

**NAME**

rpmkeys – RPM Keyring

**SYNOPSIS**

**rpmkeys** {**--import**|**--checksig**}

**DESCRIPTION**

The general forms of rpm digital signature commands are

**rpmkeys --import** *PUBKEY* ...

**rpmkeys {-K|--checksig}** *PACKAGE\_FILE* ...

The **--checksig** option checks all the digests and signatures contained in *PACKAGE\_FILE* to ensure the integrity and origin of the package. Note that signatures are now verified whenever a package is read, and **--checksig** is useful to verify all of the digests and signatures associated with a package.

Digital signatures cannot be verified without a public key. An ASCII armored public key can be added to the **rpm** database using **--import**. An imported public key is carried in a header, and key ring management is performed exactly like package management. For example, all currently imported public keys can be displayed by:

**rpm -qa gpg-pubkey\***

Details about a specific public key, when imported, can be displayed by querying. Here's information about the Red Hat GPG/DSA key:

**rpm -qi gpg-pubkey-db42a60e**

Finally, public keys can be erased after importing just like packages. Here's how to remove the Red Hat GPG/DSA key

**rpm -e gpg-pubkey-db42a60e**

**SEE ALSO**

**popt**(3),  
**rpm**(8),  
**rpmdb**(8),  
**rpmsign**(8),  
**rpm2cpio**(8),  
**rpmbuild**(8),  
**rpmspec**(8),

**rpmkeys --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>