NAME

dnssec-verify − DNSSEC zone verification tool

SYNOPSIS

dnssec−verify [**−c** class] [**−E** engine] [**−I** input−format] [**−o** origin] [**−q**] [**−v** level] [**−V**] [**−x**] [**−z**] {zone-file}

DESCRIPTION

dnssec−verify verifies that a zone is fully signed for each algorithm found in the DNSKEY RRset for the zone, and that the NSEC/NSEC3 chains are complete.

OPTIONS

−c class

This option specifies the DNS class of the zone.

−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**).

−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 verified independently. This option is not useful for non−dynamic zones.

−o origin

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

−v level

This option sets the debugging level.

−V This option prints version information.

−q This option sets quiet mode, which suppresses output. Without this option, when **dnssec−verify** is run it prints to standard output the number of keys in use, the algorithms used to verify the zone was signed correctly, and other status information. With this option, all non−error output is suppressed, and only the exit code indicates success.

−x This option verifies only that the DNSKEY RRset is signed with key−signing keys. Without this flag, it is assumed that the DNSKEY RRset is signed by all active keys. When this flag is set, it is not an error if the DNSKEY RRset is not signed by zone−signing keys. This corresponds to the **−x option in dnssec−signzone** <#cmdoption-dnssec-signzone-x>.

−z This option indicates that the KSK flag on the keys should be ignored when determining whether the zone is correctly signed. Without this flag, it is assumed that there is a non−revoked, self−signed DNSKEY with the KSK flag set for each algorithm, and that RRsets other than DNSKEY RRset are signed with a different DNSKEY without the KSK flag set.

With this flag set, BIND 9 only requires that for each algorithm, there be at least one non−revoked, self−signed DNSKEY, regardless of the KSK flag state, and that other RRsets be signed by a non−revoked key for the same algorithm that includes the self−signed key; the same key may be used for both purposes. This corresponds to the **−z option in dnssec−signzone** <# cmdoption-dnssec-signzone-z>.

zonefile

This option indicates the file containing the zone to be signed.

SEE ALSO

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

Author

Internet Systems Consortium

Copyright