

NAME

dnssec-settime – set the key timing metadata for a DNSSEC key

SYNOPSIS

dnssec-settime [-f] [-K directory] [-L ttl] [-P date/offset] [-P ds date/offset] [-P sync date/offset] [-A date/offset] [-R date/offset] [-I date/offset] [-D date/offset] [-D ds date/offset] [-D sync date/offset] [-S key] [-i interval] [-h] [-V] [-v level] [-E engine] {keyfile} [-s] [-g state] [-d state date/offset] [-k state date/offset] [-r state date/offset] [-z state date/offset]

DESCRIPTION

dnssec-settime reads a DNSSEC private key file and sets the key timing metadata as specified by the **-P**, **-A**, **-R**, **-I**, and **-D** options. The metadata can then be used by **dnssec-signzone** <#std-iscman-dnssec-signzone> or other signing software to determine when a key is to be published, whether it should be used for signing a zone, etc.

If none of these options is set on the command line, **dnssec-settime** simply prints the key timing metadata already stored in the key.

When key metadata fields are changed, both files of a key pair (**Knnnn.+aaa+iiii.key** and **Knnnn.+aaa+ii-iii.private**) are regenerated.

Metadata fields are stored in the private file. A human-readable description of the metadata is also placed in comments in the key file. The private file's permissions are always set to be inaccessible to anyone other than the owner (mode 0600).

When working with state files, it is possible to update the timing metadata in those files as well with **-s**. With this option, it is also possible to update key states with **-d** (DS), **-k** (DNSKEY), **-r** (RRSIG of KSK), or **-z** (RRSIG of ZSK). Allowed states are HIDDEN, RUMOURED, OMNIPRESENT, and UNRETENTIVE.

The goal state of the key can also be set with **-g**. This should be either HIDDEN or OMNIPRESENT, representing whether the key should be removed from the zone or published.

It is NOT RECOMMENDED to manipulate state files manually, except for testing purposes.

OPTIONS

-f This option forces an update of an old-format key with no metadata fields. Without this option, **dnssec-settime** fails when attempting to update a legacy key. With this option, the key is recreated in the new format, but with the original key data retained. The key's creation date is set to the present time. If no other values are specified, then the key's publication and activation dates are also set to the present time.

-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. If this value is not set and there is no existing DNSKEY RRset, the TTL defaults to the SOA TTL. Setting the default TTL to **0** or **none** removes it from the key.

-h This option emits a usage message and exits.

-V This option prints version information.

-v level

This option sets the debugging level.

-E engine

This option specifies the cryptographic hardware to use, when applicable.

When BIND 9 is built with OpenSSL, this needs to be set to the OpenSSL engine identifier that drives the cryptographic accelerator or hardware service module (usually **pkcs11**).

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 unset a date, 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.

ds date/offset

This option sets the date on which DS records that match this key have been seen in the parent zone.

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.

-A date/offset

This option sets the date on which the key is to be activated. After that date, the key is included in the zone and used to sign it.

-R date/offset

This option sets the date on which the key is to be revoked. After that date, the key is flagged as revoked. It is included in the zone and is used to sign it.

-I date/offset

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

-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.)

ds date/offset

This option sets the date on which the DS records that match this key have been seen removed from the parent zone.

sync date/offset

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

-S predecessor key

This option selects a key for which the key being modified is an explicit successor. The name, algorithm, size, and type of the predecessor key must exactly match those of the key being modified. The activation date of the successor key is set to the inactivation date of the predecessor. The publication date is set to the activation date minus the prepublication interval, which defaults to 30

days.

-i interval

This option sets the prepublication interval for a key. If set, then the publication and activation dates must be separated by at least this much time. If the activation date is specified but the publication date is not, the publication date defaults to this much time before the activation date; conversely, if the publication date is specified but not the activation date, activation is set to this much time after publication.

If the key is being created as an explicit successor to another key, then the default prepublication interval is 30 days; otherwise it is zero.

As with date offsets, if the argument is followed by one of the suffixes **y**, **mo**, **w**, **d**, **h**, or **mi**, the interval is measured in years, months, weeks, days, hours, or minutes, respectively. Without a suffix, the interval is measured in seconds.

KEY STATE OPTIONS

To test `dnssec-policy` it may be necessary to construct keys with artificial state information; these options are used by the testing framework for that purpose, but should never be used in production.

Known key states are `HIDDEN`, `RUMOURED`, `OMNIPRESENT`, and `UNRETENTIVE`.

-s This option indicates that when setting key timing data, the state file should also be updated.

-g state

This option sets the goal state for this key. Must be `HIDDEN` or `OMNIPRESENT`.

-d state date/offset

This option sets the DS state for this key as of the specified date, offset from the current date.

-k state date/offset

This option sets the DNSKEY state for this key as of the specified date, offset from the current date.

-r state date/offset

This option sets the RRSIG (KSK) state for this key as of the specified date, offset from the current date.

-z state date/offset

This option sets the RRSIG (ZSK) state for this key as of the specified date, offset from the current date.

PRINTING OPTIONS

`dnssec-settime` can also be used to print the timing metadata associated with a key.

-u This option indicates that times should be printed in Unix epoch format.

-p C/P/Pds/PSync/A/R/I/D/Dds/Dsync/all

This option prints a specific metadata value or set of metadata values. The **-p** option may be followed by one or more of the following letters or strings to indicate which value or values to print: **C** for the creation date, **P** for the publication date, **Pds` for the DS publication date**, **PSync** for the CDS and CDNSKEY publication date, **A** for the activation date, **R** for the revocation date, **I** for the inactivation date, **D** for the deletion date, **Dds** for the DS deletion date, and **Dsync** for the CDS and CDNSKEY deletion date. To print all of the metadata, use **all**.

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