

Packages - Feature Request #3347

[archlinux-keyring][archlinux32-keyring][archlinuxarm-keyring]: various problem for parabola

2022-09-24 11:53 AM - bill-auger

<div>Status:open</div> <div>Priority:feature</div> <div>Assignee:</div> <div>Category:</div>	<div>% Done:0%</div>
<div>Description</div> <div>archlinux32-keyring and archlinuxarm-keyring are already on the blacklist with no BR reference; so this ticket serves that purpose, at least</div> <div>the original reason was [technical], mainly to avoid sync-ing it during the normal db-import (and possibly to make them available to all arches? - not sure if that is an implicit part of the db-import procedure)</div> <div>the replacement PKGBUILD has no "# parabola changes and rationale:" specified either; so i will explain for documentation</div> <div>Blacklisted to avoid import by db-import-pkg; import separately with db-import-keyring</div> <div>furthermore, since that time, both of those keyrings, and now archlinux-keyring as well, have been problematic in "bug-like" ways - 'db-import-keyring' only does "what it says on the tin" - it could not ensure that anyone could actually install the package, and assumes that the packages are acceptable, as is - i have had to rebuild archlinuxarm-keyring once and archlinux32-keyring several times manually (just so that i could sign them myself); so i also decided to blacklist archlinux-keyring, and rebuild them all manually from now on, for the reasons given below:</div> <div>archlinux-keyring:</div> <div>recently added a systemd service, which imports updated keys from archlinux.org - some users complained that this was a privacy concern; so i looked into it - i had originally devised a ALPM hook to add via 'your-freedom', which neutralizes the service intrusively (by resetting the executable bit on the service exec target, IIRC)</div> <div>the feature itself is only useful when people forget to upgrade the system - no one should ever need to refresh-keys or import keys from any third party - arch is not exactly a third party; but still we try to maintain a standard, such that no parabola user should ever need to use a web browser, nor to contact any network server automatically, nor to contact any network server intentionally, other than those operated by the parabola project, or an endorsed upper-tier mirror - if maintainer's keys need updating, a new keyring package should be built, and they normally are - so this feature seems to be only compensating for, catering to, or otherwise encouraging a bad habit</div> <div>as we already blacklist the other keyrings, it seems reasonable to avoid the clumsy fix with a proper fix - such as, to remove the "timers wants" declaration from the service file; so that people could still enable it manually, but only if "i wants" (that a presumption, i have not tried it yet)</div> <div>digression: IMHO that is a rather pesky feature of systemd really - i tried to find some way to over-ride it (to avoid blacklisting the package, only so to change one LOC); but there does not appear to be a mechanism for it - any service which "wants" to be "wanted" by some other service, is dutifully invoked by that other service - services apparently has no mechanism to white-list or black-list collaborators - services simply invite (impose) themselves into the init routines of other services</div> <div>archlinux32-keyring:</div> <div>unless archlinux32-keyring and archlinuxarm-keyring are installed on every liveISO, and users install them during the initial pacstrap, they pose a chicken-and-egg problem for anyone who wants to install them later</div> <div>archlinux32-keyring has always been a PITA, generally (see <a href="#">#1527</a>) - even with 'archlinux32-keyring' installed, new keyring packages have routinely still had verification problems - the solution that isacdaavid and i devised at that time, was to make pacman for all arches depend on the keyrings of all arches; but the verification problems became a routine annoyance, blocking system upgrades for everyone - so recently, i adapted the pacman PKGBUILD to depend only on specific keyrings, per-arch</div> <div>archlinuxarm-keyring:</div> <div>in addition to the signature verification chicken-and-egg problem, archlinuxarm-keyring declares itself to be in the 'base-devel' group - as an 'any' package, which we include in the repo of all arches, that has the same drawback as it did when pacman required it - not unlike that systemd deal, packages simply invite (impose) themselves into standard configurations - meta-packages are clearly a</div>	

<p>better approach than package groups - nonetheless, we have them, and the only way to remove 'archlinuxarm-keyring' from the 'base-devel' group of all arches, is to re-package it</p> <p>maybe we could convince the upstream to remove that declaration - the keyrings requirement should be via pacman (as parabola's does); but for some reason archarm's pacman does not require any keyrings</p>	
<b>Related issues:</b>	
Related to Packages - Bug #1527: [archlinux32-keyring] invalid signature	<b>duplicate</b>

## History

### #1 - 2022-09-24 11:54 AM - bill-auger

- Description updated

### #2 - 2022-09-24 11:55 AM - bill-auger

- Related to Bug #1527: [archlinux32-keyring] invalid signature added

### #3 - 2022-09-24 12:03 PM - bill-auger

- Description updated

### #4 - 2022-09-24 12:45 PM - bill-auger

- Description updated