Packages - Bug #747

[RFC] PKGBUILDs should include SHA512 checksum + GPG signature

2015-06-23 03:09 AM - g4jc

Status:	open	**% Done:**	0%
Priority:	discussion		
Assignee:			
Category:			

Description

Gentoo is now using SHA512 + Whirpool and GPG signed source packages. I got the idea that this great security practice could be implemented in our PKGBUILD's as well and went to work to see if it was possible. Using just a few lines of bash, it is definitely possible.

Attached you will find a proof of concept PKGBUILD I made for a file integrity checking security software that is GPL.

This could be good practice for users of AUR/ABS, etc. where PKGBUILDs can be verified safe and untampered.

History

#1 - 2015-06-26 03:01 AM - g4jc

- File PKGBUILD.zip added

Per Emulatorman we should use .sig instead of armoured .asc to keep it uniform with currently signed packages.
I can confirm this also works as simply as...
gpg --default-key [KEYID] -b PKGBUILD

Attached is another example GPG-signed PKGBUILD of a recently requested package.

#2 - 2015-06-30 08:59 AM - Anonymous

g4jc wrote:

> Per Emulatorman we should use .sig instead of armoured .asc to keep it uniform with currently signed packages.
> I can confirm this also works as simply as...
> gpg --default-key [KEYID] -b PKGBUILD
>
> Attached is another example GPG-signed PKGBUILD of a recently requested package.

I suggest you open a consensus about it to devs list as official packaging policy for Parabola.

#3 - 2016-04-15 11:42 PM - lukeshu

- Priority changed from feature to discussion

- Subject changed from PKGBUILDs should include SHA512 checksum + GPG signature to [RFC] PKGBUILDs should include SHA512 checksum + GPG signature

#4 - 2017-01-21 12:29 AM - lukeshu

- Project changed from libretools to Packages

Files

PKGBUILD.zip	2.1 KB	2015-06-23	g4jc
PKGBUILD.zip	1.9 KB	2015-06-26	g4jc