NAME

dnssec-signzone − DNSSEC zone signing tool

SYNOPSIS

dnssec−signzone [**−a**] [**−c** class] [**−d** directory] [**−D**] [**−E** engine] [**−e** end−time] [**−f** output−file] [**−g**] [**−h**] [**−i** interval] [**−I** input−format] [**−j** jitter] [**−K** directory] [**−k** key] [**−L** serial] [**−M** maxttl] [**−N** soa−serial−format] [**−o** origin] [**−O** output−format] [**−P**] [**−Q**] [**−q**] [**−R**] [**−S**] [**−s** start−time] [**−T** ttl] [**−t**] [**−u**] [**−v** level] [**−V**] [**−X** extended end−time] [**−x**] [**−z**] [**−3** salt] [**−H** iterations] [**−A**] {zonefile} [key...]

DESCRIPTION

dnssec−signzone signs a zone; it generates NSEC and RRSIG records and produces a signed version of the zone. The security status of delegations from the signed zone (that is, whether the child zones are secure) is determined by the presence or absence of a **keyset** file for each child zone.

OPTIONS

−a This option verifies all generated signatures.

−c class

This option specifies the DNS class of the zone.

−C This option sets compatibility mode, in which a **keyset−zonename** file is generated in addition to **dsset−zonename** when signing a zone, for use by older versions of **dnssec−signzone**.

−d directory

This option indicates the directory where BIND 9 should look for **dsset−** or **keyset−** files.

−D This option indicates that only those record types automatically managed by **dnssec−signzone**, i.e., RRSIG, NSEC, NSEC3 and NSEC3PARAM records, should be included in the output. If smart signing (**−S**) is used, DNSKEY records are also included. The resulting file can be included in the original zone file with **$INCLUDE**. This option cannot be combined with **−O raw** or serial−number updating.

−E engine

This option specifies the hardware to use for cryptographic operations, such as a secure key store used for signing, 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**).

−g This option indicates that DS records for child zones should be generated from a **dsset−** or **keyset−** file. Existing DS records are removed.

−K directory

This option specifies the directory to search for DNSSEC keys. If not specified, it defaults to the current directory.

−k key This option tells BIND 9 to treat the specified key as a key−signing key, ignoring any key flags. This option may be specified multiple times.

−M maxttl

This option sets the maximum TTL for the signed zone. Any TTL higher than **maxttl** in the input zone is reduced to **maxttl** in the output. This provides certainty as to the largest possible TTL in the signed zone, which is useful to know when rolling keys. The maxttl is the longest possible time before signatures that have been retrieved by resolvers expire from resolver caches. Zones that are signed with this option should be configured to use a matching **max−zone−ttl** in **named.conf** <# std-iscman-named.conf>. (Note: This option is incompatible with **−D**, because it modifies non−DNSSEC data in the output zone.)

−s start−time

This option specifies the date and time when the generated RRSIG records become valid. This can be either an absolute or relative time. An absolute start time is indicated by a number in YYYYMMDDHHMMSS notation; 20000530144500 denotes 14:45:00 UTC on May 30th, 2000. A relative

start time is indicated by **+N**, which is N seconds from the current time. If no **start−time** is specified, the current time minus 1 hour (to allow for clock skew) is used.

−e end−time

This option specifies the date and time when the generated RRSIG records expire. As with **start−time**, an absolute time is indicated in YYYYMMDDHHMMSS notation. A time relative to the start time is indicated with **+N**, which is N seconds from the start time. A time relative to the current time is indicated with **now+N**. If no **end−time** is specified, 30 days from the start time is the default. **end−time** must be later than **start−time**.

−X extended end−time

This option specifies the date and time when the generated RRSIG records for the DNSKEY RRset expire. This is to be used in cases when the DNSKEY signatures need to persist longer than signatures on other records; e.g., when the private component of the KSK is kept offline and the KSK signature is to be refreshed manually.

As with **end−time**, an absolute time is indicated in YYYYMMDDHHMMSS notation. A time relative to the start time is indicated with **+N**, which is N seconds from the start time. A time relative to the current time is indicated with **now+N**. If no **extended end−time** is specified, the value of **end−time** is used as the default. (**end−time**, in turn, defaults to 30 days from the start time.) **extended end−time** must be later than **start−time**.

−f output−file

This option indicates the name of the output file containing the signed zone. The default is to append **.signed** to the input filename. If **output−file** is set to **−**, then the signed zone is written to the standard output, with a default output format of **full**.

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

−V This option prints version information.

−i interval

This option indicates that, when a previously signed zone is passed as input, records may be re−signed. The **interval** option specifies the cycle interval as an offset from the current time, in seconds. If a RRSIG record expires after the cycle interval, it is retained; otherwise, it is considered to be expiring soon and it is replaced.

The default cycle interval is one quarter of the difference between the signature end and start times. So if neither **end−time** nor **start−time** is specified, **dnssec−signzone** generates signatures that are valid for 30 days, with a cycle interval of 7.5 days. Therefore, if any existing RRSIG records are due to expire in less than 7.5 days, they are replaced.

Note that the calculation of cycle interval is based upon the validity period of the replacement signatures that would be generated by **dnssec−signzone**, not on the valid lifetimes of the input RRSIGs being considered for pre−expiry replacement.

−I input−format

This option sets the format of the input zone file. Possible formats are **text** (the default), and **raw**. This option is primarily intended to be used for dynamic signed zones, so that the dumped zone file in a non−text format containing updates can be signed directly. This option is not useful for non−dynamic zones.

−j jitter

When signing a zone with a fixed signature lifetime, all RRSIG records issued at the time of signing expire simultaneously. If the zone is incrementally signed, i.e., a previously signed zone is passed as input to the signer, all expired signatures must be regenerated at approximately the same time. The **jitter** option specifies a jitter window that is used to randomize the signature expire time, thus spreading incremental signature regeneration over time.

Signature lifetime jitter also, to some extent, benefits validators and servers by spreading out cache expiration, i.e., if large numbers of RRSIGs do not expire at the same time from all caches, there is less congestion than if all validators need to refetch at around the same time.

−L serial
When writing a signed zone to "raw" format, this option sets the "source serial" value in the header to the specified **serial** number. (This is expected to be used primarily for testing purposes.)

−n ncpus
This option specifies the number of threads to use. By default, one thread is started for each detected CPU.

−N soa−serial−format
This option sets the SOA serial number format of the signed zone. Possible formats are **keep** (the default), **increment**, **unixtime**, and **date**.

keep This format indicates that the SOA serial number should not be modified.

increment
This format increments the SOA serial number using **RFC 1982** <https://datatracker.ietf.org/doc/html/rfc1982.html> arithmetic.

unixtime
This format sets the SOA serial number to the number of seconds since the beginning of the Unix epoch, unless the serial number is already greater than or equal to that value, in which case it is simply incremented by one.

date This format sets the SOA serial number to today's date, in YYYYMMDDNN format, unless the serial number is already greater than or equal to that value, in which case it is simply incremented by one.

−o origin
This option sets the zone origin. If not specified, the name of the zone file is assumed to be the origin.

−O output−format
This option sets the format of the output file containing the signed zone. Possible formats are **text** (the default), which is the standard textual representation of the zone; **full**, which is text output in a format suitable for processing by external scripts; and **raw** and **raw=N**, which store the zone in binary formats for rapid loading by **named** <#std-iscman-named>. **raw=N** specifies the format version of the raw zone file: if N is 0, the raw file can be read by any version of **named** <#std-iscman-named>; if N is 1, the file can be read by release 9.9.0 or higher. The default is 1.

−P This option disables post−sign verification tests.

The post−sign verification tests ensure that for each algorithm in use there is at least one non−revoked self−signed KSK key, that all revoked KSK keys are self−signed, and that all records in the zone are signed by the algorithm. This option skips these tests.

−Q This option removes signatures from keys that are no longer active.

Normally, when a previously signed zone is passed as input to the signer, and a DNSKEY record has been removed and replaced with a new one, signatures from the old key that are still within their validity period are retained. This allows the zone to continue to validate with cached copies of the old DNSKEY RRset. The **−Q** option forces **dnssec−signzone** to remove signatures from keys that are no longer active. This enables ZSK rollover using the procedure described in **RFC 6781 Section 4.1.1.1** <https://datatracker.ietf.org/doc/html/rfc6781.html#section-4.1.1.1> ("Pre−Publish Zone Signing Key Rollover").

−q This option enables quiet mode, which suppresses unnecessary output. Without this option, when **dnssec−signzone** is run it prints three pieces of information to standard output: the number of keys in use; the algorithms used to verify the zone was signed correctly and other status information;

and the filename containing the signed zone. With the option that output is suppressed, leaving only the filename.

−R This option removes signatures from keys that are no longer published.

This option is similar to **−Q**, except it forces **dnssec−signzone** to remove signatures from keys that are no longer published. This enables ZSK rollover using the procedure described in **RFC 6781 Section 4.1.1.2** <https://datatracker.ietf.org/doc/html/rfc6781.html#section-4.1.1.2> ("Double Signature Zone Signing Key Rollover").

−S This option enables smart signing, which instructs **dnssec−signzone** to search the key repository for keys that match the zone being signed, and to include them in the zone if appropriate.

When a key is found, its timing metadata is examined to determine how it should be used, according to the following rules. Each successive rule takes priority over the prior ones:

If no timing metadata has been set for the key, the key is published in the zone and used to sign the zone.

If the key's publication date is set and is in the past, the key is published in the zone.

If the key's activation date is set and is in the past, the key is published (regardless of publication date) and used to sign the zone.

If the key's revocation date is set and is in the past, and the key is published, then the key is revoked, and the revoked key is used to sign the zone.

If either the key's unpublication or deletion date is set and in the past, the key is NOT published or used to sign the zone, regardless of any other metadata.

If the key's sync publication date is set and is in the past, synchronization records (type CDS and/or CDNSKEY) are created.

If the key's sync deletion date is set and is in the past, synchronization records (type CDS and/or CDNSKEY) are removed.

−T ttl This option specifies a TTL to be used for new DNSKEY records imported into the zone from the key repository. If not specified, the default is the TTL value from the zone's SOA record. This option is ignored when signing without **−S**, since DNSKEY records are not imported from the key repository in that case. It is also ignored if there are any pre−existing DNSKEY records at the zone apex, in which case new records' TTL values are set to match them, or if any of the imported DNSKEY records had a default TTL value. In the event of a conflict between TTL values in imported keys, the shortest one is used.

−t This option prints statistics at completion.

−u This option updates the NSEC/NSEC3 chain when re−signing a previously signed zone. With this option, a zone signed with NSEC can be switched to NSEC3, or a zone signed with NSEC3 can be switched to NSEC or to NSEC3 with different parameters. Without this option, **dnssec−signzone** retains the existing chain when re−signing.

−v level

This option sets the debugging level.

−x This option indicates that BIND 9 should only sign the DNSKEY, CDNSKEY, and CDS RRsets with key−signing keys, and should omit signatures from zone−signing keys. (This is similar to the **dnssec−dnskey−kskonly yes;** zone option in **named** <#std-iscman-named>.)

−z This option indicates that BIND 9 should ignore the KSK flag on keys when determining what to sign. This causes KSK−flagged keys to sign all records, not just the DNSKEY RRset. (This is similar to the **update−check−ksk no;** zone option in **named** <#std-iscman-named>.)

−3 salt This option generates an NSEC3 chain with the given hex−encoded salt. A dash (−) can be used to indicate that no salt is to be used when generating the NSEC3 chain.

Note:
−3 − is the recommended configuration. Adding salt provides no practical benefits. See **RFC 9276** <https://datatracker.ietf.org/doc/html/rfc9276.html>.

−H iterations
This option indicates that, when generating an NSEC3 chain, BIND 9 should use this many iterations. The default is 0.

Warning:
Values greater than 0 cause interoperability issues and also increase the risk of CPU−exhausting DoS attacks. See **RFC 9276** <https://datatracker.ietf.org/doc/html/rfc9276.html>.

−A This option indicates that, when generating an NSEC3 chain, BIND 9 should set the OPTOUT flag on all NSEC3 records and should not generate NSEC3 records for insecure delegations.

Warning:
Do not use this option unless all its implications are fully understood. This option is intended only for extremely large zones (comparable to **com.**) with sparse secure delegations. See**RFC 9276** <https://datatracker.ietf.org/doc/html/rfc9276.html>.

−AA This option turns the OPTOUT flag off for all records. This is useful when using the **−u** option to modify an NSEC3 chain which previously had OPTOUT set.

zonefile
This option sets the file containing the zone to be signed.

key This option specifies which keys should be used to sign the zone. If no keys are specified, the zone is examined for DNSKEY records at the zone apex. If these records are found and there are matching private keys in the current directory, they are used for signing.

EXAMPLE

The following command signs the **example.com** zone with the ECDSAP256SHA256 key generated by **dnssec−keygen** <#std-iscman-dnssec-keygen> (Kexample.com.+013+17247). Because the **−S** option is not being used, the zone's keys must be in the master file (**db.example.com**). This invocation looks for **dsset** files in the current directory, so that DS records can be imported from them (**−g**).

```
% dnssec−signzone −g −o example.com db.example.com \
Kexample.com.+013+17247
db.example.com.signed
%
```

In the above example, **dnssec−signzone** creates the file **db.example.com.signed**. This file should be referenced in a zone statement in the **named.conf** <#std-iscman-named.conf> file.

This example re−signs a previously signed zone with default parameters. The private keys are assumed to be in the current directory.

```
% cp db.example.com.signed db.example.com
% dnssec−signzone −o example.com db.example.com
db.example.com.signed
%
```

SEE ALSO

dnssec−keygen(8) <#std-iscman-dnssec-keygen>, BIND 9 Administrator Reference Manual, **RFC 4033** <https://datatracker.ietf.org/doc/html/rfc4033.html>, **RFC 6781** <https://datatracker.ietf.org/doc/html/rfc6781.html>.

Author

Internet Systems Consortium

Copyright