Gpg4win/CheckIntegrity - GnuPG wiki

5-6 minutes

Check integrity of Gpg4win packages

You shall only run applications on your computer that you trust. This page shows several methods to check that the software called Gpg4win that you have just downloaded originates from the Gpg4win Initiative. **Using one method is good enough.**

Contents

Code Signing Certificate (recommended)

All Gpg4win installer files since April 2016 are code signed. Look at Gpg4win package integrity to see which is the name and the certificate of the publisher (for the date the package was signed). Windows can check the integrity and show the publisher of a signed software package. Compare this to what you have looked up.

Optional for some additional safety: compare the certificate of the publisher not just by name, but also by using the SHA256 hash checksum of the certificate (aka `sha2_fpr`). Some tools only display SHA1 to be compared with `sha1_fpr`, which is not as good as comparing SHA256, but still gives extra security over just comparing the name.

Method A: UAC (recommended)

When trying to run the installer on Windows, the **User Access Control dialog will show the publisher**. (If you have disabled User Access Control use a different method.)

Method B: file properties

A second way to show the publisher is to use the file properties in the explorer. Right click on the installer -> properties -> digital signatures -> Details of signatures. (Try this if no publisher is shown by the UAC in rare cases after a download with Firefox or Iridium (Chromium). For details see T3379.)

Method C: signtool

A third way if the previous methods do not work: use SignTool which is a part of the Microsoft development tools: Open open a command line, navigate to the folder and enter

```
SignTool verify /pa /v gpg4win*.exe
```

Now you should see which certificate signed the installer and you can compare the publisher.

Checksums

Once you have downloaded the file, you can verify that it matches the published checksums (that you have gotten via a trusted channel). Open a command line, navigate to your Download-Folder, and use a command like the following, but adapt the filename to the version you have downloaded and you want to check:

```
certutil -hashfile gpg4win-3.1.15.exe sha256
```

Once you have entered the command, it will return an alphanumeric string, which you can compare to the one on the Gpg4win package integrity site. It has to match for all hexadecimal digits. (Sometimes colons or spaces are used to group the checksum.) Make sure to compare it to the checksum with the right algorithm (SHA-256).

If the tool does not work

... see of you have a different tool that can calculate SHA-256 checksums on your machine and use it instead.

On systems that run older operating systems than Windows 8: Install a certain Windows Patch, which delivers the functionality.

Less reliable is falling back using `sha1` stead of the `sha256` in the above command line and comparing it to the SHA-1 checksum. Some elder versions of Windows may not come with a standard tool to calculate SHA-256 and we still publish SHA-1 checksums because checking against them is better than not checking with a cryptographic checksum.

OpenPGP signatures

If you upgrade your Gpg4win version, you already have gnupg installed and you can verify the integrity of the downloaded file, by its OpenPGP signature. To do so, you have to download, next the file, the signature of the file. You'll find the download-links on the Gpg4win package integrity site. The pubkey, with which the files are signed, is also given on that page. You have to import the public key and now you can validate the signature of the file with the command

```
gpg --verify gpg4win*.exe.sig gpg4win*.exe
```

File lengths (as diagnostics)

This is not a verification method, but I way trying to find out why a method my have failed. One cause of a bad download is that the internet connection broke down during the download. In this case the size of the file on your harddisk is smaller than it should be.

Navigate to the folder, where you downloaded the Gpg4win packages to, and enter

```
dir
```

The command will list all files and their sizes in the directory. You can then compare those results with the sizes given on the Gpg4win package integrity site.

This can help you spot a corrupt file where the downloading got aborted or something. It will not protect you against an attacker.

Troubleshooting

If you encounter any problems, please feel free to ask them at the forums or on the mailinglist. If you already figured out, how to fix your issue, please leave your answer here