NAME

dnssec-keyfromlabel − DNSSEC key generation tool

SYNOPSIS

dnssec−keyfromlabel {**−l** label} [**−3**] [**−a** algorithm] [**−A** date/offset] [**−c** class] [**−D** date/offset] [**−D** sync date/offset] [**−E** engine] [**−f** flag] [**−G**] [**−I** date/offset] [**−i** interval] [**−k**] [**−K** directory] [**−L** ttl] [**−n** nametype] [**−P** date/offset] [**−P** sync date/offset] [**−p** protocol] [**−R** date/offset] [**−S** key] [**−t** type] [**−v** level] [**−V**] [**−y**] {name}

DESCRIPTION

dnssec−keyfromlabel generates a pair of key files that reference a key object stored in a cryptographic hardware service module (HSM). The private key file can be used for DNSSEC signing of zone data as if it were a conventional signing key created by **dnssec−keygen** <#std-iscman-dnssec-keygen>, but the key material is stored within the HSM and the actual signing takes place there.

The **name** of the key is specified on the command line. This must match the name of the zone for which the key is being generated.

OPTIONS

−a algorithm

This option selects the cryptographic algorithm. The value of **algorithm** must be one of RSASHA1 (deprecated), NSEC3RSASHA1 (deprecated), RSASHA256, RSASHA512, ECDSAP256SHA256, ECDSAP384SHA384, ED25519, or ED448.

These values are case−insensitive. In some cases, abbreviations are supported, such as ECDSA256 for ECDSAP256SHA256 and ECDSA384 for ECDSAP384SHA384. If RSASHA1 (deprecated) is specified along with the **−3** option, then NSEC3RSASHA1 (deprecated) is used instead.

This option is mandatory except when using the **−S** option, which copies the algorithm from the predecessory key.

Changed in version 9.12.0: The default value RSASHA1 (deprecated) for newly generated keys was removed.

−3 This option uses an NSEC3−capable algorithm to generate a DNSSEC key. If this option is used with an algorithm that has both NSEC and NSEC3 versions, then the NSEC3 version is used; for example, **dnssec−keygen −3a RSASHA1** specifies the NSEC3RSASHA1 (deprecated) algorithm.

−E engine

This option specifies the cryptographic hardware to use.

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**).

−l label

This option specifies the label for a key pair in the crypto hardware.

When BIND 9 is built with OpenSSL−based PKCS#11 support, the label is an arbitrary string that identifies a particular key. It may be preceded by an optional OpenSSL engine name, followed by a colon, as in **pkcs11:keylabel**.

−n nametype

This option specifies the owner type of the key. The value of **nametype** must either be ZONE (for a DNSSEC zone key (KEY/DNSKEY)), HOST or ENTITY (for a key associated with a host (KEY)), USER (for a key associated with a user (KEY)), or OTHER (DNSKEY). These values are case−insensitive.

−C This option enables compatibility mode, which generates an old−style key, without any metadata. By default, **dnssec−keyfromlabel** includes the key's creation date in the metadata stored with the private key; other dates may be set there as well, including publication date, activation date, etc. Keys that include this data may be incompatible with older versions of BIND; the **−C** option suppresses them.

−c class
This option indicates that the DNS record containing the key should have the specified class. If not specified, class IN is used.

−f flag This option sets the specified flag in the **flag** field of the KEY/DNSKEY record. The only recognized flags are KSK (Key−Signing Key) and REVOKE.

−G This option generates a key, but does not publish it or sign with it. This option is incompatible with **−P** and **−A**.

−h This option prints a short summary of the options and arguments to **dnssec−keyfromlabel**.

−K directory
This option sets the directory in which the key files are to be written.

−k This option generates KEY records rather than DNSKEY records.

−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 would take precedence. Setting the default TTL to **0** or **none** removes it.

−p protocol
This option sets the protocol value for the key. The protocol is a number between 0 and 255. The default is 3 (DNSSEC). Other possible values for this argument are listed in **RFC 2535** <https://datatracker.ietf.org/doc/html/rfc2535.html> and its successors.

−S key This option generates a key as an explicit successor to an existing key. The name, algorithm, size, and type of the key are set to match the predecessor. The activation date of the new key is set to the inactivation date of the existing one. The publication date is set to the activation date minus the prepublication interval, which defaults to 30 days.

−t type This option indicates the type of the key. **type** must be one of AUTHCONF, NOAUTHCONF, NOAUTH, or NOCONF. The default is AUTHCONF. AUTH refers to the ability to authenticate data, and CONF to the ability to encrypt data.

−v level
This option sets the debugging level.

−V This option prints version information.

−y This option allows DNSSEC key files to be generated even if the key ID would collide with that of an existing key, in the event of either key being revoked. (This is only safe to enable if **RFC 5011** <https://datatracker.ietf.org/doc/html/rfc5011.html> trust anchor maintenance is not used with either of the keys involved.)

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. If not set, and if the **−G** option has not been used, the default is the current date.

  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. If not set, and if the **−G** option has not been used, the default is the current date.

−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.)

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

−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.

GENERATED KEY FILES

When **dnssec−keyfromlabel** completes successfully, it prints a string of the form **Knnnn.+aaa+iiiii** to the standard output. This is an identification string for the key files it has generated.

- **nnnn** is the key name.
- **aaa** is the numeric representation of the algorithm.
- **iiiii** is the key identifier (or footprint).

dnssec−keyfromlabel creates two files, with names based on the printed string.**Knnnn.+aaa+iiiii.k ey** contains the public key, and **Knnnn.+aaa+iiiii.private** contains the private key.

The **.key** file contains a DNS KEY record that can be inserted into a zone file (directly or with an $INCLUDE statement).

The **.private** file contains algorithm−specific fields. For obvious security reasons, this file does not have general read permission.

SEE ALSO

dnssec−keygen(8) <#std-iscman-dnssec-keygen>, **dnssec−signzone(8)** <#std-iscman-dnssec-signzone>, BIND 9 Administrator Reference Manual, **RFC 4034** <https://datatracker.ietf.org/doc/html/rfc4034.html>, **RFC 7512** <https://datatracker.ietf.org/doc/html/rfc7512.html>.

Author

Internet Systems Consortium

Copyright