Payment Services

Sofie - Activating TLS1.2 For Https Connexions

User Guide

Version of Document :	1.01
Status :	Draft
Release Date :	04/10/2018
Prepared by :	Six Payment Services
Recipients:	Users

1 Document Version Control

Date	Description of Change	Change done by	Version
12/09/2018	First version published	OL	1.0
04/10/2018	Upfate link to external document	OL	1.01

Summary of changes

Chapter	Description of Change
all	version 1.0
5	Update link to documentation

2 Contents

3 Introduction

3.1 Scope of this document

This document explains the changes induced by the deactivation of some methods used to establish a secure connection between the SOFiE client and the central SOFiE server.

3.2 Out of scope

This document does not explain how a secure connection between a client and a server is established.

3.3 Prerequisite

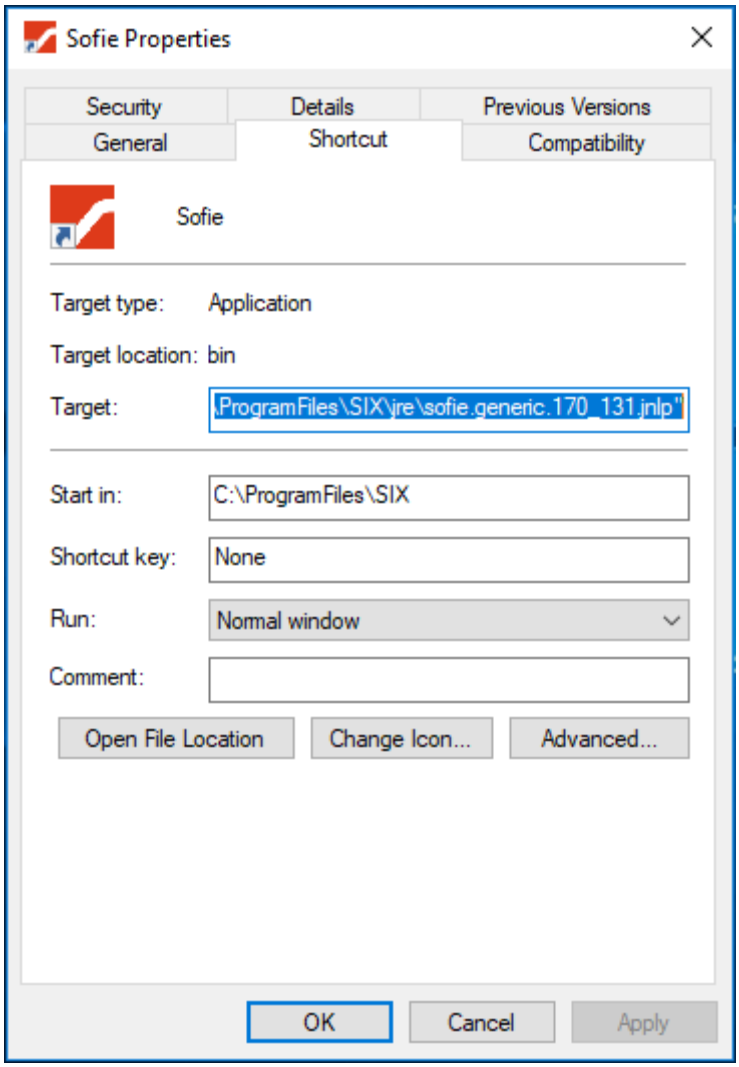
The reader of this document has basic computer knowledge, has an operational SOFiE client and has the knowledge and access required to modify the installation of this client and its configuration.

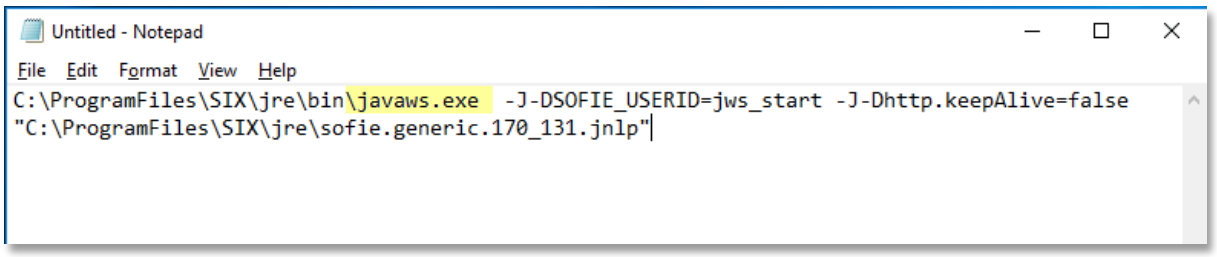
4 Determine what type of installation is used

To check what type of installation you are using to launch SOFiE, please check the method you are using to launch this program.

Right-click and choose the "Properties"

Copy the contents of the "Target" field to a text editor, such as e.g. Notepad.



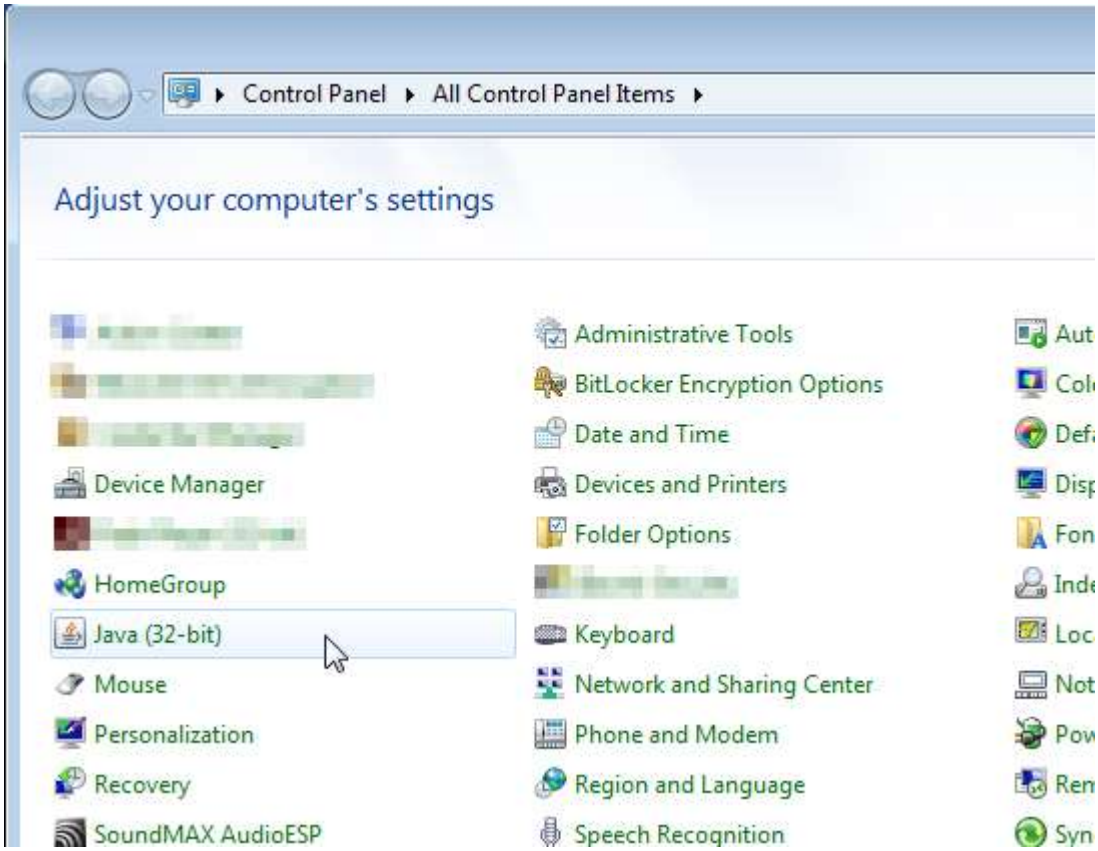


When the command launched is "javaws.exe", it means that you launch the SOFiE client via the "JavaWebStart" technology and that you must check that the configuration of your PC allows the use of the "TLS 1.2" protocol with your SOFiE installation. The procedure is explained in the chapter "Checking JavaWebStart's Configuration".

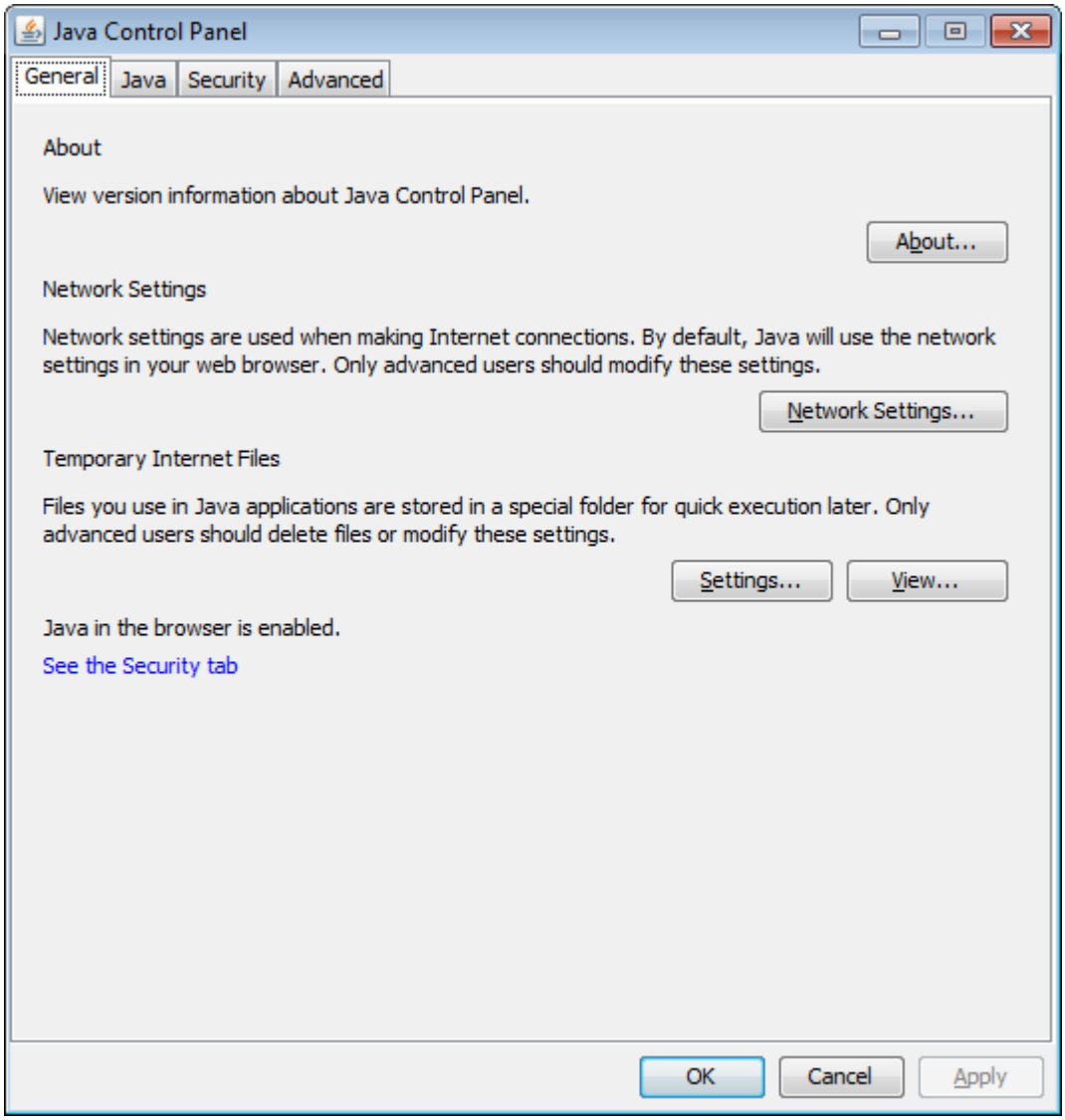
If it is another command, most likely one with a name ending with ".bat", please go to the chapter "Checking the configuration without JavaWebStart".

5 Checking JavaWebStart's Configuration

Open the Control Panel.

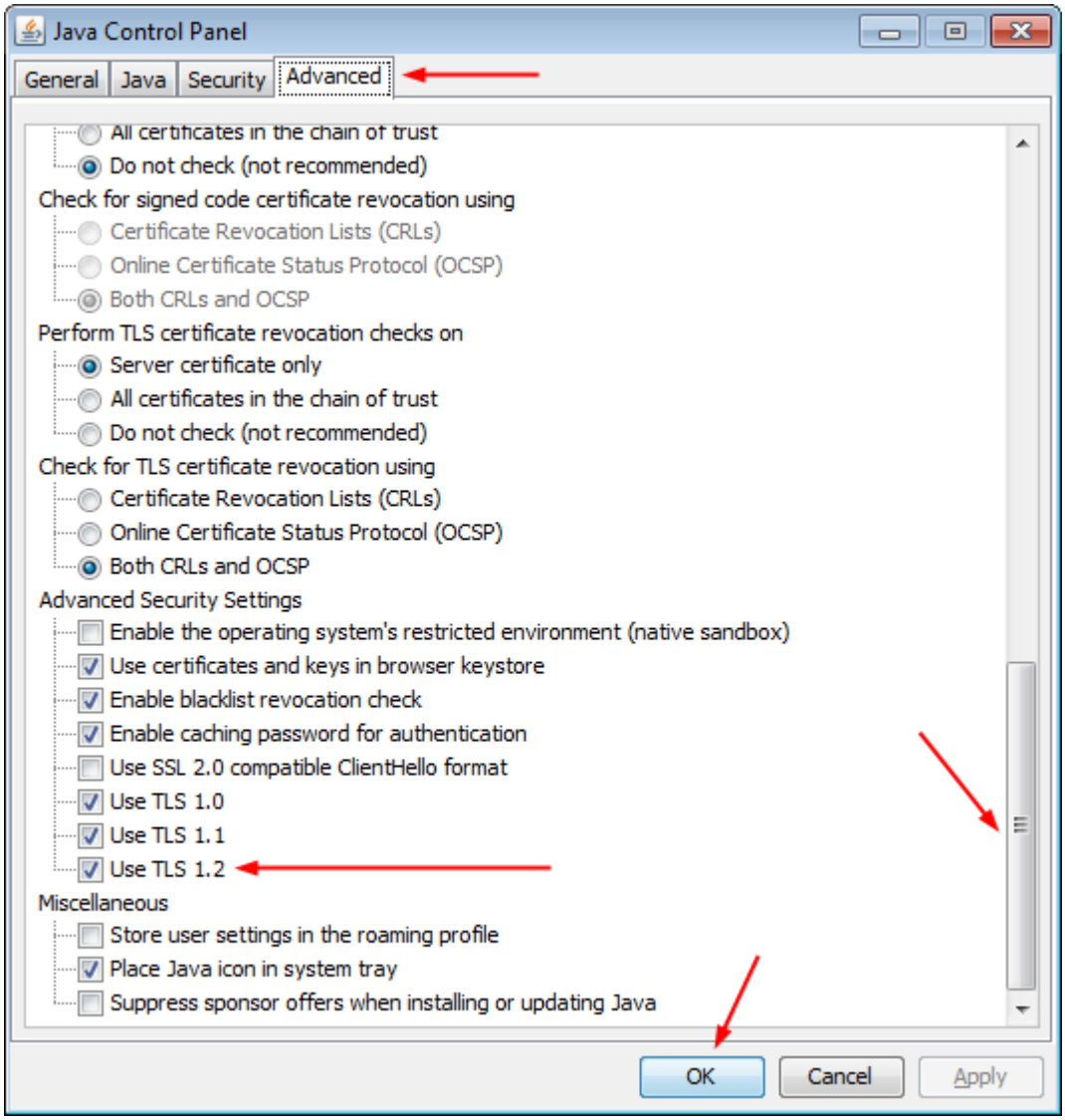


Launch the "Java" panel.



Select the "Advanced" tab and scroll down to the bottom of the list.

If the "Use TLS 1.2" option is not yet enabled, please change it’s status now.



Close this window by clicking on "OK"!

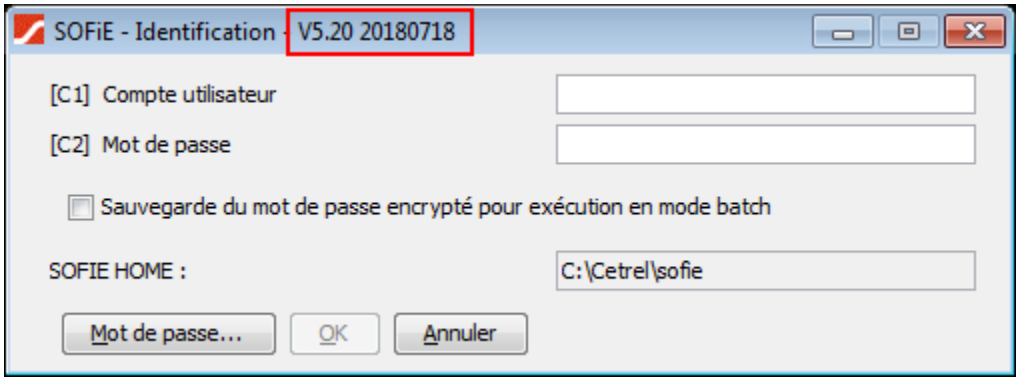
In order to ensure that you can send and receive files after December 1, 2018, please also update the SOFiE client and use at least version "5.21".

By default, the SOFiE application is configured to automatically update itself when it is launched. From September 19th, 2018, in the afternoon, your SOFiE identification screen, the main window, and the "Help - About" menu should display "V5.21.20180919". Otherwise, a manual update is described in the document "SOFiE Manual Update Procedure".

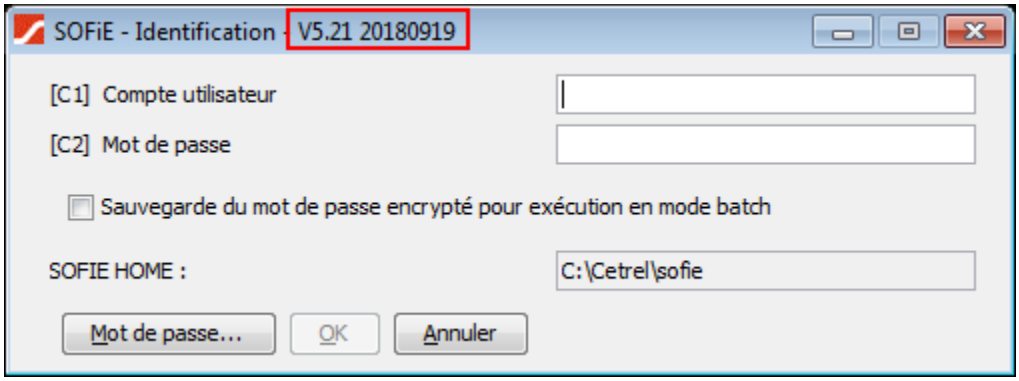
6 Checking the configuration without JavaWebStart

Verify that you are using version 5.21 or later of the SOFiE client. The version number is displayed on the authentication window (login).

Below is an example from a version prior to "5.21".

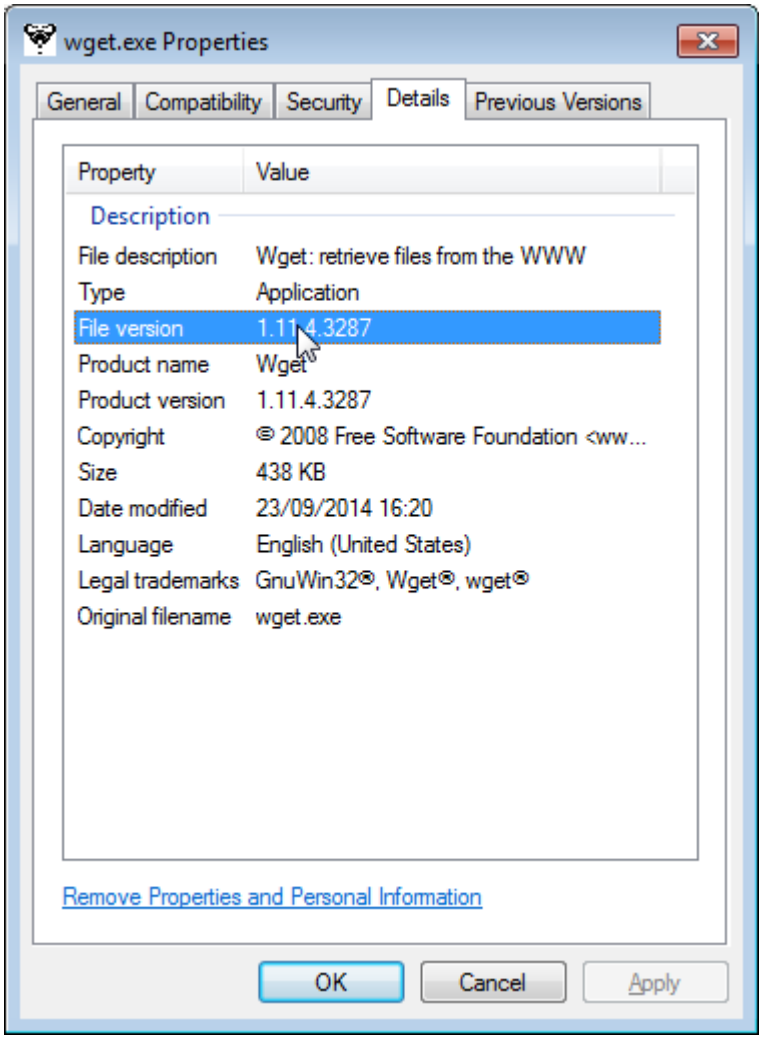


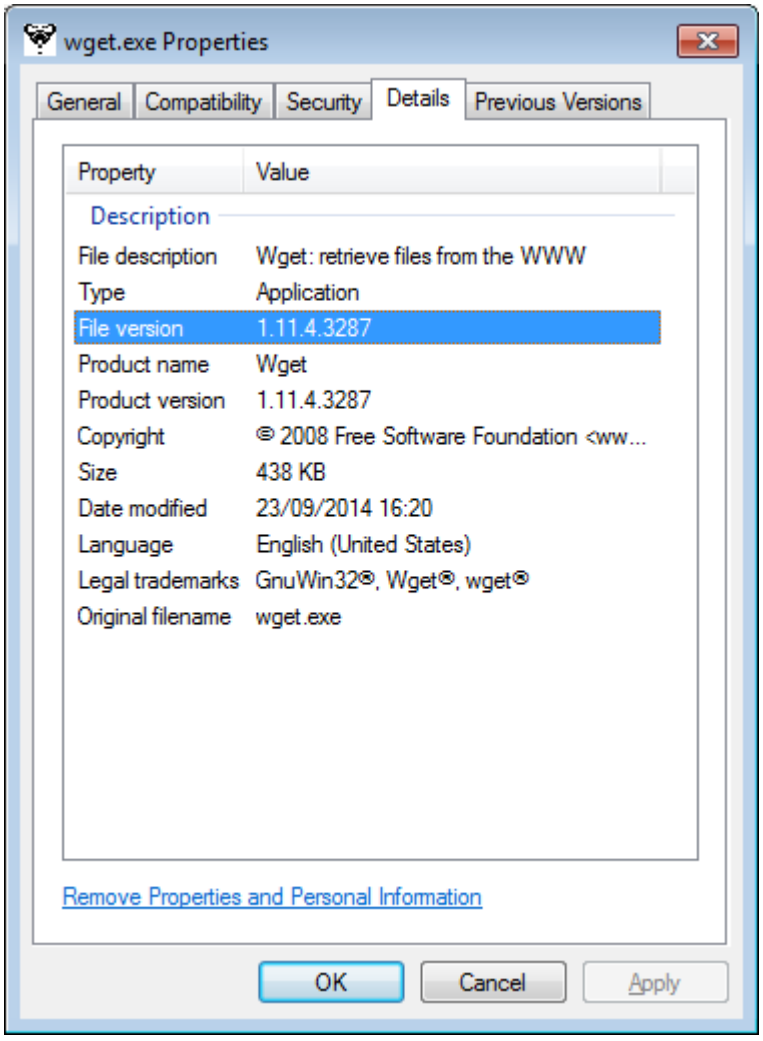
Below is an example from version "5.21", made available to users on September 19, 2018.



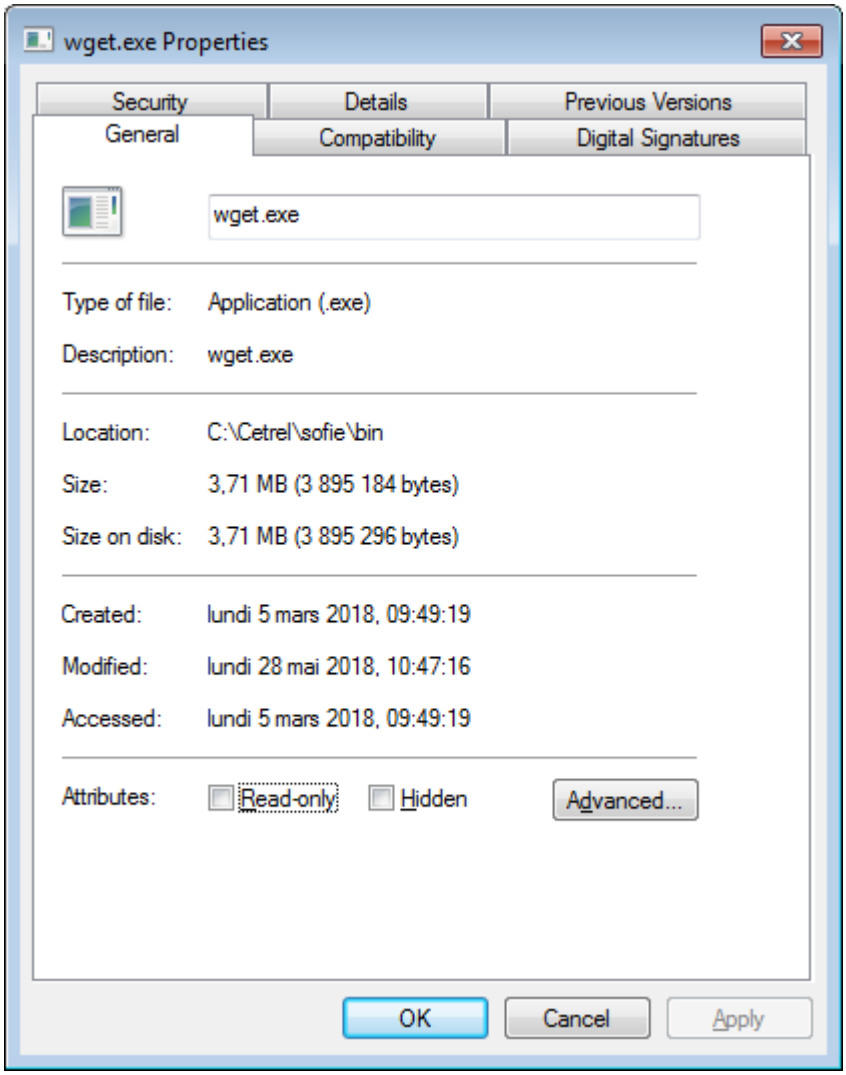
In these examples, the SOFiE profile is installed in the "C:\Cetrel\sofie" directory. After successfully authenticating yourself at least once using version 5.21, you can check that the file "wget.exe" under "C:\Cetrel\sofie\bin\" has been updated and has the same properties as the example below

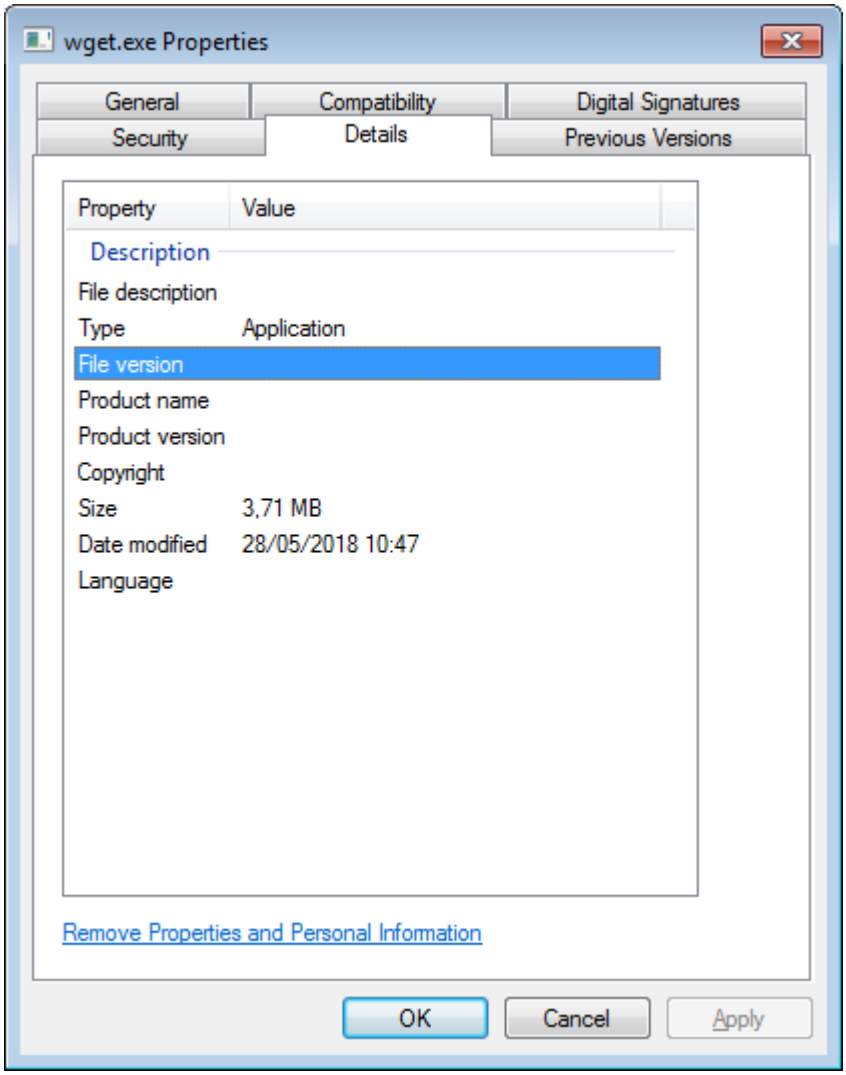
Below, the properties of the version that **does not support** the TLS1.2 protocol:

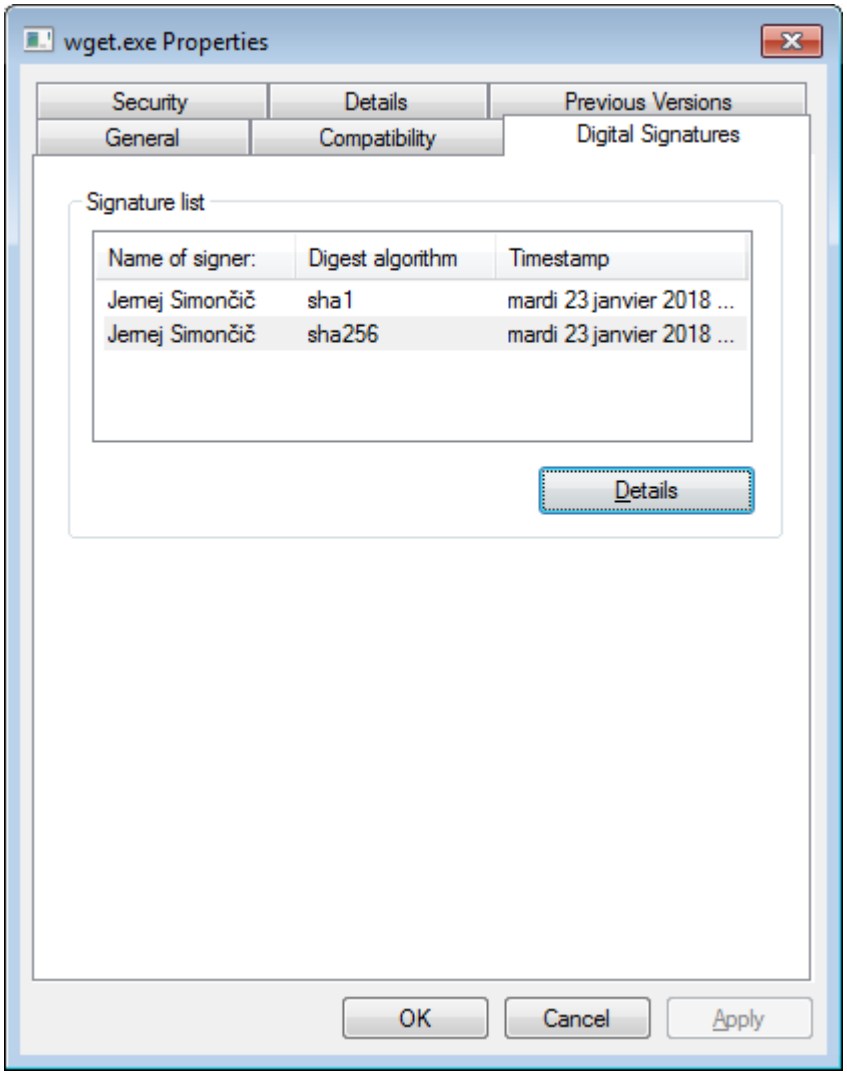




Next, the version supporting TLS1.2 :







If you have this version of "wget.exe" and your computer has Internet access, SOFiE client updates should continue to be installed automatically.

If this is not the case, you must:

Check that the account you use to connect to this computer has the right to modify this file.

That this file is not write-protected

In any case, contact your IT department for more information and help.

7 7 FAQS

7.1 Why TLS1.2?

IT is evolving every day. What was still at the top of technology yesterday may be seen as obsolete tomorrow. The same applies to the protocols used and they must be stopped before the new, ever more powerful computers can decrypt the data in a reasonable amount of time without the need for private keys. Another reason may be the discovery of flaws in the protocol itself.

7.2 What if the SOFiE client has not been updated before the deactivation date of protocols below TLS1.2?

If you launch the SOFiE client via JavaWebStart, automatic updates should be possible because this tool supports the "TLS1.2" protocol. If you do not use JavaWebStart, then the "wget" command may not be up to date and the update will not be done automatically when SOFiE is launched.

In both cases, a manual update is required. The programs and archives for installing the SOFiE client are available on the SIX-Payment-Services website.

SOFiE main page

7.3 Should the SOFiE certificate be renewed or replaced?

Updating the protocols used for communication between SOFiE clients and the central SOFiE server has no influence on the SOFiE certificate used.

You can continue to use this certificate as usual and renew it only if its expiry date is near.

7.4 Does the use of TLS protocols below version 1.2 in my Internet browser play any role in the operation of my SOFiE client?

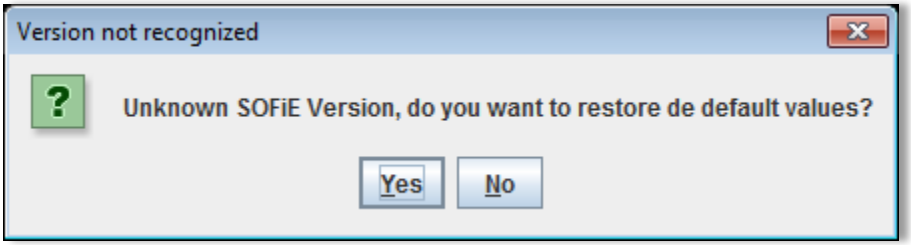
No, the use of the TLS1.2 protocol by JavaWebstart or the "wget" command is not influenced by the settings of the Internet browser.

7.5 I use JavaWebStart to launch the graphical interface and I also use the batch mode. What should I do?

In this case, you must perform both checks.

In addition, regardless of whether the TLS1.2 protocol is enabled, you must always ensure that the version of SOFiE that is launched via one of the two methods is identical. Each method stores the SOFiE client in a different place. So you end up having two copies of the SOFiE client, potentially with a different version. The version number is also stored in the profile data. You may therefore get the error message below when you launch an older version.

In the graphical interface:



Please answer "No" and update the SOFiE client.

In the log file whose name does not contain the SOFiE identifier:

```
ERROR 13 Sep 2018 08:50:11 [lu.cetrel.sofie.client.SofieMain] - Version not recognized : 5.25
```

(Note: The version number was updated manually to cause this error message. At the time of writing, version 5.25 does not yet exist.)

8 Contact information

- Contract sales or technical questions :
  - Tel : (+352) 355 66 - 600
  - Email : helpdesk.lux@six-payment-services.com