MIBGAS
MERCADO IBÉRICO DEL GAS

WORKSTATION SETUP GUIDE FOR ACCESSING THE MIBGAS PLATFORM

Date: 11/03/2024

Version 5.4

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 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.

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.

NB: This version of the document is designed to be accessed through browsers Edge and Chrome to the Gas Market's website. However, EDGE is the recommended browser, and OMIE will offer support for it. Accessing the market with Chrome is allowed, but this is not officially supported by MIBGAS

2. PRIOR REQUISITES

2.1 Main components and versions

The following are the main software/hardware components required for using the MIBGAS Platform. These are the recommended requirements, and a higher configuration is possible:

» Hardware:

  › PC or laptop.

  › Processor: Intel Core i5 or i7, 12th generation.

  › Memory: 16GB RAM.

  › Hard Drive: SSD disk with at least 250GB.

» Operating system:

  › Windows 11 (recommended)

  › Windows 10

» Browser

  › Microsoft Edge (supported and recommended browser)

» 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. Using of certificates in smart card format is not supported.

» The Fortify app (included in the MIBGAS web installer) for the digital signature of deliveries.

» Open Web Start (included in the MIBGAS web installer). Required to run the Download Center and the Trading Module; which when first run, it will install the necessary version of the Amazon Corretto Java Virtual Machine, distributed by MIBGAS.

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

2.1.1   Trading module setup for the Iberian Organized Market

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.

More information on ports, URLs and IPs used to access the MIBGAS platforms can be found in the presentation Emergency System (SIOME) - Implemented improvements, also available through the "Other documentation" section of MIBGAS Registry and Queries Platform help page (https://www.market.mibgas.es).

2.1.2 Screen resolution

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

» 1920x1080 pixels, scale and text size set at 100%.

» 65536 colours.

2.1.3 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 https://www.mibgas.es.

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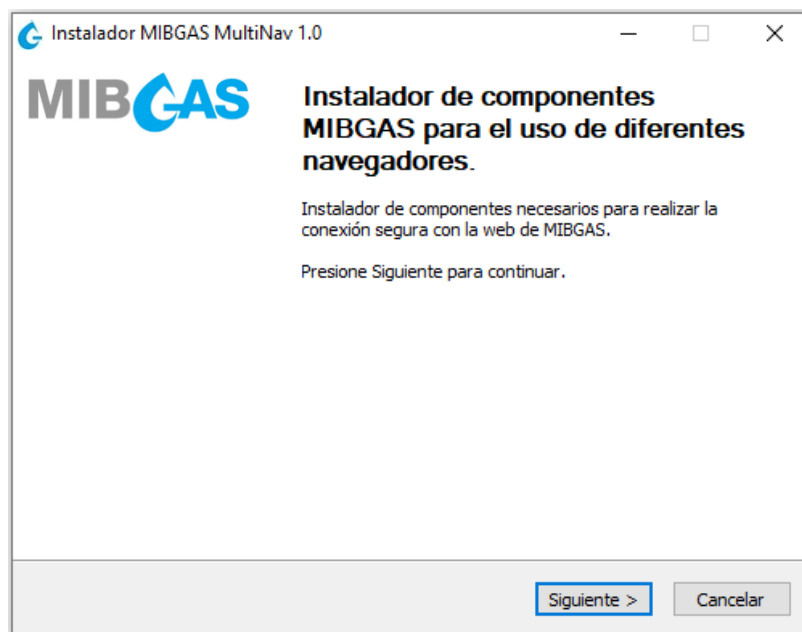
Clicking on "Next" calls up the window for selecting the parameters to be installed:

If you access the system without having any version of Fortify installed or running, a screen will be shown warning that you need to have the Fortify application installed.

www.test.market.mibgas.es dice

Se necesita tener activa la aplicación de Fortify especifica de REE y OMIE

Aceptar
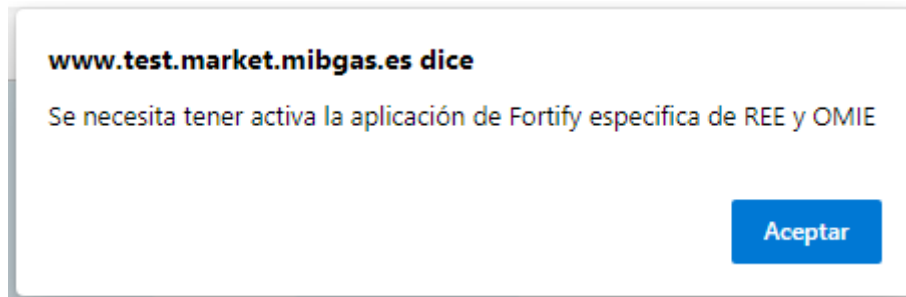
Installing OpenWebStart is only necessary if the Download Centre or the Trading Module will be used. All other options correspond to elements that are needed, and they cannot be deactivated. After clicking "Install," the changes will be applied.

Next, the Fortify installer will appear:

Instalación de Fortify 1.3.7

Bienvenido al Asistente de Instalación de Fortify 1.3.7

Este programa instalará Fortify 1.3.7 en su ordenador.

Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.

Presione Siguiente para continuar.

Siguiente >   Cancelar

NB: Due to the Fortify installer's characteristics, the application is installed for all users on that device, but it only starts automatically if the user who installed it is the administrator. However, any device user can start it (as long as there is no open session "in the background" for another user with Fortify initialized; in that case, that user must first close their session).

Sections 4.2 and 4.3 outline the steps to verify Fortify's startup and the initial authorization procedure once the MIBGAS Platform has been accessed.

Then, if the corresponding option has been chosen, OpenWebStart will be installed unattended (will not present any screen to the user) for all users:

Once the installation has finished, the process will continue with all the other settings of the MIBGAS installer.
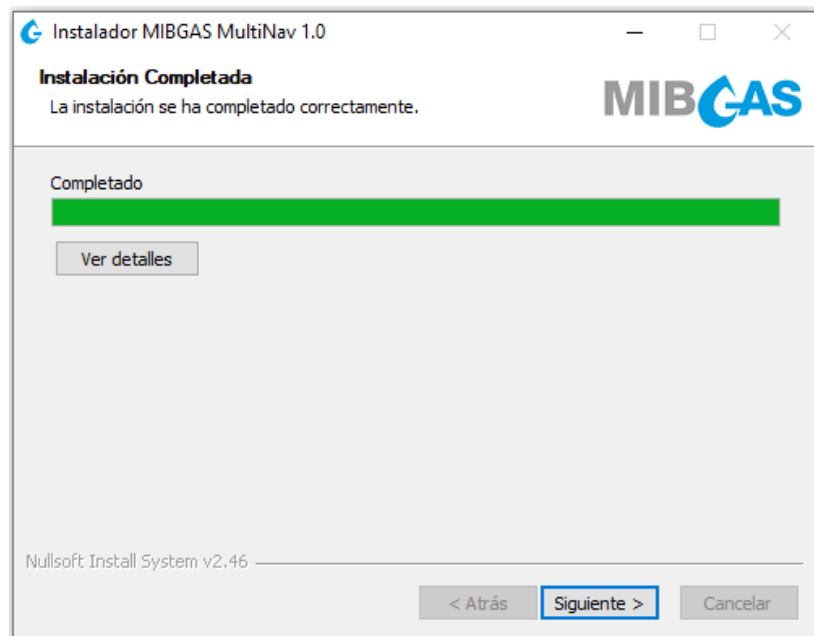
Once the installation process has finished on the client workstation, logging onto the system requires registering the digital user certificate as described in section 5.

In the event of any logon problems following the workstation's automatic setup, see section 4 (Checks on setup problems) and if the problem is not addressed in this guide, there is a document of "*Frequently Asked Questions (FAQs) about the Workstation Setup for the MIBGAS Platform*" located at www.mibgas.es

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 Initial Fortify authorization

The first time the system is accessed by each browser, the Fortify application will request authorization to access the certificate store and associate the selected certificate with the Market Website URL and the browser used. To do this, the screen shown below will be shown. There, you must check that the code shown in both windows is the same, and both must be accepted.
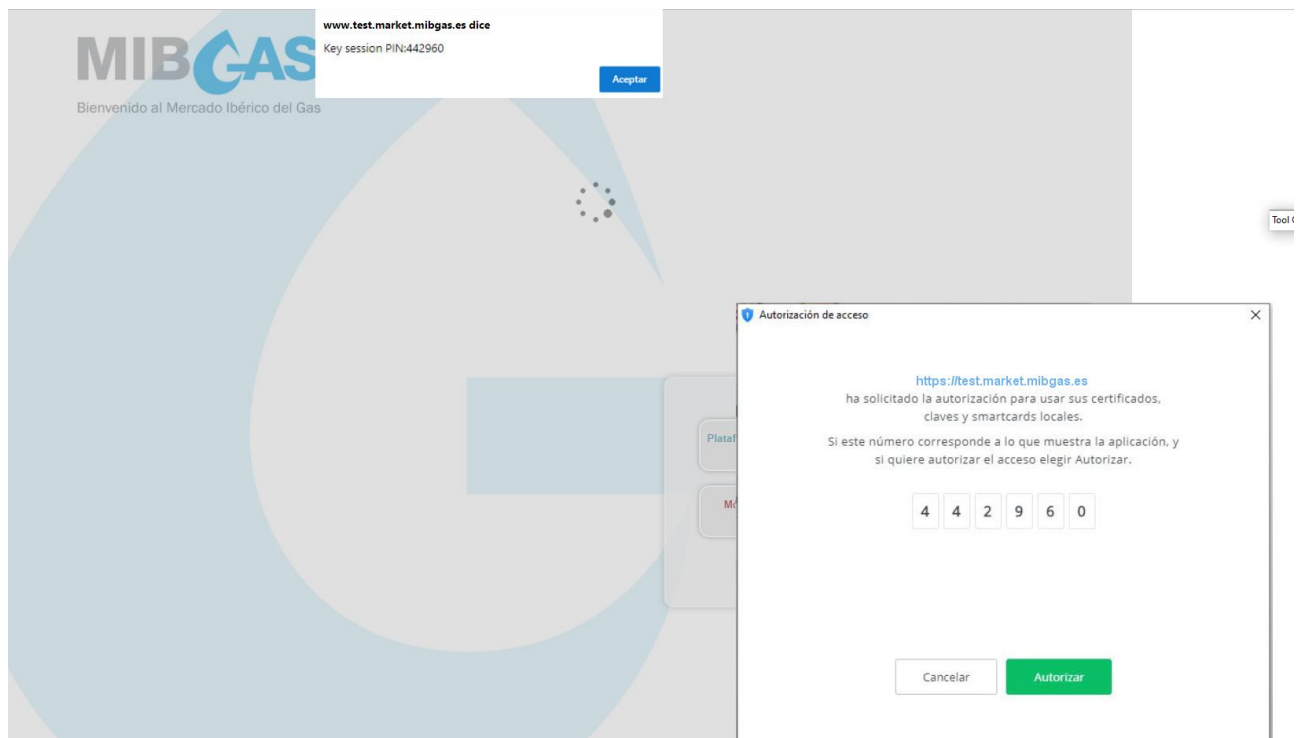
4.2 Fortify start up check

To check that Fortify is running, go to the notification area on the Windows taskbar; there, this icon should be shown:

You can check that it is the version authorized by REE and OMIE by right-clicking to show the 'About' window; there, you should see the message highlighted in the image:
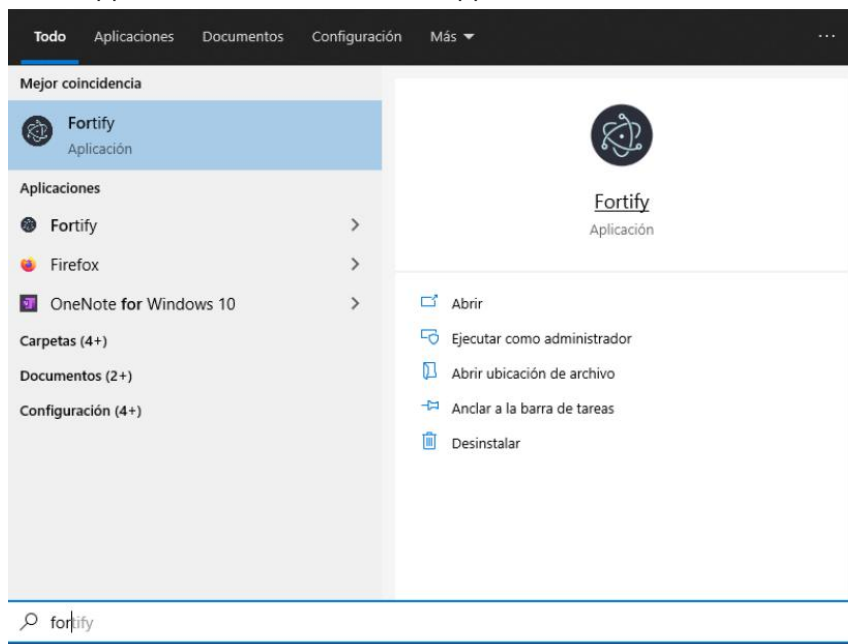
If you can't find that icon in the notification area, you can manually start the application as follows:

» Using Windows finder, type "Fortify" into the text box.
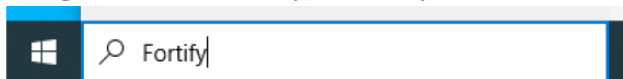
» If the application is installed, it will appear as available to run, like in the image shown.

» If the window's search doesn't find the application, enter the path C:\Fortify and locate the executable Fortify.exe.

If Fortify doesn't start automatically for that user, as would be the case of a user without administrator privileges, a shortcut to Fortify.exe can be added to the startup folder. This way, it will run every time the user logs into Windows. To do this:

» Run the following command: *shell:startup*
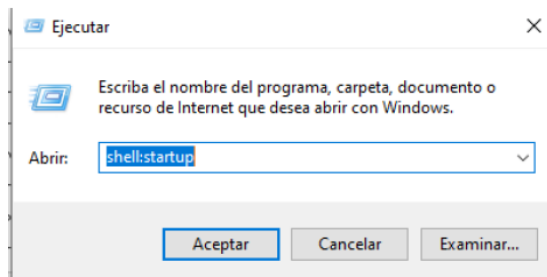
>> A window will open with the user's Home folder. Create the shortcut to Fortify.exe here (very important: create a shortcut, not a copy of the executable):

If a user leaves the session open on a computer with Fortify launched and another user logs in on the same computer, Fortify will display an error message and will not work:
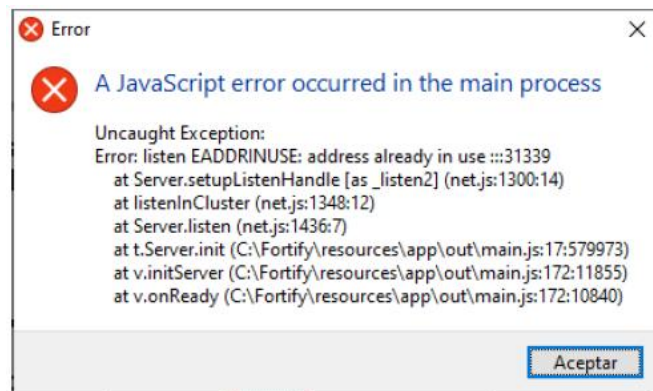

In this case, the first user needs to log out, or the user with this error must close Fortify, thus ending the process, and run Fortify again. Fortify can be closed:

- Through the icon located in the notification area (next to the Windows clock)
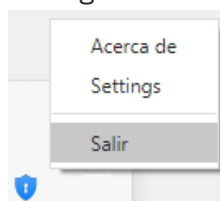
- Forcing fortify.exe processes to close with Windows Task Manager.
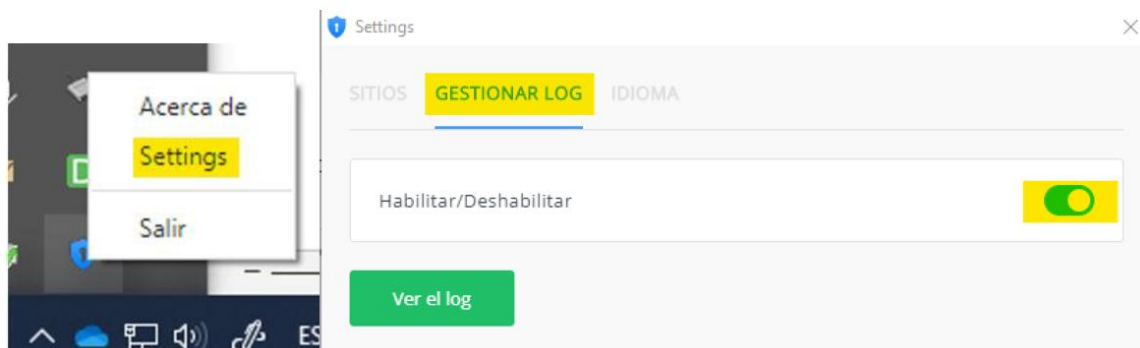
On Fortify's initial startup, it may ask for permissions for the Windows Firewall:
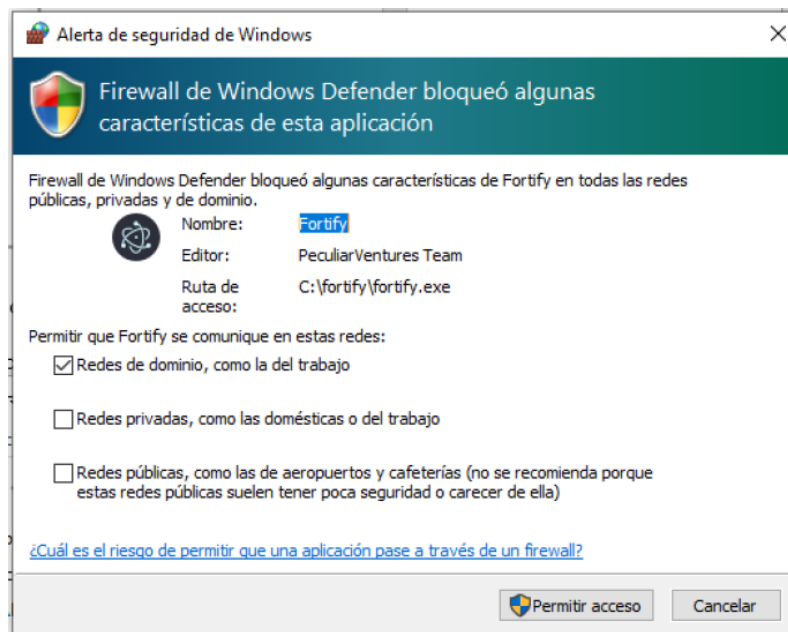
Leave "Network domains, such as work" checked and click "Allow access." Windows will ask for administrator credentials.

Activate Fortify LOGs:

Right-click on the Fortify icon , on the icons next to the Windows Date/Time, and select "Settings."

Click on "MANAGE LOG" and slide the button to the right so that it looks like the upper-right screenshot. Close the window with the "X".

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. The following points detail the installation steps.

Registering the ROOT CA in EDGE (only in case there are any issues).

This step is only necessary if, for whatever reason (generally, the organization's domain/security policies), registering the OMIE Root Certificate fails or if it is removed from the Windows certificate store after the computer is restarted, for instance.
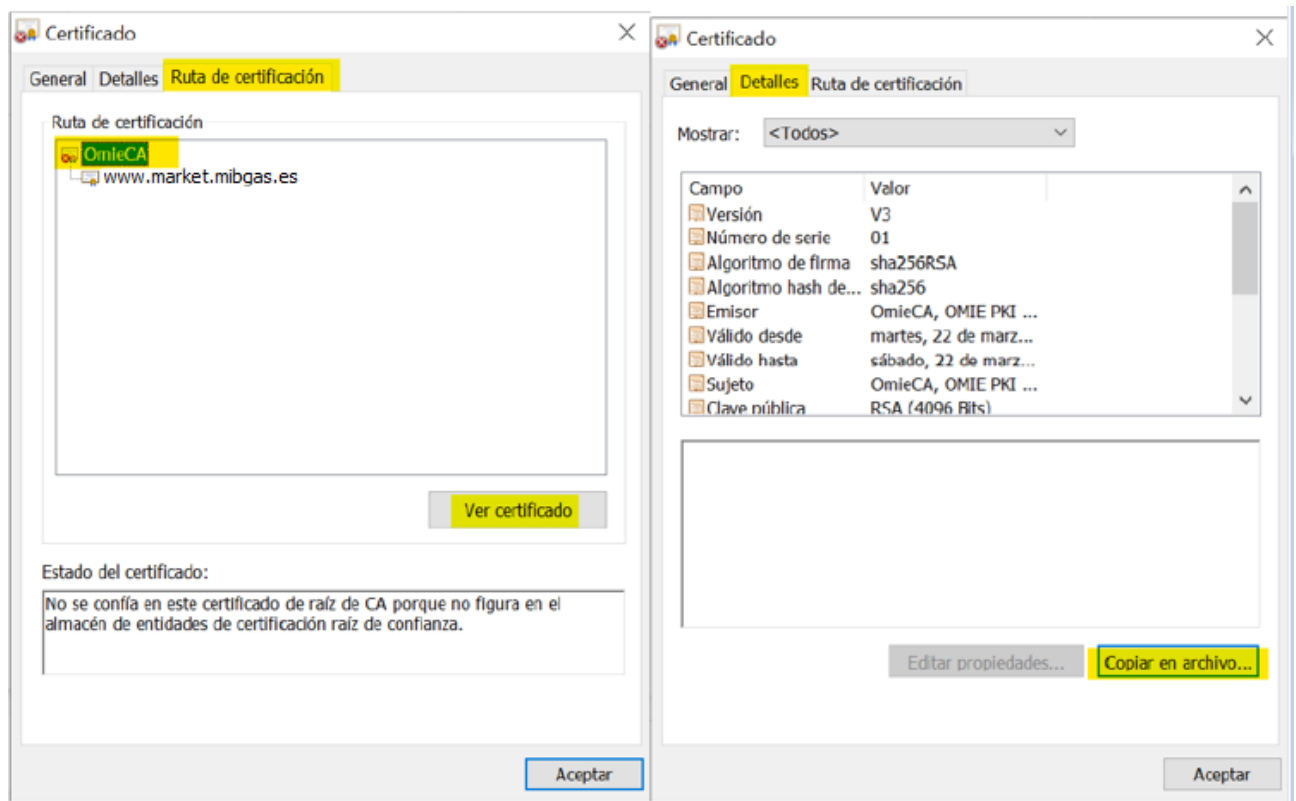
If the OMIE ROOT CA certificate isn't installed, you will get a warning like this one when trying to log into the Market Website:
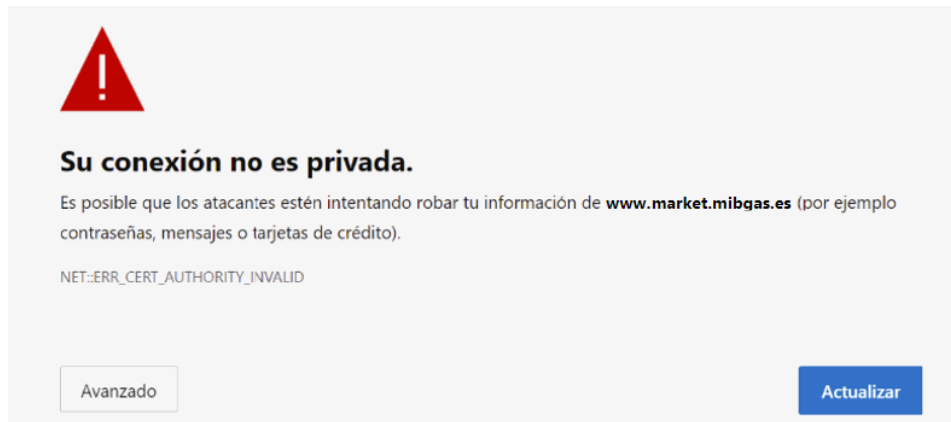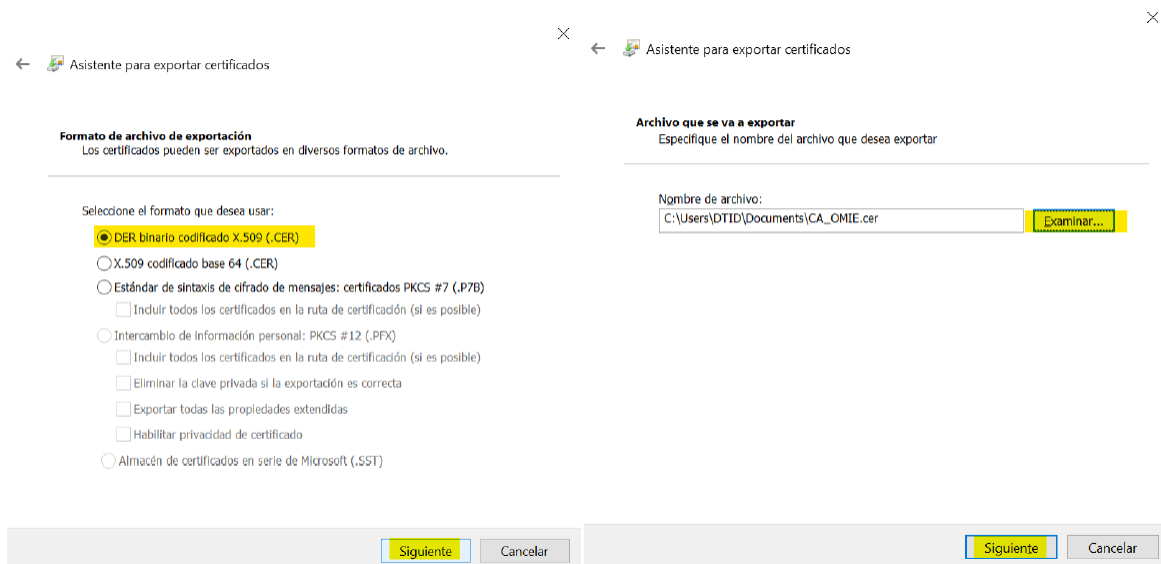

The first step will be to get a copy of this root certificate. To do this:
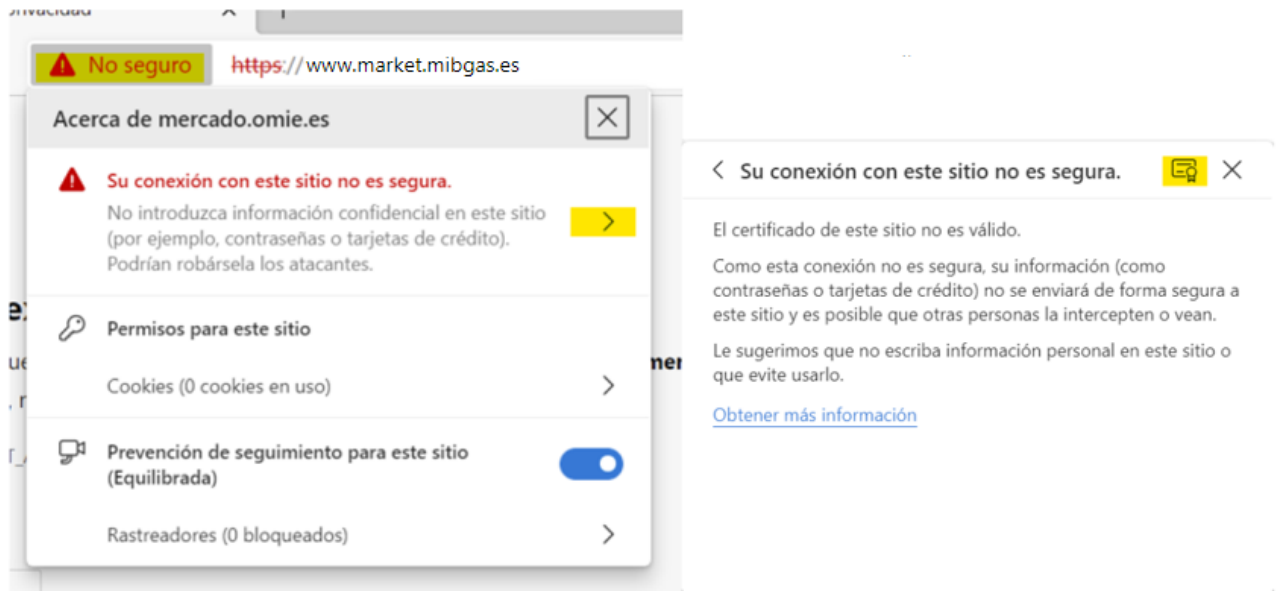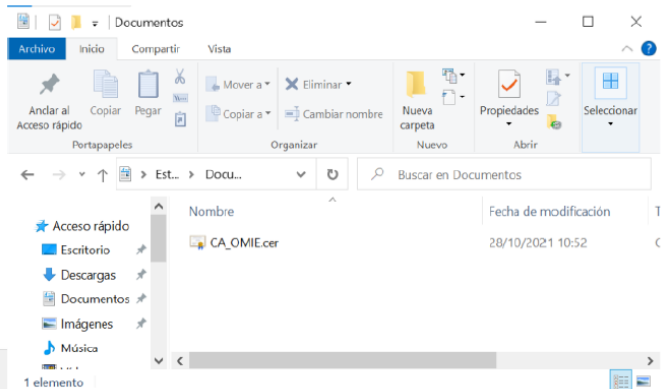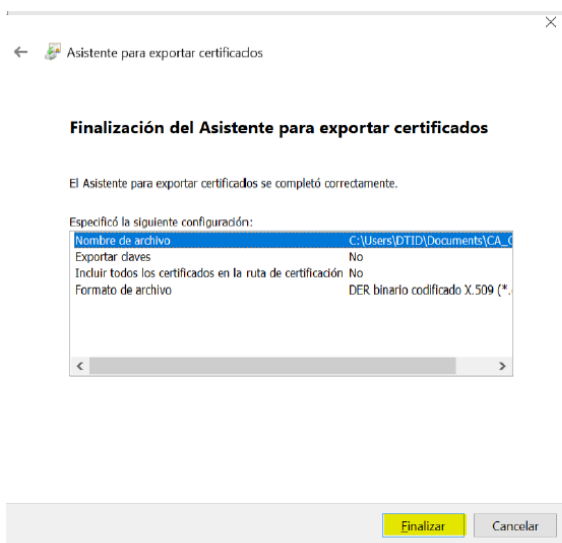

» Click on the "Not secure" warning and on the ">" symbol.
» Click on the certificate symbol:

» Click on "Certification Path," then on the "OmieCA" entry, and on "View certificate."
» Click on "Details" and "Copy to file."

» Select "DER binary…" and click "Next."
» Click on "Browse," find the path where you want to save the certificate, give the file a name (for example, CA_OMIE.cer), and click Next.
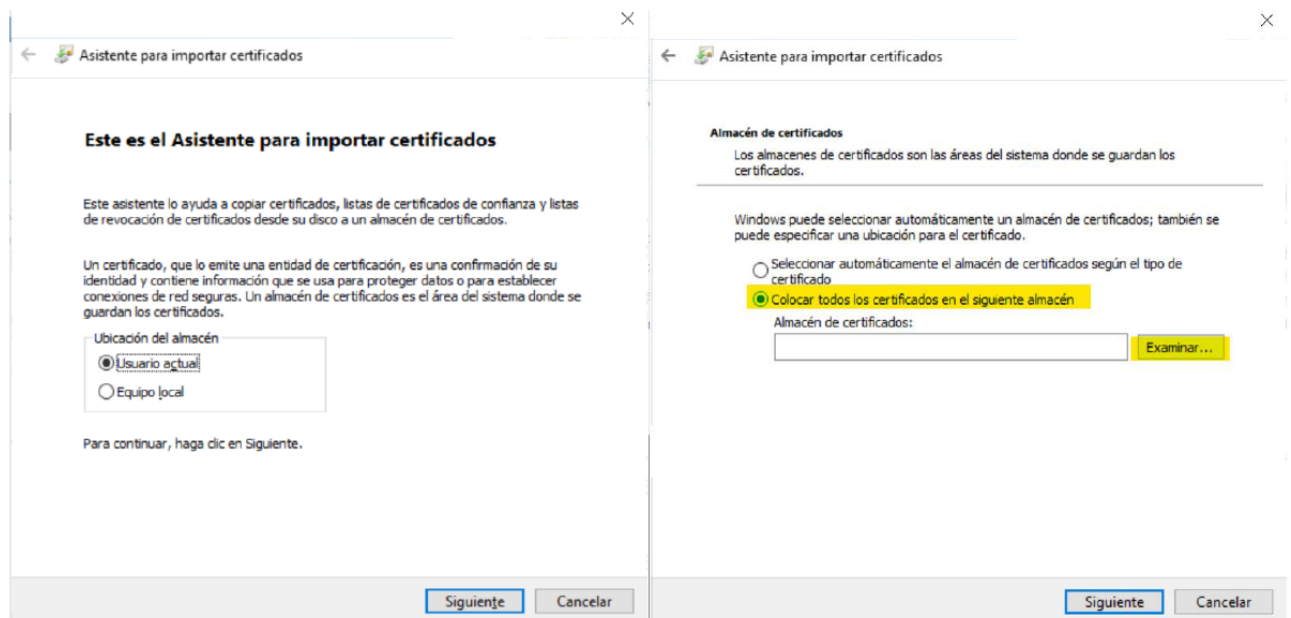
» Click on "Finish."

From this point on, we will have the OMIE Root Certificate to import it or configure it in domain policies.

Importing on a computer would be done as follows:

» Double-click on the file previously created (in the example, CA_OMIE.cer).
» A window will pop-up, click the "Install certificate" button.

» Select one of the two options. If you choose "Local computer," Administrator credentials will be required. Click "Next."
» CRITICAL STEP: Select "Place all certificates in the following store."
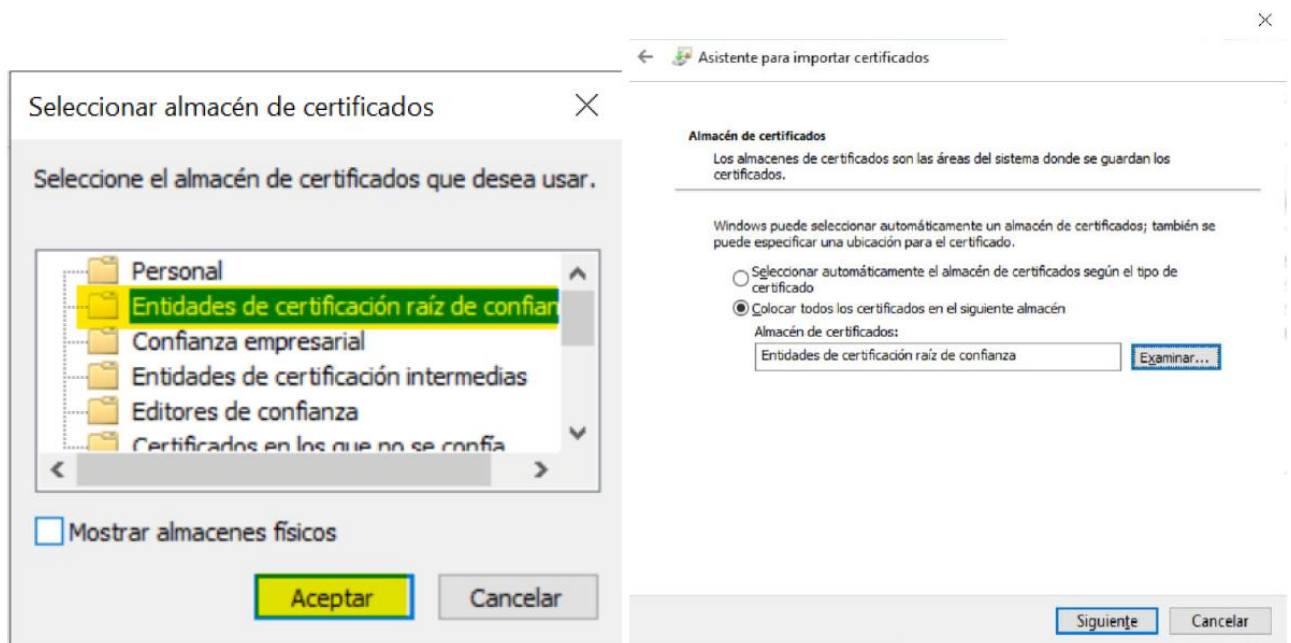
» CRITICAL STEP: Select "Trusted Root Certification Authorities." Click "OK."
» Click "Next."
» In the next window, click "Finalize"
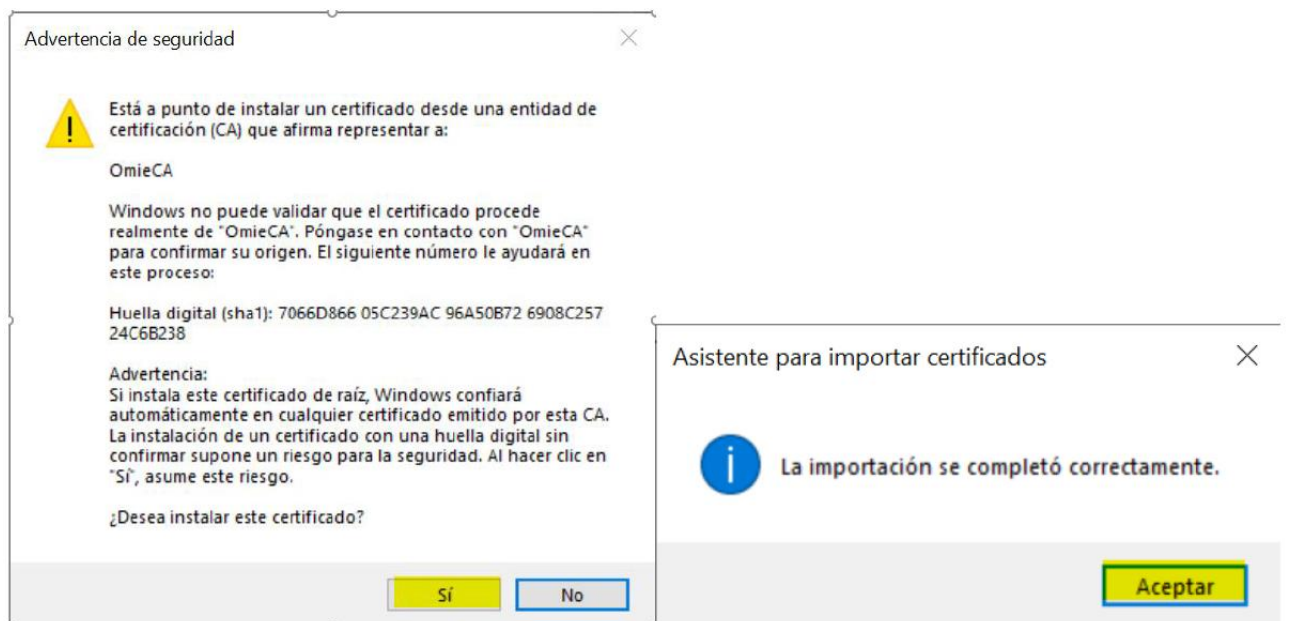
» Click "Yes."
» Click "Accept."

Now, the error displayed at the beginning of this section will no longer occur when accessing the MIBGAS Platform Website.

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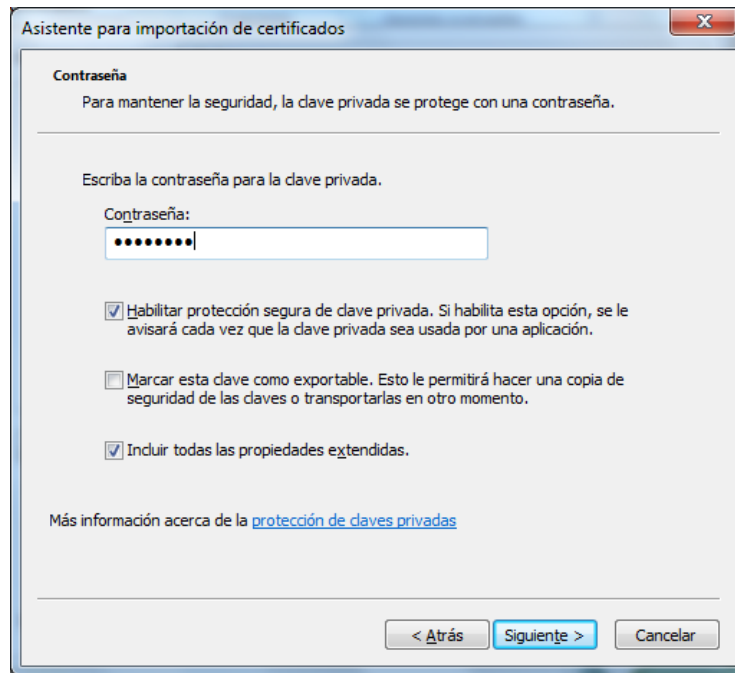
Type the password for the private key provided by MIBGAS, and check the box *"Enable strong private key protection"*.

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

If at any time an error occurs that is not addressed in this guide, please refer to the "Frequently Asked Questions (FAQs) About the Workstation Setup for the MIBGAS Platform" document (Iberian Gas Market: Information system: Access to our system: Technical documentation), located in https://www.mibgas.es/