NAME

dnssec-dsfromkey − DNSSEC DS RR generation tool

SYNOPSIS

dnssec−dsfromkey [**−1** | **−2** | **−a** alg] [**−C**] [**−T** TTL] [**−v** level] [**−K** directory] {keyfile}

dnssec−dsfromkey [**−1** | **−2** | **−a** alg] [**−C**] [**−T** TTL] [**−v** level] [**−c** class] [**−A**] {**−f** file} [dnsname]

dnssec−dsfromkey [**−1** | **−2** | **−a** alg] [**−C**] [**−T** TTL] [**−v** level] [**−c** class] [**−K** directory] {**−s**} {dnsname}

dnssec−dsfromkey [**−h** | **−V**]

DESCRIPTION

The **dnssec−dsfromkey** command outputs DS (Delegation Signer) resource records (RRs), or CDS (Child DS) RRs with the **−C** option.

By default, only KSKs are converted (keys with flags = 257). The **−A** option includes ZSKs (flags = 256). Revoked keys are never included.

The input keys can be specified in a number of ways:

By default, **dnssec−dsfromkey** reads a key file named in the format **Knnnn.+aaa+iiiii.key**, as generated by **dnssec−keygen** <#std-iscman-dnssec-keygen>.

With the **−f file** option, **dnssec−dsfromkey** reads keys from a zone file or partial zone file (which can contain just the DNSKEY records).

With the **−s** option, **dnssec−dsfromkey** reads a **keyset−** file, as generated by **dnssec−keygen** <# std-iscman-dnssec-keygen> **−C**.

OPTIONS

−1 This option is an abbreviation for **−a SHA1**. This digest is deprecated.

−2 This option is an abbreviation for **−a SHA−256**.

−a algorithm

This option specifies a digest algorithm to use when converting DNSKEY records to DS records. This option can be repeated, so that multiple DS records are created for each DNSKEY record.

The algorithm must be one of SHA−1 (deprecated), SHA−256, or SHA−384. These values are case−insensitive, and the hyphen may be omitted. If no algorithm is specified, the default is SHA−256.

−A This option indicates that ZSKs are to be included when generating DS records. Without this option, only keys which have the KSK flag set are converted to DS records and printed. This option is only useful in **−f** zone file mode.

−c class

This option specifies the DNS class; the default is IN. This option is only useful in **−s** keyset or **−f** zone file mode.

−C This option generates CDS records rather than DS records.

−f file This option sets zone file mode, in which the final dnsname argument of **dnssec−dsfromkey** is the DNS domain name of a zone whose master file can be read from **file**. If the zone name is the same as **file**, then it may be omitted.

If **file** is **−**, then the zone data is read from the standard input. This makes it possible to use the output of the **dig** <#std-iscman-dig> command as input, as in:

dig dnskey example.com | dnssec−dsfromkey −f − example.com

−h This option prints usage information.

−K directory
This option tells BIND 9 to look for key files or **keyset−** files in **directory**.

−s This option enables keyset mode, in which the final dnsname argument from **dnssec−dsfromkey** is the DNS domain name used to locate a **keyset−** file.

−T TTL
This option specifies the TTL of the DS records. By default the TTL is omitted.

−v level
This option sets the debugging level.

−V This option prints version information.

EXAMPLE

To build the SHA−256 DS RR from the **Kexample.com.+003+26160** keyfile, issue the following command:

dnssec−dsfromkey −2 Kexample.com.+003+26160

The command returns something similar to:

example.com. IN DS 26160 5 2 3A1EADA7A74B8D0BA86726B0C227AA85AB8BBD2B2004F41A868A54F0C5EA0B94

FILES

The keyfile can be designated by the key identification **Knnnn.+aaa+iiiii** or the full file name **Knnnn.+aaa+iiiii.key**, as generated by **dnssec−keygen** <#std-iscman-dnssec-keygen>.

The keyset file name is built from the **directory**, the string **keyset−**, and the **dnsname**.

CAVEAT

A keyfile error may return "file not found," even if the file exists.

SEE ALSO

dnssec−keygen(8) <#std-iscman-dnssec-keygen>, **dnssec−signzone(8)** <#std-iscman-dnssec-signzone>, BIND 9 Administrator Reference Manual, **RFC 3658** <https://datatracker.ietf.org/doc/html/rfc3658.html> (DS RRs), **RFC 4509** <https://datatracker.ietf.org/doc/html/rfc4509.html> (SHA−256 for DS RRs), **RFC 6605** <https://datatracker.ietf.org/doc/html/rfc6605.html> (SHA−384 for DS RRs), **RFC 7344** <https://datatracker.ietf.org/doc/html/rfc7344.html> (CDS and CDNSKEY RRs).

Author

Internet Systems Consortium

Copyright