MIBGAS

MERCADO IBÉRICO DEL GAS

WORKSTATION SETUP GUIDE FOR ACCESSING THE MIBGAS PLATFORM

Date: 29/3/2021

Version: 4.2.1

CONTENTS

1 INTRODUCTION

This guide describes the requirements of a client workstation for accessing the MIBGAS Platform, and the necessary steps to be taken for properly setting up and logging onto the Platform for Registrations and Consultations, the Trading Platform and the Guarantee Management Platform.

The MIBGAS's web environments require *Internet Explorer*, the *Java Plug-in* for running *Java* applets in the browser, and the Java Web Start application. In addition, their access requires the use of the digital user certificates provided by MIBGAS.

The client workstation must be configured using of the Client Workstation Installer for accessing the MIBGAS Platform. This installer, provided by MIBGAS, permits the installation to be made automatically, reducing the number of manual steps that need to be taken The use of this installer is required, either for configuring the Java version already installed, updating to the recommended Java version or installing Java for the first time.

For troubleshooting purposes, this document ends with a list of possible solutions to any problems a user might encounter when installing and setting up a client workstation.

NB: The purpose of the images included in this document is to help to follow and identify each installation step. They are presented as screen shots examples. Due to the continuous software (installer, IE navigator…) and MIBGAS Platform upgrade the images that appear in this document may not correspond to the latest information available.

2 PRIOR REQUISITES

2.1 Main components and versions

The following are the main software components required for using the MIBGAS Platform:

- Hardware:
  - PC or laptop.
  - Processor: Intel Core i5 or i7, 3rd generation.
  - Memory: 4GB or 8GB RAM.
  - Hard Drive: Minimum 150GB.
- Operating system:
  - Windows 7
  - Windows 8 and 8.1
  - Windows 10 (recommended)
- Internet Explorer
  - 32-bit version
  - Browsers IE10 and 11

NB: *Windows 8 provides one web platform that supports two browsing experiences: Internet Explorer in the new Windows UI that is optimized for touch devices, and the familiar browsing experience of Internet Explorer for the desktop. The former is not supported in the system, so the desktop option needs to be used.*

- Java Virtual Machine (32 bits)

Updated information on the latest version of the Virtual Machine recommended and endorsed for logging onto the Organised Gas Market's websites is to be found on the MIBGAS public website (http://www.mibgas.es), in the section "Technical Documentation" in "Information System".

- Digital certificates
  - For users of the client workstation
  - As Signing Entity (Root CA) of OMIE

NB: *The digital certificates issued for the MIBGAS Platform are in software format. Nevertheless, when accessing the Platform for Registrations and Consultations or the Guarantee Management Platform, if an Agent decides to enable an existing certificate in card form that is valid for other markets (Electricity, Auctions), the client workstation requires the use of a card reader.*

There now follows a more detailed description of these requirements, together with additional setup options.

2.1.1 Internet Explorer

The Internet Explorer browser for using the Platform for Registrations and Consultations should always be the 32-bit version (even when the Operating System is 64 bits).

2.1.2 Trading module setup

The Trading module establishes an AMQP connection (https://www.amqp.org/) with the server (broker). This connection is furthermore protected using SSL (which is established with the client certificate selected when opening the application).

In order to allow this connection, a client is to allow a connection to be made to the server's port **5671**, making sure that any firewalls are correctly set up and do not block this connection.

2.1.3 Screen resolution

The proper viewing of the MIBGAS Platform requires a system designed with an optimum setup of:

- **1280x1024 pixels and 65536 colours.**

The following are the recommended maximum screen configurations:

- Resolution 1366x768 and medium font size (125%)
- Resolution 1600x900 and medium font size (125%)

2.1.4 Date and time configuration

It is required to adjust local date and time of the client workstation running the Trading Platform so that it is a correct time and it is synchronized with a reliable time server. This will avoid potential anomalies related to wrong time configuration of the workstation accessing MIBGAS platforms.

3 USING THE CLIENT WORKSTATION INSTALLER

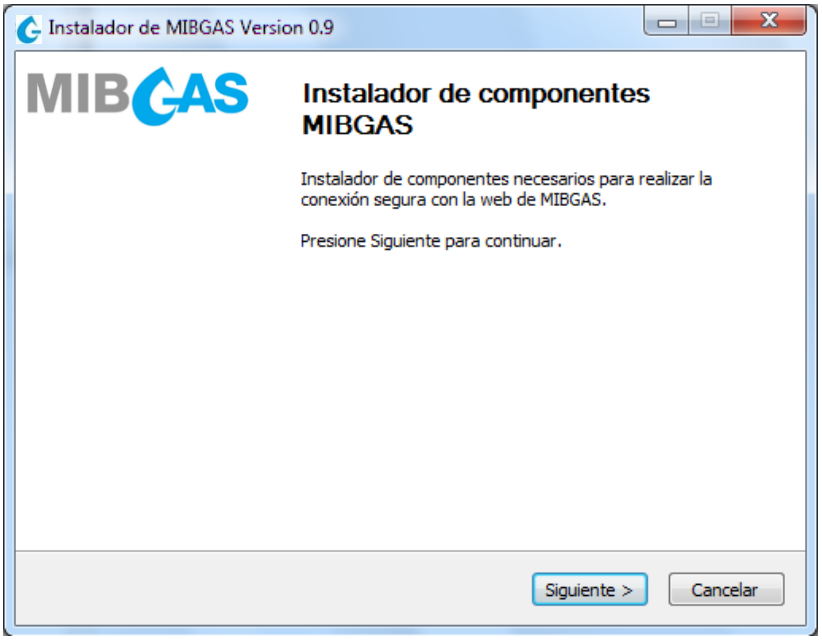
The installer provided by MIBGAS enables the installation process to be performed automatically, reducing the number of manual steps that need to be taken. This installer can be downloaded from the MIBGAS public website (http://www.mibgas.es).

In case of accessing the system without no 32 bits Java version installed, a screen will be shown where it is suggested the installer execution and it will facilitate access to the correct page of the public website.

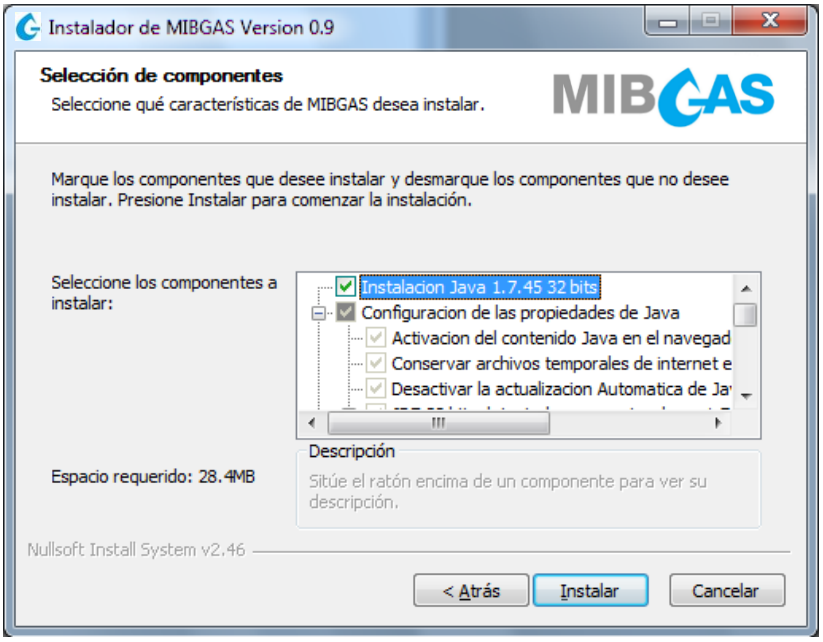
Once downloaded, it is advisable to be connected to the internet when running the installer, although this is not essential, as the installer contains both the JRE package to be installed and the settings to be modified within the .exe file. It is also advisable not to interrupt the installation once it is running.

Given that the installer changes the user profile parameters in Windows, it should be run from the user session in which the MIBGAS Platform is to be operated. If the user running the installer does not have administrator privileges, an initial screen will be displayed with the window for logging on as an administrator.

This is the installer's initial window:

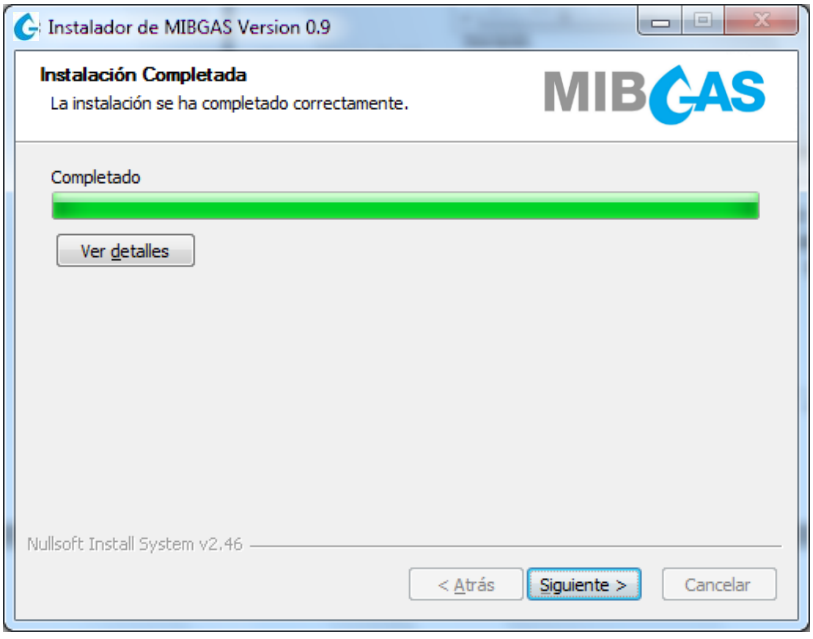


Clicking on "Next" calls up the window for selecting the parameters to be installed:



Depending on the 32-bit version of the Java Virtual Machine installed on the equipment, a prompt will appear with a recommendation to install the version included in the installer, although the user may disable this option. All the other options correspond to setup parameters for the Virtual Machine and for Internet Explorer, which cannot be disabled. Clicking on “Install” saves the changes.

If the option has been taken to install the Virtual Machine, its installer will run first. Once the installation has finished, the process will continue with all the other settings of the MIBGAS installer.



If we need to operate on the MIBGAS Platform from the same client workstation with several users of the operating system, we need to run the installer from each user session we want to set up, disabling the option of installing the Java Virtual Machine if it has already been installed.

Once the installation process has finished on the client workstation, logging onto the system requires registering the digital user certificate as described in section 5.

In the event of any logon problems following the workstation's automatic setup, see section 6 (Troubleshooting) and **¡Error! No se encuentra el origen de la referencia.** (Checks on setup problems) in this guide.

> ***NB:*** *If you have had to log on as an administrator, the changes in settings will apply to both the administrator and the user that opened the session in the Operating System.*

4 CHECKS ON SETUP PROBLEMS

All settings included in this section are automatically configured by the installer, as explained on section 3. However, they are detailed here as a support in the case some settings have to be made manually.

4.1 Internet Explorer

The 32-bit version of Internet Explorer should always be used (even when the Operating System is 64 bits).

Furthermore, given that the establishment of a session with the Server uses the *Secure Sockets Layer* (SSL) with strong encryption (128 or 256 bits), the browser needs to be able to support this level of encryption. Check the level of encryption the browser supports simply by clicking on the menu option "*Help → About Internet Explorer*", and checking that the version of Internet Explorer is higher than 10:

The following setup options are to be taken into account for the browser:

» Enable the downloading of signed applets

The browser needs to be set to download signed applets. This simply involves selecting a "**Medium**" security level in the "**Internet**" zone, which is the default security setting when installing Internet Explorer. These settings can be checked by following the steps below in the browser:

Tools → Internet Options → Security

Within this screen, select the "**Internet**" tab and enable the "**Medium-high**" security level. If the MIBGAS websites ("**.mibgas.es*") have been included within "**Trusted sites**", this area should have a "**Medium**" security level

This level of security is adequate for most secure web servers, and it means that any applets downloaded may be run, although this will always need to be confirmed by the user.

If you cannot access the website, check that the settings for trusted sites include at least the following:

- **For accessing the main environment of the Organised Gas Market:** "**.mibgas.es*"

- Permit the use of COOKIES

The browser needs to accept the use of COOKIES (small text files that the server installs on the client computer). The COOKIES on the Organised Gas Market's website interface are used solely for tracking the current session.

All that needs to be done to permit the use of COOKIES is register the access URL in the "**Trusted Sites**" area, or select a medium privacy setting (which is the browser's default option) for the internet zone in:

Tools → Internet Options → Privacy

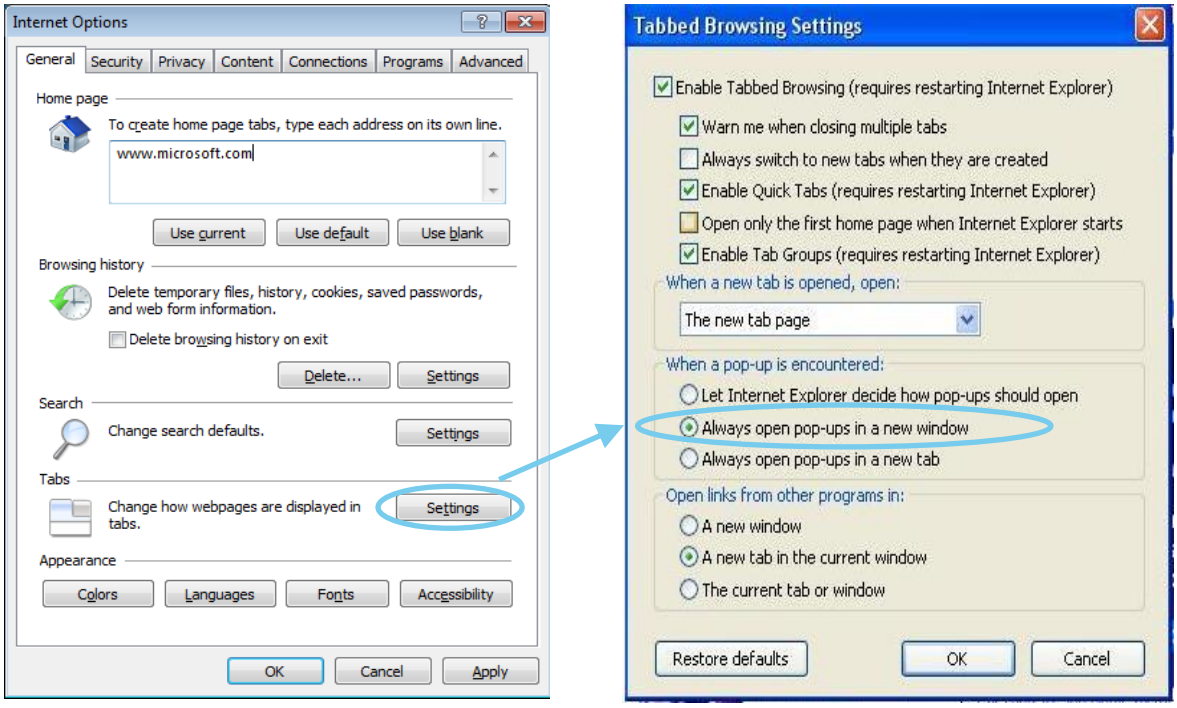
- Permit pop-up windows

The browser must not block pop-up windows on the Organised Gas Market's website, as they include windows that are necessary for the system's proper operation. If there are any tools installed that block the use of pop-up windows (e.g., *MSN* or *Google* bars) the settings for these tools need to ensure that the website's pop-up windows are not blocked.

Accordingly, it is advisable to turn off the pop-up blocker, at least for all MIBGAS servers, doing so through the use of the "**.mibgas.es*" mask and specifying a low level of filtering (for more information, see section 6.5).

It is advisable to keep the browser's defaults tab settings, which means that the pop-up windows always open in a new window. These settings are to be found at:

Tools → Internet Options → General → Tabs → Settings



» Turn off ActiveX filtering

ActiveX filtering needs to be turned off, so check that this option has been disabled through the menu:

Tools → ActiveX Filtering

» Reviewing minimum options

When the client's security settings have already been customised through the use of other applications, or due to corporate security policies, there follows a description of the **minimum options** that need to be enabled for the system's proper use (only the necessary options have been described, so the ones that do not appear have no impact on the application). These values are to be enabled in the Internet zone, unless the MIBGAS websites have been included in other zones (local intranet, trusted sites, restricted sites), in which case they are to be enabled in the corresponding zone.

Tools → Internet Options → Security → Internet

Automatic prompting
Active scripting
(✓) Enable
Automatic prompting of Java applets
(✓) Enable
ActiveX controls and complements
Download signed ActiveX controls
(✓) Prompt[1]
Run ActiveX controls and complements
(✓) Enable
Initialise and script ActiveX controls marked as safe for scripting
(✓) Enable
Downloads
File downloading
(✓) Enable[2]

As regards the **advanced settings** options, the following option needs to be checked:

Tools → Internet Options → Advanced Options

Security
[✓] Use TLS 1.1
[✓] Use TLS 1.2

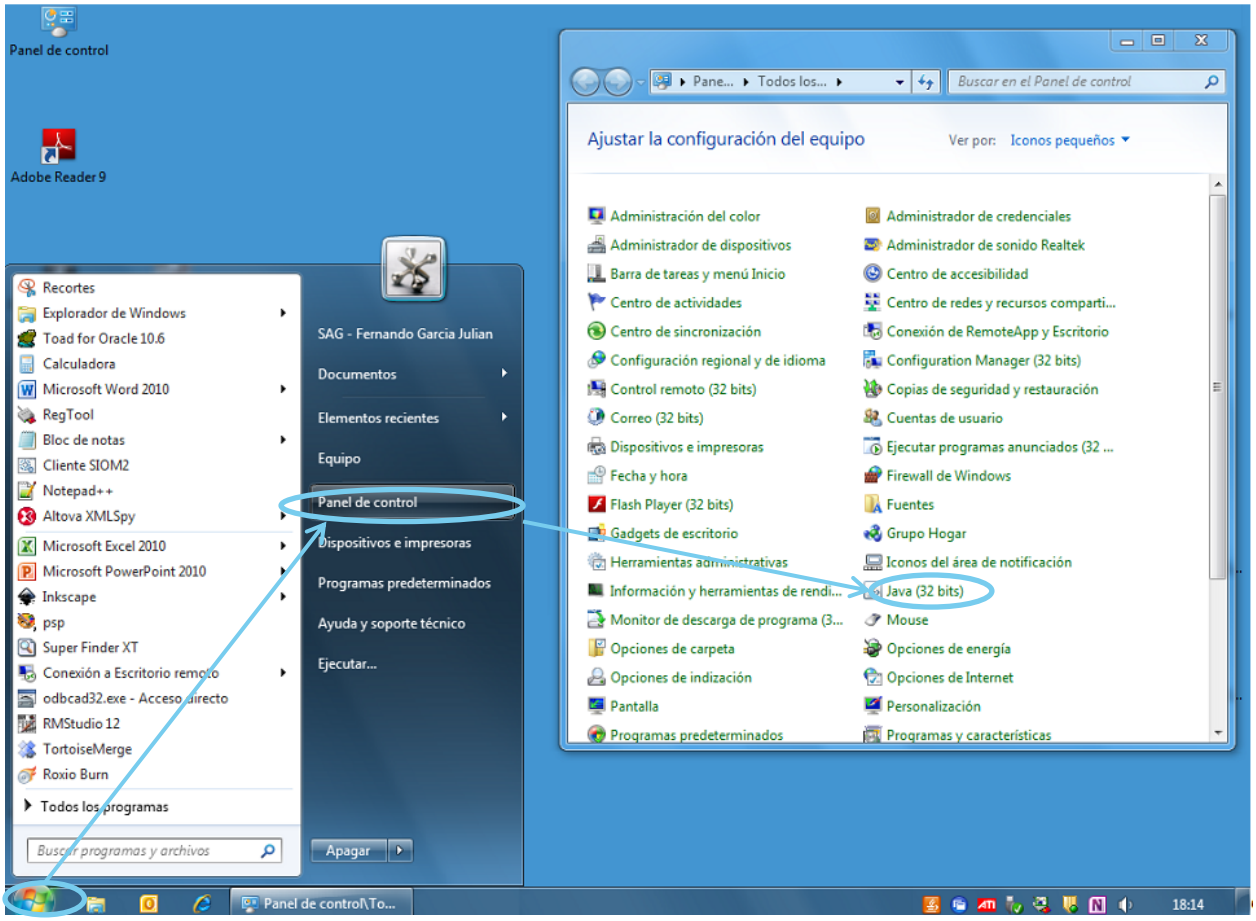
[1] *Required for downloading the applets to the client workstation the first time the application is accessed.*
[2] *Required for downloading orders and other data to a file.*

4.2 Java Virtual Machine

The Organised Gas Market's website interface makes intensive use of executable components that are downloaded from the web server. These components are Java programs that are also referred to as applets, and have previously been signed by MIBGAS so that the browser can verify their authenticity and ensure their use does not lead to any kind of security issue.

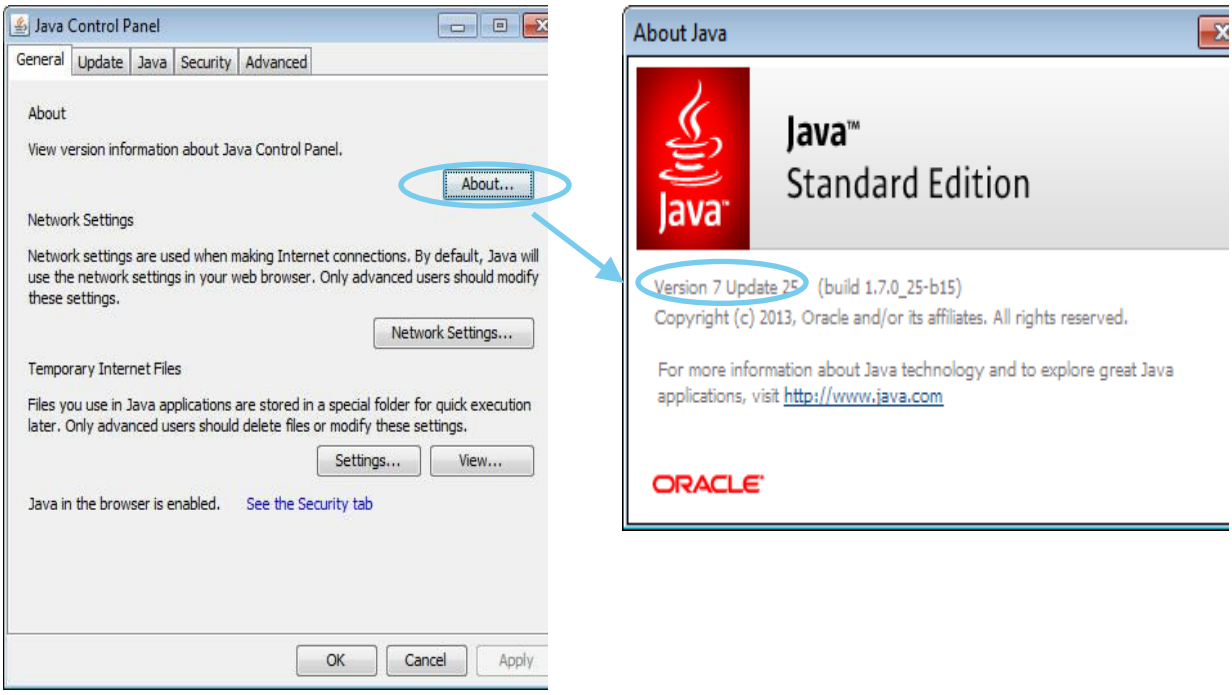
Accordingly, the browser's Java Virtual Machine (JVM), which is the environment for running applets, needs to be installed and enabled. The required JVM is the one provided by Oracle, and needs to be the 32-bit version. The browser uses the JVM through a plug-in, which is installed together with the JVM.

You can check that this JVM is installed by seeing whether the "Java" option is available within the Windows Control Panel:

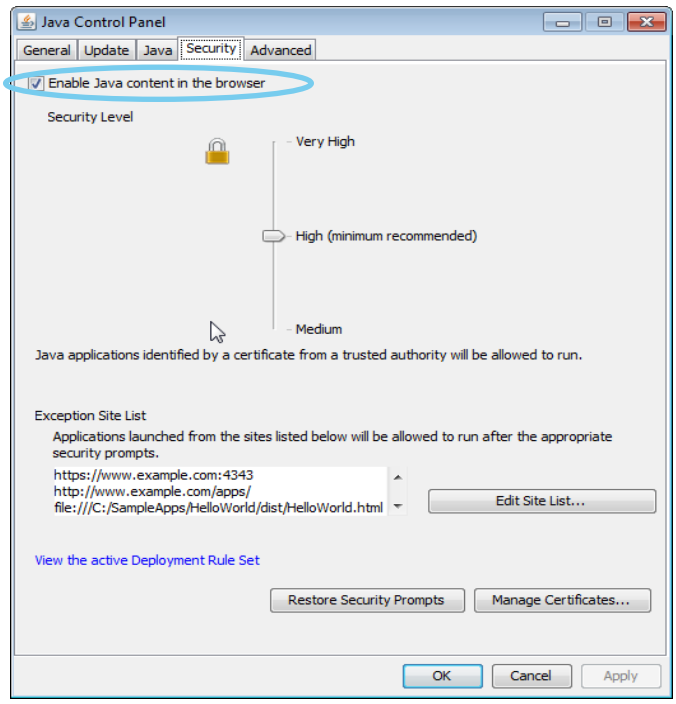


If that option is not available, the JVM needs to be downloaded and installed from Oracle, so log onto the website and click on download (see instructions further on).

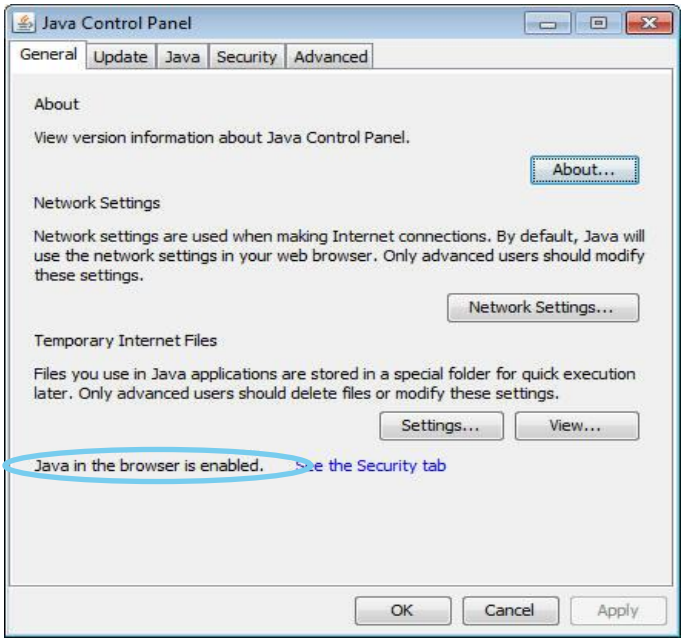
If JVM has already been installed, check the version by opening the Java Control Panel, and clicking on "About...":



Ensure that the JVM is properly enabled for the browser by checking the following option on the Java Control Panel:



The following message will appear in the “General” tab on the control panel:



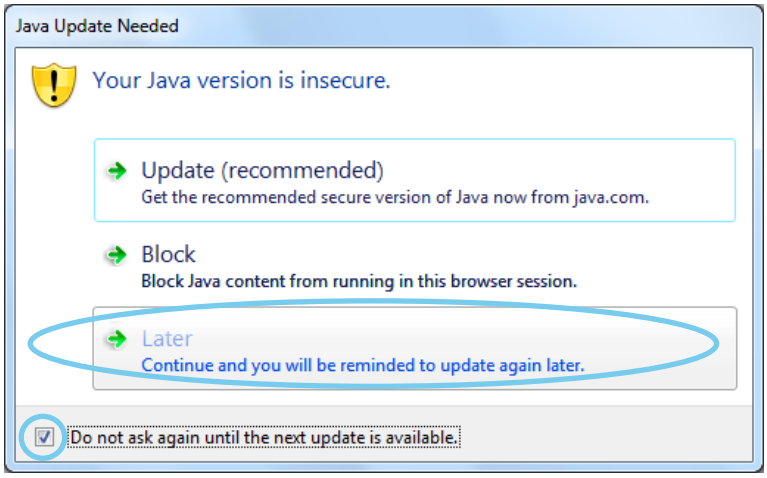
It is also necessary to ensure that "Advanced" tab is selected next options:

Advanced Security Settings
(✓) Use TLS 1.1
(✓) Use TLS 1.2

In the event the installed version is not a valid one, the procedure for updating to a suitable version is to uninstall the installed version and access the Organised Gas Market's website. From here, and as described in section **¡Error! No se encuentra el origen de la referencia.**, the right version of the JVM will be installed automatically, with no need to first download any other version (in order to carry out this installation, the user connected to the operating system needs to have administrator privileges).

The current version should be uninstalled through the option "Add or remove programs" on the Windows Control Panel, selecting the item "J2SE Runtime Environment" with the corresponding version, and clicking on "Remove".

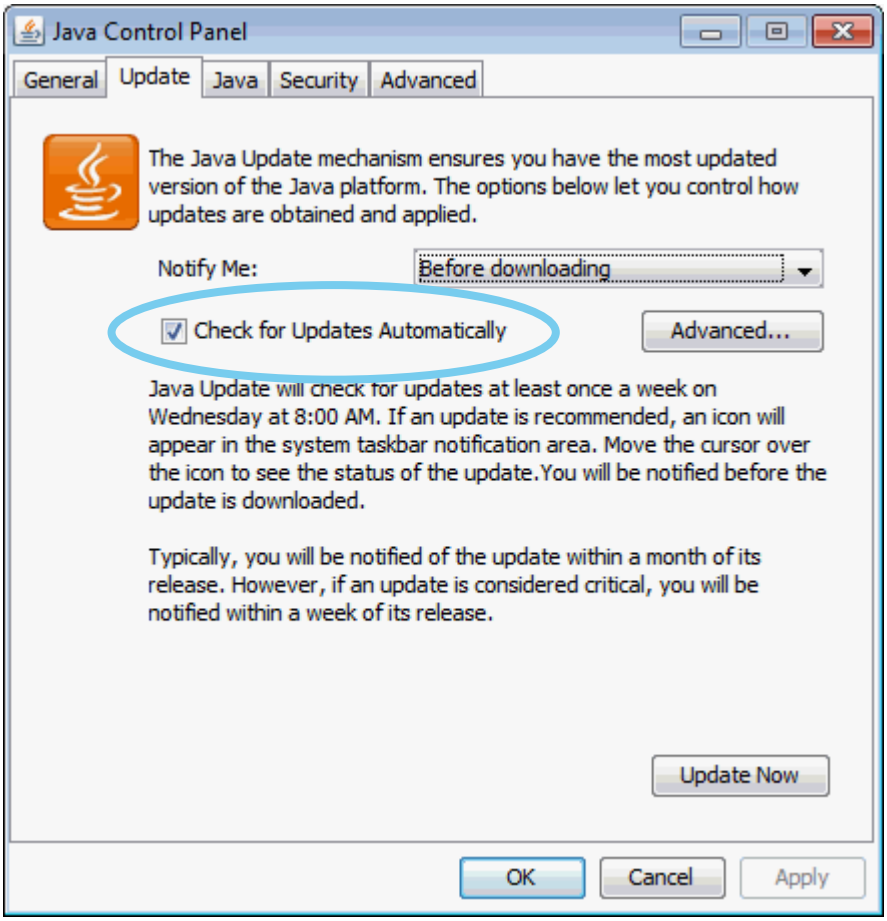
Once the virtual machine has been installed, when logging onto the website an alert may appear indicating that there is a new version of Java available, with the text "Your Java version is insecure." To stop the message being displayed again, check the box at the bottom of the screen "Do not ask again until the next update is available", and then click on "Later".



Use of the Update option is not recommended, as any new versions released must first be approved prior to their use in the system.

This message may pop again when a new version of the virtual machine is released.

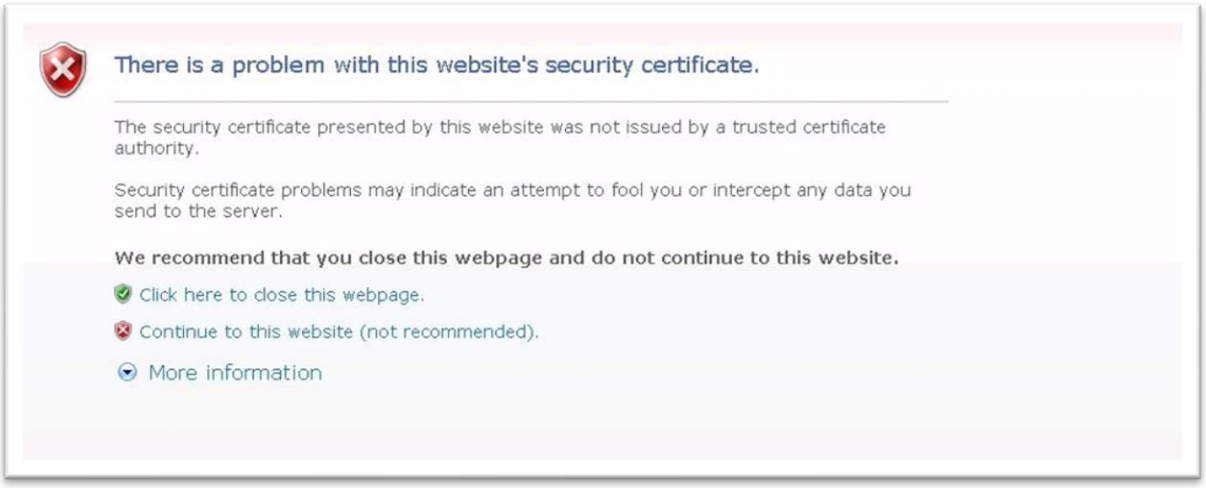
In the event that Oracle free a new JRE version which it is not certified to its use in SIOM, it is convenient to deactivate he JVM automatic actualization. This is configured in the next box from the Control Panel:



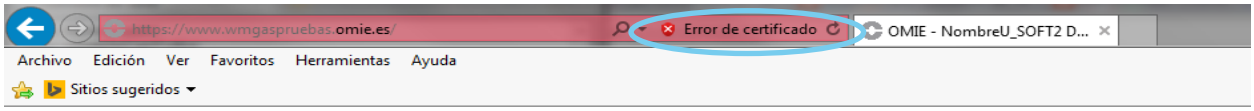
4.3 Certificate of Signing Entity (OMIE Root CA)

An essential requirement for the correct installation of the specific components of the Organised Gas Market's websites is to have installed the OMIE CA Certificate of Signing Entity on the browser.

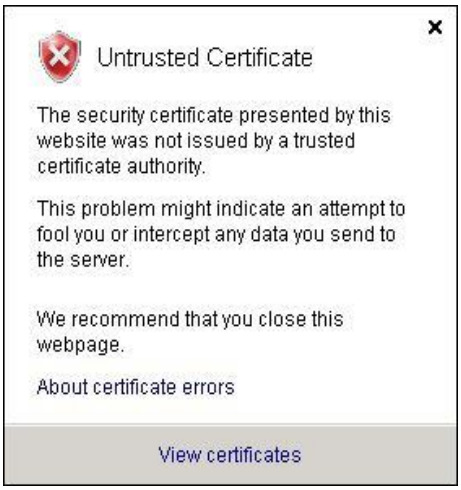
When entering the system for the first time, or whenever that certificate has not been installed, the following warning screen will be displayed. Click on "**Go to this website**":



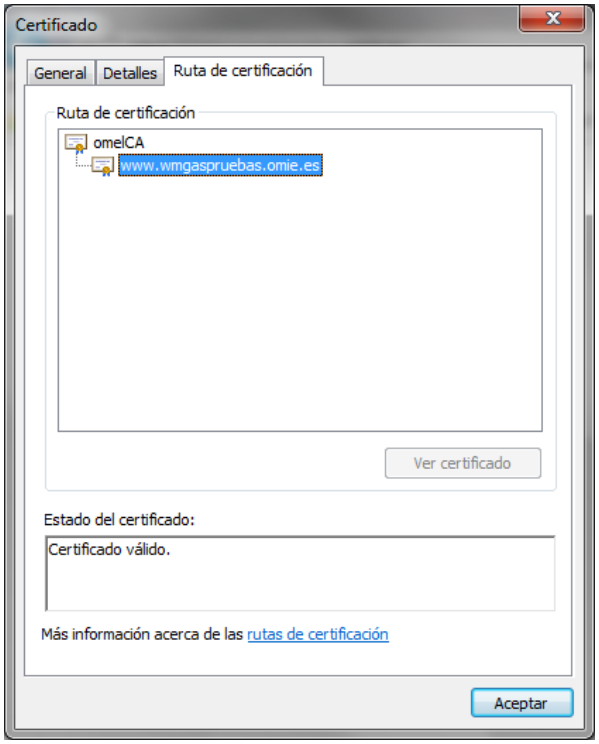
Then click on the button "**Certificate error**" that is displayed on the right in the address bar:



This window will appear. Click on "**View certificates**":



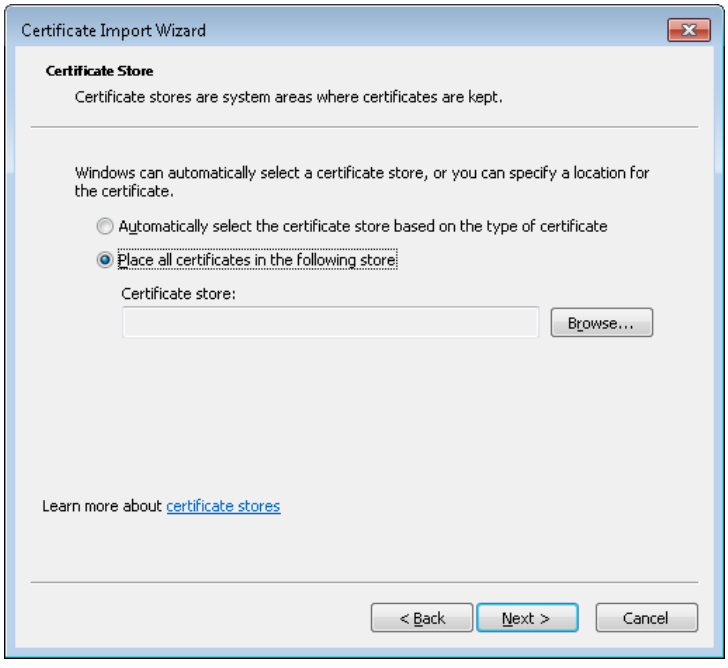
In the next window, open the third tab (Certification path). Select the root of the tree (OmieCA) and click on "**View Certificate**":



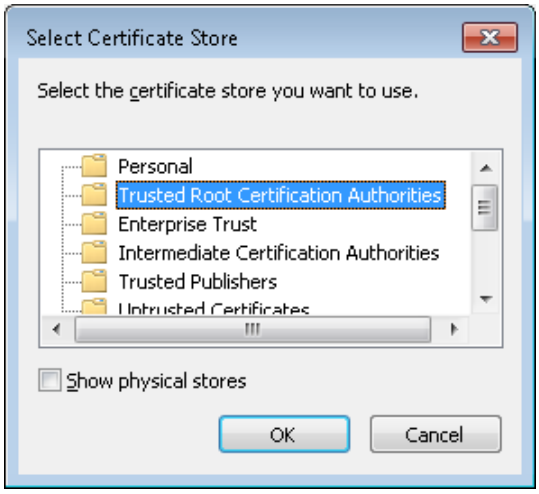
In the next window, click on "**Install certificate**":

Click on "**Next**":

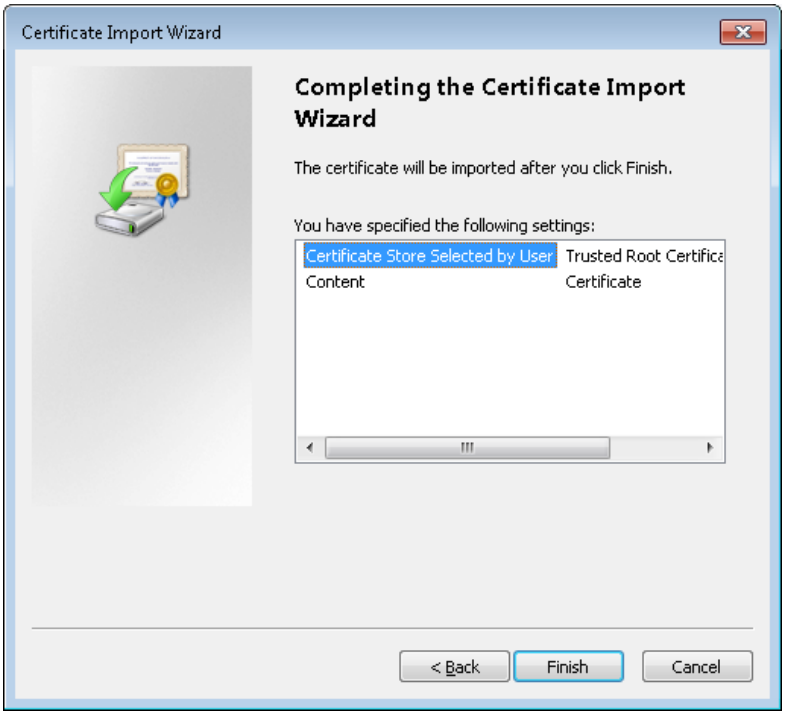
In the next window, check the option "**Place all certificates in the following store**", and click on "**Browse...**".



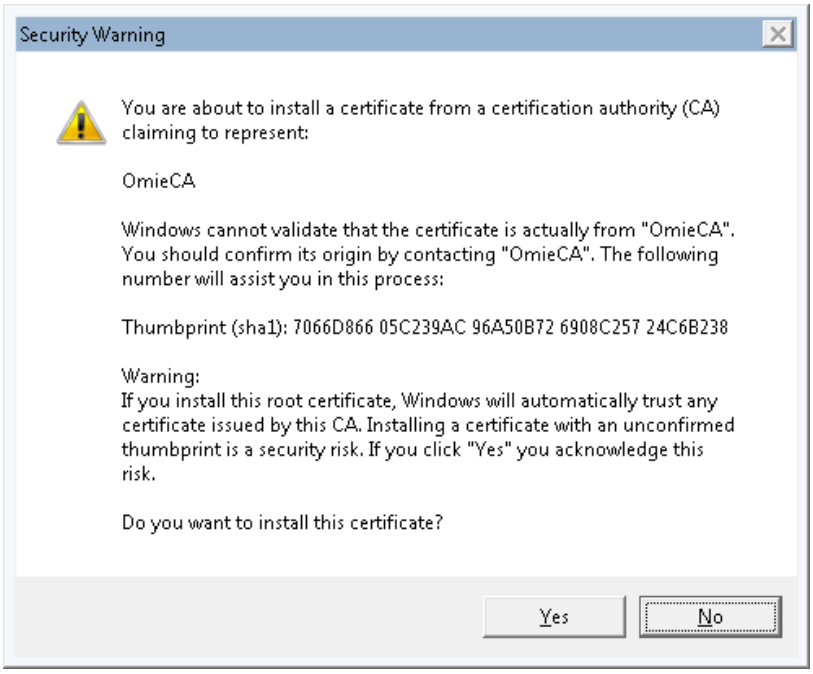
In the next window, select "**Trusted Root Certification Authorities**", and click on "**OK**".



In the previous window, click on "**OK**", and then "**Finish**" in the window displayed:



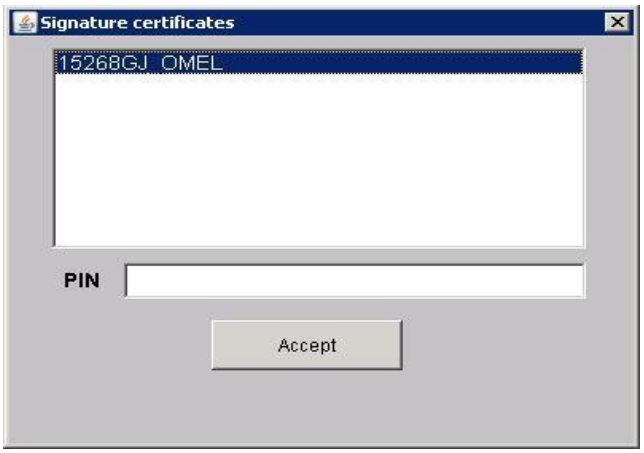
The following window is then displayed. Click on "**Yes**" to install the certificate:



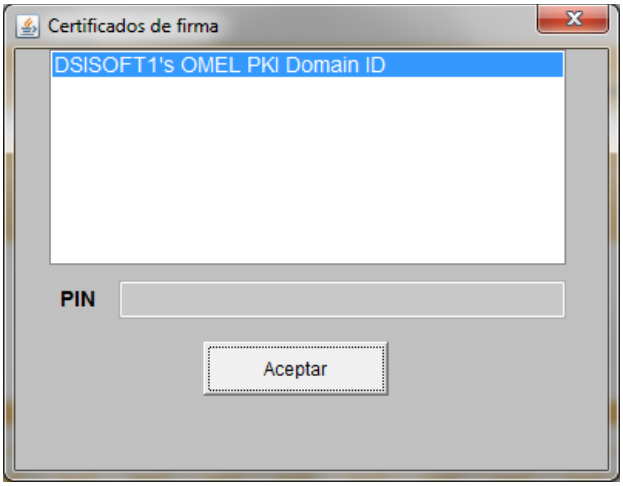
The browser confirms the successful installation of the certificate. Click on "**OK**":

4.4 Signature Applet Settings

A 'Signature Applet' is a Java component used for transmitting digitally signed data files to MIBGAS, such as, for example, 'Agent Data' from the Platform for Registrations and Consultations. Its appearance, whenever a signed transmission has to be made, is as follows:



The applet shows the certificate to be used for digitally signing the transmission, which will be the same as the one used for logging onto the system. There is also a box for the certificate's PIN for those cases involving a smartcard certificate. If a software certificate has been used, the box will be disabled, and the browser itself will subsequently prompt confirmation of the certificate's use, with or without a password, according to the security level chosen when registering it.



This applet has a settings file located at '**C:\OMEL\ConfAppletFirmaGas.xml**'. The applet uses an initial default setup in case the file does not exist, creating it for subsequent modification by the user. When first installing the workstation, this file will not be created until the website's home page has been accessed.

The content of this file is as follows:

```
<?xml version='1.0'?>
<!--
   NOTE: Any change in this file will be taken into account when the
   browser is next restarted.
-->
<ConfAppletFirma>
   <Security>
         <PINTimeout>0</PINTimeout>
   </Security>
   <Log>
         <DirEnviosFirmados>c:\omel\EnviosFirmados</DirEnviosFirmados>
   </Log>
</ConfAppletFirma>
```

Two configurable parameters are established in this file:

- **PINTimeout**: This time expressed in minutes establishes the maximum time that the applet waits between each signed transmission before it asks the user to-enter the PIN. If the maximum time specified has not elapsed between signed transmissions, the user will not be asked to re-enter the PIN. A '0' value indicates that the user will always be asked for the PIN. This parameter has a maximum value of 30 minutes. If a higher value is set, the default time of 30 minutes will prevail.
- **DirEnviosFirmados** Destination directory of signed transmissions. A structure of subdirectories will be created in this directory, with all the signed transmissions made by the user with the applet organised by types of transmissions ("DatosAgente */AgentData*", "DatosContacto/*ContactData*", "LimitesTipoProducto/*ProductTypeLimits*", etc.). When a non-existent directory is specified, the applet will automatically create it. If the directory cannot be created, the destination directory will be the default one defined by the applet, which is **'c:\omel\EnviosFirmados'**.

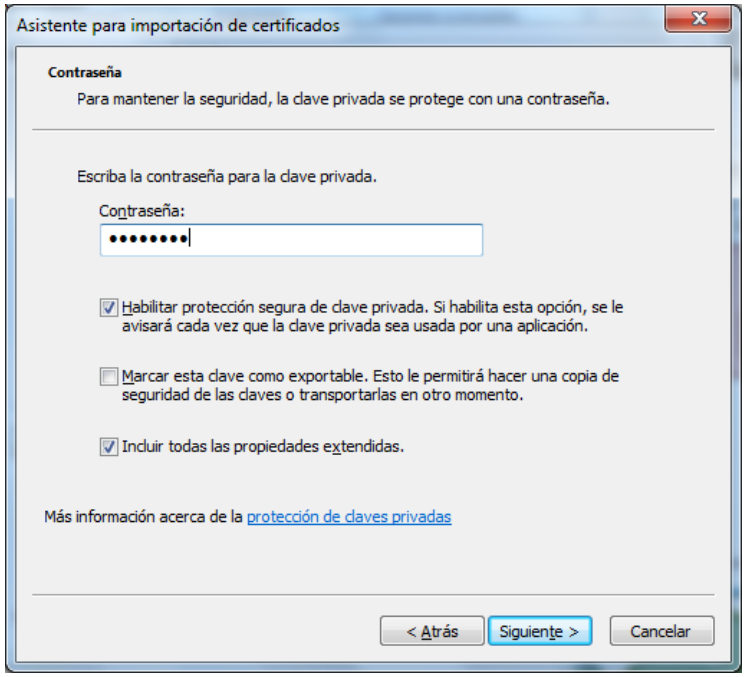
  Any change in this file will apply when the browser is next opened.

5 REGISTERING DIGITAL USER CERTIFICATES

Those certificates in files, or software certificates, are to be submitted in ".p12" format (standard PKCS #12). To register certificates submitted in this format, follow the steps now described.

Download the ".p12" into a directory that can be accessed from the workstation where the certificate is to be registered. Select the file and enable it by double-clicking (this process may also be launched from the browser, via "*Tools/Internet Options/Content/Certificates/ Import*").

Follow the steps as prompted on the screen, using the default options, until the following screen is displayed:



Type the password for the private key provided by MIBGAS, and check the box "*Enable strong private key protection*".

Continue with the default options until the next screen appears:

Click on “Security level...”:

This screen allows choosing between a “Medium” or “High” security level for setting up the system’s performance when using the certificate to log onto the website or signing a data transmission. If you choose “Medium”, the browser will only display a warning, prompting the user to confirm access to the private key. If you choose “High”, the browser will also request a password for accessing that private key.

It is advisable to select “High” and choose a password to be used as a PIN for accessing the system and signing the transmission of data. In this case, clicking on “Next” will call up the next screen, where the password chosen can be typed in and confirmed.

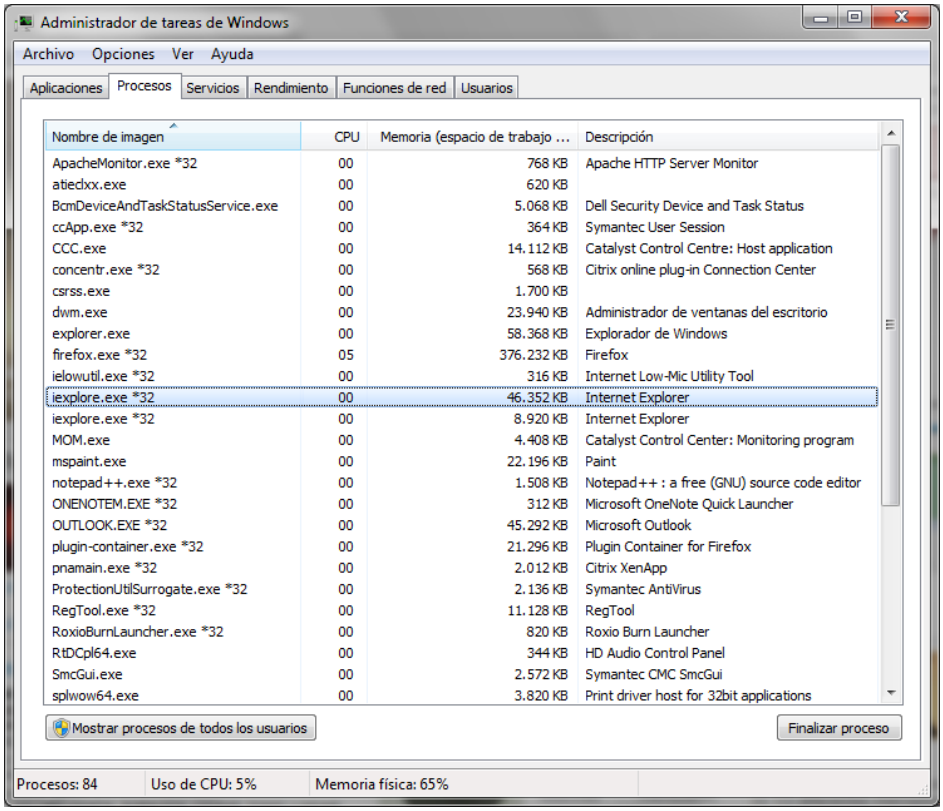
Clicking on “Finish” and then “OK” will display the message that signals the end of the process.

6 TROUBLESHOOTING

6.1 The card's PIN takes a long time to be prompted, or the browser stops responding

This problem (detected only with card certificates) may be caused by the fact there are other sessions running with Internet Explorer. This problem is solved by closing all the browser's sessions, and then logging onto the system again.

If the problem persists, check whether there are any active processes in the system's Task Manager, under the name *IEXPLORE.EXE*, as the screenshot shows. In this case, shut down these processes manually from the Task Manager (clicking on "End Process", and then log onto the system again.

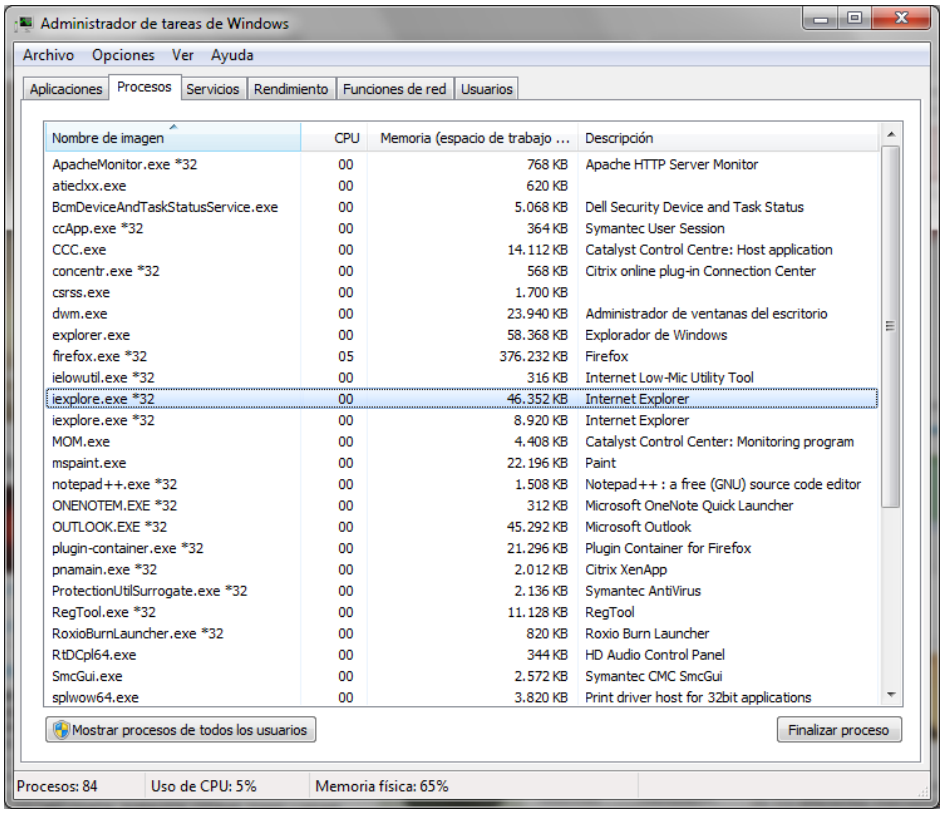


6.2 The browser displays the message “A session is already active on the same user workstation”

Due to the restrictions imposed on the Platform for Registrations and Consultations, the following error might appear in Internet Explorer

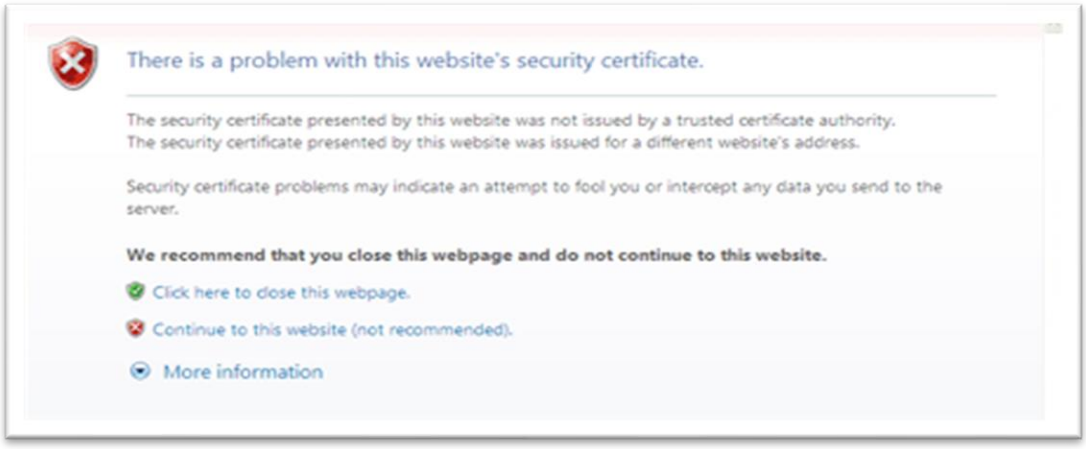
The problem is caused by logging onto the Platform for Registrations and Consultations through the same Internet Explorer session with two different certificates. The solution is to follow the instructions provided on the error screen and open a new session from the menu “File/New session”.

If there is no browser running, and the problem persists, check whether there are any active processes in the Task Manager under the name *IEXPLORE.EXE*, as the screenshot shows. In this case, shut these processes down manually from the Task Manager (clicking on “End Process”, and then log onto the system again.



6.3 "Certificate Error" appears when logging onto the system

As explained in section 4.3, this window appears when the certificate of OMIE CA Signing Entity has not been registered in the browser.



This may occur, even though the certificate has already been registered, when the user of the Operating System has not previously logged onto the website or due to the update of the Root CA in the Organised Gas Market.

In order to solve this problem, follow the steps described in sections 4.3 and 6.10 in this document.

6.4 The server does not permit access to the system

When errors are displayed such as "*Unable to load page*" or "*Access Forbidden*", this may be because the browser being used does not support 128-bit encryption.

Check the browser's level of encryption by following the steps described in section 4.2.

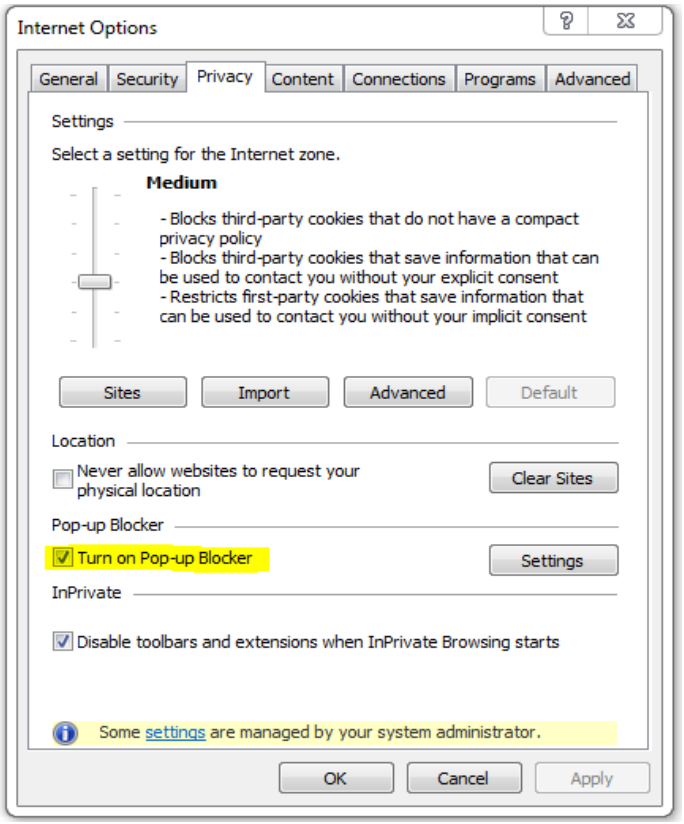
The current versions of the browser for download from Microsoft include the necessary level of encryption. The problem may be that it is an old version, or one that does not distinguish between versions with and without strong encryption for reasons of international law. The problem can therefore be solved by installing the newest version of the browser.

6.5 Blocking pop-up windows

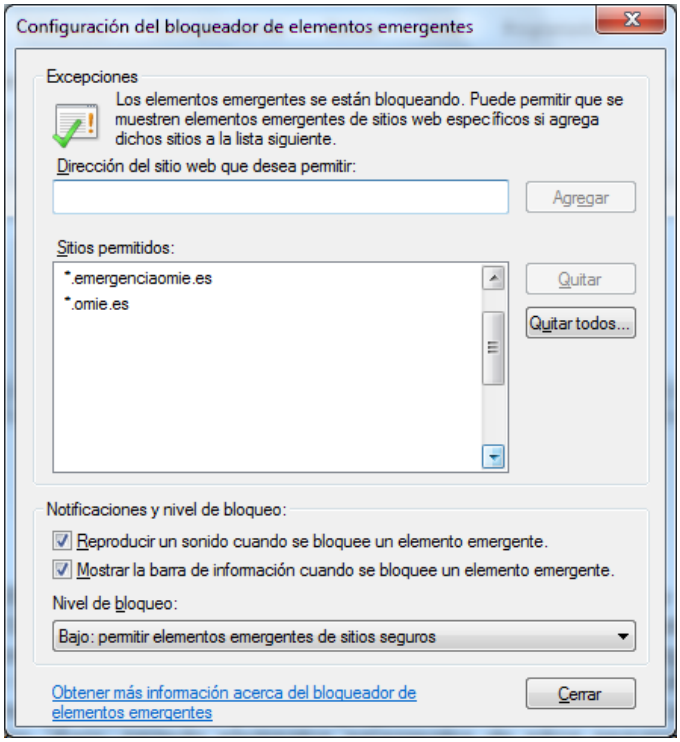
The procedure for installing the components of the Organised Gas Market's websites uses pop-up windows for performing some of its steps (see section 4.2). If pop-up windows have been blocked in the browser, the installation will not be successful, and the user will not be able to operate with the website.

The settings for blocking windows is as follows

Tools → Internet Options → Privacy → Pop-up Blocker

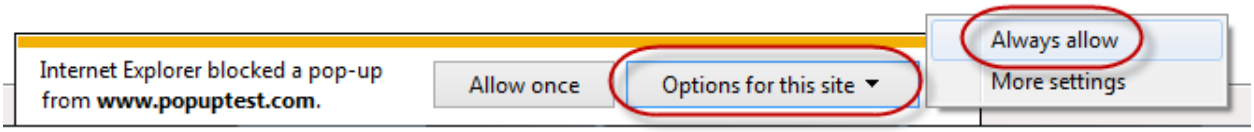


If the option "*Pop-up Blocker*" is checked, as in the above screenshot, the user will not be able to access the website properly. This problem is solved by unchecking this option, or allowing the MIBGAS web servers to open pop-up windows. To do so, click on "*Settings*", and in the dialogue box "*Address of Website to allow*" type "**.mibgas.es*" and click on "*Add*". In addition, in "*Filter Level*"" select the option *"Low: Allow pop-ups from secure sites"* (see next screenshot).



This will allow problem-free access to all MIBGAS web servers.

If pop-up windows have been blocked, and the MIBGAS ones have not been allowed, the following message line will be displayed on the browser, with the following options when clicking on it:



When choosing the option "*Always allow pop-ups on this website...*" a confirmation window may appear.

Once accepted, the pop-up windows blocker will be disabled for this server, so log onto it again. Nevertheless, it is advisable to follow the first procedure described in this section, as it allows accessing all MIBGAS servers with a single operation.

In addition, pop-up windows may be blocked in other ways, such as by installing tools that, among other function, allow blocking these types of windows. Such is the case of the "bars" of *MSN* or *Google* (amongst others). If one of these tools has been installed, it needs to be set it up so that at least it does not block the pop-up windows on MIBGAS websites ("**.mibgas.es*"). To do so, consult the handbooks provided with the tools.

6.6 Problems installing components

If there is a problem after executing the installer, when clicking on the link "ENTER" the following message may appear:

If the problem persists after repeating the operation, try performing the following operation.

- Close the browser
- Check which version of JVM has been installed and enabled (there might be more than one version installed). To do so, run the command "java –version" in the system (*Start / Programs / Accessories / Command Prompt*), and check the version that is shown, for example:

  - java version "1.8.0_161"
  - Java(TM) SE Runtime Environment (build 1.8.0_161-b12)
  - Java HotSpot(TM) Client VM (build 25.161-b12, mixed mode, sharing)

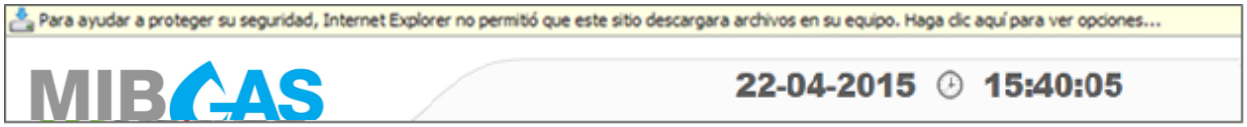
- Access the path "*C:\Program files (x86)\Java\jre*[vers]*\lib\ext*" (where [vers] is the enabled version, which in the preceding example would be "8"), and delete the files (if they exist) AuxiliaryClasses*.jar, and iaik*.jar.
- Execute the installer again, un-checking Java installation.

If this does not solve the problem, it may be due to certain problems that have been detected when installing and uninstalling certain versions of Java. To avoid these problems, take the following steps:

- Close the browser
- Uninstall the version of Java that is enabled, and also delete the directory "*C:\Program files\Java\jre*[vers]**" and its entire content.
- Execute the installer again, checking Java installation.

6.7 File download warning

When attempting to download a file (e.g., download a request or answer in the consultation of signed trades), the following warning may be displayed:



Although the download of the file has been confirmed, the browser will display the website's home page.

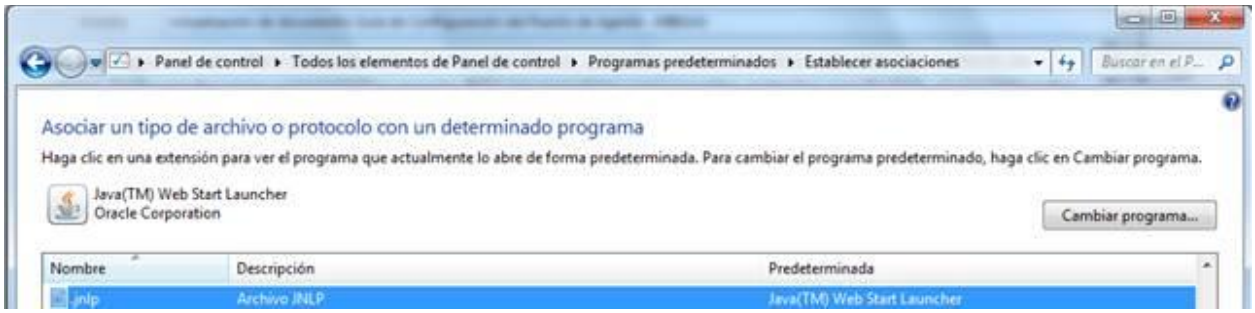
The solution is to check the browser's minimum settings options (as described in section 4.2):

*Tools / Internet Options/ Security / Internet [*or the zone the website is in*] / Custom Level / Download / Automatic prompting for file downloads / Enable.*

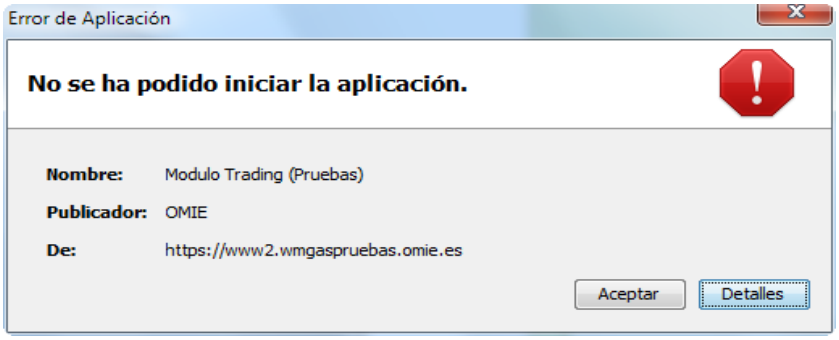
This means that this warning message will not be displayed when requesting a file download, and only the standard dialogue will appear that allows opening it or saving it to a drive.

6.8 Problem launching the Trading Platform

As the MIBGAS Platform's trading module uses Java Web Start, running it properly requires establishing the extension .jnlp for that program, following these instructions, so that the MIBGAS Platform's trading module will launch automatically.



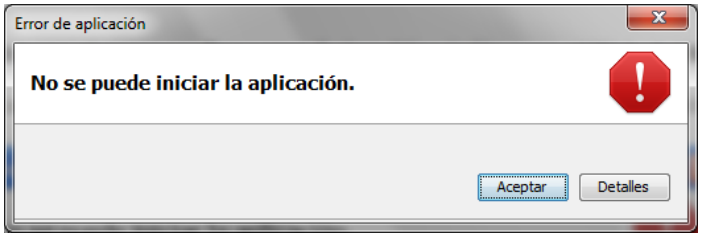
In addition, new versions of the Trading Platform sometimes display the following launch error:



This can be solved by deleting the file *"ClasesAuxiliaresTrading.jar"* located in the folder "*C:\Program files (x86)\Java\jre*[vers]*\lib\ext" "* (where [vers] is the enabled version of Java). After deleting it, you need to re-run the installer as described in point *"*3 *Updating Components"* in this guide to install this Java applet in the system.

6.9 Problem launching the Download Centre

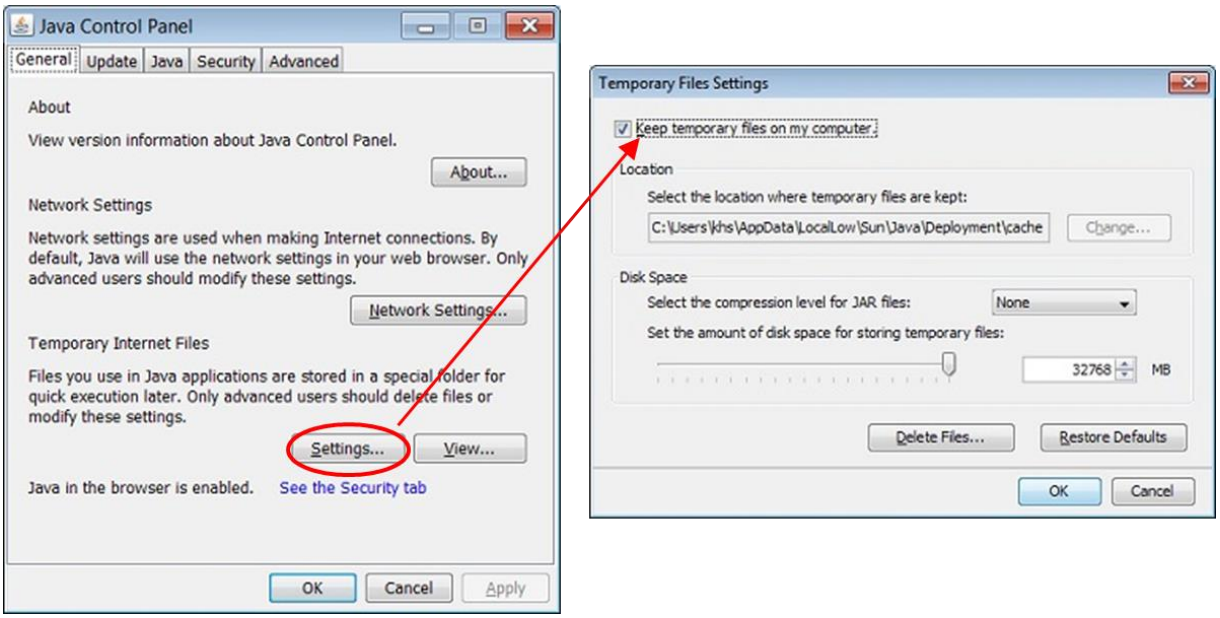
After launching “Download Centre” the following error message may sometimes appear:



This error is due to incorrect Java settings that block the launch of the application. This problem can be solved by changing the settings from the control panel.

These settings can be found at:

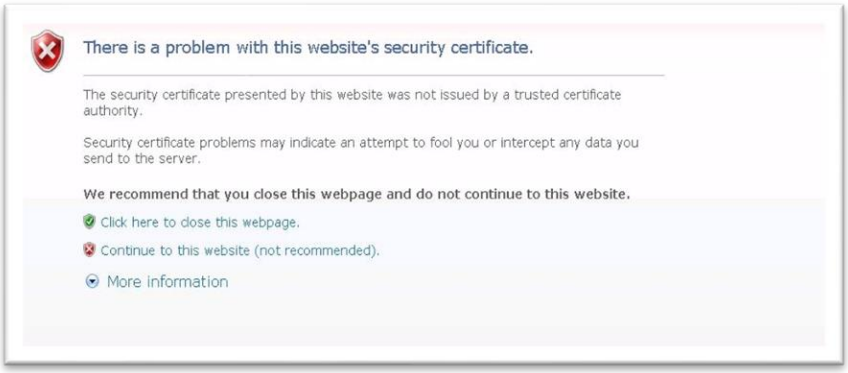
Control Panel → Java → General → Temporary Internet Files → Settings

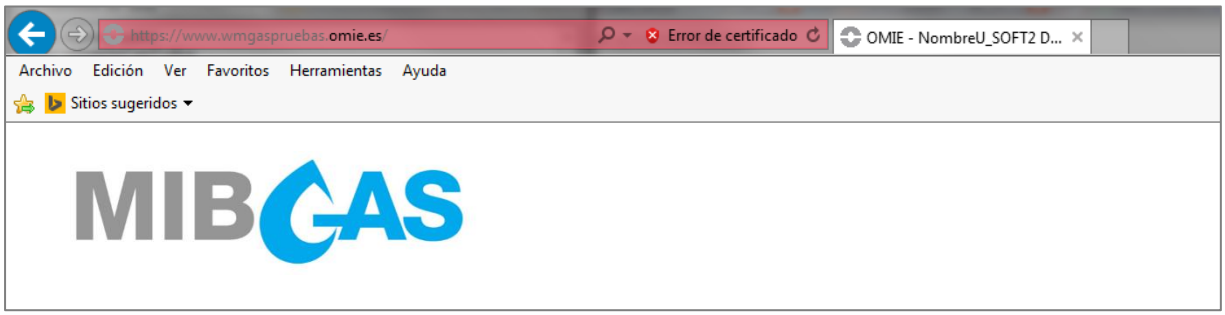


Once there, check the box “Keep temporary files on my computer”.

6.10 Unsuccessful installation of the OMIE ROOT CA

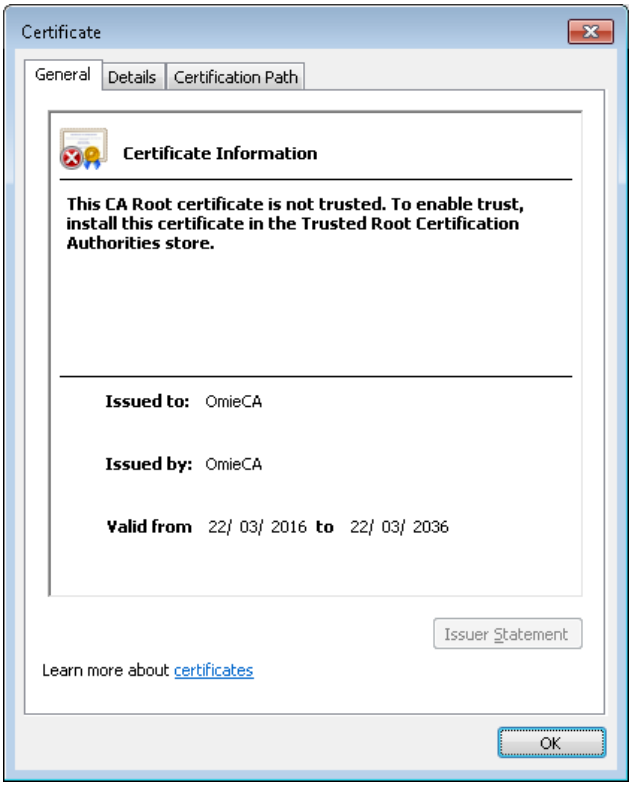
It may be the case that after installing the OMIE ROOT CA, a security warning continues to appear, and the certificate error:





This problem may be due to the fact that the OMIE ROOT CA has not been installed in the correct certificates store (as the default options provided by the browser may install the certificate in the store "*Intermediate certificate authorities*", instead of in "*Trusted root certificate authorities*").

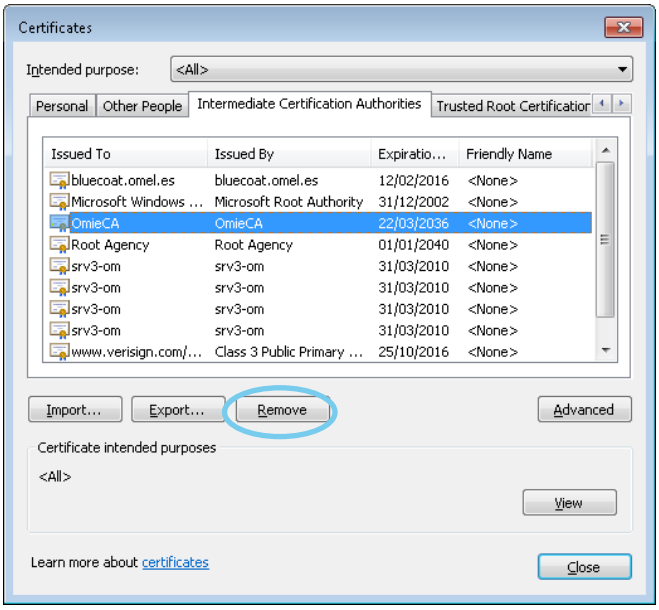
What's more, this situation does not allow re-installing it in the correct store, as if the steps are followed as described in section 4.3, the button "Install certificate" does not appear. This is because the certificate has already been installed in a store.



The solution therefore involves first uninstalling the certificate. To do so, from the browser access the following path:

Tools → Internet Options → Content → Certificates → Intermediate Certificate Authorities

At this point, select the certificate "**OmieCA**" and click on "Remove":



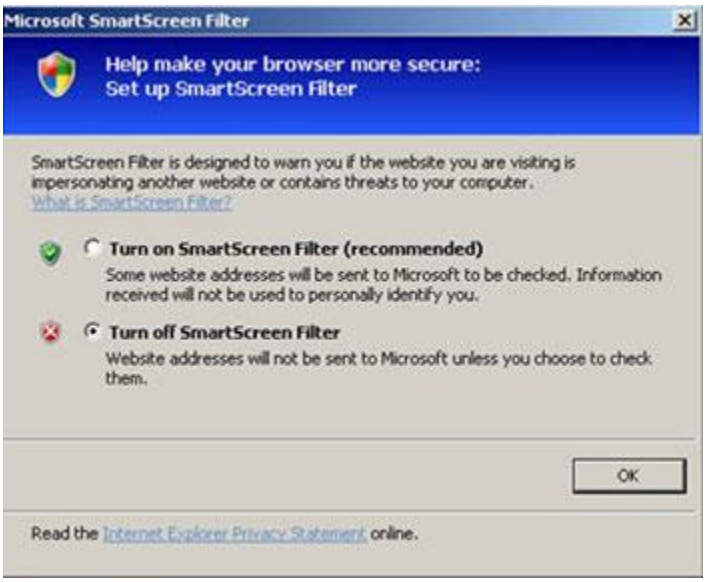
After confirming the operation, the certificate will have been uninstalled. The next stage is to repeat the steps described in section 4.3 for the proper installation of the OMIE ROOT CA.

6.11 Two windows open in the Download Centre

When running the Download Centre from the market website, it sometimes launches twice (two windows open in Automatic Download, which means that the logon certificate is also requested twice).

This problem has been detected when the "SmartScreen Filter" is enabled. This problem is solved by disabling this filter. The "SmartScreen Filter" is to be found at:

Tools → SmartScreen Filter → Turn Off SmartScreen Filter



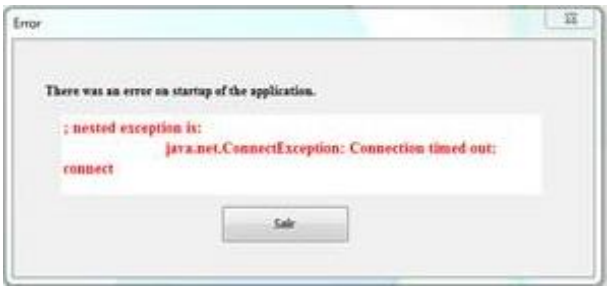
6.12 AMQP port blocked

The Agent's network and security infrastructure should permit the use of AMQP protocol, and clients have to be specifically able to connect to port 5671 on the server, as explained in section 2.1.2.

In the event that the Agent's infrastructure, whether this involves its workstation or any one of the network or security features installed, is not enabled for AMQP protocol, some errors accessing to the Trading Platform and the Platform for Registrations and Consultations may occur.

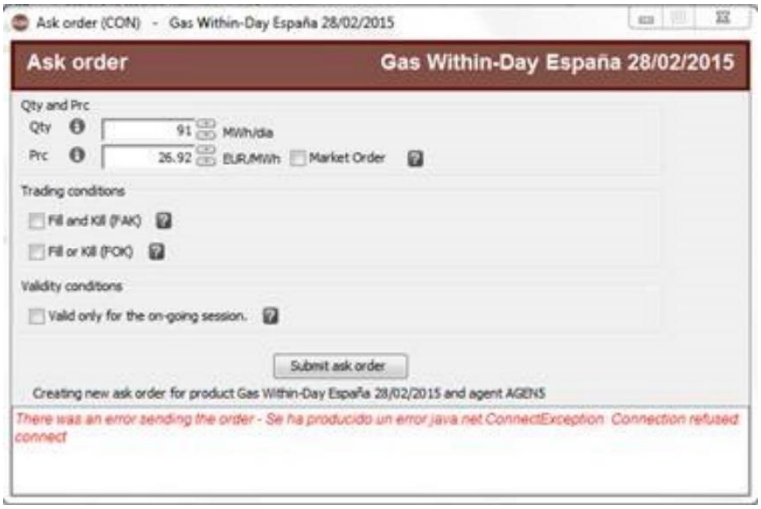
These are some images with possible errors relating to the blockade of the port of AMQP protocol:

- When accessing to the Registration and Consults Platform:



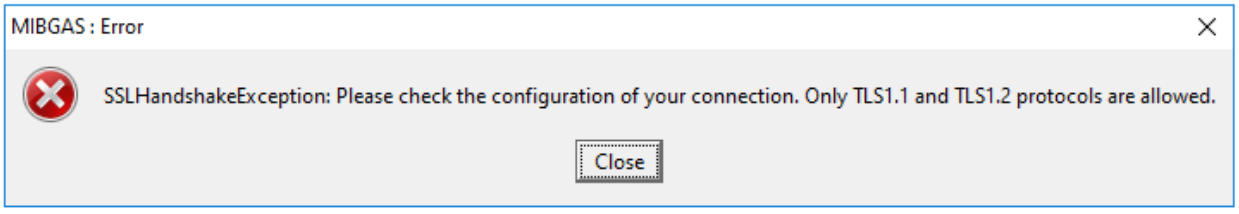
After accepting, it will appear the following error messages:

- When submitting a bid/ask offer in the Trading Platform:



6.13 Wrong configuration of Java security protocols

If Java security protocols are not correctly configured (for instance, if TLS 1.1 and TLS 1.2 protocols have not been activated), the following error message could be displayed when starting the Trading Platform or during its execution:



In order to solve this problem, please review the minimum configuration options of the Java Virtual Machine (as described on section 4.2).

MERCADO IBÉRICO DEL GAS

Alfonso XI, 6. 28014 Madrid (España)
www.mibgas.es | T (+34) 91 268 26 01