QGIS Application - Bug report #11772
GPG: stop using 32-bit key ID

2014-12-01 06:30 AM - Patryk Sciborek

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Build/Install		
Affected QGIS version:	2.6.0	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	fixed/implemented
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	20001

Description

Hi!

I'd like to add QGIS Archive Automatic Signing Key (2014) to my keystore. Unfortunately there is no way to tell if key received from keyserver is correct because you use only 32-bit key ID (eg. http://www.qgis.org/en/site/forusers/alldownloads.html#debian).

Since you can generate collision in few seconds (see: https://evil32.com/) it would be much better if you use full key fingerprint or at least provide it somewhere so user can verify it manually.

Kind regards,
Patryk

History

#1 - 2015-08-19 10:09 AM - Jürgen Fischer

- Resolution set to fixed/implemented

- Status changed from Open to Closed

Fixed in a3fe6b1