

APT - Keyrings

APT repository signing uses GPG keys to authenticate packages and repository metadata before installation. Modern Debian and Ubuntu systems prefer isolated, unarmored or armored keyring files coupled directly to individual .list or .sources configuration files rather than global legacy keyrings.

File/Directory Path	Status	Description
/etc/apt/keyrings/	Recommended	Standard directory for storing third-party repository GPG keys. Kept isolated per repository and explicitly referenced via the signed-by option in APT sources configuration files.
/etc/apt/trusted.gpg.d/	Legacy / Active	Directory containing fragment keyrings (or export files with extension .gpg or .asc). APT trusts all keys in this directory globally for any repository unless restricted.
/etc/apt/trusted.gpg	Deprecated	Legacy primary keyring file where apt-key add previously stored GPG keys. Deprecated because any key added here is trusted globally across every repository.
/usr/share/keyrings/	Standard	Directory managed by OS package manager (dpkg/apt) containing official system distribution signing keys (e.g., ubuntu-archive-keyring.gpg or debian-archive-keyring.gpg).
/etc/apt/sources.list	Active	Main system configuration file for APT software repositories. Accepts signed-by=/path/to/key.gpg directives inline to pin a key to a specific repository line.
/etc/apt/sources.list.d/	Active	Directory containing modular repository source configuration files (.list or .sources). Frequently pairs with custom keyrings stored under /etc/apt/keyrings/.
Repository server: InRelease	Remote File	Combined repository index file containing package hashes and an inline GPG signature created by the repository maintainers.
Repository server: Release	Remote File	Repository metadata index listing package file hashes. Used alongside Release.gpg for verification.
Repository server: Release.gpg	Remote File	Detached GPG signature file used to authenticate an unsigned Release file.

- Storing repository signing keys in global keyrings creates a serious security risk because any key added to /etc/apt/trusted.gpg or /etc/apt/trusted.gpg.d/ can authenticate packages from any repository on the system, not just the one it was intended for.
- Modern APT security requires storing keys as individual files in /etc/apt/keyrings and explicitly linking them to their repositories using the signed-by option, ensuring each key can only authenticate its designated repository.
- ASCII-armored PGP keys must be converted to binary GPG keyring format using `gpg --dearmor` before APT can use them, as APT only accepts keys in binary .gpg format for repository authentication.
- Every modern repository configuration must include the signed-by=/etc/apt/keyrings/<keyring>.gpg parameter in its definition, otherwise APT cannot determine which key to use and will fail to authenticate the repository.
- Repository entries can be managed in three equivalent ways: adding lines directly to /etc/apt/sources.list, creating separate .list files in /etc/apt/sources.list.d/, or using the structured deb822 format in .sources files.

- Understanding directory purposes is critical: `/etc/apt/keyrings` stores administrator-managed keys, `/usr/share/keyrings` contains package-managed keys, and `/etc/apt/trusted.gpg.d/` represents the deprecated legacy approach that should be avoided.
- While keys can be retrieved from key servers using `gpg --recv-keys`, downloading them directly via HTTPS is more reliable and avoids potential issues with slow, unreliable, or blocked key servers, though both methods work with scoped keyrings.

From:

<https://wiki.oscardegroot.nl/> - HomeWiki

Permanent link:

<https://wiki.oscardegroot.nl/doku.php?id=linux:debian:apt-keyrings&rev=1788549765>

Last update: **2026/09/04 19:22**

