SYNOPSIS

dnssec-importkey [-K *directory*] [-L *t1*] [-P *date/offset*] [-P *sync date/offset*] [-D *date/offset*] [-D *sync date/offset*] [-h] [-v *level*] [-V] {*keyfile*}

dnssec-importkey {-f *filename*} [-K *directory*] [-L *t1*] [-P *date/offset*] [-P *sync date/offset*] [-D *date/offset*] [-D *sync date/offset*] [-h] [-v *level*] [-V] [*dnsname*]

DESCRIPTION

dnssec-importkey reads a public DNSKEY record and generates a pair of .key/.private files. The DNSKEY record may be read from an existing .key file, in which case a corresponding .private file is generated, or it may be read from any other file or from the standard input, in which case both .key and .private files are generated.

The newly created .private file does *not* contain private key data, and cannot be used for signing. However, having a .private file makes it possible to set publication (-P) and deletion (-D) times for the key, which means the public key can be added to and removed from the DNSKEY RRset on schedule even if the true private key is stored offline.

When using **dnssec-policy**, do not use **dnssec-importkey** to import key files that cannot be used for signing. In this case, simply publish the imported DNSKEY record in the zone, and make sure that the files are outside the configured **key-directory**.

OPTIONS**-f filename**

This option indicates the zone file mode. Instead of a public keyfile name, the argument is the DNS domain name of a zone master file, which can be read from **filename**. If the domain name is the same as **filename**, then it may be omitted.

If **filename** is set to "-", then the zone data is read from the standard input.

-K directory

This option sets the directory in which the key files are to reside.

-L ttl This option sets the default TTL to use for this key when it is converted into a DNSKEY RR. This is the TTL used when the key is imported into a zone, unless there was already a DNSKEY RRset in place, in which case the existing TTL takes precedence. Setting the default TTL to **0** or **none** removes it from the key.

-h This option emits a usage message and exits.

-v level

This option sets the debugging level.

-V This option prints version information.

TIMING OPTIONS

Dates can be expressed in the format YYYYMMDD or YYYYMMDDHHMMSS. (which is the format used inside key files), or 'Day Mon DD HH:MM:SS YYYY' (as printed by **dnssec-settime -p**), or UNIX epoch time (as printed by **dnssec-settime -up**), or the literal **now**.

The argument can be followed by + or - and an offset from the given time. The literal **now** can be omitted before an offset. The offset can be followed by one of the suffixes **y**, **mo**, **w**, **d**, **h**, or **mi**, so that it is computed in years (defined as 365 24-hour days, ignoring leap years), months (defined as 30 24-hour days), weeks, days, hours, or minutes, respectively. Without a suffix, the offset is computed in seconds.

To explicitly prevent a date from being set, use **none**, **never**, or **unset**.

All these formats are case-insensitive.

-P date/offset

This option sets the date on which a key is to be published to the zone. After that date, the key is included in the zone but is not used to sign it.

sync date/offset

This option sets the date on which CDS and CDNSKEY records that match this key are to be published to the zone.

-D date/offset

This option sets the date on which the key is to be deleted. After that date, the key is no longer included in the zone. (However, it may remain in the key repository.)

sync date/offset

This option sets the date on which the CDS and CDNSKEY records that match this key are to be deleted.

FILES

A keyfile can be designed by the key identification **Knnnnn.+aaa+iiii** or the full file name **Knnnnn.+aaa+ii-iii.key**, as generated by **dnssec-keygen** <#std-iscman-dnssec-keygen>.

SEE ALSO

dnssec-keygen(8) <#std-iscman-dnssec-keygen>, **dnssec-signzone(8)** <#std-iscman-dnssec-signzone>, BIND 9 Administrator Reference Manual, **RFC 5011** <<https://datatracker.ietf.org/doc/html/rfc5011.html>>.

Author

Internet Systems Consortium

Copyright

2026, Internet Systems Consortium