



Setup Guide for the OMIE Information Systems Access Point

Alfonso XI, 6
28014 Madrid
www.omie.es

Ref. GuiaConfAccesoSistemasOMIE-EDGE_EN.docx

Versión 1.2.3
Fecha: 2023-10-25

CONTENTS

1	INTRODUCTION	3
2	SYSTEM REQUIREMENTS	4
2.1	MAIN COMPONENTS AND VERSIONS	4
2.2	SCREEN RESOLUTION	4
3	USING THE CLIENT WORKSTATION INSTALLER	5
3.1	FORTIFY BOOT CHECK	9
4	MANUAL CONFIGURATION OF THE CLIENT WORKSTATION	13
4.1	INITIAL FORTIFY AUTHORIZATION	13
4.2	CARD READER INSTALLATION (ONLY FOR CARD CERTIFICATES)	13
4.3	REGISTERING THE OMIE ROOT CA CERTIFICATE	14
4.3.1	<i>Registering the ROOT CA in EDGE (only in case there are any issues).</i>	14
4.4	REGISTERING A USER CERTIFICATE	19
4.4.1	<i>Certificates on smart cards</i>	19
4.4.2	<i>Software certificates</i>	21
4.5	OPENWEBSTART	23
5	COMMON ISSUES	24

1 INTRODUCTION

This guide describes the requirements for accessing the OMIE Information Systems at a client workstation and the necessary steps to start using the Web environments of the Electricity Market's Information System (hereinafter, SIOM).

The SIOM Web environments require using user certificates provided by OMIE either in smart card format or in a file format (software certificate) to log in.

To set up the client workstation, the Client Workstation Installer will be used to access the OMIE Information Systems. By using this installer provided by OMIE, the installation process is automated, minimizing the manual actions that have to be carried out.

It does not include sections for installing standard software and in a client hardware components, such as the operating system, a browser, or the hardware installation of the card reader. However, the necessary requirements in terms of versions, as well as some details on their configuration for proper operation, are provided in detail in the following sections. For basic product installation, you must refer to the respective installation guides or help.

Note: *EDGE is the recommended browser, and OMIE will offer support for it. Though accessing the market may be possible with other browsers, they are not officially supported by OMIE as they are not specifically tested for it.*

Note: *If the user is setting up a new machine and wants to have access to both **MIBGAS** and **OMIE's** services, they will need to run only one of the installers (it is indifferent which one).*

If the device is already configured to access MIBGAS services with EDGE, you can continue with the steps in this guide. The installer will not reinstall components detected as already installed.

2 SYSTEM REQUIREMENTS

2.1 Main components and versions

The main software and hardware components required to use the SIOM Web environments are the following:

- Operating system:
 - Windows 10
 - Windows 11 (recommended)
- Browser:
 - Microsoft Edge (supported and recommended browser)
- Card reader (only for card certificates)
- Registration of the certificates to be used.
- Installation of the OMIE Root CA.
- The Fortify app (included in the OMIE web installer) for the digital signature of deliveries.
- Open Web Start (included in the OMIE web installer). Required to run the Download Center; which when first run, it will install the necessary version of the Amazon Corretto Java Virtual Machine, distributed by OMIE.

These requirements are described in more detail below, along with additional configuration options.

2.2 Screen resolution

The website was designed for an optimal configuration of **1280x1024 pixels and 65536 colors**.

The following are recommended as maximum display settings:

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

3 USING THE CLIENT WORKSTATION INSTALLER

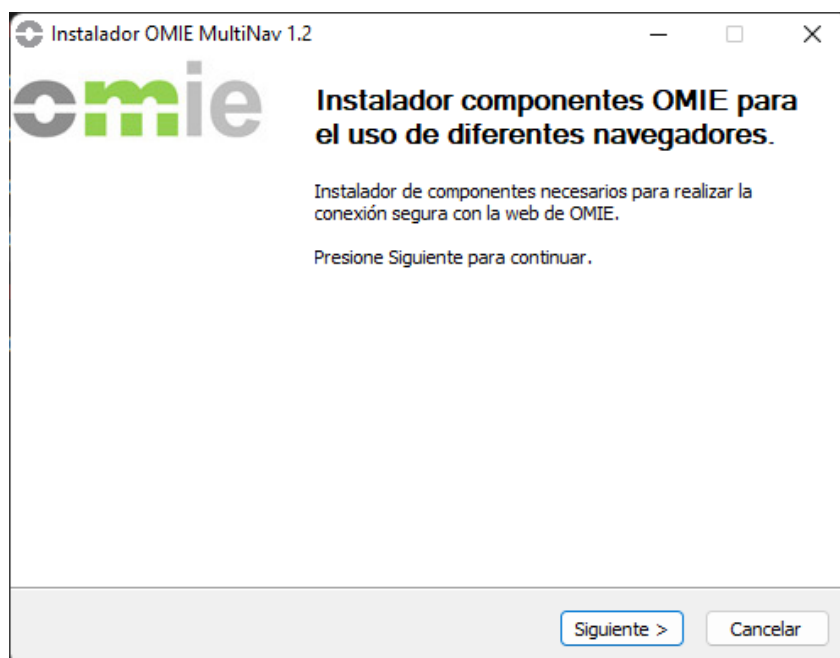
The installer provided by OMIE ([OMIE_Setup_EDGE.zip](#)) automates the installation process, minimizing the manual actions that have to be done. This installer can be downloaded from OMIE's Public Website ([www.omie.es](#)→Publications).



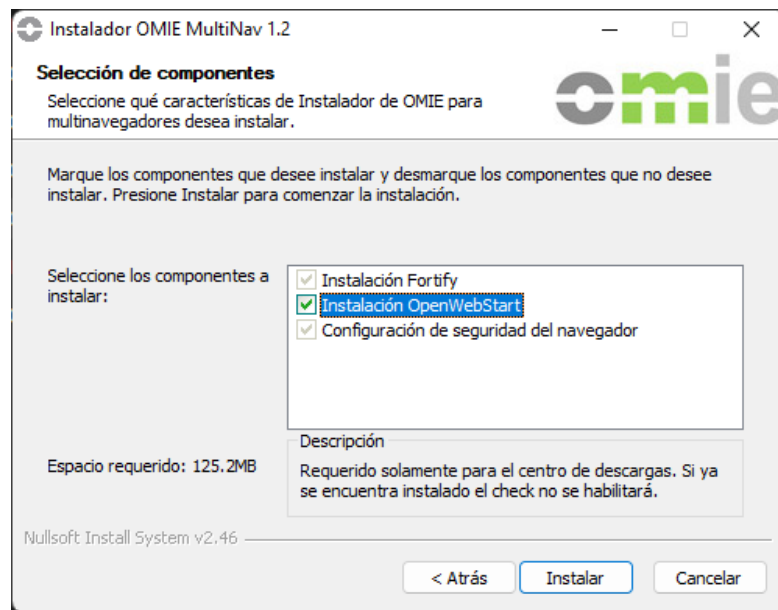
Extract the file from the ZIP folder and run.

Note: If the active user on the computer doesn't have administrator permissions, the window for entering administrator credentials will first appear.

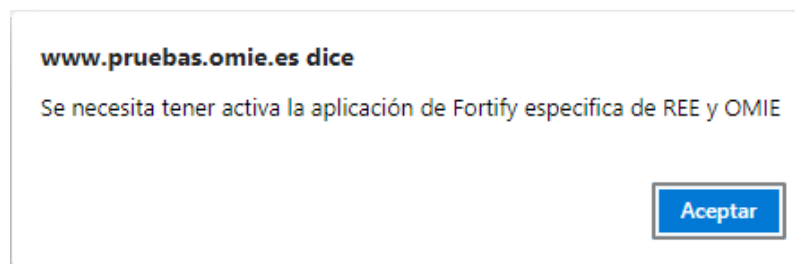
On startup, the installer looks like this:



When you press “Next,” the window with options for the features to install will appear. If the installer detects that any of the components is already installed, it will be unchecked and will not be checked unless that component is uninstalled first:



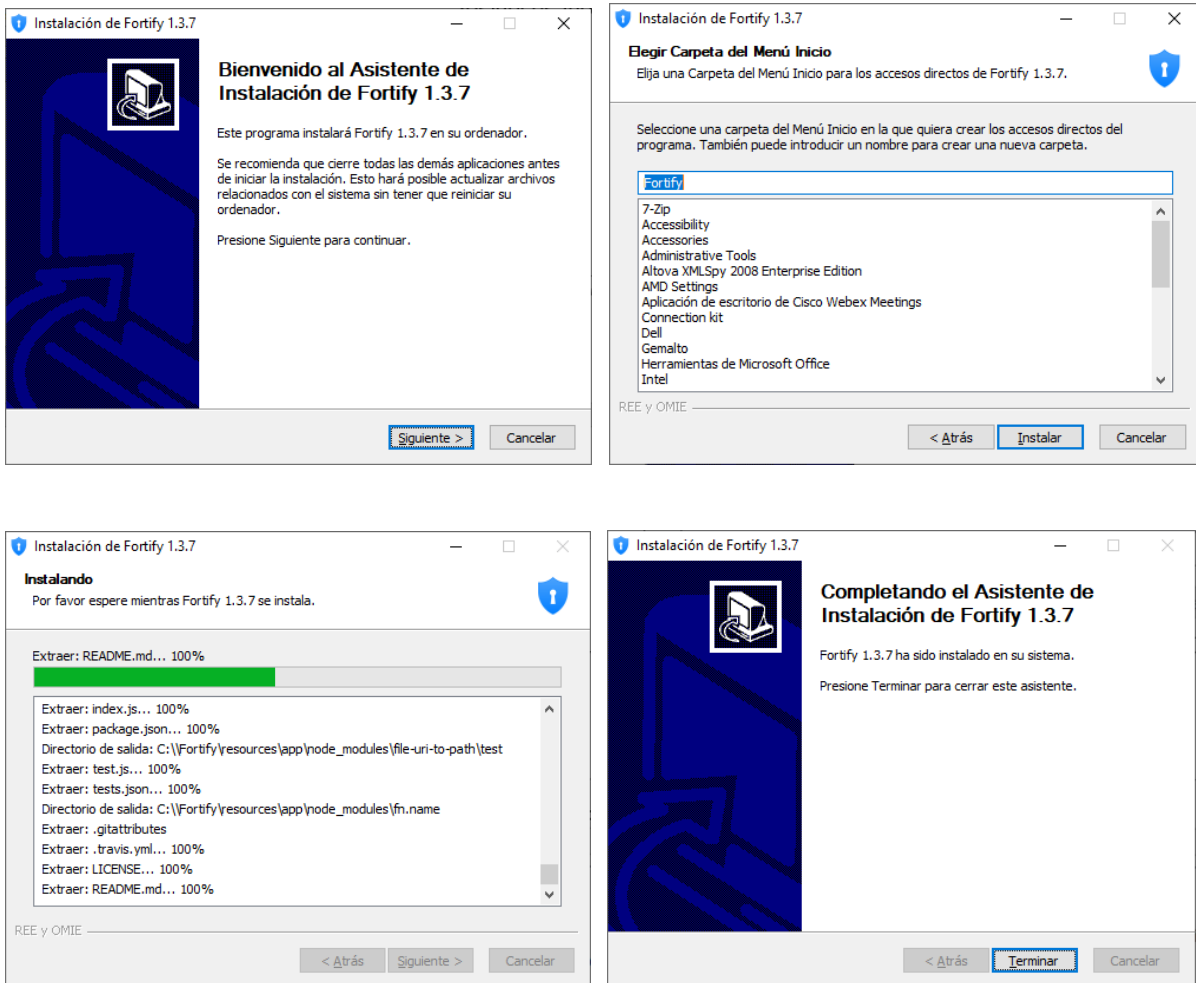
If you access the system without having any version of Fortify installed or running, a screen will appear informing you that you need to have the Fortify application installed.



Installing OpenWebStart is only necessary if the Download Center 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:



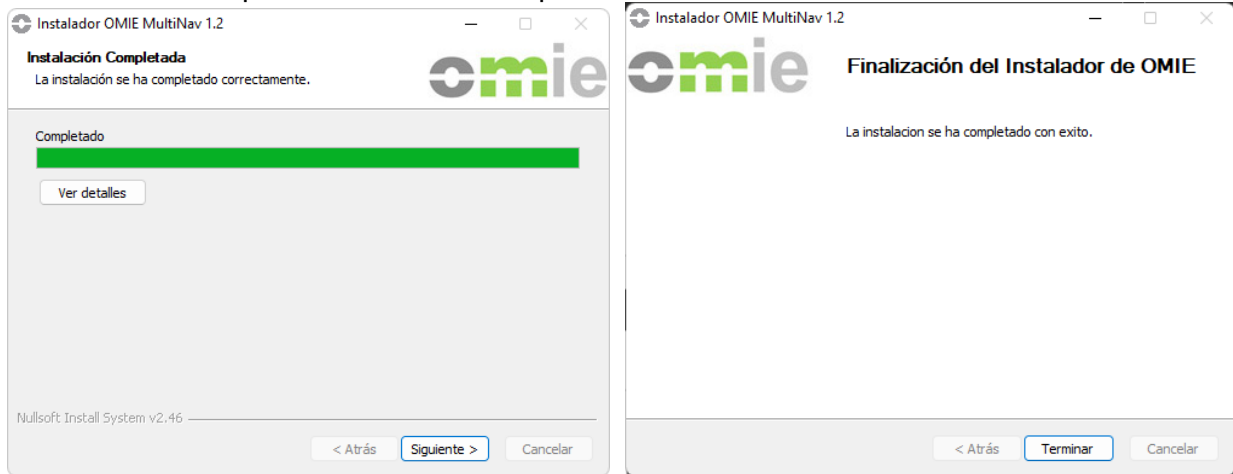
Note: Due to the Fortify installer's characteristics, the application is installed for all users on that device, but it only starts automatically if the user who installed it is the administrator. However, any device user can start it (as long as there is no open session "in the background" for another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

Sections 3.1 and 4.1 outline the steps to verify Fortify's startup and the initial authorization procedure once the SIOM website 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:


Note: The document, "Download Center User Manual," describes the startup mode for the Download Center; for this, OpenWebStart must be installed.

This is the last step in the SIOM installer process.



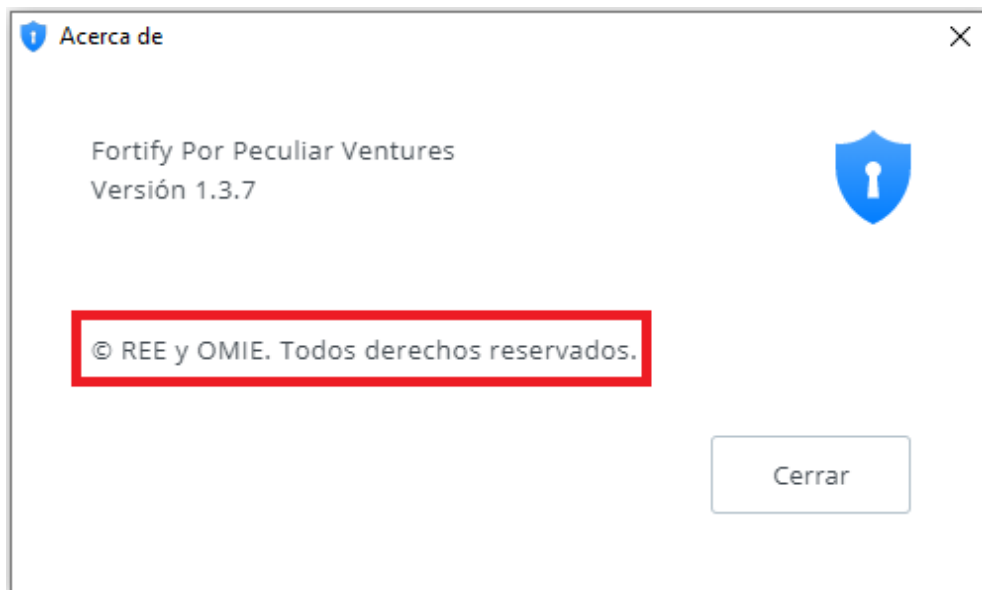
Note: Restarting the computer is recommended afterward to see if Fortify loads at startup. See section 3.1 of the guide.

3.1 Fortify boot check

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

Note: *In case of doubt, it is recommended to restart the equipment first and check if, after starting, the icon appears. In the case of a user with administrator privileges (case of local Administrator or a single user on the computer) it should be started by default. Otherwise, it is recommended to follow the steps indicated in point 3.2.*

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:

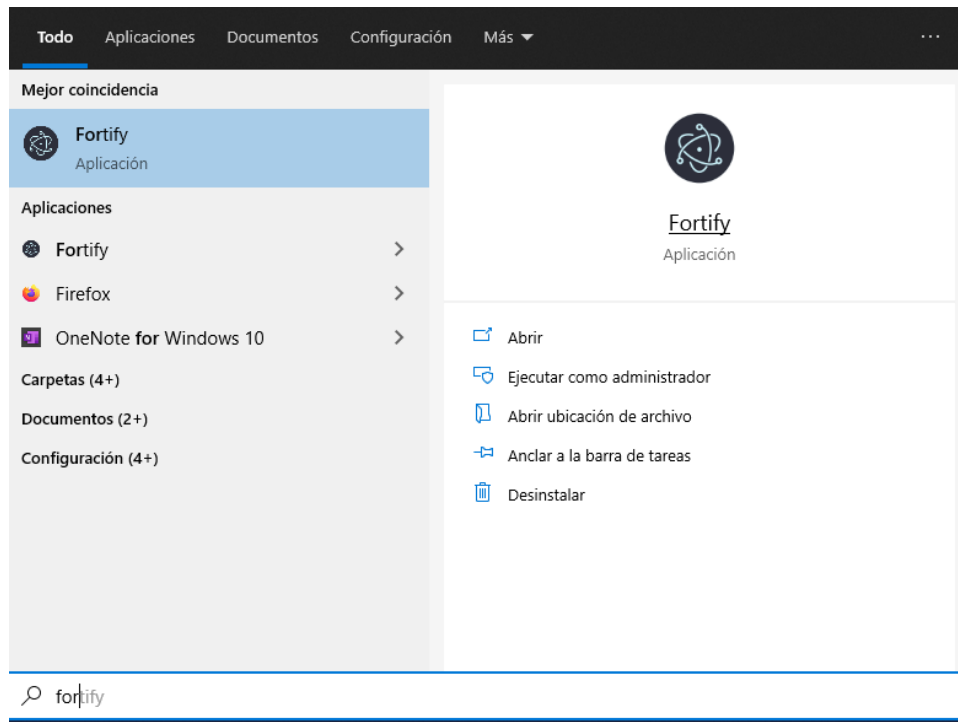


If you can't find that icon in the notification area, you can manually start the application as follows:

1. Using Windows finder, type "Fortify" into the text box.

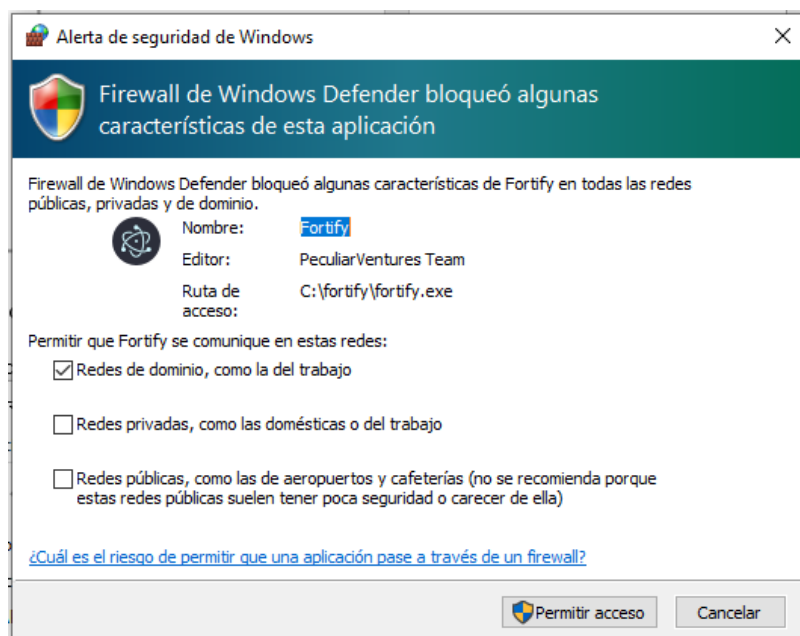


If the application is installed, it will appear as available to run, like in the image shown.




2. If the application doesn't appear in the search, enter the path *C:\Fortify* and locate the executable *Fortify.exe*.

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 , then on the icons next to the Windows Date/Time, and select "Settings."

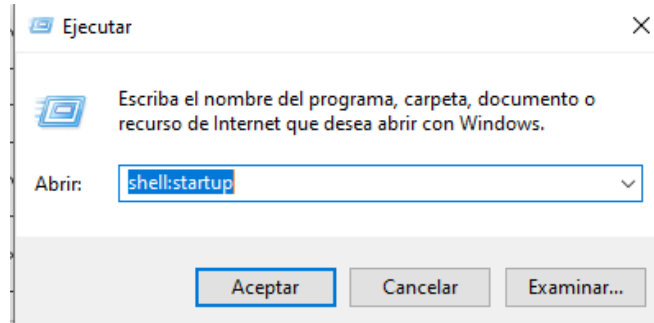


Click on "MANAGE LOG" and slide the button to the right so that it looks like the upper-right screenshot. Close the window with the "X."

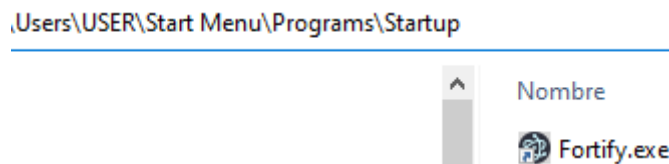
3.2 Additional steps for a user without administration privileges

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:

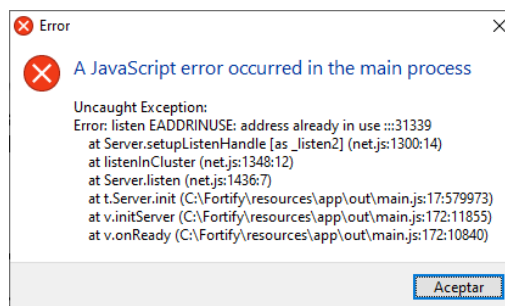
1. Run the following command: `shell:startup`



2. 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 the Javascript error message EADDRINUSE and will not work:



In this case, the first user needs to log out or at least close Fortify.

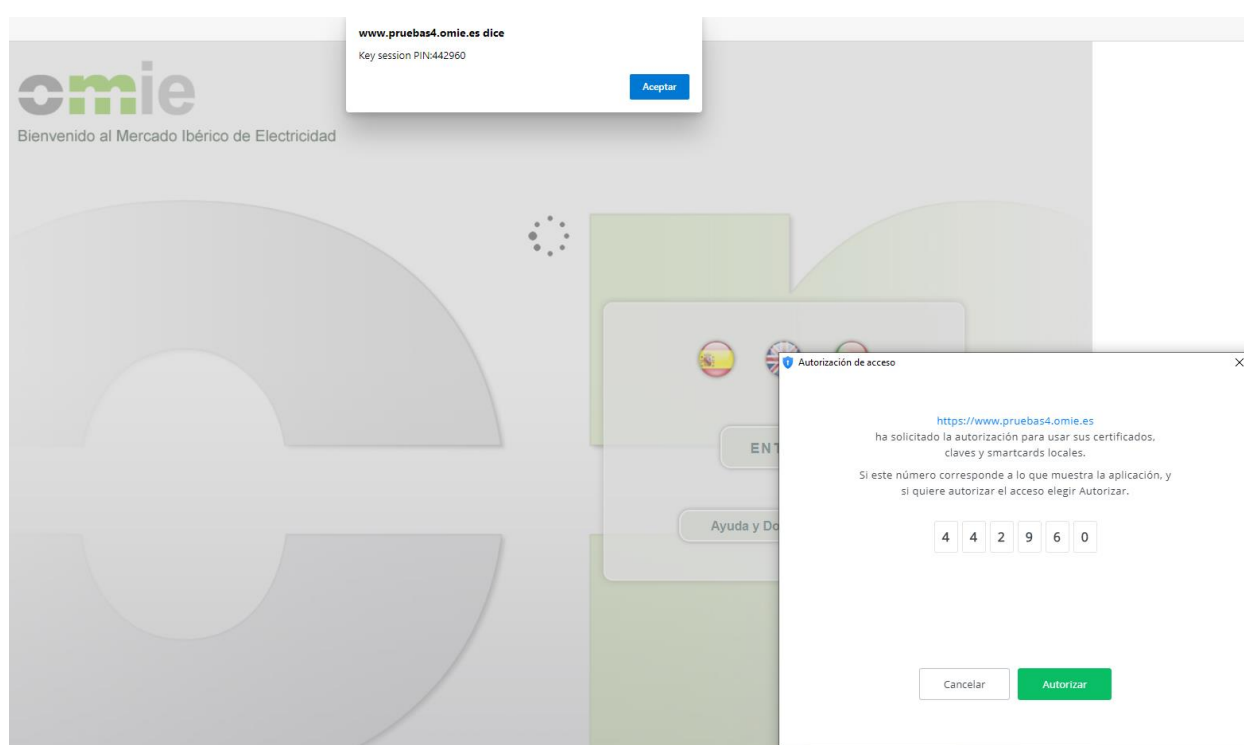
Nota: The same error can be replicated if the user with administrator privileges takes the step of putting a shortcut to Fortify in their Startup folder, in which case to reverse it they must remove the shortcut from the previous folder.

4 MANUAL CONFIGURATION OF THE CLIENT WORKSTATION

This section provides additional information that may be needed for the proper configuration of the client workstation.

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 appear. There, you must check that the code shown in both windows is the same, and both must be accepted.



4.2 Card Reader installation (Only for Card Certificates)

To access SIOM websites, it is necessary to have an individual X.509 security certificate, which OMIE issues either in Gemplus smart card format or in a file. When using card certificates, a smart card reader is necessary.

The user can use any reader compatible with the PC/SC standard that has the Gemplus software installed. The steps to follow are outlined in the ['Gemplus Software Installation Guide for Accessing SIOM.'](#) which is provided as a separate document. It is necessary to have the reader installed and to be able to use the security card with the browser to proceed with the following setup steps for the station.

4.3 Registering the OMIE ROOT CA certificate

The client workstation installer installs the OMIE ROOT CA for Edge. However, also, due to domain policies applied at the agent's workstation, the installation of this certificate could fail during installation.

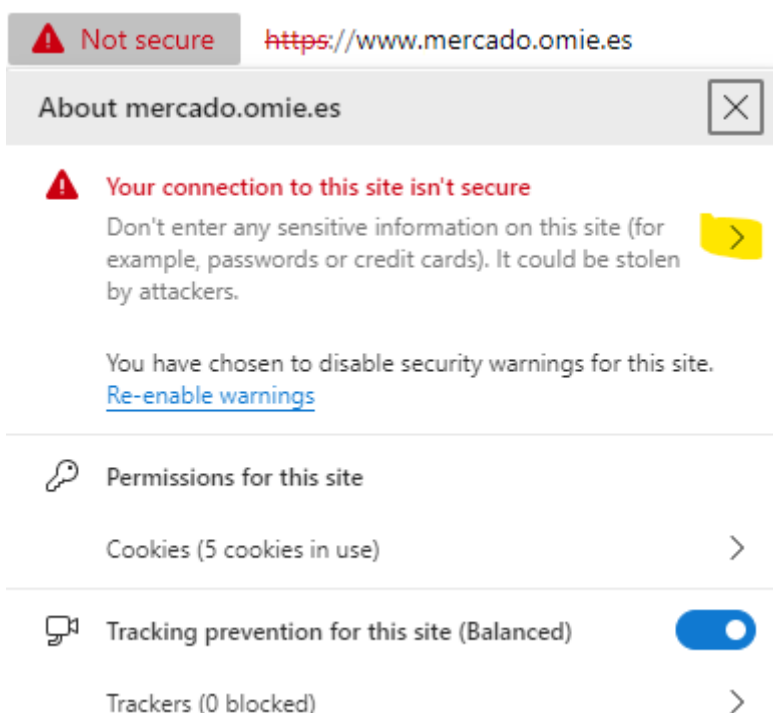
4.3.1 Registering the ROOT CA in EDGE (only in case there are any issues).

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 notice 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:




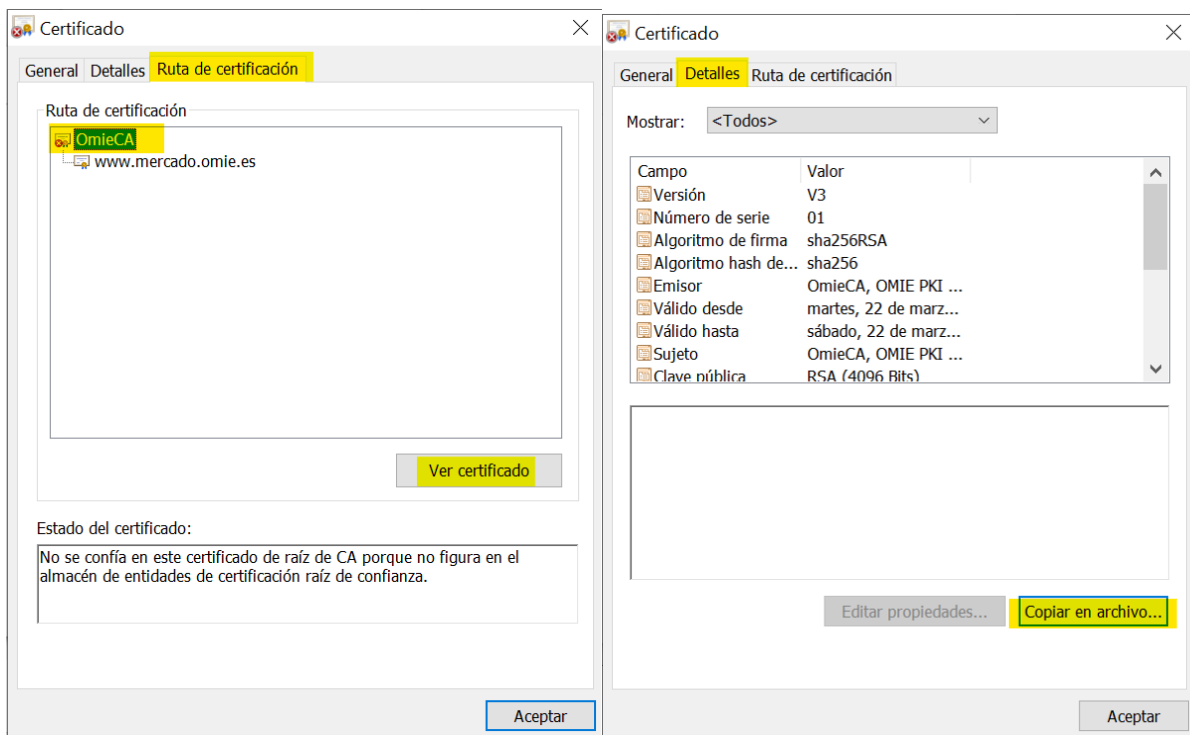
The certificate for this site is not valid.

Because this connection is not secure, information (such as passwords or credit cards) will not be securely sent to this site and may be intercepted or seen by others.

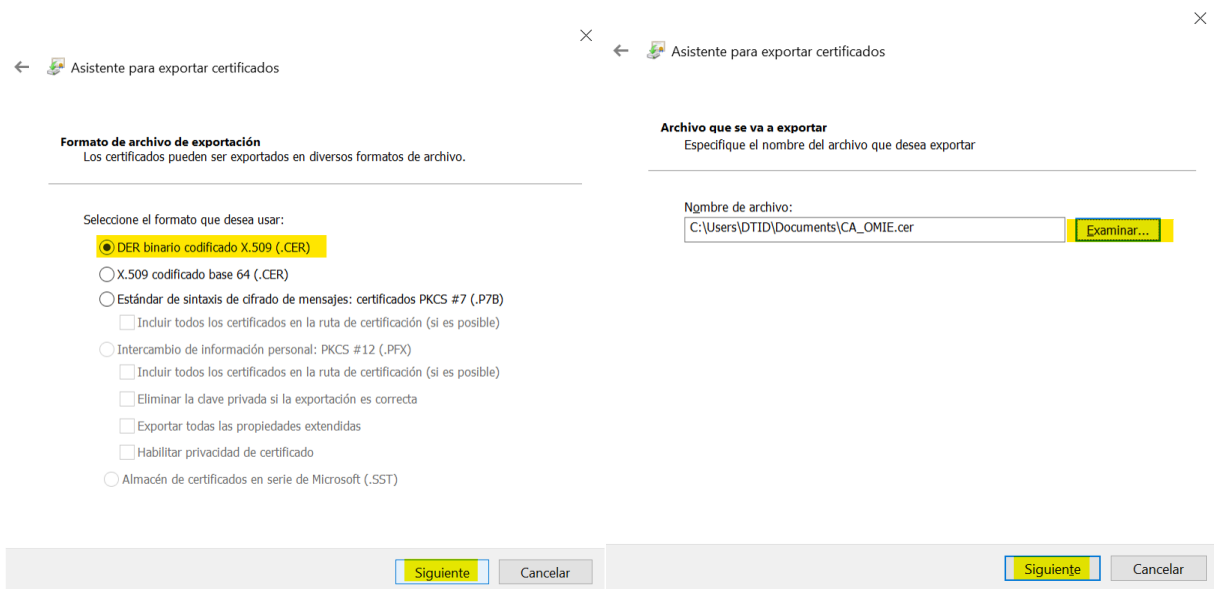
We suggest you don't enter personal information into this site or avoid using this site.

[Learn more](#)

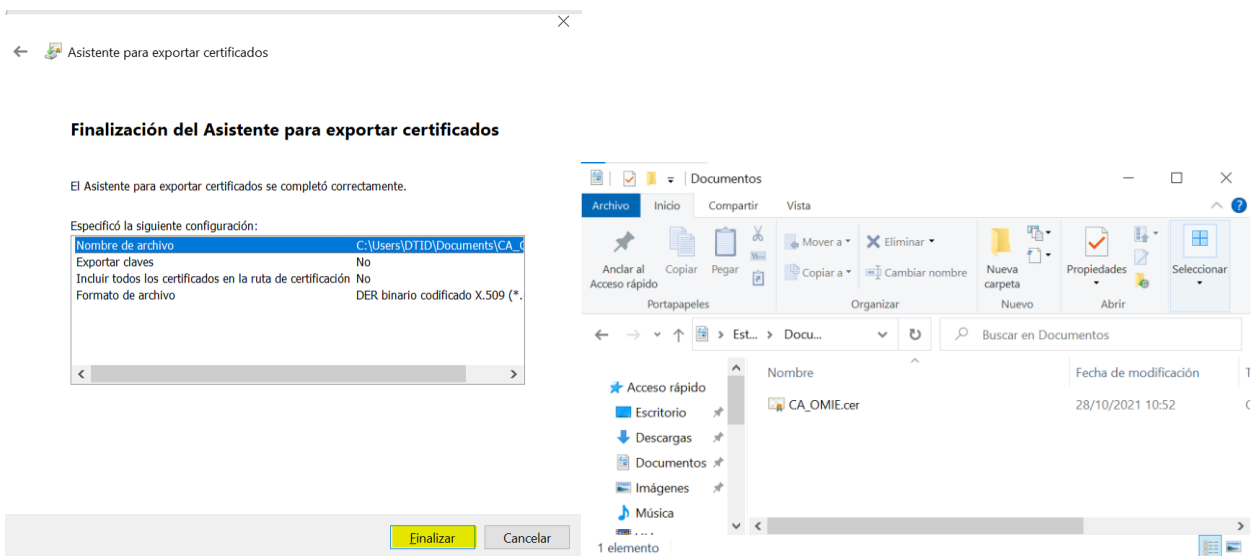
- Click on the “Not secure” warning and on the “>” symbol.
- Click on the certificate symbol: 



- 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.

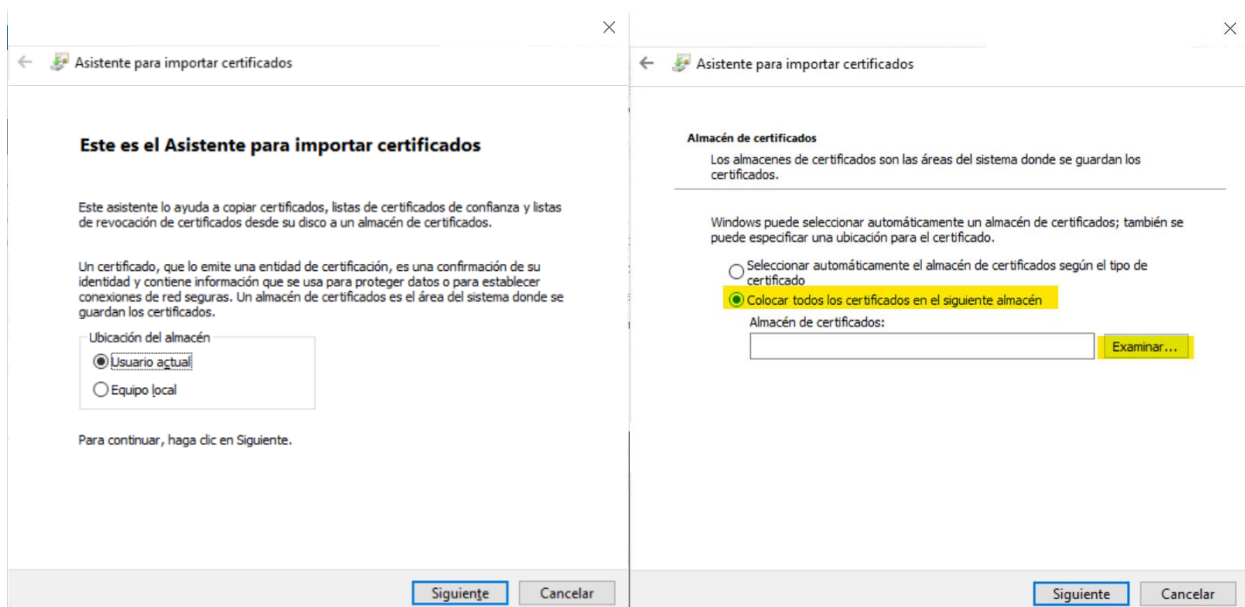


- Click on “Finish.”

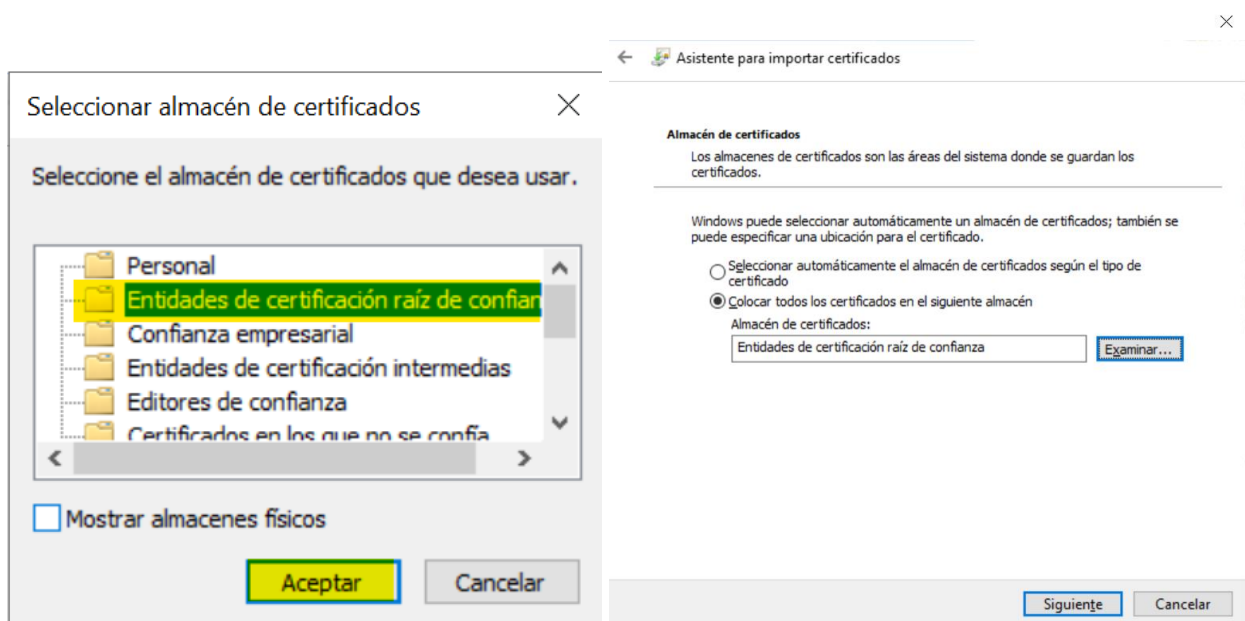
From this point on, we will have the OMIE Root Certificate to import it or configure it in domain policies.

Importing on a computer would be done as follows:

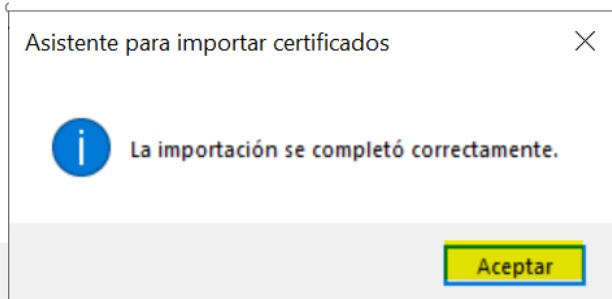
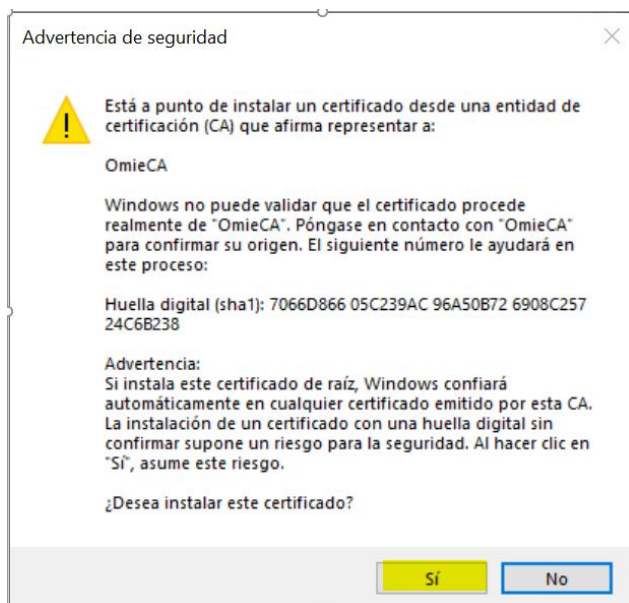
- Double-click on the file previously created (in the example, CA_OMIE.cer).
- In the window that appears, click the **Instalar certificado...** button.



- 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 **Finalizar**.




- Click "Yes."
- Click "Accept."

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

4.4 Registering a User Certificate

4.4.1 Certificates on smart cards

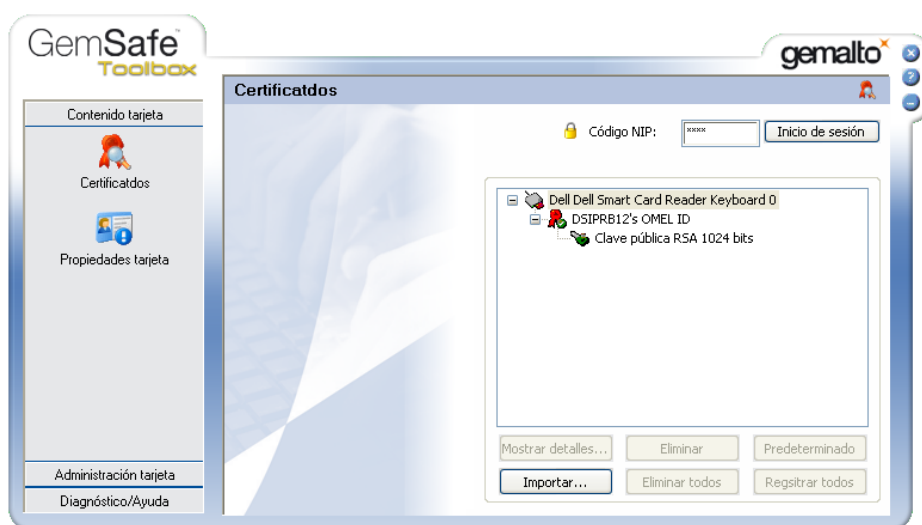
Note: This is only necessary if the computer doesn't automatically start the "Regtool" application included with the GemSafe software . If this application is launched, the software itself is responsible for registering the certificate in the Windows store when a card is inserted and unregistering it when it is taken out.

When using a new security card for the first time at a user workstation, remember that **it is necessary to register the certificate delivered on the card in Windows** so that it can be used from the browser (this is a requirement for Internet Explorer). This is how to register a user certificate through the Card Reader software:

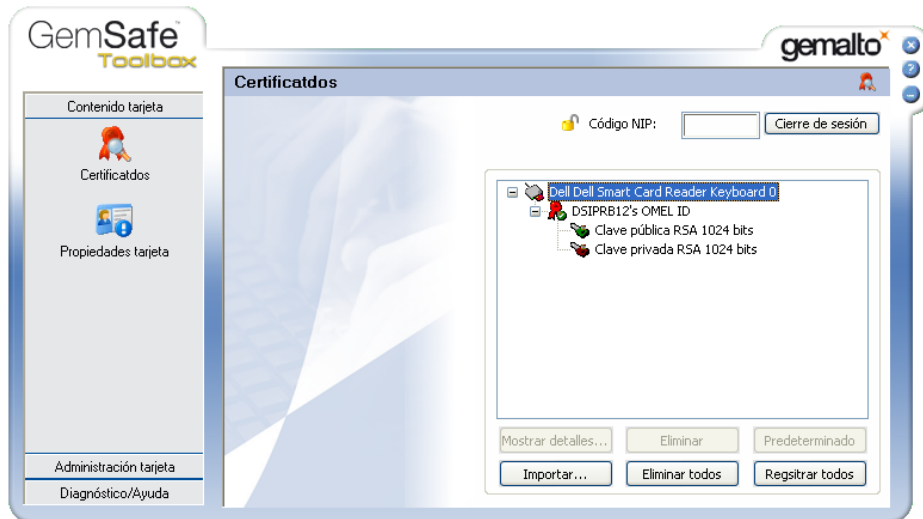
Insert the card in the reader and start the *GemSafe Toolbox* program from Windows:



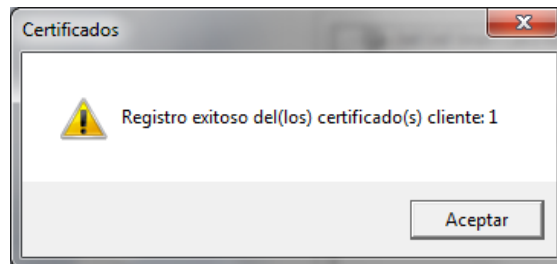
Click on *Card content* → *Certificates* and enter the card's PIN in the *PIN Code* section. Press the *Log-in* button to log in:



To register the certificate, select the cardholder icon and then press the *Register all* button:



After a few seconds, the following screen will appear, indicating that the certificate has been registered.



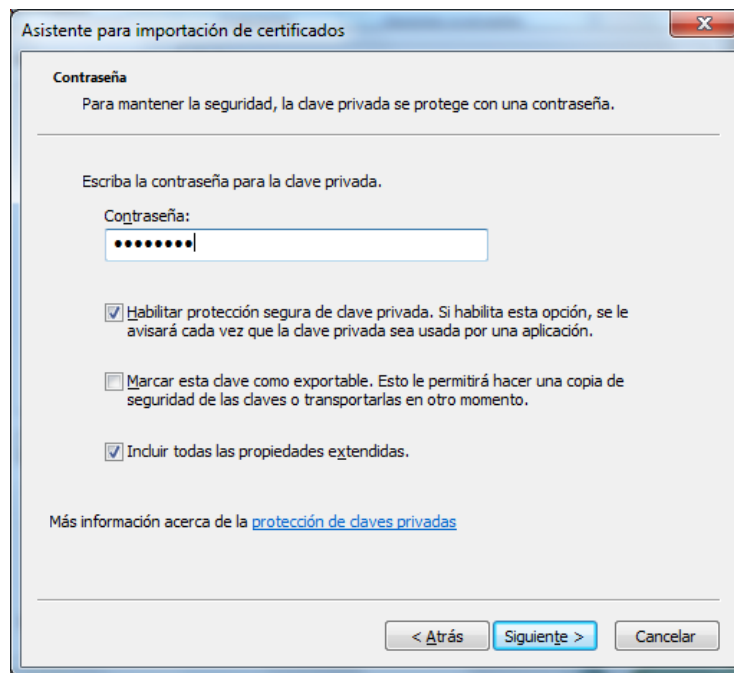
Click *OK*. The certificate registration process is complete.

4.4.2 Software certificates

Certificates in file format, or software certificates, are delivered in “.p12” format (PKCS #12 standard). To register certificates provided in this format, you must follow the steps outlined below.

Download the “.p12” file in a directory that’s accessible from the workstation where the certificate is to be registered. Select the file and double-click to activate it.

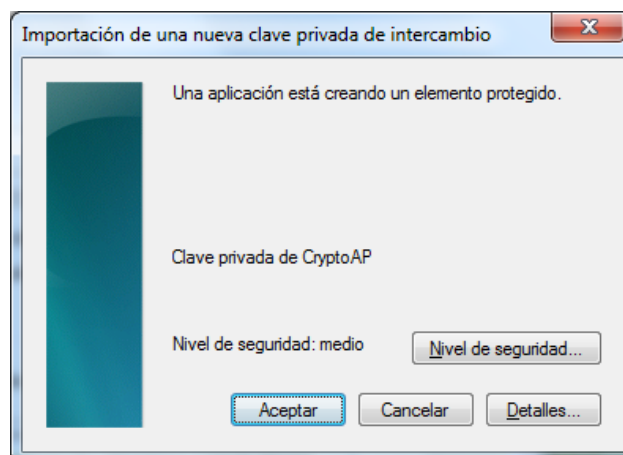
For a more secure configuration, it is recommended to follow the steps that appear on the screen using the default options until you reach the following screen (by default the first option “Enable strong private key protection” will be unchecked):



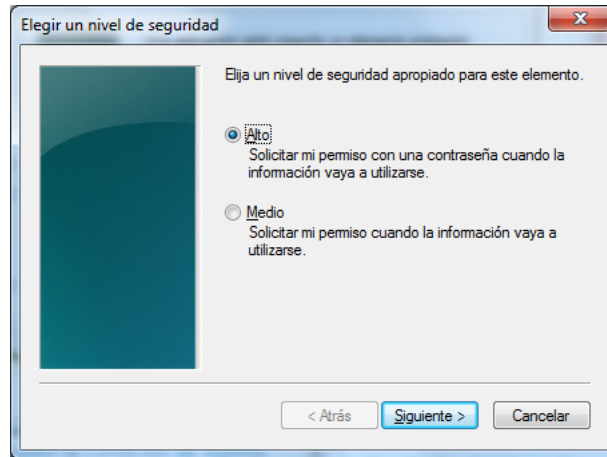
Enter the password for the private key provided by OMIE, and check the box “Enable secure protection of private keys.”

Note: If you choose not to check this box, continue to the next window and click on Finish.

Continue with the default options until the following screen:



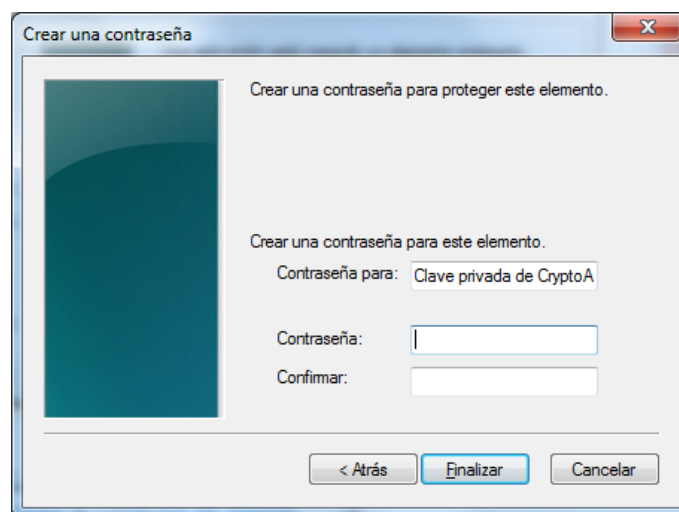
Click on “Security level...”:



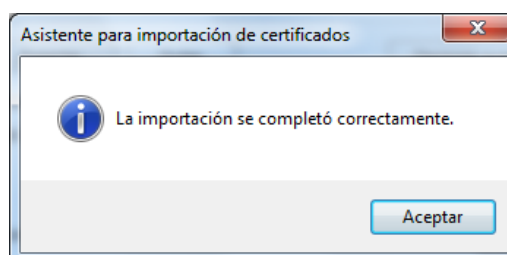
On this screen, you can select a “Medium” or “High” security level to set up the system’s behavior when using the certificate for accessing SIOM or signing delivery of information.

- For the “Medium” level, the browser will only show the user a warning to confirm access to the private key.
- For the “High” level, the browser will also request to choose and insert a password to access that private key.

It is recommended to select the “High” level and choose a password that will be used as a PIN for accessing the system and signing the data to be sent. In this case, when you click on “Continue,” the following screen will be shown; there, you can enter and confirm the chosen password (it will not be known by OMIE).



After clicking on “Finish” and then on “OK,” a message indicating the end of the process will be shown.



4.5 OpenWebStart

The installer automatically performs the necessary configuration for the operation of the Download Center.

In the document "[Download Center User Manual](#)" ([OMIE | Publications: Technical Documentation](#))", point 2.2, there are some optional manual configuration steps detailed.



5 COMMON ISSUES

If at any time an error occurs that is not addressed in this guide, please refer to the [“Frequently Asked Questions \(FAQs\) on Setting Up the OMIE Information Systems Access Point”](#) document ([OMIE | Publications: Technical Documentation](#)).

