NAME

apt-key − Deprecated APT key management utility

SYNOPSIS

apt−key [**−−keyring** *filename*] {add *filename* | del *keyid* | export *keyid* | exportall | list | finger | adv | update | net−update | {−v | −−version} | {−h | −−help}}

DESCRIPTION

apt−key is used to manage the list of keys used by apt to authenticate packages. Packages which have been authenticated using these keys will be considered trusted.

Use of **apt−key** is deprecated, except for the use of **apt−key del** in maintainer scripts to remove existing keys from the main keyring. If such usage of **apt−key** is desired the additional installation of the GNU Privacy Guard suite (packaged in gnupg) is required.

apt−key(8) will last be available in Debian 11 and Ubuntu 22.04.

SUPPORTED KEYRING FILES

apt−key supports only the binary OpenPGP format (also known as "GPG key public ring") in files with the "gpg" extension, not the keybox database format introduced in newer **gpg**(1) versions as default for keyring files. Binary keyring files intended to be used with any apt version should therefore always be created with **gpg −−export**.

Alternatively, if all systems which should be using the created keyring have at least apt version >= 1.4 installed, you can use the ASCII armored format with the "asc" extension instead which can be created with **gpg −−armor −−export**.

COMMANDS

add *filename* (deprecated)
Add a new key to the list of trusted keys. The key is read from the filename given with the parameter *filename* or if the filename is − from standard input.

It is critical that keys added manually via **apt−key** are verified to belong to the owner of the repositories they claim to be for otherwise the **apt-secure**(8) infrastructure is completely undermined.

Note: Instead of using this command a keyring should be placed directly in the /etc/apt/trusted.gpg.d/ directory with a descriptive name and either "gpg" or "asc" as file extension.

del *keyid* (mostly deprecated)
Remove a key from the list of trusted keys.

export *keyid* (deprecated)
Output the key *keyid* to standard output.

exportall (deprecated)
Output all trusted keys to standard output.

list, **finger** (deprecated)
List trusted keys with fingerprints.

adv (deprecated)
Pass advanced options to gpg. With **adv −−recv−key** you can e.g. download key from keyservers directly into the trusted set of keys. Note that there are *no* checks performed, so it is easy to completely undermine the **apt-secure**(8) infrastructure if used without care.

update (deprecated)
Update the local keyring with the archive keyring and remove from the local keyring the archive keys which are no longer valid. The archive keyring is shipped in the archive−keyring package of your distribution, e.g. the ubuntu−keyring package in Ubuntu.

Note that a distribution does not need to and in fact should not use this command any longer and instead ship keyring files in the /etc/apt/trusted.gpg.d/ directory directly as this avoids a dependency on

gnupg and it is easier to manage keys by simply adding and removing files for maintainers and users alike.

net−update (deprecated)
Perform an update working similarly to the **update** command above, but get the archive keyring from a URI instead and validate it against a master key. This requires an installed **wget**(1) and an APT build configured to have a server to fetch from and a master keyring to validate. APT in Debian does not support this command, relying on **update** instead, but Ubuntu's APT does.

OPTIONS

Note that options need to be defined before the commands described in the previous section.

−−**keyring** *filename* (deprecated)
With this option it is possible to specify a particular keyring file the command should operate on. The default is that a command is executed on the trusted.gpg file as well as on all parts in the trusted.gpg.d directory, though trusted.gpg is the primary keyring which means that e.g. new keys are added to this one.

DEPRECATION

Except for using **apt−key del** in maintainer scripts, the use of **apt−key** is deprecated. This section shows how to replace existing use of **apt−key**.

If your existing use of **apt−key add** looks like this:

wget −qO− https://myrepo.example/myrepo.asc | sudo apt−key add −

Then you can directly replace this with (though note the recommendation below):

wget −qO− https://myrepo.example/myrepo.asc | sudo tee /etc/apt/trusted.gpg.d/myrepo.asc

Make sure to use the "asc" extension for ASCII armored keys and the "gpg" extension for the binary OpenPGP format (also known as "GPG key public ring"). The binary OpenPGP format works for all apt versions, while the ASCII armored format works for apt version >= 1.4.

Recommended: Instead of placing keys into the /etc/apt/trusted.gpg.d directory, you can place them anywhere on your filesystem by using the Signed−By option in your sources.list and pointing to the filename of the key. See **sources.list**(5) for details. Since APT 2.4, /etc/apt/keyrings is provided as the recommended location for keys not managed by packages. When using a deb822−style sources.list, and with apt version >= 2.4, the Signed−By option can also be used to include the full ASCII armored keyring directly in the sources.list without an additional file.

FILES

/etc/apt/trusted.gpg
Keyring of local trusted keys, new keys will be added here. Configuration Item: Dir::Etc::Trusted.

/etc/apt/trusted.gpg.d/
File fragments for the trusted keys, additional keyrings can be stored here (by other packages or the administrator). Configuration Item Dir::Etc::TrustedParts.

/etc/apt/keyrings/
Place to store additional keyrings to be used with Signed−By.

SEE ALSO

apt-get(8), **apt-secure**(8)

BUGS

APT bug page[1]. If you wish to report a bug in APT, please see /usr/share/doc/debian/bug−reporting.txt or the **reportbug**(1) command.

AUTHOR

APT was written by the APT team <apt@packages.debian.org>.

AUTHORS

Jason Gunthorpe

APT team

NOTES

1. APT bug page
   http://bugs.debian.org/src:apt