File integrity check using hash value calculation

The integrity of files is an elementary component in the operation of secure applications. Only if it can be determined that a file is unchanged can its integrity be assumed.
By improperly modifying installation files, malicious code can be added, for example, which is installed in the event of execution. In this case, the original file is used solely as a transport medium. The predetermined installation of the application fails in most cases.

A simple way to determine the integrity of a file is to check the unique checksum. For this purpose, the provider of the file provides the original checksum. This is usually done directly on the website where the file is provided. If you receive the desired file, which does not necessarily have to be your own download, you can compare your own copy of the file with the checksum of the provider.

Microsoft PowerShell provides a simple way to perform a hash value calculation. By the command call:

```
Get-FileHash -Algorithm SHA256 -Path [Path to the desired file]
```

the checksum is calculated. This can then be compared directly with the information provided, e.g., in the ifm moneo|OS download area under file info.

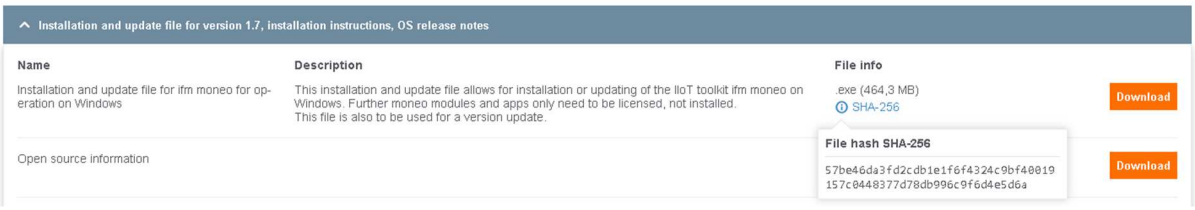
Example checksum calculation:

```
Get-FileHash -Algorithm SHA256 -Path C:\ifm_moneo_1.7.0.278713_QA.exe
```

```
PS C:\> Get-FileHash -Algorithm SHA256 -Path C:\ifm_moneo_1.7.0.278713_QA.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          57BE46DA3FD2CDB1E1F6F4324C9BF40019157C0448377D78DB996C9F6D4E5D6A       C:\ifm_moneo_1.7.0.278713_QA.exe
```

Calling the file information on the moneo|OS download page



If both HASH values are equal, it can be assumed that the checked file is in its original state.