Rocky Enterprise Linux 9.2 Manual Pages on command 'rpmsign.8'

$ man rpmsign.8

RPMSIGN(8)   RPMSIGN(8)

NAME

    rpmsign - RPM Package Signing

SYNOPSIS

  SIGNING PACKAGES:

    rpm --addsign|--resign [rpmsign-options] PACKAGE_FILE ...

    rpm --delsign PACKAGE_FILE ...

    rpm --delfilesign PACKAGE_FILE ...

  rpmsign-options

    [--rpmv3] [--fskpath KEY] [--signfiles]

DESCRIPTION

    Both of the --addsign and --resign options generate and insert new signatures for each

    package PACKAGE_FILE given, replacing any existing signatures. There are two options for

    historical reasons, there is no difference in behavior currently.

    To create a signature rpm needs to verify the package's checksum. As a result packages

    with a MD5/SHA1 checksums cannot be signed in FIPS mode.

    rpm --delsign PACKAGE_FILE ...

    Delete all signatures from each package PACKAGE_FILE given.

    rpm --delfilesign PACKAGE_FILE ...

    Delete all IMA and fsverity file signatures from each package PACKAGE_FILE given.

  SIGN OPTIONS

    --rpmv3

        Force RPM V3 header+payload signature addition. These are expensive and redundant

baggage on packages where a separate payload digest exists (packages built with rpm >= 4.14). Rpm will automatically detect the need for V3 signatures, but this op‐ tion can be used to force their creation if the packages must be fully signature verifiable with rpm < 4.14 or other interoperability reasons.

--fskpath KEY

Used with --signfiles, use file signing key Key.

--certpath CERT

Used with --signverity, use file signing certificate Cert.

--verityalgo ALG

Used with --signverity, to specify the signing algorithm. sha256 and sha512 are supported, with sha256 being the default if this argument is not specified. This can also be specified with the macro %_verity_algorithm

--signfiles

Sign package files. The macro %_binary_filedigest_algorithm must be set to a sup‐ ported algorithm before building the package. The supported algorithms are SHA1, SHA256, SHA384, and SHA512, which are represented as 2, 8, 9, and 10 respectively. The file signing key (RSA private key) must be set before signing the package, it can be configured on the command line with --fskpath or the macro %_file_sign‐ ing_key.

--signverity

Sign package files with fsverity signatures. The file signing key (RSA private key) and the signing certificate must be set before signing the package.   The key can be configured on the command line with --fskpath or the macro %_file_sign‐ ing_key, and the cert can be configured on the command line with --certpath or the macro %_file_signing_cert.

USING GPG TO SIGN PACKAGES

In order to sign packages using GPG, rpm must be configured to run GPG and be able to find a key ring with the appropriate keys. By default, rpm uses the same conventions as GPG to find key rings, namely the $GNUPGHOME environment variable. If your key rings are not lo‐ cated where GPG expects them to be, you will need to configure the macro %_gpg_path to be the location of the GPG key rings to use. If you want to be able to sign packages you create yourself, you also need to create your own public and secret key pair (see the GPG manual). You will also need to configure the rpm macros

%_gpg_name

      The name of the "user" whose key you wish to use to sign your packages.

For example, to be able to use GPG to sign packages as the user "John Doe <jdoe@foo.com>"

from the key rings located in /etc/rpm/.gpg using the executable /usr/bin/gpg you would

include

      %_gpg_path /etc/rpm/.gpg

      %_gpg_name John Doe <jdoe@foo.com>

      %__gpg /usr/bin/gpg

in a macro configuration file.   Use /etc/rpm/macros for per-system configuration and

~/.rpmmacros for per-user configuration. Typically it's sufficient to   set   just

%_gpg_name.

SEE ALSO

      popt(3),

      rpm(8),

      rpmdb(8),

      rpmkeys(8),

      rpm2cpio(8),

      rpmbuild(8),

      rpmspec(8),

rpmsign --help - as rpm supports customizing the options via popt aliases it's impossible

to guarantee that what's described in the manual matches what's available.

http://www.rpm.org/ <URL:http://www.rpm.org/>

AUTHORS

      Marc Ewing <marc@redhat.com>

      Jeff Johnson <jbj@redhat.com>

      Erik Troan <ewt@redhat.com>

      Panu Matilainen <pmatilai@redhat.com>

      Fionnuala Gunter <fin@linux.vnet.ibm.com>

      Jes Sorensen <jsorensen@fb.com>

                  Red Hat, Inc   RPMSIGN(8)