Station Setup Guide to Access OMIE Information Systems

INDEX

1   INTRODUCTION

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

SIOM websites require *Microsoft Internet Explorer* browser and *Java Plug-in* for running Java components in the browser. Likewise, it is required to access using user certificates provided by OMIE, either on smartcard or file (software certificate) support.

For the configuration of the client station the Client Station Installer will be used to access OMIE Information systems. Using this installer provided by OMIE, the installation process is automatic, minimizing manual actions that need to be performed.

There are no sections on the installation of hardware and standard software components, such as the operating system, browser, or the hardware installation of the card reader. However, the following paragraphs outline the necessary requirements as regards versions and some setup details for the same to ensure proper working. For the basic installation of products, you should consult their installation or help guides.

2 PRE-REQUISITES

2.1 Main components and versions

The main software and hardware components required for the SIOM Web Sites are the following:

- Operating system:
  - Windows 7
  - Windows 8 / 8.1
  - Windows 10 (recommended)

- Microsoft Internet Explorer browser
  - Versions 10 and 11 (recommended), all of them for 32 bits
  - Auctions Web sites allow also Internet Explorer 8 / 9

> *Note:* Windows 8 offers two browser experiences, a touch-optimized, modern-style experience and a classic desktop. The former is not supported by the system. Therefore, the desktop version has to be used.

- Java Virtual Machine

  The most updated information about the latest recommended and approved version of the Virtual Machine for access to the SIOM websites is located on OMIE Public website (www.omie.es), on section "Technical documentation" inside "Trading System".

- Card reader (only for smartcard certificates)

- User certificate registration

- OMIE Root CA Certificate

The following sections describe in more detail these requisites and additional configuration options.

2.1.1 Microsoft Internet Explorer browser

The Internet Explorer browser to access SIOM websites should always be the 32-bit version (although the OS is 64 bits).

2.1.2 Screen setup

The website was designed for an optimal setup of **1280x1024 pixels and 65536 colours**.

As maximum screen configuration, the following are recommended:

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

3 CLIENT STATION AUTOMATIC INSTALLER

Using the installer provided by OMIE, the installation process is automatic, minimizing manual actions that need to be performed. This installer can be downloaded from OMIE Public website (www.omie.es).

When logging into the system without any 32 bit Java version installed, the user will get a page suggesting the execution of the installer, with a link to the specific page on the OMIE Public website.

Se ha detectado que no existe ninguna versión de Java de 32 bits instalada en este equipo. Por favor descargue y ejecute el Instalador OMIE y vuelva a intentar entrar en la Web despues de cerrar el navegador.

No installed 32 bit Java version has been detected in this workstation. Please, download and execute the OMIE Automatic Installer, close your browser and try to log in the Web again.

INSTALLER

— WEB INSTALLER
Download from here the OMIE Automatic Installer for an easy installation and configuration of your workstation to access OMIE Electricity Market Website.
The installer provides the following functionality: Minimum requirements verification, optional installation of the JVM, copy of OMIE additional web components, JVM settings and Internet Explorer advanced options configuration.

files/omiesetup_32_0.exe

Once you run the installer, the following window will be shown (only Spanish version available):

Note: If the active user on the computer does not have administrative permissions, previously the input credentials window of an administrator user appears.

By clicking "Next", the selection window will display the features that will be installed.
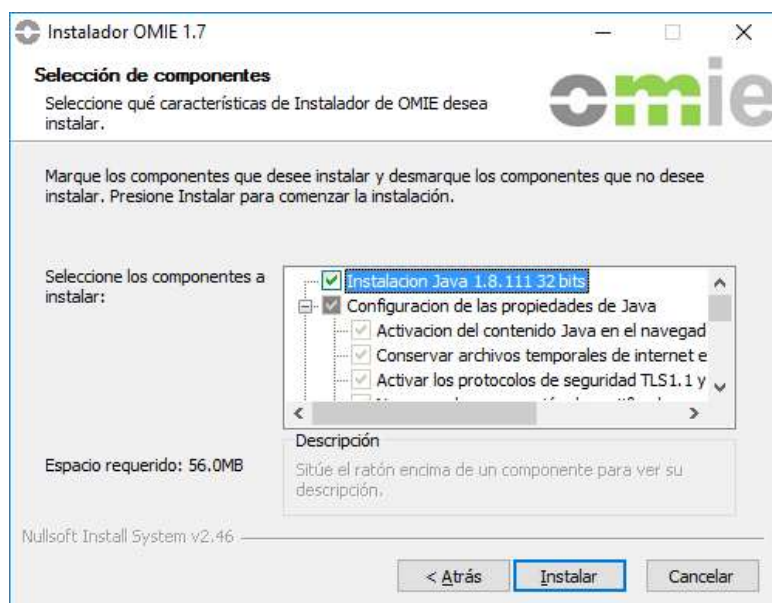
Depending on the version of the Java Virtual Machine 32-bit installed on your computer, the installation of the included version in the installer will be optional, the user can disable this option. The remaining options correspond to elements of the virtual machine configuration and Internet Explorer browser, which cannot be disabled. After clicking "Install", the changes will be applied.

If you have selected to install the virtual machine, first the installer will run from it.
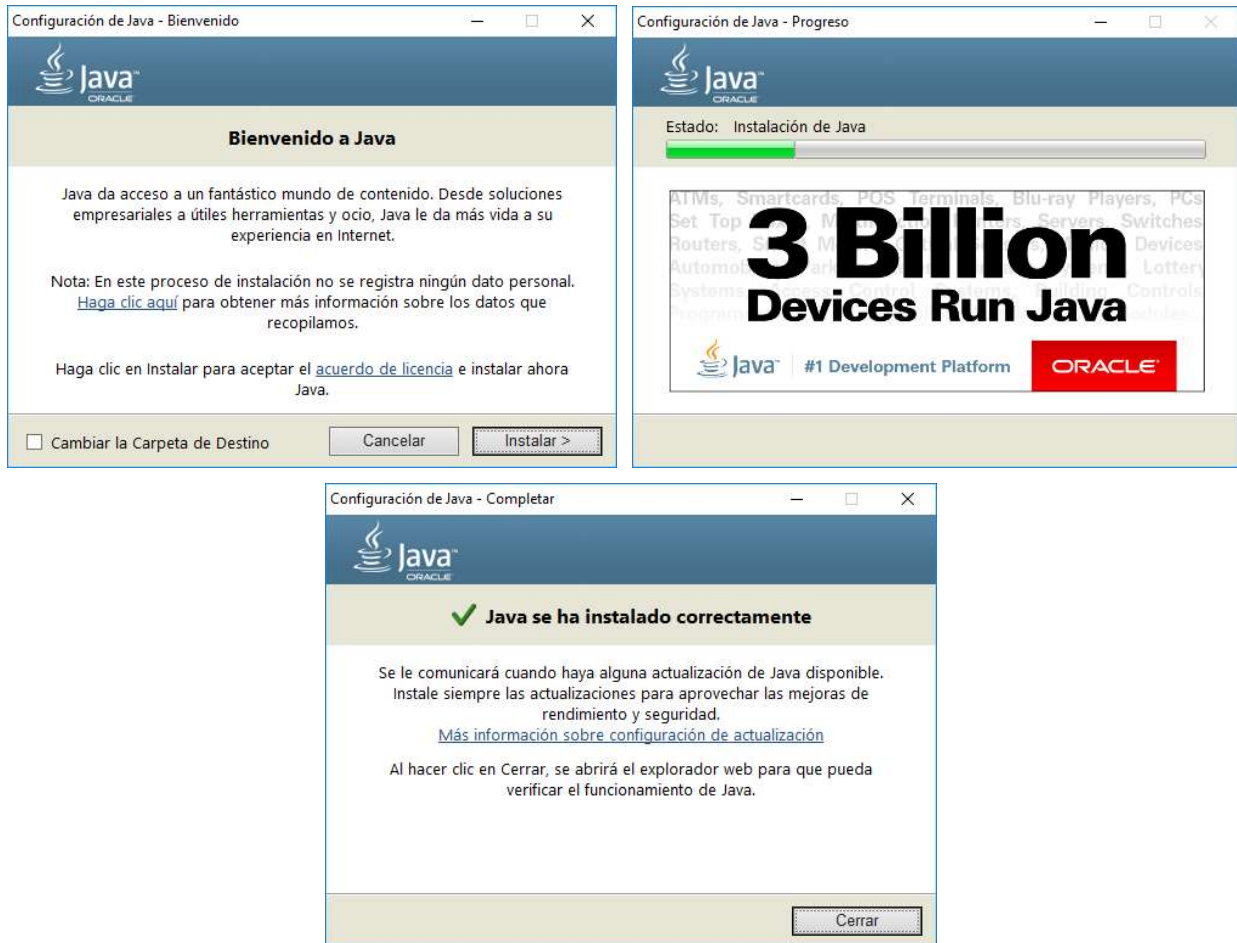
Once this installation is completed, continue with the other features.
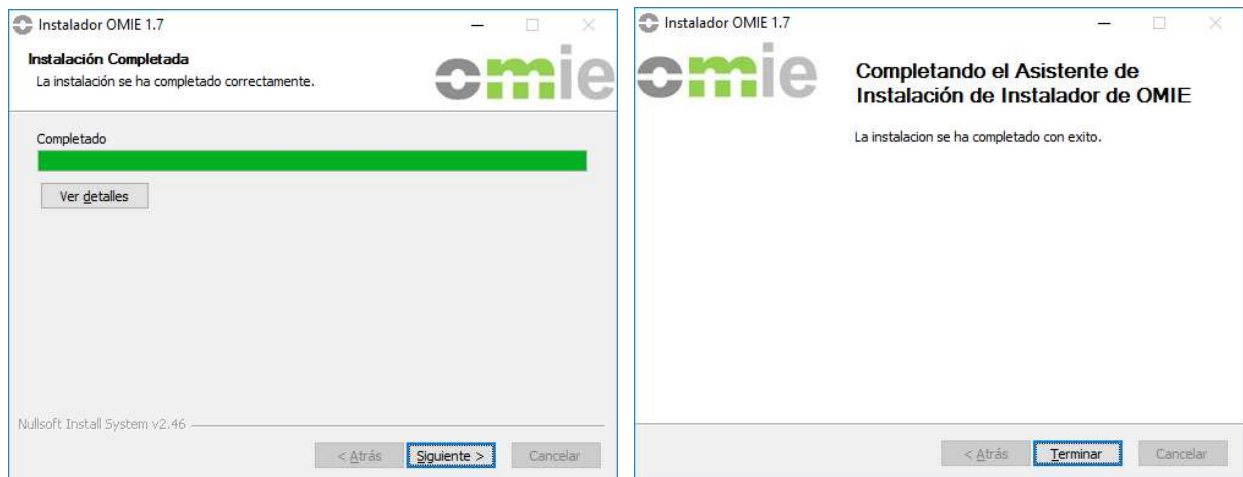
Note: In case of using additional administrator credentials, configuration changes will be applied to both the original user and the administrator profile used to log into the operating system.

4 CLIENT STATION MANUAL SETUP

In this section, additional information is available, which may be needed for the correct configuration of the client position.

4.1 Java configuration

If the version is not valid, update by removing the installed version and access OMIE's website. From there, and as described in chapter 3, the correct JVM will automatically be installed by the OMIE Installer (in order to carry out this installation, the user connected to the operating system is required to have the necessary Administrator privileges).

The current version must be removed from the "Programs and features" option in the Windows Control Panel, by selecting entry "J2SE Runtime Environment" or "Java" with the corresponding version, and by clicking on Remove.

When accessing the Web an alert can be displayed showing that there is a new Java version available, with the label "Your Java version is insecure". In order not to display this message again, check the box "Do not ask again until the next update is available", and then click "Later".
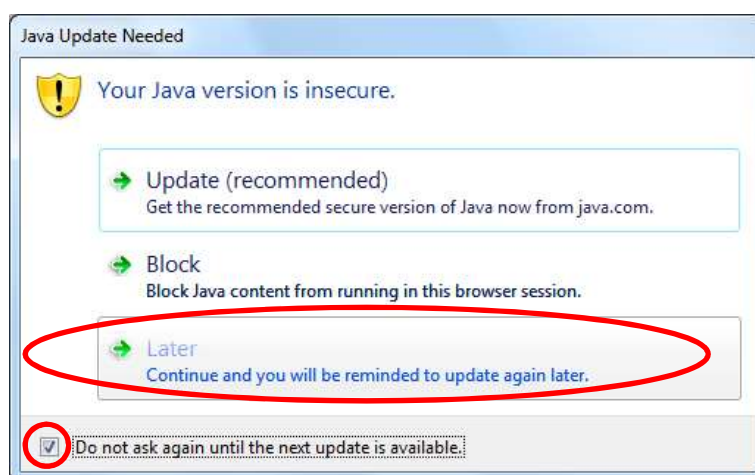
The "Update" option is not recommended since new published Java versions must be previously certified for the system.

This message could be displayed again when a new JVM version is published.

In addition, due to the possibility of Oracle releasing a new version of JRE which has not yet been certified for use in SIOM, you are recommended to disable the automatic update of the JVM. This is configured by disabling the next box in the Java Control Panel:

4.2 Card reader installation (Only for smartcard certificates)

In order to access SIOM Websites, a X.509 personal security certificate it's needed, which OMIE issues on a Gemplus smart card or file. In case of using a certificate issued in a smartcard a smart card reader is needed.

The user can use any standard PC/SC compatible reader, in which Gemplus software must be installed. The **'Gemplus software installation guide'**, which is provided as a separate document, outlines the steps to be followed. The card reader must be previously installed and you must be able to use the security card with Internet Explorer in order to be able to follow the steps listed below for setting up the station.

If you wish to install a GemPCTwin card reader, the specific drivers for this card reader will need to be installed once the Gemplus software has been installed.

4.3 User certificate registration

4.3.1 Smartcard certificates

When using a new security card for the first time at a user station, keep in mind that you **will need to register with Windows the certificate** stored in the card so that it can be used from the browser (it is a requirement of Internet Explorer).

Use the Card reader software to register a certificate, as follows:

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

Click on *Card contents → Certificates* (Contenido tarjeta → *Certificados)* and enter the card PIN in the *NIP Code* section. Click on the *Start session* button to start the session:
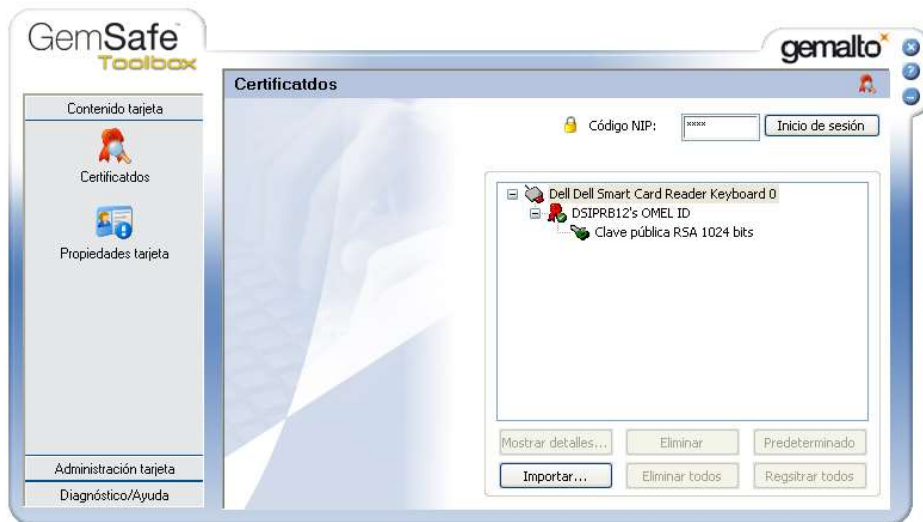
To register the certificate, select the card icon and click on *Register all (Registrar todos)*:
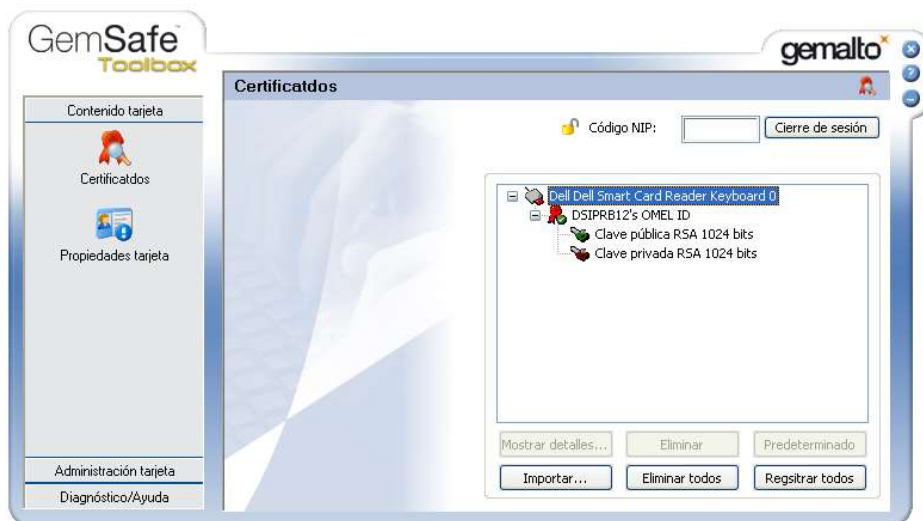
The following screen will display after a few seconds indicating that the certificate has been registered.
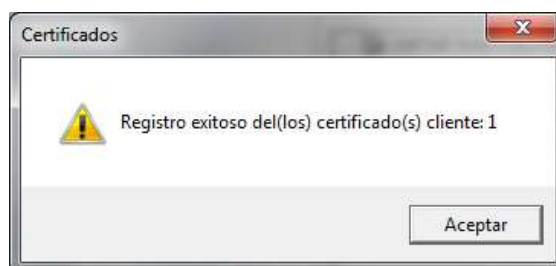
Click *Accept (Aceptar)* to finish the process of registration of the certificate.

4.3.2 Software certificates

File support certificates a.k.a. software certificates, are issued on ".p12" file (PKCS #12 standard). For registering issued software certificates, follow the next steps.

Download ".p12" file in an accessible location from the station where software certificate is going to be registered. Select the file with double click (this process can be started from the web browser too in "*Tools / Internet options / Content / Certificates / Import*")

Follow the given steps showing in the screen using the default options until this window is shown:

Type OMIE's issued private key password and check "Enable strong private key protection" box.

Follow with default options until this window is shown:

Click on "Set security level…"

In this window, "Medium" or "High" level can be selected for setting up system behaviour when using certificate to SIOM access or information sent signing. Selecting "Medium" browser only will show a confirmation window when private key access is needed. Selecting "High", browser will request the password for the private key access.

It's recommended to select "High" level and choose a password as a PIN for system access and data sent signing. Doing this, this window will appear after clicking "Next" for typing and confirm the chosen password:
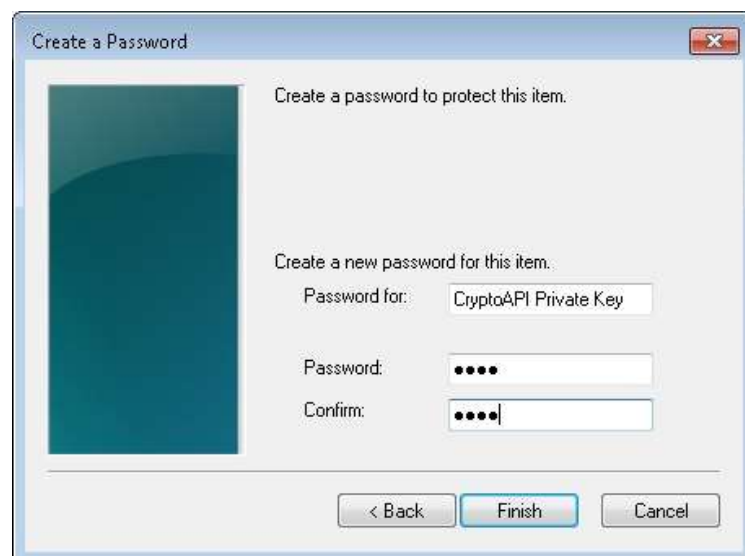
Alter clicking on "Finish" and "OK", this window will mean the end of the process:

4.4 Signature applet setup

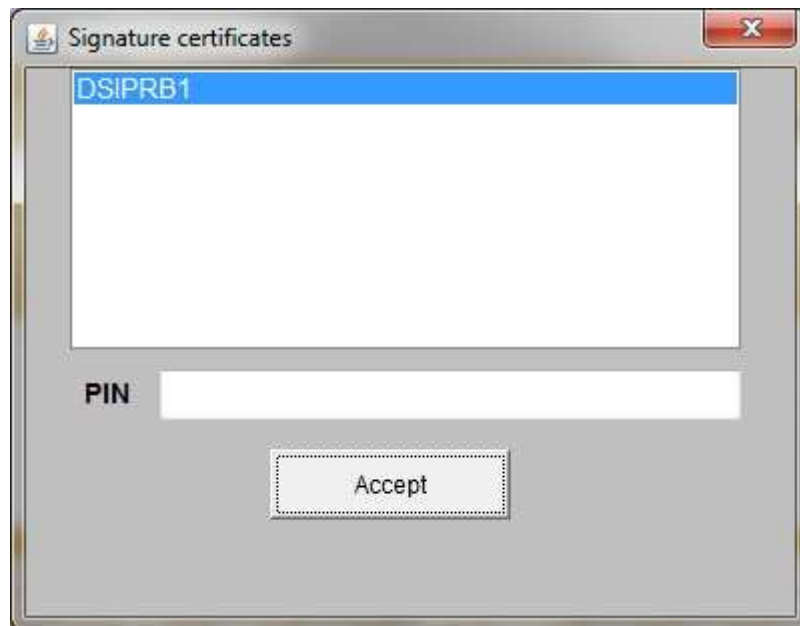The 'Signature applet' is the Java component used to send digitally signed information to OMIE. Its graphical view when any signed transmission is made is as follows:

This applet shows the certificate to use for digital signing data sending, that it's the same certificate used for system connection. It also shows a field to type the certificate's PIN in case a smartcard is being used. If a software certificate is being used this field will be disabled and it will be the web browser itself who will ask for the confirmation of using that certificate, with or without password according to the security level chosen in the first installation.

This 'Applet' has a setup file located in '**C:\OMEL\ConfAppletFirma.xml**'. The default 'Applet' establishes an initial configuration in the event that the said file does not exist, creating it for subsequent modification of the user. On the first installation of the station, this file will not be created until the website main page is accessed

---

The content of the said file is as follows:

```xml
<?xml version='1.0'?>
<!--
    NOTA : Cualquier cambio en este fichero se tendrá en cuenta a
           partir del próximo reinicio del navegador.
-->
<ConfAppletFirma>
    <Seguridad>
        <PINTimeout>0</PINTimeout>
    </Seguridad>
    <Log>

    <DirEnviosFirmados>c:\omel\EnviosFirmados</DirEnviosFirmados>
    </Log>
</ConfAppletFirma>
```

Two configurable parameters are established in this file:

- **PINTimeout**: PIN time-out. This time expressed in minutes establishes the maximum time that the Applet waits between the signed transmission in order to once again request the user PIN. If the maximum time defined has not passed between the signed transmission, the user will not be asked for the PIN again. The '0' value indicates that the user will always be asked for the PIN. This parameter has a maximum value established in 30 minutes. If set at a greater value, a default time of 30 minutes will be used.

- **DirEnviosFirmados**: Destination directory of the signed transmissions. A structure of subdirectories with all the signed transmissions made by the user with the 'Applet', will be created in this directory, organised by types of transmissions ("BidsMD", "ExecutionsCB", "BidsAuctions", "Claims Auctions", etc.). In the event that a non-existent directory is specified, the Applet will automatically create it. If the said directory cannot be created, the destination directory will be the one by default defined by the Applet, which is '**c:\omel\EnviosFirmados**'.

Any change in this file will not take effect until the browser is restarted.

5 FREQUENT PROBLEMS

5.1 Error messages appear during installation of applets

When any of the following situations arise:

- The user who makes the first installation does not have administrator privileges,
- The Administrator did not give component update privileges to Advanced Users, and an Advanced User enters the system when OMIE has included an update of applet versions,
- A Normal User logs onto the system when OMIE has included an update of applet versions,

The browser main page will automatically close and the following message will display:
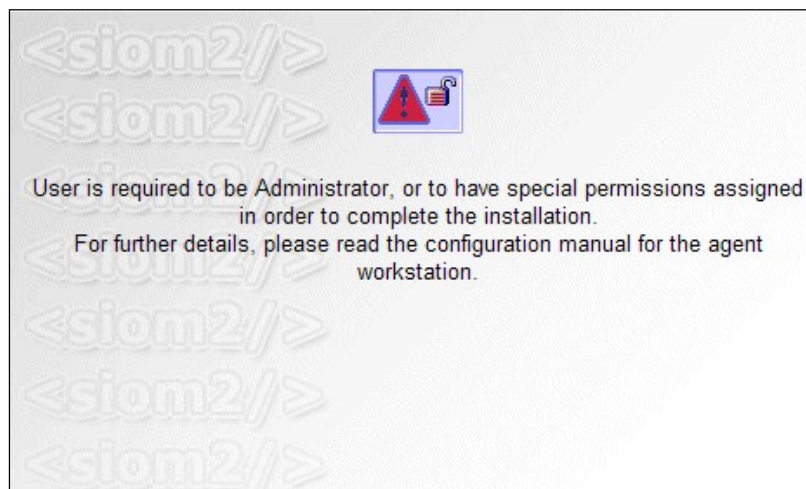

To avoid this, access to the system must be made with a user with administrator privileges, or as an Advanced User if the Administrator has given privileges to Advanced Users to make subsequent updates.

5.2   The card PIN request takes a long time, or the browser stalls

This problem may be due to the fact that there are other Internet Explorer sessions open. To solve the problem, close all browser sessions, and repeat the entry to the system.

If the problem persists, check to see if there are processes active in the system Task Manager, under the name *IEXPLORE.EXE*, as shown in the image. In such an event, these processes must be manually closed from the Task Manager (by clicking on "End Process"), before trying to access to the system again.
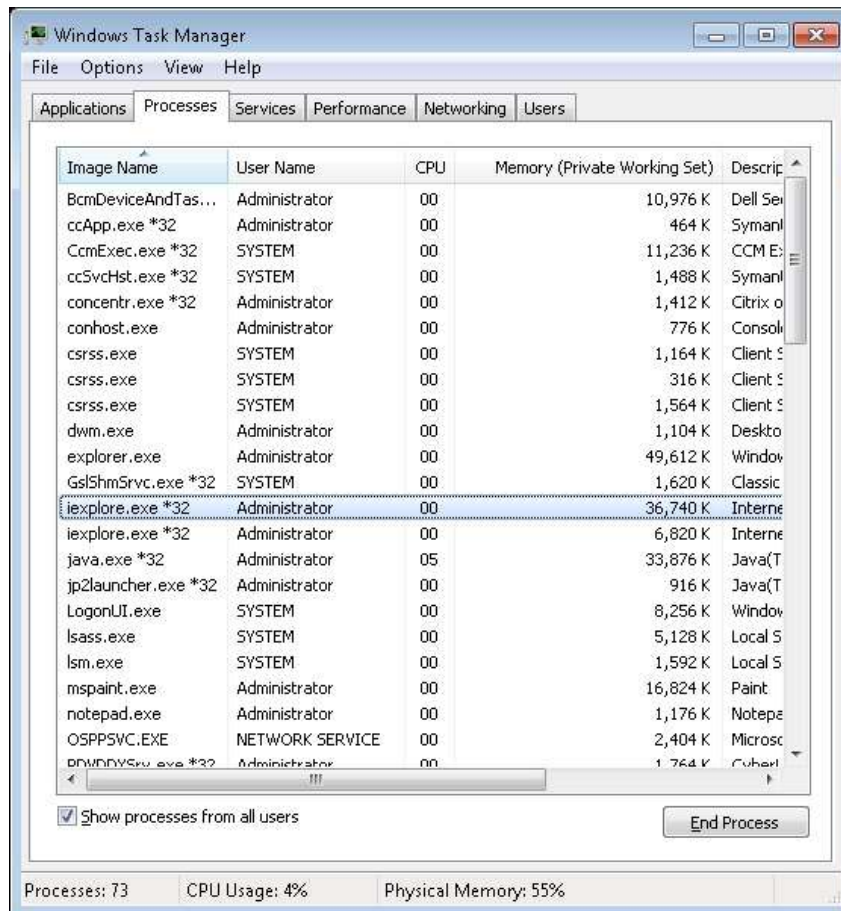
5.3 "Security alert" appears on logging onto the system

As explained in section 2.7, this window opens when the OMIE CA Signing Entity certificate has not been registered in the browser.

This can occur, even if the said certificate has already been registered, if you are using an operating system user that has not previously accessed the SIOM website or due to the update of the root CA in SIOM.

To solve this problem, follow the steps outlined in the present document, from section 4.6, onwards, and review the browser set up options for the user, as described in section 4.2.

5.4 The server does not allow access to the system

If error messages such as "*The page cannot be displayed*" or "*Access Forbidden*" appear, they may be due to the fact that you are using a browser that does not support 128-bit encryption.

To check the encryption level supported by the browser that you are using, follow the steps outlined in section 4.2.

Currently, the browser versions that can be downloaded from Microsoft have the necessary level of encryption. The problem may be due to the fact that an old version is being used, or one obtained when versions containing strong encryption and those that did not were differentiated for international legal reasons. Consequently, the problem is solved by installing an updated version of the browser.

5.5   Use of *Namespaces* in XML documents (only for Electricity Market website)

When XML documents which do not include the correct specification of the namespace are sent, either through the browser or through Web Services, an error message displays. In the case of transmission through the browser, a window with the following message displays:

A document parsing error has occurred:
The XML file does not have the correct namespace 'http://www.omel.es/Schemas'

For a XML document sent to OMIE to have the correct namespace, its header must include the contents as shown in the following example:

```
<MensajeOfertasMD xmlns="http://www.omel.es/Schemas">
  <IdMensaje v="OfertasMD-2004-10-05"/>
    <FechaMensaje v="2004-10-04T09:19:43-00:00"/>
    <IdRemitente v="AGENT"/>
  ...
</MensajeOfertasMD>
```

The error produced in the event of using a Web Service interface, taking as an example the forwarding of bids to the Daily Market, would be the following, which indicates that the server would be unable to find the element *'MensajeOfertasMD'* associated with the corresponding *Namespace*, within the document sent:

```
AxisFault
 faultCode:
    {http://xml.apache.org/axis/}Server.userException
 faultString:
    org.xml.sax.SAXParseException:
       Declaration not found for element 'MensajeOfertasMD'.
```

The *namespace* is used to avoid nomenclature conflicts between XML documents which could have the same labels with different purposes. With an aim to avoid possible future conflicts, strict appliance of standards and the specification of the *namespace* shall be mandatory.

Below are two examples of documents with nomenclature conflict:

Document with stock Exchange information:

```
<table>
  <value>
    <ticker>TLR3</ticker>
    <last>18.23</last>
  </value>
</table>
```

Document with product information:

```
<table>
  <name>American coffee table</name>
  <width>80</width>
  <length>120</length>
</table>
```

If these two types of document are aggregated in one document, there will be a conflict of elements as both documents contain the element *<table>.*

The use of *Namespaces* solves this type of problem by assigning a name space to a group of labels. *Namespaces* are usually defined in the XML document root, thus assigning this namespace to all the elements including children. Below are the two former XML documents which have been corrected to incorporate their *Namespace*:

Document with stock Exchange information:

```
<table xmlns="http://www.mibolsa.com/tabla">
  <value>
    <ticker>TLR3</ticker>
    <last>18.23</last>
  </value>
</table>
```

Document with product information:

```
<table xmlns="http://www.muebles.es/Catalogo">
  <name>American coffee table</name>
  <width>80</width>
  <length>120</length>
</table>
```

Due to the foregoing, all XML documents sent to OMIE and received from OMIE shall have the correct namespace to avoid possible conflicts.

5.6 Blocking pop-up windows

The process for installing components of SIOM websites uses pop-up Windows to execute some of the steps (see section 4.2). In the event that popup windows are blocked in the browser, the said installation will not run correctly, and prevent operation in the web.

To configure block popup windows, do as follows

*Tools → Internet Options → Privacy → Turn on Pop-up Blocker*
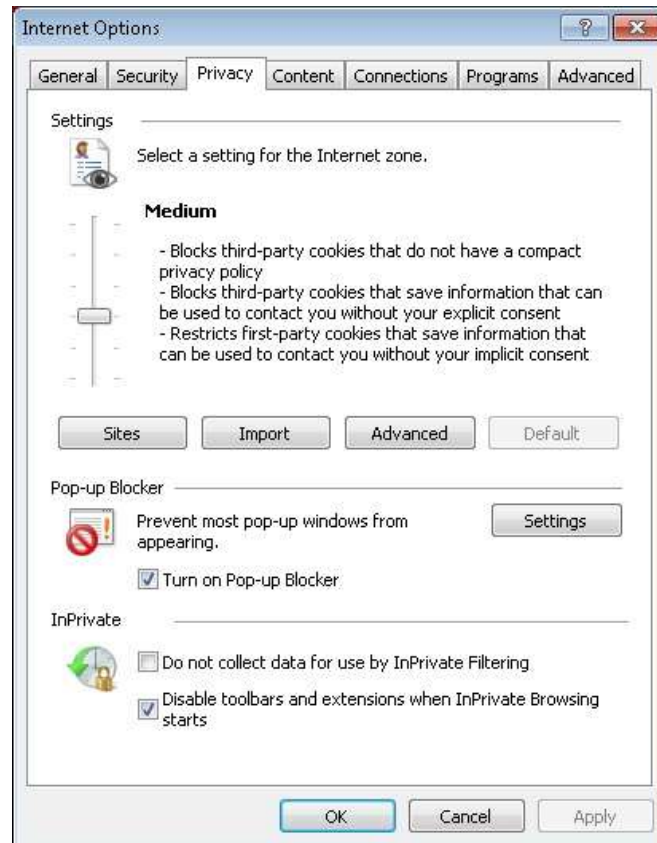
If the "*Pop-up Blocker*" option is enabled, you won't be able to access SIOM correctly. To solve this problem, you must disable this option, or specify that OMIE's Web servers can open pop-up windows. To do so, click on "*Settings*", and the "A*ddress of website to allow*" text box and type "**.omie.es*" and click on "*Add*". In order to access the emergency environment without problems, the same configuration should also be made for "**.emergenciaomie.es*". In addition, you must specify as "*Filter level*" the option "*Low: Allow pop-ups from secure sites*" (see screen shot below).
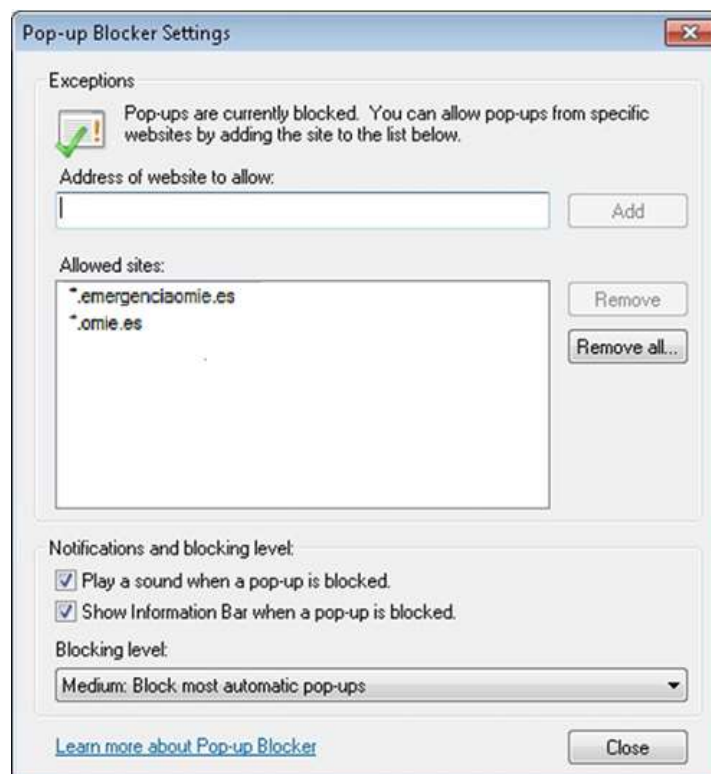
You will then have no problem in accessing all OMIE web servers.

In the event that the pop-up windows are blocked, and the OMIE windows have not been allowed, the following warning line may display in the browser, and the following options will display:
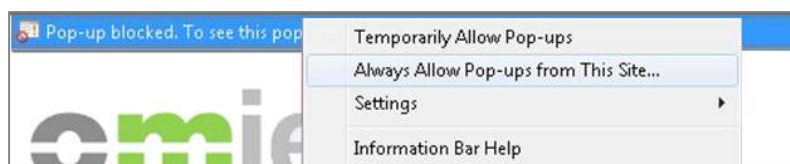
If you choose the "*Always allow pop-ups from this site*" option, the following confirmation window will display (example for the website "http://*www.pruebas.omie.es*"):

If you click on "*Yes*", the Block up windows will be disabled for this server, and you can make another attempt to access the website.

However, the first procedure described in this section is recommended, as it allows access to all OMIE servers with just one operation.

On the other hand, the blocking of pop-up windows can be enabled in other ways, such as for example by installing tools which, among other functions, allow the blocking of the said windows. This is the case of the *MSN* or *Google* bars (among others). In the event that one of these tools is installed, you will need to configure it so that OMIE web pop-up windows ("**.omie.es*" and "**.emergenciaomie.es*"), at least, are not blocked. To do so, check the documents provided by the said tools.

5.7   File download warning

If you try to download a file (for example, download the request or response from a signed transactions enquiry), the following warning message may display:

Although you indicate that you wish to download the file, the browser displays the web's main page.

To solve this problem, you must make the following modification to the browser setup (as is indicated in section 4.2):

> *Tools / Internet options / Security / Internet [or zone in which the OMIE web is located] / Custom level / Downloads / Automatic prompting for file downloads / Enable.*

In this way, when requesting a file to be downloaded, the warning message will not display, and only the standard dialog box for opening it or saving it to disk will display.

5.8   Problems starting Download Center (only for the Electricity Market Website)

As the Download Center uses Java Web Start, running it properly requires establishing the extension .jnlp for that program, following these instructions, so that the Download Center will launch automatically.

> *Settings → Apps → Default apps → Choose default apps by file type*
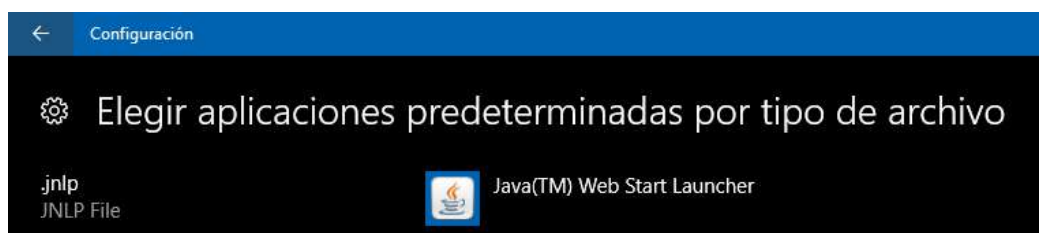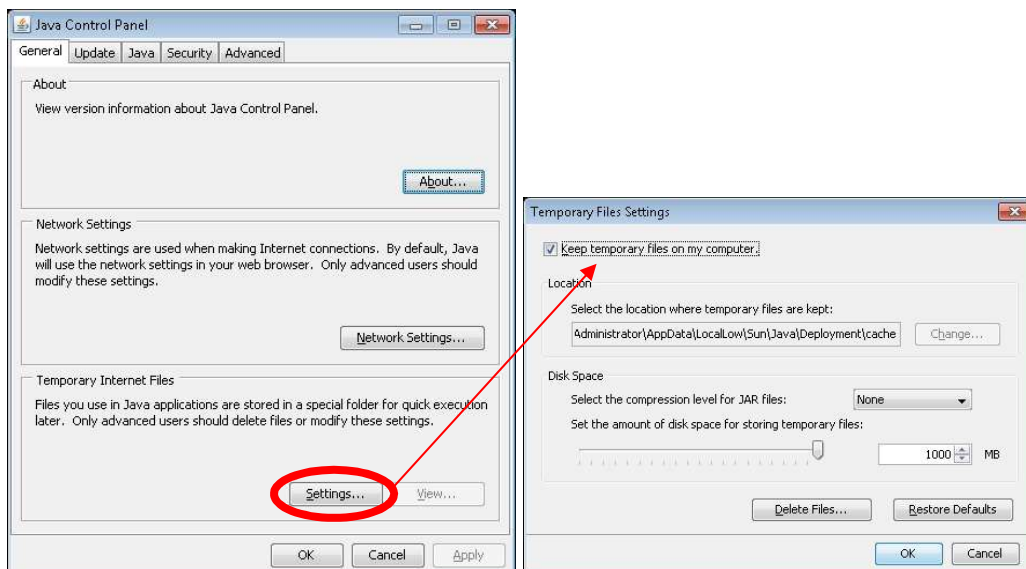

On the other hand, in some cases after starting "Download Center" the following exception may occur:

This error is due to the incorrect configuration of JAVA, which prevents the application from booting. To solve this problem, change the settings from the control panel.
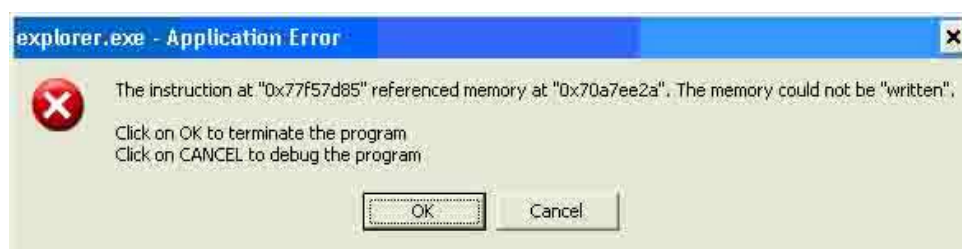
The said setup is found in:

> *Control panel → Java → General → Temporary Internet Files → Settings*

From here, activate verification "Keep temporary files on my computer".

## 5.9 Problems logging onto the Web with no Java installed

In some cases when logging on to the Web with no Java JRE installed, the following error message displays:

This error is due to a security mechanism incorporated in Explorer to avoid execution of malicious code ("*Data Execution Prevention*"). When installing JRE, just like in other browser extensions, this problem can arise if the said extensions are not updated for compatibility with this mechanism.

If you wish to carry out the installation from the Web, you can disable the verification as follows:

Tools → Internet Options → Advanced → Security
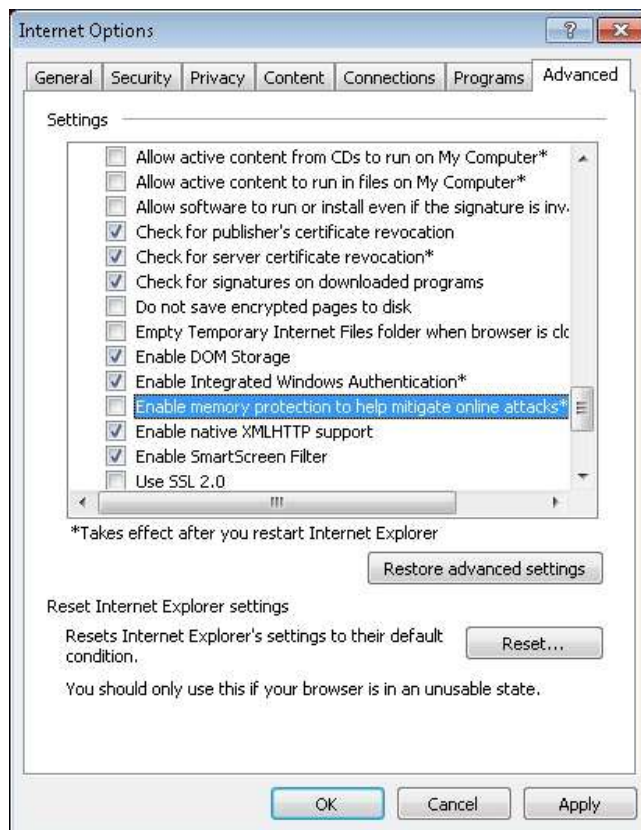
Disable the "*Enable memory protection to help mitigate online attacks*" check box, reboot the browser and log on to the system again. You are recommended to reactivate this box after the installation process.

Another alternative is to download Java from the website itself;

> http://www.oracle.com/technetwork/java/javase/downloads/index.html

Download the "JRE" version compatible with the application.

Once it has been downloaded, install as outlined in point 3.1 and then log onto the web again.

5.10 Incorrect installation of OMIE Root CA Certificate

It can happen that, after installation of OMIE Root CA Certificate, the security alert and the certificate error message are still displayed, and also the certificate error:

This problem can be due to the fact that the OMIE Root CA Certificate has not been installed in the proper certificate store (if the browser default options are kept, the certificate can be installed in the "*Intermediate Certification Authorities*" store, instead of the "*Trusted Root Certification Authorities*" store).

In Addition, in this situation it is not possible to install it again in the proper store, because if you follow the steps described on section 4.6, the button "Install certificate" does not appear. This is due to the fact that such certificate is already installed in a store.
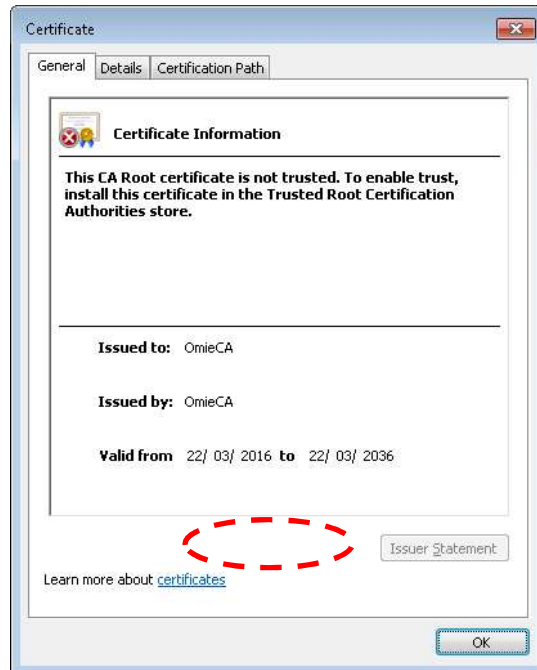
Therefore, the solution is to uninstall the certificate first. In order to do so, you should enter from the browser into:

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

From that point, you should select the "**OmieCA**" certificate and click on "**Remove**".
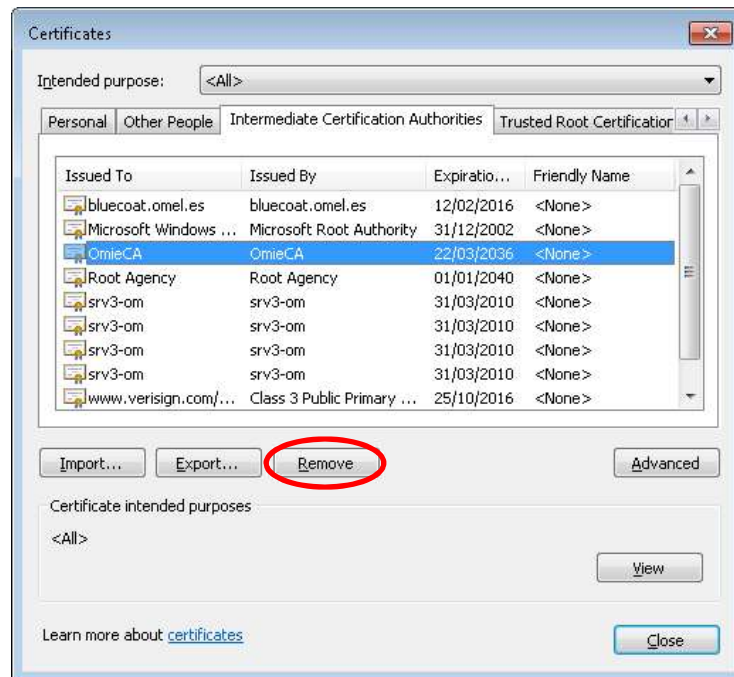
After confirmation, the certificate should have been uninstalled. Then, you should follow the steps described on section 4.6 in order to properly install the OMIE Root CA Certificate.

5.11 Two Windows of the Download Center are opened (only for the Electricity Market website)

Sometimes, when you launch the Download Center from the Electricity Market website, it is started twice (two windows are opened, so the certificate is also requested twice).

This problem has been detected Internet Explorer 9 with the "SmartScreen Filter" turned on. In order to solve this problem it is required to turn off this filter. The "SmartScreen Filter" can be found at:

Tools → SmartScreen Filter

5.12 A message on unsupported browser version is shown (only for the Electricity Market website)

When using Internet Explorer 8, you can get the following message:
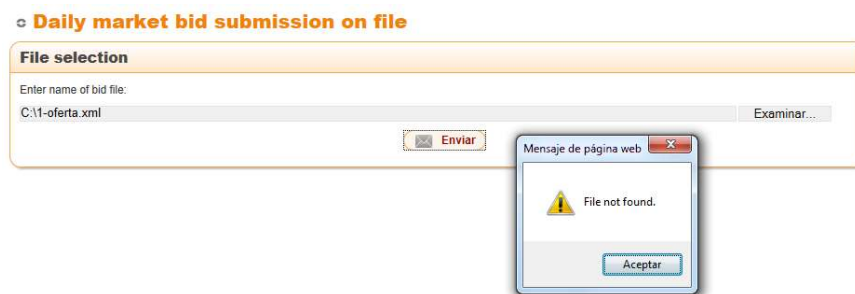

The reason is that the browser is running on "Compatibility View".

In order to solve this problem, please follow the instructions on Compatibility View settings described on section 4.2.

5.13 Error when submitting bids on file.

When submitting bids on file, the following message could be displayed, preventing from submitting the file:

In order to fix it, follow section 4.2 on paragraph "*Minimum options review*".

> *Tools / Internet Options / Security / Internet [*or the zone the Web Site is included*] / Custom level / Miscellaneous / Include local directory path when uploading files to a server/ Enable.*