NAME
apt-key − 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.

Note that if usage of **apt−key** is desired the additional installation of the GNU Privacy Guard suite (packaged in gnupg) is required. For this reason alone the programmatic usage (especially in package maintainerscripts!) is strongly discouraged. Further more the output format of all commands is undefined and can and does change whenever the underlying commands change. **apt−key** will try to detect such usage and generates warnings on stderr in these cases.

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*

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*

Remove a key from the list of trusted keys.

export *keyid*

Output the key *keyid* to standard output.

exportall

Output all trusted keys to standard output.

list, **finger**

List trusted keys with fingerprints.

adv

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 debian−archive−keyring package in Debian.

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

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*

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.

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.

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