NAME

dnssec-keygen − DNSSEC key generation tool

SYNOPSIS

dnssec−keygen [**−3**] [**−A** date/offset] [**−a** algorithm] [**−b** keysize] [**−C**] [**−c** class] [**−D** date/offset] [**−d** bits] [**−D** sync date/offset] [**−E** engine] [**−f** flag] [**−G**] [**−g** generator] [**−h**] [**−I** date/offset] [**−i** interval] [**−K** directory] [**−k** policy] [**−L** ttl] [**−l** file] [**−n** nametype] [**−P** date/offset] [**−P** sync date/offset] [**−p** protocol] [**−q**] [**−R** date/offset] [**−S** key] [**−s** strength] [**−T** rrtype] [**−t** type] [**−V**] [**−v** level] {name}

DESCRIPTION

dnssec−keygen generates keys for DNSSEC (Secure DNS), as defined in **RFC 2535** <https://datatracker.ietf.org/doc/html/rfc2535.html> and **RFC 4034** <https://datatracker.ietf.org/doc/html/rfc4034.html>.

The **name** of the key is specified on the command line. For DNSSEC keys, this must match the name of the zone for which the key is being generated.

OPTIONS

−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 selected; for example, **dnssec−keygen −3 −a RSASHA1** specifies the NSEC3RSASHA1 (deprecated) algorithm.

−a algorithm

This option selects the cryptographic algorithm. For DNSSEC keys, the value of **algorithm** must be one of RSASHA1 (deprecated), NSEC3RSASHA1 deprecated), RSASHA256, RSASHA512, ECDSAP256SHA256, ECDSAP384SHA384, ED25519, or ED448. For TKEY, the value must be DH (Diffie−Hellman); specifying this value automatically sets the **−T KEY** option as well.

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, NSEC3RSASHA1 (deprecated) is used instead.

This parameter *must* be specified except when using the **−S** option, which copies the algorithm from the predecessor key.

In prior releases, HMAC algorithms could be generated for use as TSIG keys, but that feature was removed in BIND 9.13.0. Use **tsig−keygen** <#std-iscman-tsig-keygen> to generate TSIG keys.

−b keysize

This option specifies the number of bits in the key. The choice of key size depends on the algorithm used: RSA keys must be between 1024 and 4096 bits; Diffie−Hellman keys must be between 128 and 4096 bits. Elliptic curve algorithms do not need this parameter.

If the key size is not specified, some algorithms have pre−defined defaults. For example, RSA keys for use as DNSSEC zone−signing keys have a default size of 1024 bits; RSA keys for use as key−signing keys (KSKs, generated with **−f KSK**) default to 2048 bits.

−C This option enables compatibility mode, which generates an old−style key, without any timing metadata. By default, **dnssec−keygen** 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.

−d bits This option specifies the key size in bits. For the algorithms RSASHA1, NSEC3RSASA1, RSASHA256, and RSASHA512 the key size must be between 1024 and 4096 bits; DH size is between 128 and 4096 bits. This option is ignored for algorithms ECDSAP256SHA256, ECDSAP384SHA384, ED25519, and ED448.

−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**).

−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**.

−g generator
This option indicates the generator to use if generating a Diffie−Hellman key. Allowed values are 2 and 5. If no generator is specified, a known prime from **RFC 2539** <https://datatracker.ietf.org/doc/html/rfc2539.html> is used if possible; otherwise the default is 2.

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

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

−k policy
This option creates keys for a specific **dnssec−policy**. If a policy uses multiple keys, **dnssec−keygen** generates multiple keys. This also creates a ".state" file to keep track of the key state.

This option creates keys according to the **dnssec−policy** configuration, hence it cannot be used at the same time as many of the other options that **dnssec−keygen** provides.

−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** is the same as leaving it unset.

−l file This option provides a configuration file that contains a **dnssec−policy** statement (matching the policy set with **−k**).

−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. The default is ZONE for DNSKEY generation.

−p protocol
This option sets the protocol value for the generated key, for use with **−T 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.

−q This option sets quiet mode, which suppresses unnecessary output, including progress indication. Without this option, when **dnssec−keygen** is run interactively to generate an RSA or DSA key pair, it prints a string of symbols to **stderr** indicating the progress of the key generation. A **.** indicates that a random number has been found which passed an initial sieve test; **+** means a number has passed a single round of the Miller−Rabin primality test; and a space ( ) means that the number has passed all the tests and is a satisfactory key.

−S key This option creates a new key which is an explicit successor to an existing key. The name, algorithm, size, and type of the key are set to match the existing key. 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.

−s strength
This option specifies the strength value of the key. The strength is a number between 0 and 15, and currently has no defined purpose in DNSSEC.

−T rrtype
This option specifies the resource record type to use for the key. **rrtype** must be either DNSKEY or KEY. The default is DNSKEY when using a DNSSEC algorithm, but it can be overridden to KEY for use with SIG(0).

−t type This option indicates the type of the key for use with **−T 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 This option prints version information.

−v level
This option sets the debugging level.

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**.

−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. If set, and **−P** is not set, the publication date is set to the activation date minus the prepublication interval.

−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 KEYS

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

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

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

The **.key** file contains a DNSKEY or KEY record. When a zone is being signed by **named** <# std-iscman-named> or **dnssec−signzone −S** <#cmdoption-dnssec-signzone-S>, DNSKEY records are included automatically. In other cases, the **.key** file can be inserted into a zone file manually or with an **$INCLUDE** statement.

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

EXAMPLE

To generate an ECDSAP256SHA256 zone−signing key for the zone **example.com**, issue the command:

dnssec−keygen −a ECDSAP256SHA256 example.com

The command prints a string of the form:

Kexample.com.+013+26160

In this example, **dnssec−keygen** creates the files **Kexample.com.+013+26160.key** and **Kexample.com.+013+26160.private**.

To generate a matching key−signing key, issue the command:

dnssec−keygen −a ECDSAP256SHA256 −f KSK example.com

SEE ALSO

dnssec−signzone(8) <#std-iscman-dnssec-signzone>, BIND 9 Administrator Reference Manual, **RFC 2539** <https://datatracker.ietf.org/doc/html/rfc2539.html>, **RFC 2845** <https://datatracker.ietf.org/doc/html/rfc2845.html>, **RFC 4034** <https://datatracker.ietf.org/doc/html/rfc4034.html>.

Author

Internet Systems Consortium

Copyright