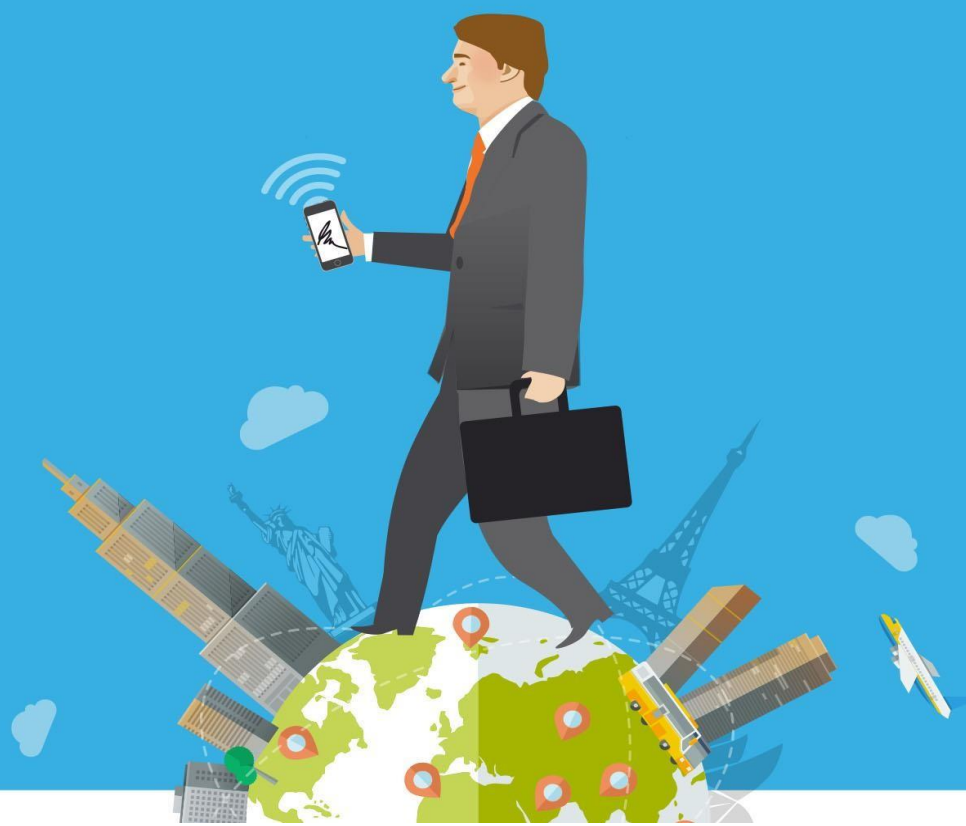




C/ Acceso Ademuz, Nº 12-1º-Pta 1 - 46980 Paterna (Valencia)
www.ivnosys.com - Tel. 960 031 203

DRIVER KEY CONTROLLER

DESIGN, CONFIGURATION AND USE GUIDE



COPYRIGHT©

The material contained in this document is the property of Ivnosys Soluciones.
No part of this site may be reproduced in any form or by any means, nor may it be used with
other organisations for other purposes without our prior written permission.

[illegible]



LIST OF CONTENTS

TABLE OF CONTENTS	1
1. KEYCONTROLLER DRIVER FOR IVSIGN	2
2. STANDARD INSTALLATION AND CONFIGURATION	3
2.1. MANUAL OR STANDARD INSTALLATION	3
2.2. MANUAL OR STANDARD CONFIGURATION	8
3. UNATTENDED INSTALLATION AND CONFIGURATION	11
3.1. UNATTENDED INSTALLATION	11
3.2. UNATTENDED CONFIGURATION	13
4. DRIVER INSTALLATION VIA GPO	17
4.1. BASIC AUTHENTICATION	21
4.2. FEDERATED AUTHENTICATION	23
5. PKCS ENVIRONMENT CONFIGURATION#11	26
6. VERSION UPDATE PROCEDURE	30
7. MANAGEMENT AND USE OF KEYCONTROLLER	31
7.1. NOTIFICATION SYSTEM	31
7.2. CONTROL PANEL	32
7.3. ENABLING/DISABLING CERTIFICATES	33





1. KEYCONTROLLER DRIVER FOR IVSIGN

IvSign is the solution for secure electronic signatures.

With **IvSign** it will not be necessary to have the certificate installed on the device itself, thanks to the centralization of all the certificates in **IvSign** itself.

IvSign allows the secure storage of digital certificates, in order to authorize their use in the equipment of different users, processes and web pages in a centralized way and with traceability of the operations.

It is the only means of technically and legally guaranteeing a person's identity on the Internet, the electronic signature of documents and encrypting communications and content.

This requires the installation and subsequent configuration of the **KeyController Driver**.





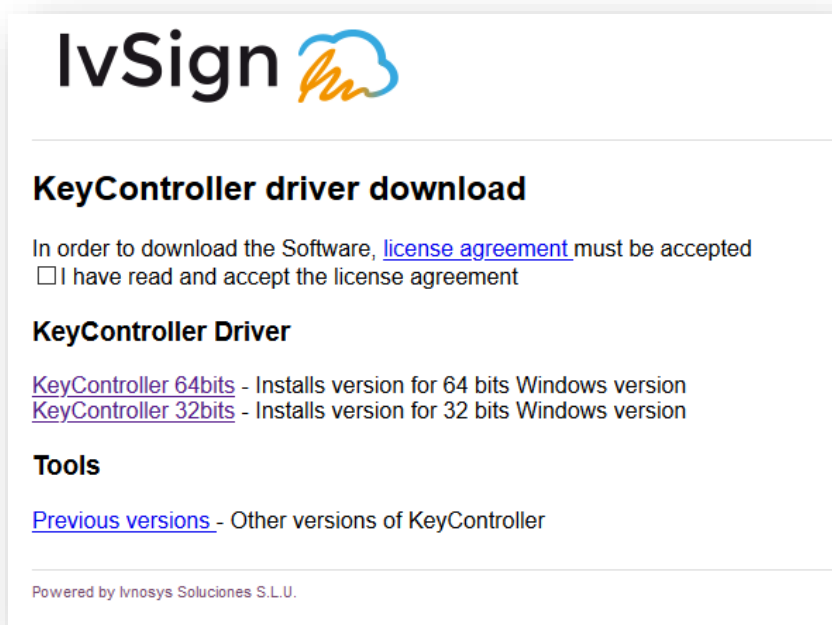
2. STANDARD INSTALLATION AND CONFIGURATION

2.1. MANUAL OR STANDARD INSTALLATION

To use the certificate with your Windows applications, in the same way as for a SmartCard or Software certificate, you will need the **KeyController Driver**, which you can download and configure by following these simple steps.

By accessing the following url: <https://ivsdriver.com>

you must read and accept the licence agreement, before downloading, by clicking on the option '**I have read and accept the licence agreement**'.



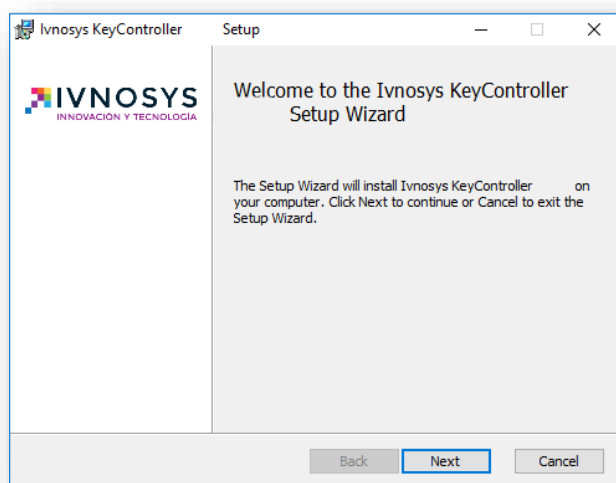
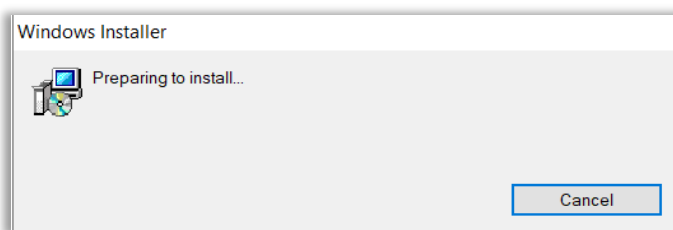
After clicking on the corresponding link, you must execute the downloaded file and the installation wizard will be displayed.



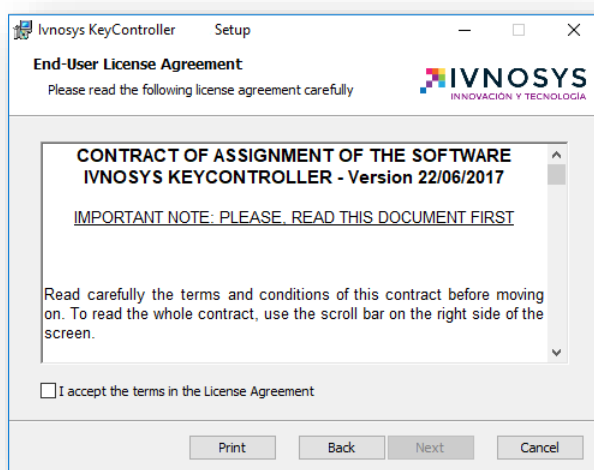
Note:

To install the driver you need to have administrator permissions on the computer.





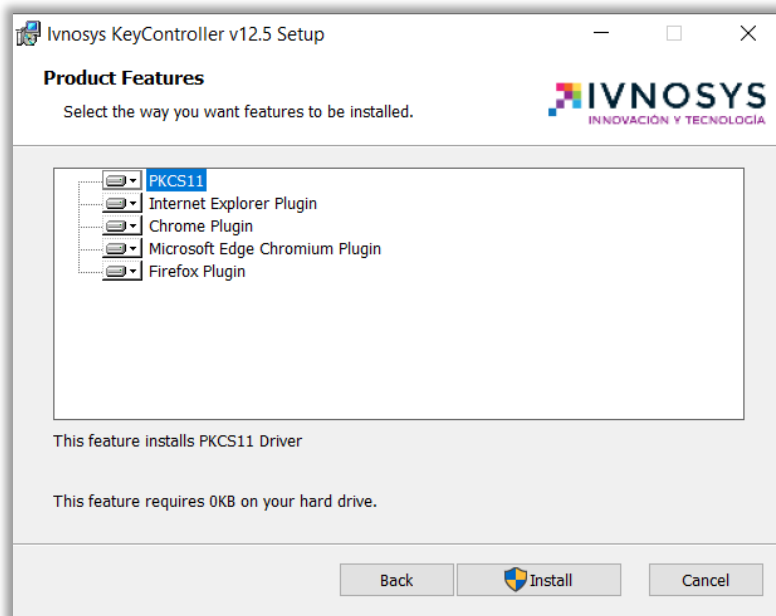
Check the box **I accept the terms of the license agreement** and the button to start the installation will be activated.



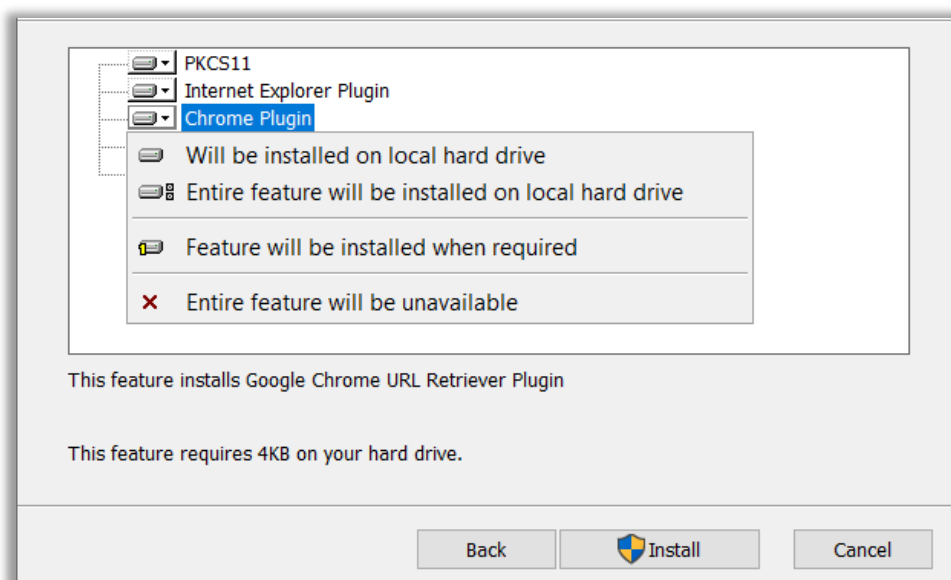


The next screen allows you to select the KeyController Driver components that you want to include in the installation process.

However, the recommendation is to keep the default values, maintaining the installation of all components.



Clicking on each component will open the context menu with all the options available for each component.





By default, all components will be marked with the option **To be installed on the local hard disk drive**.

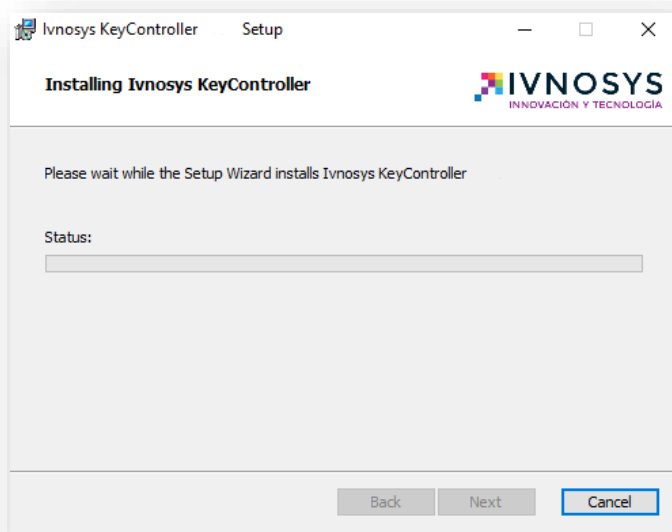
If you do not wish to install it, check the option **The full feature will not be available**.

After clicking on the **Next** option, confirmation will be requested to start the installation process, based on the previously selected parameters.

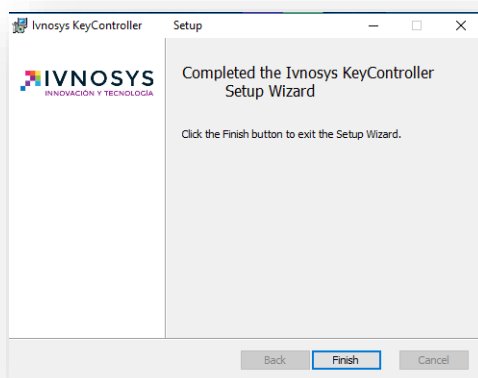


By clicking on the **Install** option, the window indicating the status of the installation will be displayed through the progress bar.

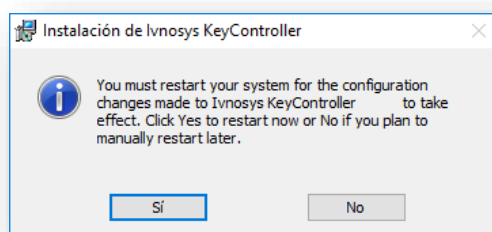




Once the installation is complete, click on the **FINISH** button to exit the wizard.



Finally, you will be prompted to restart the computer by the following dialogue box:

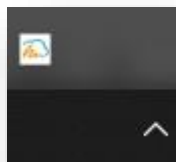




IMPORTANT. Restarting the computer is a requirement to ensure proper operation of the system. If it is not allowed or if a restart is omitted, the driver may not run correctly or may exhibit unstable behaviour.

In case it is not possible to restart the equipment immediately, it must be ensured that this restart is carried out after the fact, before end-users start working with the driver.

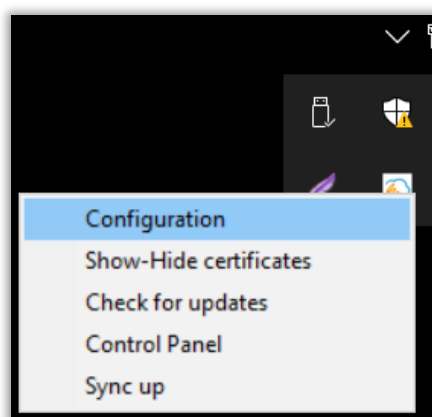
The **Driver KeyController** icon will be displayed on the right side of the Windows taskbar in the notification area.



2.2. MANUAL OR STANDARD CONFIGURATION

In order to use the centralized certificates in **IvSign**, the application must be configured following the steps indicated below.

By clicking on the **Driver KeyController** icon in the notification area with the right mouse button, the following menu of options will be displayed.



Click on the **Configuration** option, which must be completed with the following information:

- **Server:** the value corresponding to the URL address of the platform (e.g. ivsign.net) shall be entered in this field.
- **Authentication:** select the *Integrated Authentication* or *User and Password* option, as appropriate.





- **Integrated authentication:** this option will take the data from the active Windows session, verifying that the user exists in the organization's Active Directory, provided that the user is on the same network as the IvSign server.
- **Username and Password:** you must indicate the data provided in the email *Welcome to the IvSign service*, to access the platform. This information will be validated in IvSign's own database.
- **Organization ID:** indicate the organization identifier, in case you do not have it, please contact your project manager.



NOTE

If the password has been changed, enter the new password and not the one from the e-mail.

You can check if the credentials you have entered are correct by clicking on the **Test** button.

If the credentials entered are correct or incorrect, a message indicating this will be displayed at the bottom of the configuration window.





Configuration CSP

KeyController **IVNOSYS**
INNOVACIÓN Y TECNOLOGÍA

Server: ivsign.net
Authentication: User and password
Organization ID: orga
User: user
Password: ****

Try out Accept Cancel

Error authenticating user (*)

Configuration CSP

KeyController **IVNOSYS**
INNOVACIÓN Y TECNOLOGÍA

Server: ivsign.net
Authentication: User and password
Organization ID: orga
User: user
Password: ****

Try out Accept Cancel

Configuration validated correctly

Once the checks of the indicated configuration have been completed, click on **OK**.

Certificates that you have centralized in **IvSign**, will be displayed from browsers and applications that make use of the standard Windows store.

If it is not displayed automatically, it is advisable to restart the system.



NOTE. Centralized certificates cannot be removed from the system manually, nor can their private key be exported, as they are not in any case located on the equipment where they are configured.





3. UNATTENDED INSTALLATION AND CONFIGURATION

3.1. UNATTENDED INSTALLATION

Since version 5, the KeyController installation includes new components and additional installation options. For example, the system prompts you to restart your computer after the installation process is complete. This is a requirement of the version in order to ensure the correct functioning of the system.

In the case of unattended installation, this requirement can be omitted or customized based on the installation options used.

The following table details the available options:

Options	Description
Components	To exclude all additional components from the installation process, the following parameters must be included: "ADDLOCAL=ALL REMOVE=PluginChrome,PluginIE,Pkcs11" On the other hand, it is possible to disable components specifically. This can be done in two ways: Either by using the above command (specifying only one component) or by using the DISABLE option and the component name, as shown below: "DISABLE_PluginChrome=1" "DISABLE_PluginIE=1" "DISABLE_Pkcs11=1"
Restart	/norestart : Prevents the computer from restarting after the installation process is complete.  NOTE: If this parameter is not included, the computer will restart automatically after installation, with no possibility for the user to cancel the installation.





Some examples are given below:

EXAMPLE. Installation of KeyController excluding all components and avoiding reboot after installation:

```
msiexec /q /i KeyController.msi ADDLOCAL=ALL REMOVE=PluginChrome,PluginIE,Pkcs11 /norestart
```

***It is important that the /norestart is at the end of the line.**

EXAMPLE: Installing KeyController excluding only the Google Chrome component (by the first method) and forcing a reboot of the computer after the installation process:

```
msiexec /q /i KeyController.msi ADDLOCAL=ALL REMOVE=PluginChrome
```

EXAMPLE: Installation of KeyController excluding only the Google Chrome component (by the second method) and forcing a reboot of the computer after the installation process:

```
msiexec /q /i KeyController.msi DISABLE_PluginChrome=1
```



IMPORTANT: Restarting the computer is a requirement to ensure proper operation of the driver. If it is not allowed or if a reboot is omitted, the system may not run correctly or may exhibit unstable behavior.

In case it is not possible to restart the equipment immediately, it must be ensured that this restart is carried out after the fact, before end-users start working with the driver.





3.2. UNATTENDED CONFIGURATION

Option 01: configuration with command line parameters

The MSI installer allows the driver to be configured with default values at the time of installation.

Some of the **parameters** are as follows:

Parameter	Description
Server	Sets the default server configuration for new users.
Serverfix	Sets the server configured as mandatory for all users (the value cannot be changed by the user).
Auth	Sets the authentication type: • pass > Basic authentication • win > Integrated authentication • external > External authentication, using SAML
Authfix	Sets the authentication type as mandatory (the value cannot be changed by the user).
Orga	Sets the IvSign organizational code.
Orgafix	Sets the organization code as mandatory (the value cannot be changed by the user).
noupdates	Allows to disable version checks (using the value 1)
nocertdisable	Allows to remove the possibility to enable-disable certificates from the menu (using the value 1).
accesopanel	Enables the "Control Panel" option in the KeyController context menu (using the value 1).
SSOPanel	Specifies whether autologin is allowed in CertManager through the "Control Panel" option or from a notification (using the value 1). If the user is required to enter a password, it must be set to 0.





autoregister

Sets whether KeyController should create the user reference in IvSign, when the user logs on to the device (using the value 1).

This option is only supported for integrated authentication systems.

disabledforapps

Sets the applications for which the driver will not be available. If a value is set to user or fixed, this value will be ignored.

disabledforappsfix

Sets the applications for which the driver will not be available. If this value is set, it will ALWAYS be considered, no matter what the user or the default has.

The list of variables indicated in the table above does not mean that they can only be configured once installed. These variables can be modified from the Windows registry, if you have permissions to edit them.

If any previous configuration has been made in the IvSign organization, this configuration will prevail instead of the one configured in the equipment itself.



IMPORTANT NOTE.

Note that to perform the unattended installation with the **/q** parameter, the console must be run in administrator mode.





Some examples are given below:

EXAMPLE: Basic installation example where the user is allowed to edit the form fields and the update check is disabled.

```
msiexec /q /i KeyController.msi server=ivsign.net auth=win orga=XXXX noudates=1  
nocertdisable=1
```

EXAMPLE: The above example is then repeated, but restricting / locking the fields for the user.

```
msiexec /q /i KeyController.msi serverfix= ivsign.net authfix=win orgafix=XXXX noudates=1  
nocertdisable=1
```

Option 02: Configuration via the Windows registry

It is possible to modify the default and mandatory configuration of the server and driver authentication method of a device by modifications in the registry.

The **registry entries** available are:

Register entries	Description
[HKEY_CURRENT_USER Software Software KeyController].	Sets the specific configuration for a user
[HKEY_LOCAL_MACHINE_MACHINE\SOFTWARE\Client\KeyController\fixed].	Sets mandatory values for all users with no possibility of modification.
[HKEY_LOCAL_MACHINE_SOFTWARE\Client\KeyController\default].	Contains the default configuration values. KeyController uses these values if no configuration information is available in the two paths above.





EXAMPLE: Let's take an example configuration using ivsign.net and force integrated authentication. The **reg** file to run would be as follows:

```
.....Windows
Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Clients\KeyController\fixed]
"server"=" ivsign.net"
"auth"="win
"
```

EXAMPLE: Additionally, an example with federated authentication is included by default:

```
.....Windows
Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Clients\KeyController\default]
"server"=" ivsign.net"
"auth"="federated"
"fedcode"="XXXXXXXXXXXX
"
```





4. DRIVER INSTALLATION VIA GPO

In order to make the KeyController driver available on all required computers, an installation must be performed via the domain policies.

The first step is to place the installation files (for both 32-bit and 64-bit architectures) on a shared resource, accessible to all workstations and with permissions for all users.

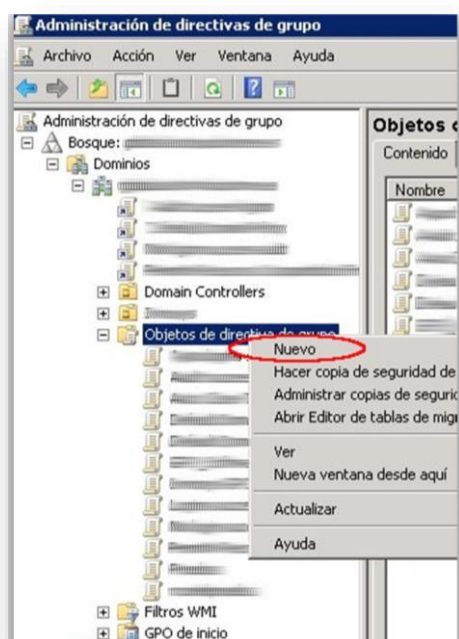


IMPORTANT NOTE.

It is important that the installers are MSI.

STEPS TO BE TAKEN

To generate the policy to perform the unattended installation, it is done through the **Group Policy Manager**. To access this panel, from the domain controller, the command "**gpmc**" must be executed.



Within this pane, by scrolling down to the domain used, and under **Group Policy Objects**, a new one must be created.

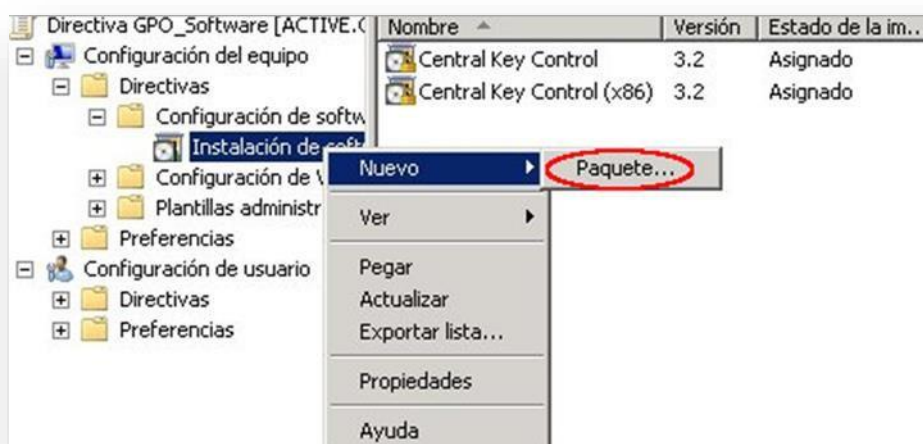




Edit the policy created.



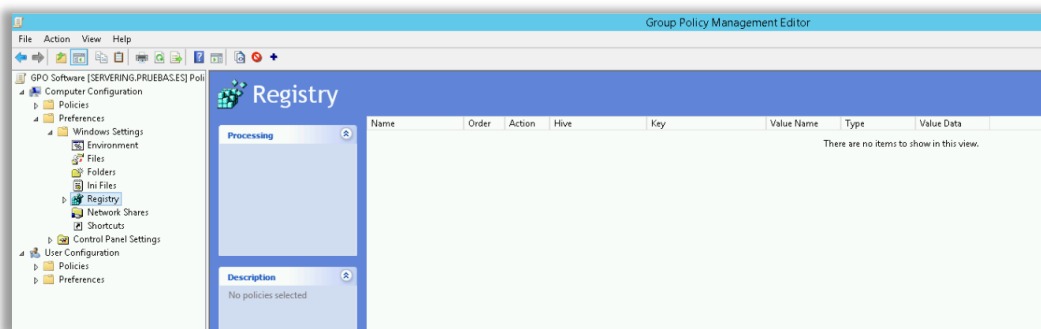
In the new window, follow the path: **Device Configuration > Políticas > Software Configuration > Software Installation**. In this last section, a new package will be created for each MSI.



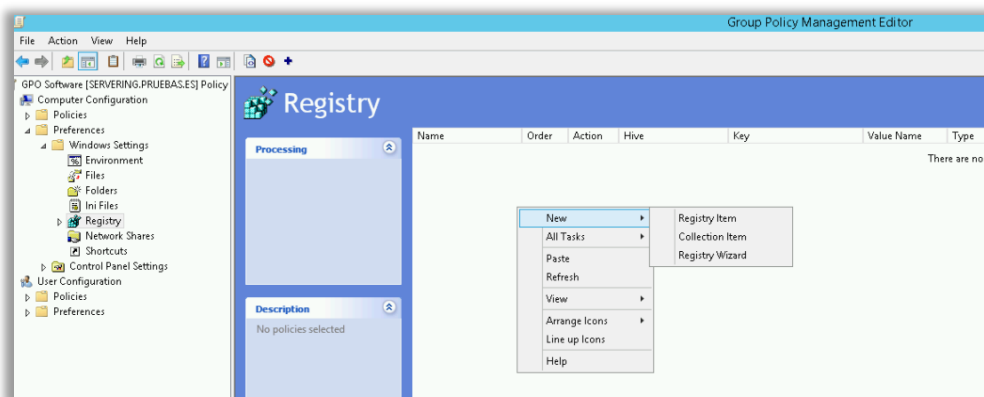


Once the 32-bit and 64-bit packages are available, the next step is to configure the driver variables, to access the following path:

Computer Configuration > Preferences > Windows Settings > Registry



The variables will be configured by right clicking with the mouse on the Registry window > **New** > **Registry Item**.



IMPORTANT NOTE.

The variables depend on the configuration, for more information consult your project manager.





In the KeyController parameterization options, there are certain fields that can be locked so that users cannot change their value.

See the section on [configuration with command line parameters](#) for the.

As an example of setting fixed and editable variables, see the example images:

Field fixed or not editable by the user (**fixed**).

1. User editable field (**default**).



**IMPORTANT NOTE.**

It is important that the "**Action**" field contains the value "**Replace**" to avoid configuration problems.

The following are several **recommended configurations** (depending on the authentication method) for final installations on client workstations (in production).

4.1. BASIC AUTHENTICATION

The following table indicates the recommended configuration with basic authentication in which the *noupdates* and *nocertdisable* fields are locked.

Parameter	Config (editable or locked)	Value
server	fixed	*
auth	fixed	pass
orga	fixed	**
noupdates	default	1
nocertdisable	default	1

***server**: Contains the url of IvSign

****orga**: Sets the IvSign organizational code.

[If you do not have this information, you should ask your Project Manager for it].

As a result of the above configuration, the driver will be configured as follows:





Configuration CSP

KeyController **IVNOSYS**
INNOVACIÓN Y TECNOLOGÍA

Server: ivsign.net

Authentication: User and password

Organization ID: orga

User: user

Password: *****

Try out Accept Cancel

Unvalidated configuration





4.2. FEDERATED AUTHENTICATION

This configuration sets the recommended configuration with federated authentication in which the *noupdates* and *nocertdisable* fields are locked.

Parameter	Config (editable or locked)	Value
server	fixed	*
auth	fixed	federated
fedcode	fixed	**
orga	fixed	***
noupdates	default	1
nocertdisable	default	1

***server**: Contains the url of IvSign

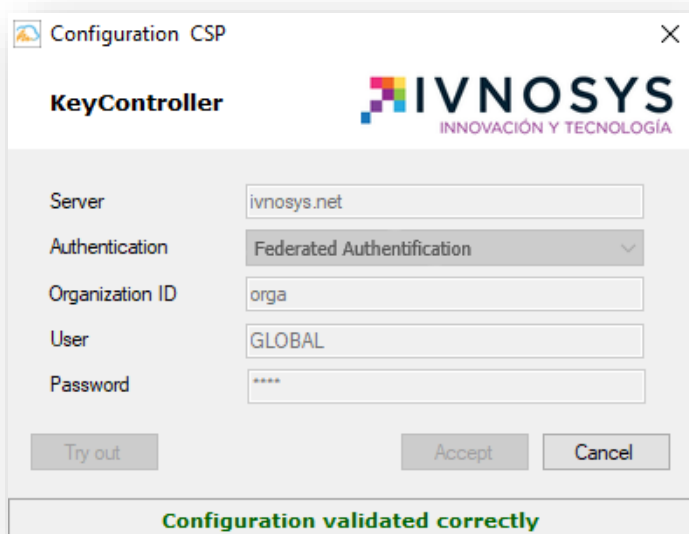
****fedcode**: Federation code. Required for the use of federated authentication and provided at the beginning of the project.

*****orga**: Sets the IvSign organizational code.

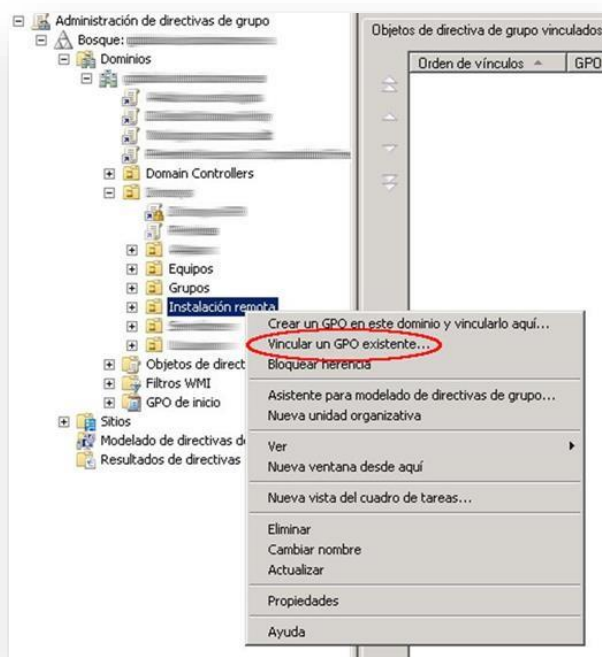
[If you do not have this information, you should ask your Project Manager for it].

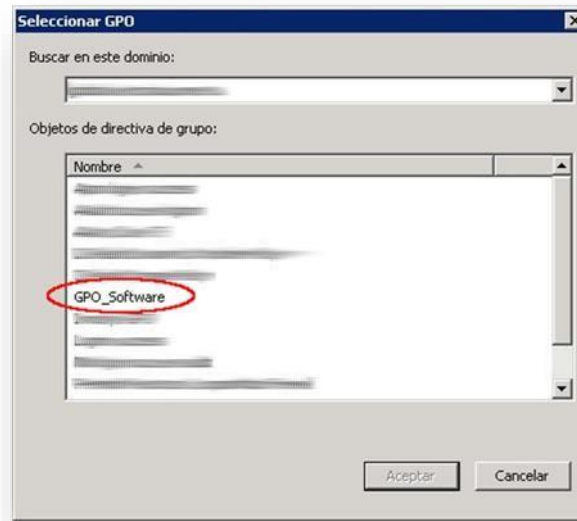
As a result of the above configuration, the driver will be configured as follows:





Finally, in the Group Policy Manager, select the organizational unit containing the computers on which you want to install the driver, and apply the GPO configured in the previous steps by selecting Link an existing GPO.





For the installation to take effect, you can either wait for the computers in question to be re-booted or force an update of the group policies using the command "**gpupdate /force**" (this command must be launched on each client computer).

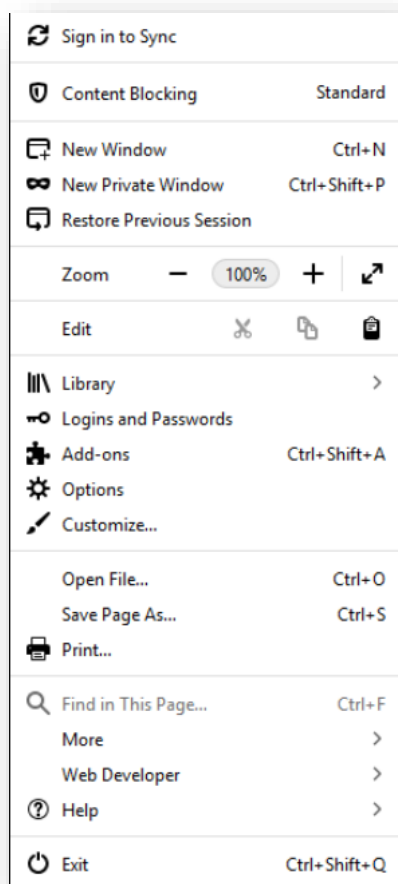




5. CONFIGURATION OF PKCS ENVIRONMENTS#11

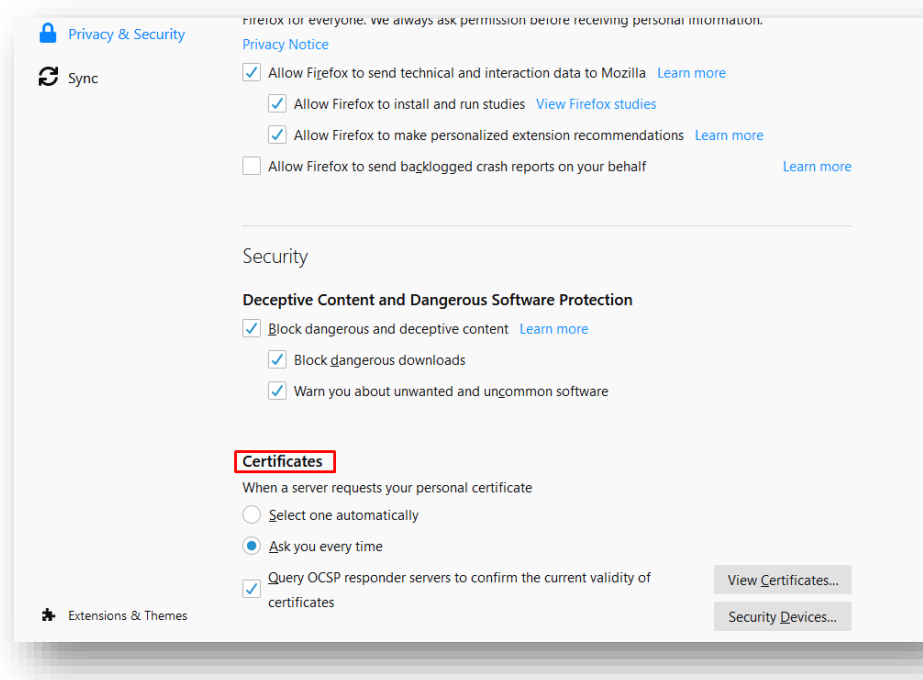
In browsers such as Firefox or other systems that require standard PKCS#11 access, it will be necessary to configure **KeyController Driver** as a specific cryptographic provider, as if it were a SmartCard. The procedure is as follows:

1. Access the **Options** menu



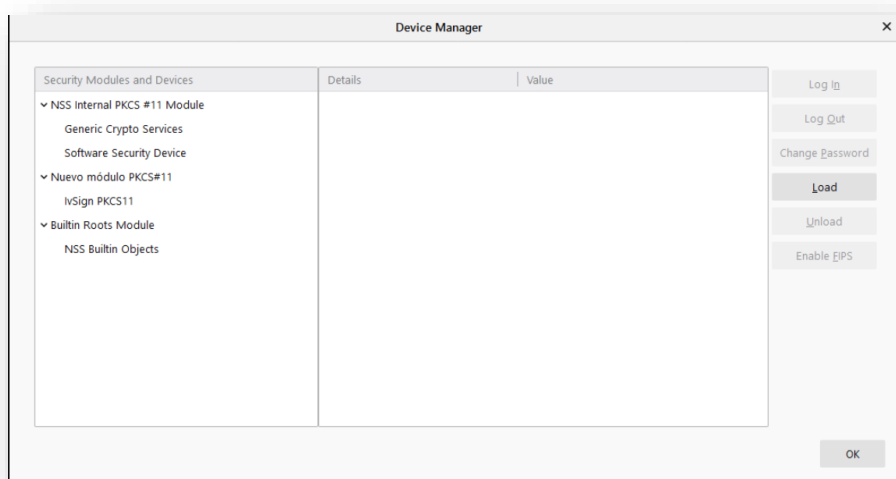


2. In the Privacy and Security section, look for Certificates.



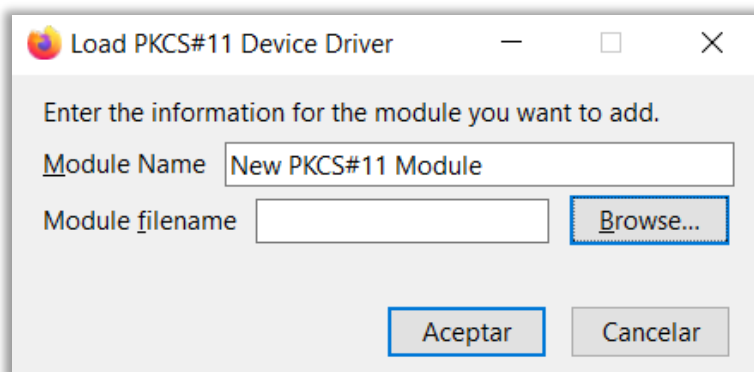
3. Then click on the **Security Devices** button.

The following screen will appear:





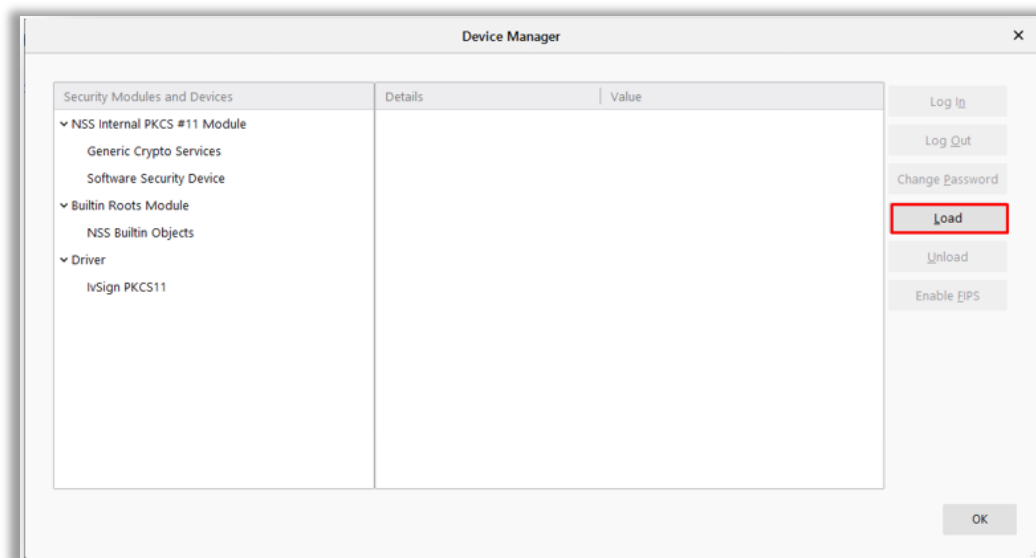
4. Click the **Load button** and select the **PKCS#11** module:



The **location of the driver** is by default in...

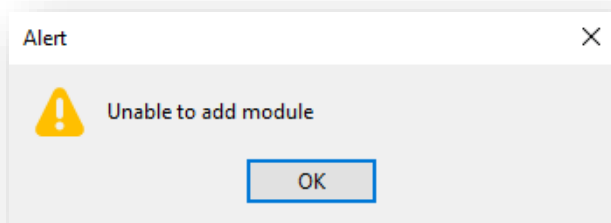
C:\Windows\System32\IVSignPKCS11_64.dll

If everything is correct, it should be configured as follows:

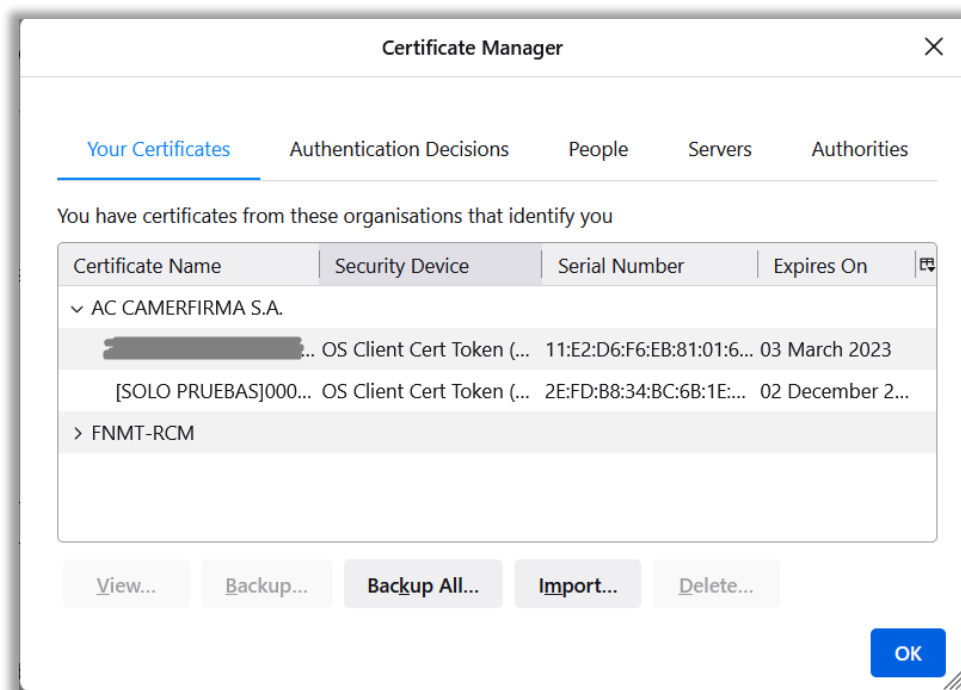




If the path is not correct or the driver version is selected that does not correspond to the browser's build architecture, the following warning will be displayed, and it will not have been configured correctly:



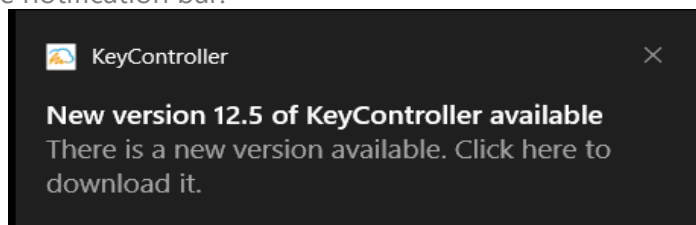
The certificates will then appear in Firefox like any other certificate imported from a p12 or SmartCard:





6. VERSION UPDATE PROCEDURE

Periodically, the **Driver KeyController** will inform about the latest version available, in a notification window in the notification bar.



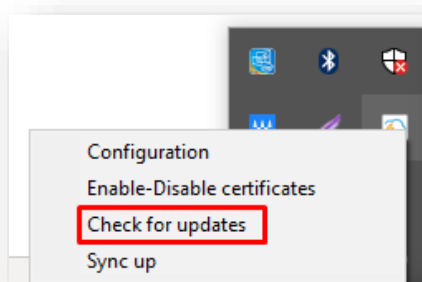
Clicking on the message will download the file that you must **EXECUTE** for the updates to be applied.



IMPORTANT NOTE.

It is essential to have administrator permissions on the computer for it to run correctly.

If you want to check if a new version is available without waiting for the automatic notification, you can do so by clicking on the icon located in the notification bar with the right mouse button on the **Check for updates** option.





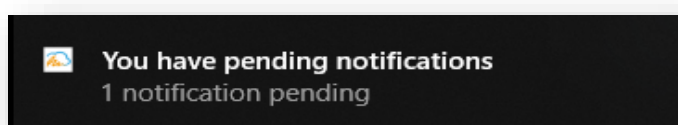
7. MANAGEMENT AND USE OF KEYCONTROLLER

7.1. NOTIFICATION SYSTEM

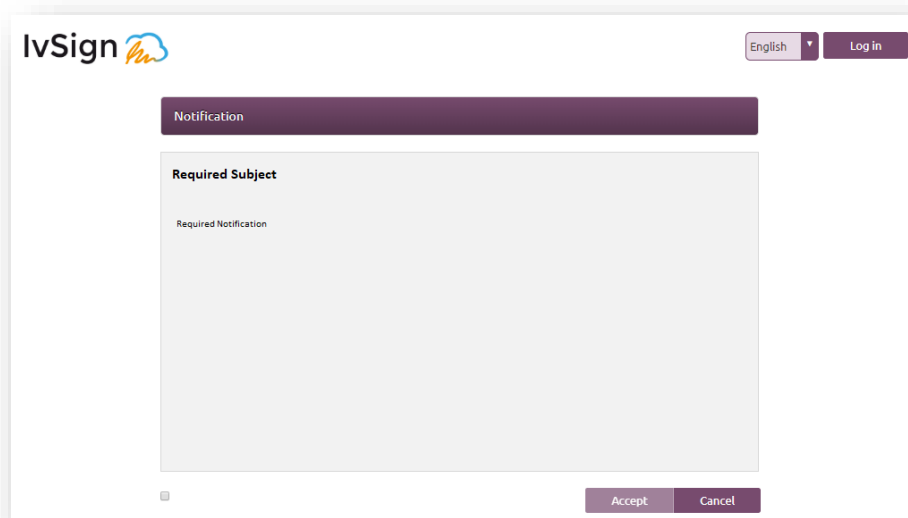
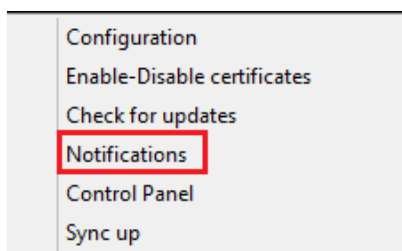
The **IvSign** platform sends informative notifications to users about the platform's own procedures.

To read these notifications you need to access the **IvSign** platform.

The **Driver KeyController** warns that there are notifications pending to be read by displaying the following message:



The **KeyController Driver** Notifications option **is** available when it detects that there are notifications pending to be read. By clicking on the Notifications menu, it opens the browser linked to the **IvSign** platform, so that the user can read the notifications.

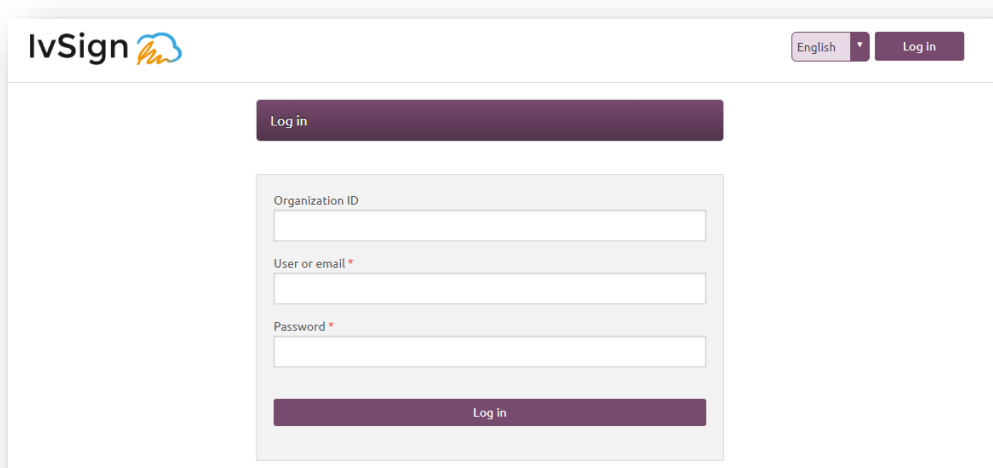
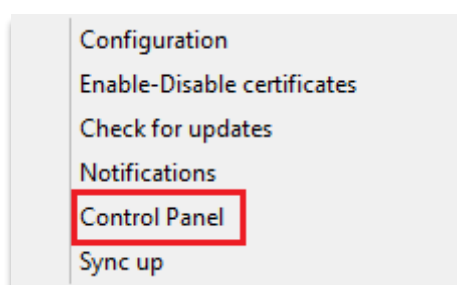




7.2. CONTROL PANEL

The "**Control Panel**" menu option is a direct access from the **Driver KeyController** to the **IvSign** platform.

By clicking on this menu, the browser opens and links to the **IvSign** platform so that the user can log in and access all the options of the platform itself.



It needs to be activated at the configuration level on the computer with the variable *accesopanel=1*, either from the Windows registry or when installing it via command line.





7.3. ENABLING/DISABLING CERTIFICATES

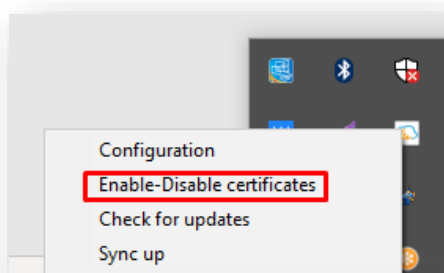


IMPORTANT NOTE.

This option will be available by default unless *nocertdisable=1* is set to hide it when installing.

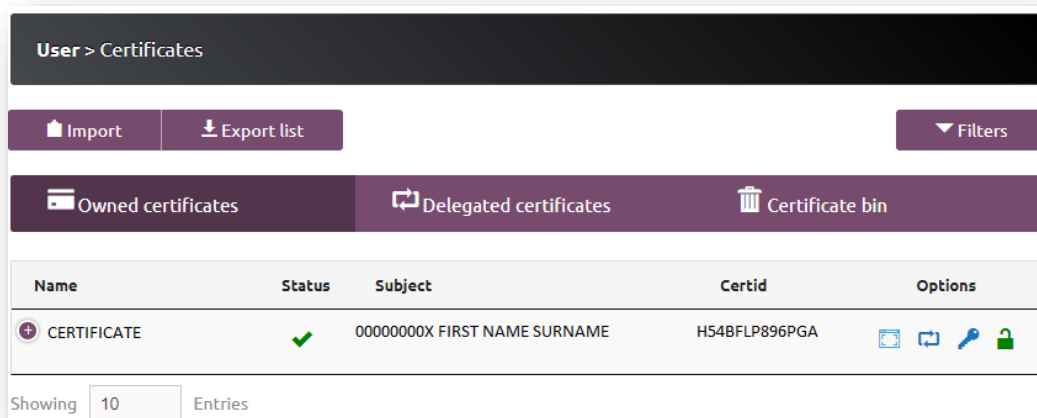
In the case of having many certificates, to prevent all of them from being displayed every time we need to perform an action with them (signing, accessing a website,...) the **Enable/Disable certificates** option is available.

Click on the **Driver KeyController** icon in the notification area with the right mouse button.



This option only allows you to work with certificates that are currently enabled in IvSign.

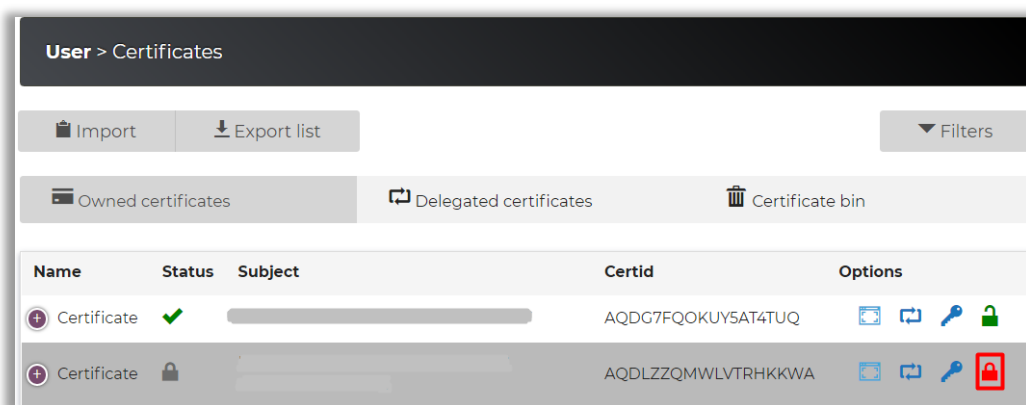
Those with the icon in  the OPTIONS column **will be displayed**.





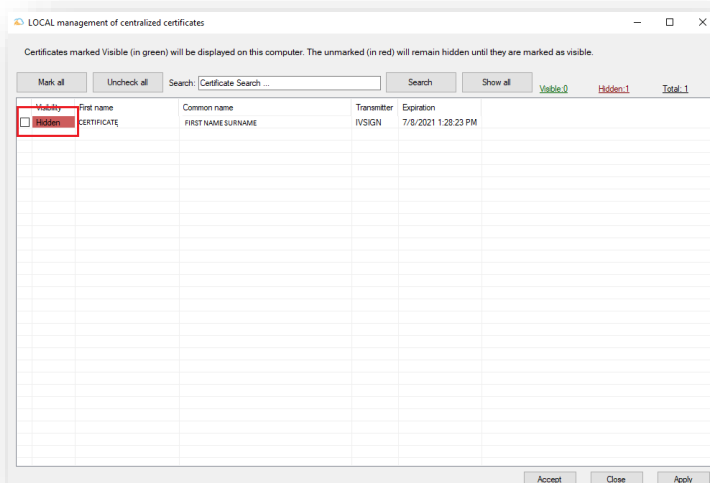
Those that are disabled in IvSign (for having entered the wrong PIN several times, for having been disabled manually, ...), will not be available in the driver.

Those with the icon in  the OPTIONS column **will not be displayed**.



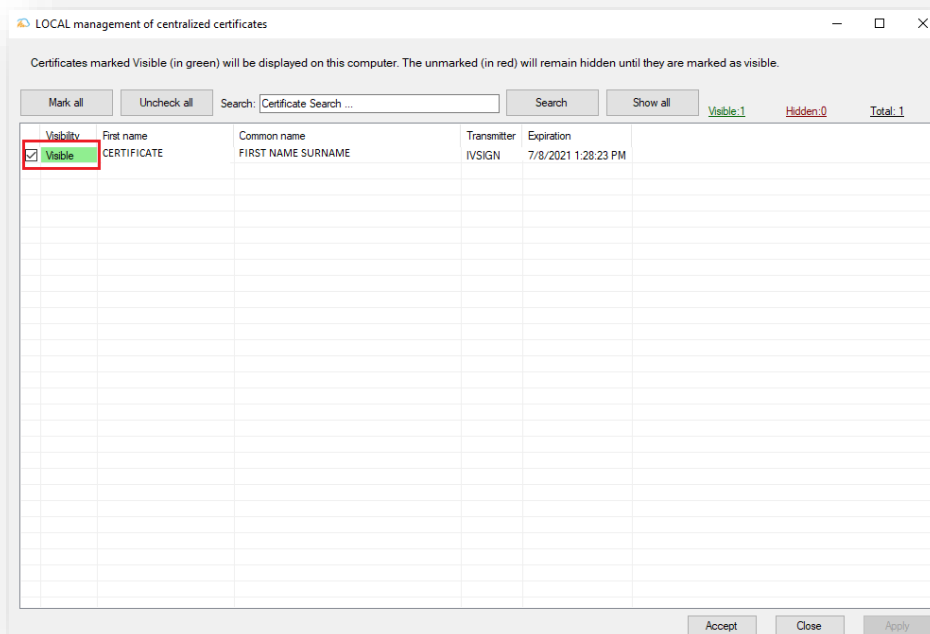
These enable or disable actions will only affect the computer from which it is being accessed. That is to say, if there is a certificate delegated to another user, the enable or disable changes will only work in the equipment where it is being done. The person who has that delegated certificate will have to enable or disable theirs on their computer.

To display a certificate that is hidden, click on the **HIDDEN** checkbox of that certificate.



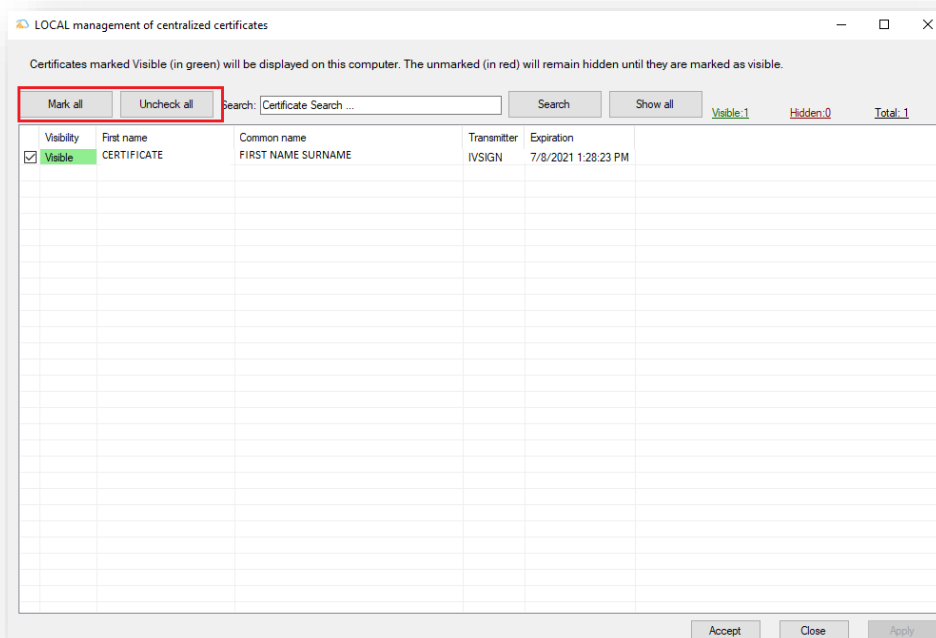
To not display a certificate that is visible, click on the **VISIBLE** checkbox of that certificate.





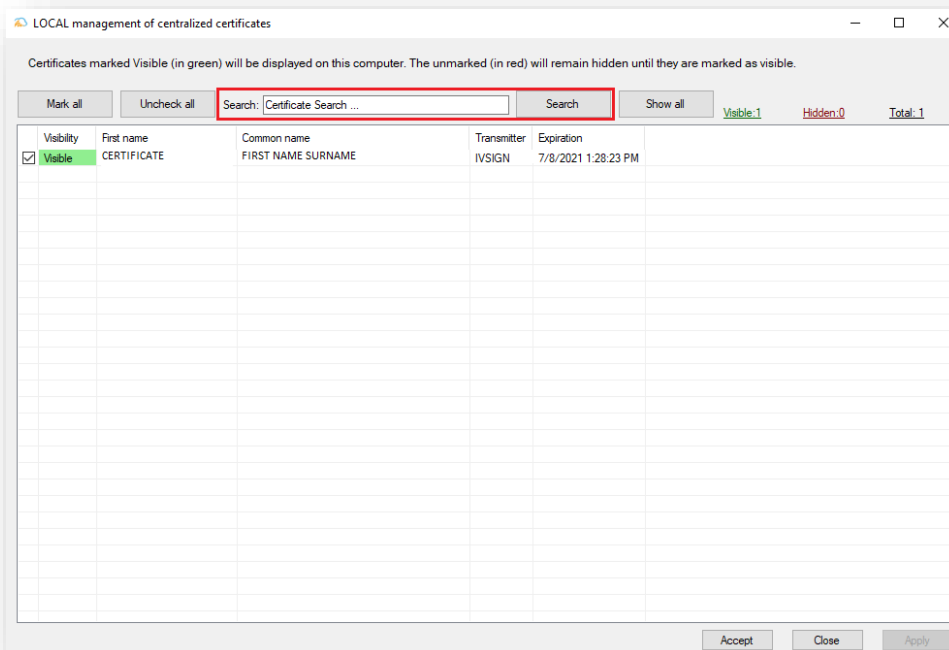
In both cases, the VISIBILITY will change automatically.

These actions can be performed individually or in bulk by clicking on **Check all** or **Uncheck all**.



The certificates can be filtered by the content of all the columns (Visibility, Name, Common Name, Issuer or Expiration) by entering the text in the **Search** field and pressing ENTER or the **Search** button. All the certificates that match the text indicated will be displayed.





To show all certificates again and to be able to make another filter, click on **Show all**.

