Consejo General de Colegios
Administradores de Fincas
España

Manual de instalación del Driver KeyController

CAFirma

COPYRIGHT©

El copyright de este documento es propiedad de Ivnosys Soluciones.

**No está permitido su reproducción total o parcial
ni su uso con otras organizaciones para ningún otro propósito,
excepto autorización previa por escrito.**

IVNOSYS
INNOVACIÓN Y TECNOLOGÍA

CONTENIDO

1. *Driver KeyController para CAFirma – Plataforma de Centralización de Claves* _____ 2
2. *Instalación del driver criptográfico Driver KeyController* _____ 3
3. *Configuración del driver criptográfico Driver KeyController* _____ 9
4. *Habilitar/Deshabilitar certificados* _____ 11
5. *Actualizaciones del driver criptográfico Driver KeyController* _____ 15

1. Driver KeyController para CAFirma – Plataforma de Centralización de Claves

CAFirma – Plataforma de Centralización de Claves es la solución para la firma electrónica segura.

Con **CAFirma**, no será necesario tener el certificado instalado en el propio dispositivo, gracias a que permite la centralización de todos los certificados en la propia **CAFirma.**

CAFirma consiente el almacenamiento de firma segura de los certificados digitales, para autorizar su uso en equipos de diversos usuarios, procesos y páginas web de forma centralizada y con trazabilidad de las operaciones.

Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en internet, la firma electrónica de documento y cifrar las comunicaciones y contenido.

Para ello es necesaria la instalación y posterior configuración del **Driver KeyController**.

2. Instalación del driver criptográfico Driver KeyController

Para usar el certificado con sus aplicaciones Windows, de igual modo que si se tratase de un certificado en SmartCard o Software, necesitará disponer del Driver KeyController que podrá descargar y configurar siguiendo estos sencillos pasos.

Accediendo a la siguiente url: https://ivsdriver.com/ deberá leer y aceptar el acuerdo de licencia, antes de proceder a su descarga, pulsando la opción '**He leído y acepto el acuerdo de licencia**'.

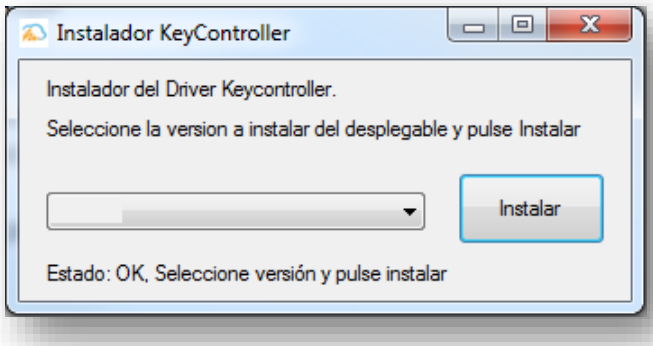
Para descargar el driver dispondrá de dos opciones:

- Pulsar sobre **KeyController Installer**: detectará la arquitectura correspondiente a su equipo y descargará e instalará la última versión disponible para su equipo.
- Pulsar sobre la versión correspondiente, según la arquitectura de su procesador:
  - **KeyController 64 bits**: para equipos con arquitectura de 64 bits.
  - **KeyController 32 bits**: para equipos con arquitectura de 32 bits.

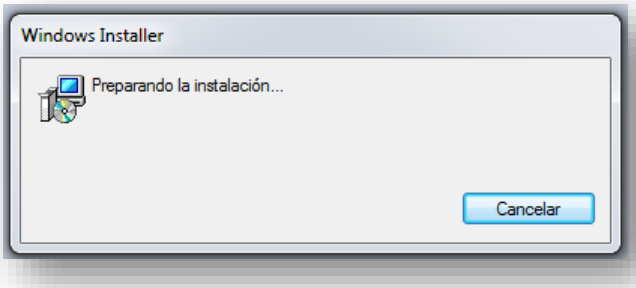
Tras pulsar sobre el enlace correspondiente, deberá ejecutar el fichero descargado.

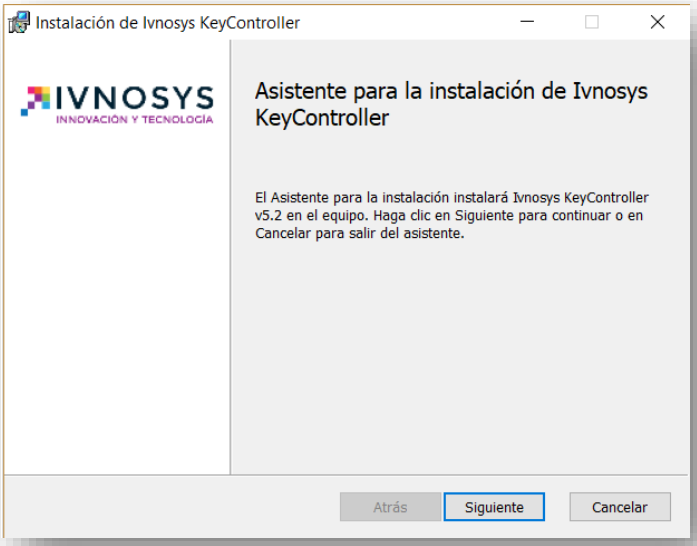
NOTA. Para instalar el driver es necesario tener permisos de administrador en el equipo.

Se mostrará la ventana para la instalación, en la que podrá seleccionar la versión que desea instalar.



A continuación, tras pulsar **Instalar**, se mostrará el asistente para la instalación.

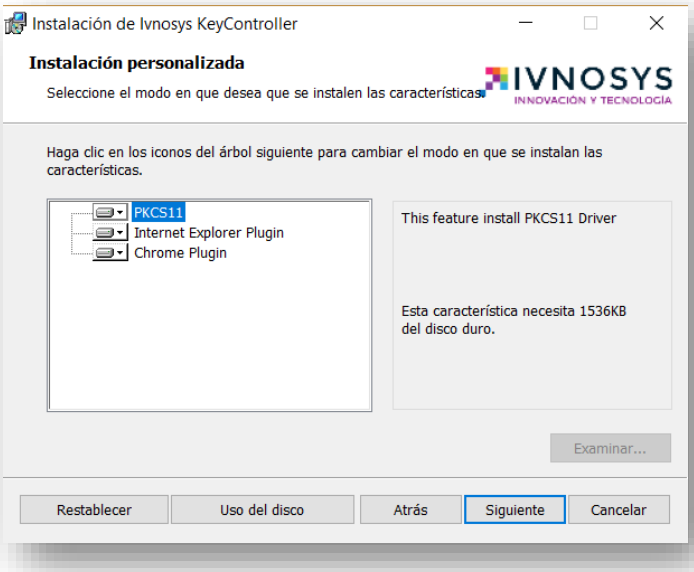




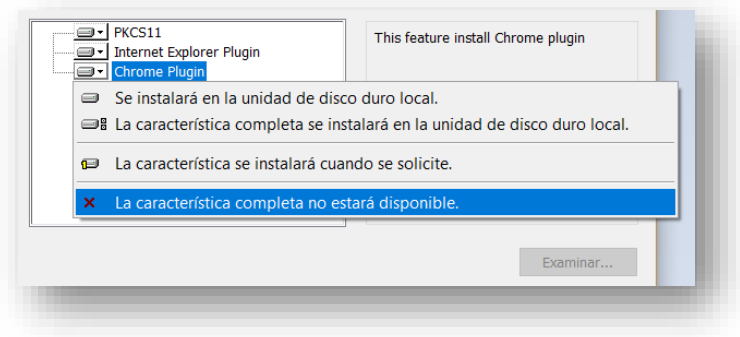
Tras aceptar los términos de la licencia, marcando la casilla ACEPTO LOS TÉRMINOS DEL CONTRATO DE LICENCIA, se activará el botón que permite iniciar la instalación.

La siguiente pantalla permite seleccionar los componentes del Driver KeyController que se desea incluir en el proceso de instalación.

No obstante, la recomendación es que se mantengan los valores por defecto, manteniendo la instalación de todos los componentes.



Al pulsar sobre cada componente, se abrirá el menú contextual con todas las opciones disponibles para cada uno.

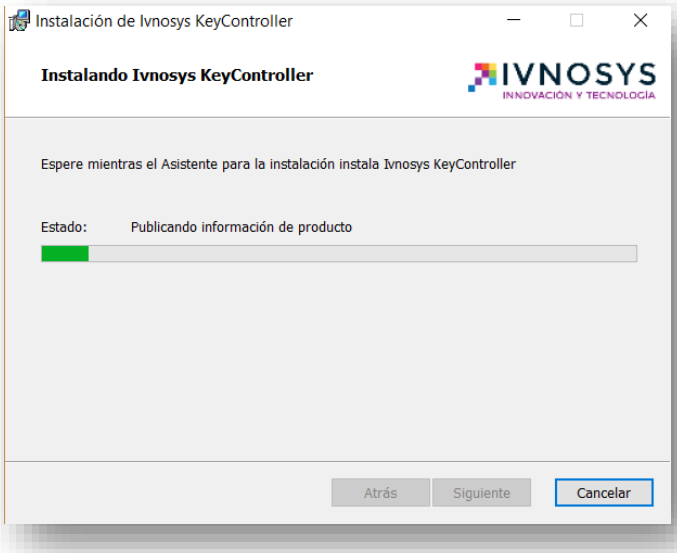


Por defecto todos los componentes vendrán marcados con la opción **Se instalará en la unidad de disco duro local**.

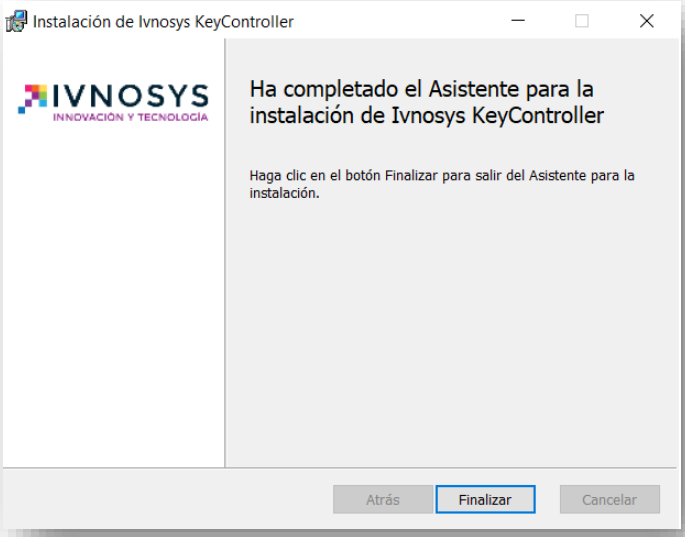
Si no se desea instalar, se deberá marcar la opción **La característica completa no estará disponible**.

Tras pulsar sobre la opción **Siguiente**, se solicitará confirmación para iniciar el proceso de instalación, en base a los parámetros seleccionados previamente.

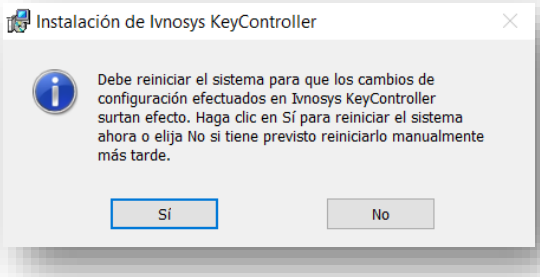
Pulsando sobre la opción **Instalar**, se mostrará la ventana que indicará el estado de la instalación, a través de la barra de progreso.



Finalizada la instalación, se pulsará el botón **FINALIZAR** para salir del asistente.



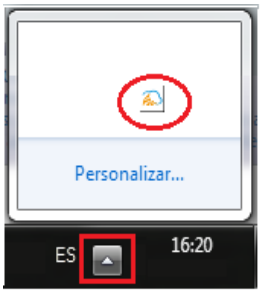
Por último, se solicitará el reinicio del equipo mediante el siguiente cuadro de diálogo:



IMPORTANTE: El reinicio del equipo es un requisito para garantizar el correcto funcionamiento del sistema. Si no se permite o si se omite dicho reinicio, es posible que el driver no se ejecute correctamente o que presente un comportamiento inestable.

En el caso de que no sea posible reiniciar el equipo de forma inmediata, hay que asegurarse de que este reinicio se lleve a cabo a posteriori, antes de que los usuarios finales empiecen a trabajar con el driver.

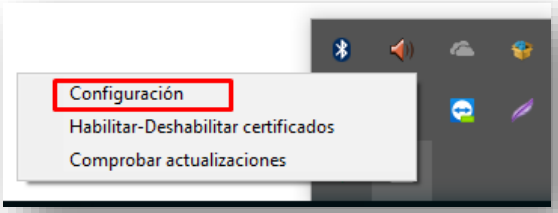
El icono del **Driver KeyController** se mostrará en la zona derecha de la barra de tareas de Windows, en el área de notificaciones.



3. Configuración del driver criptográfico Driver KeyController

Para poder hacer uso de los certificados centralizados en **CAFirma**, se deberá configurar la aplicación siguiendo los pasos indicados a continuación.

Pulsando sobre el icono del **Driver KeyController**, situado en el área de notificaciones, con el botón derecho del ratón, se mostrará el siguiente menú de opciones.



Se deberá pulsar sobre la opción **Configuración**, que deberá completarse con la siguiente información:

- **Servidor**: caf.ivsign.net
- **Autenticación**: seleccionar la opción Usuario y contraseña.
- **ID Organización**: se deberá dejar vacío o con la información que aparezca por defecto.
- **Usuario** y **Password**: deberá indicar los datos facilitados en el correo *Bienvenido al servicio CAFirma – Plataforma de Centralización de Claves*, para acceder a https://caf.ivsign.net
    - **Si se ha modificado la contraseña, deberá introducir la nueva y no la del correo.**

Podrá comprobar si las credenciales indicadas son correctas, pulsando el botón **Probar**.

Si las credenciales indicadas son correctas o incorrectas, se mostrará un mensaje indicándolo, en la parte inferior de la ventana de configuración.

Finalizadas las comprobaciones de la configuración indicada, se pulsará **Aceptar**.

Los certificados que tuviera centralizados en **CAFirma**, se mostrarán desde los navegadores y aplicaciones que hagan uso del almacén estándar de Windows.

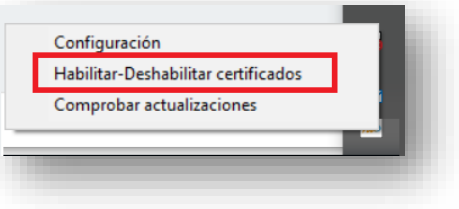
En caso de no mostrarse de forma automática, sería recomendable reiniciar el sistema.

NOTA. Los certificados centralizados no pueden ser eliminados del sistema manualmente, ni tampoco podrá ser exportada su clave privada, pues en ningún caso se encuentran en el equipo donde se configuran.

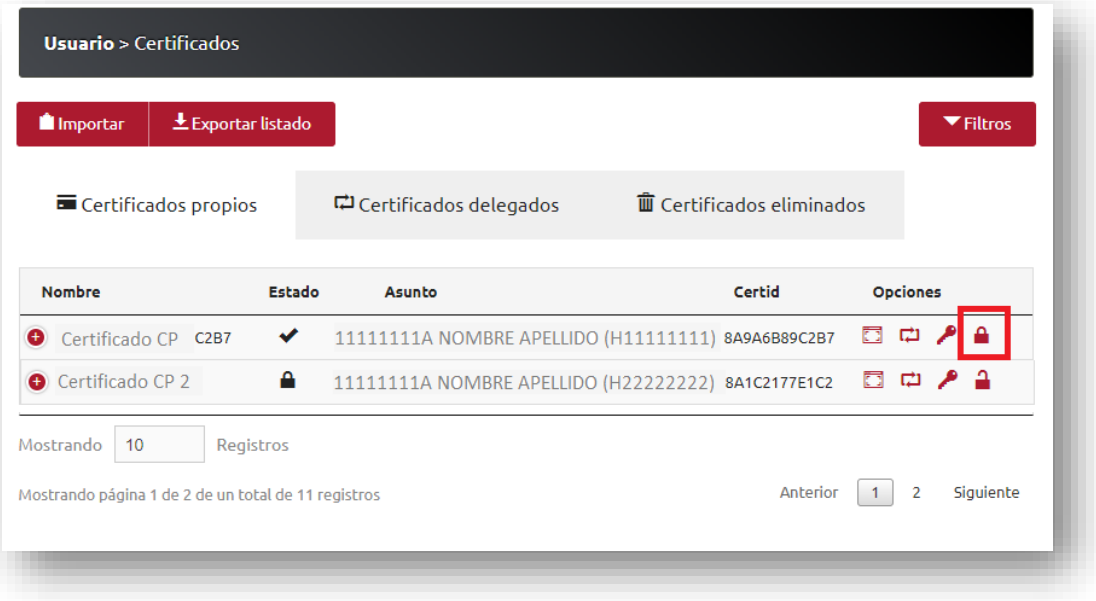
4. Habilitar/Deshabilitar certificados

En el caso de disponer de muchos certificados, para evitar que se muestren todos cada vez que necesitemos realizar alguna acción con ellos (firmar, acceder a una web,…) está disponible la opción de **Habilitar/Deshabilitar certificados**.

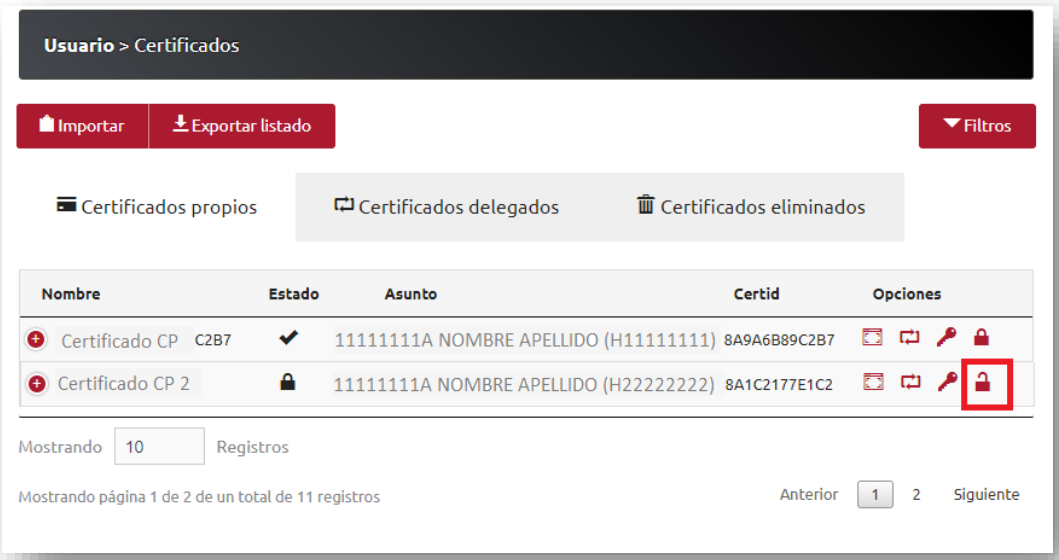
Pulsando sobre el icono del **Driver KeyController**, situado en el área de notificaciones, con el botón derecho del ratón.



Esta opción únicamente permite trabajar con los certificados que actualmente están habilitados en CAFIRMA – Plataforma de Centralización de Claves IvSign.
Los que dispongan del icono 🔒 en la columna OPCIONES **si se mostrarán**.

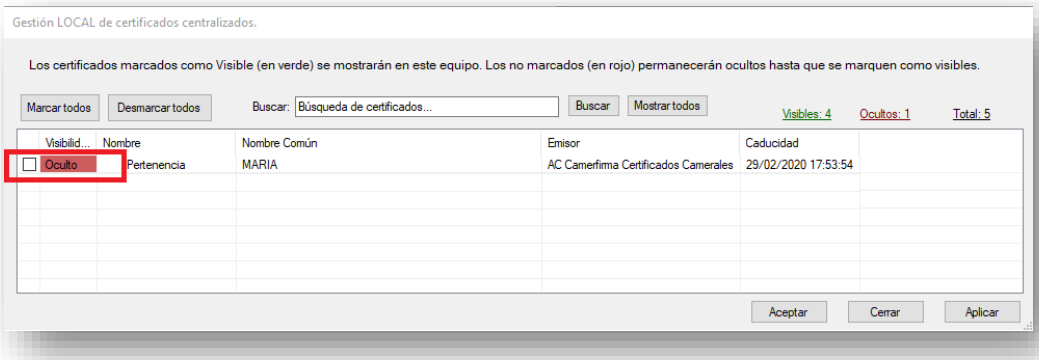


Los que se encuentren deshabilitados en CAFIRMA (por haberse puesto mal el PIN varias veces, por haber sido deshabilitados manualmente, …), no se mostrarán disponibles en el driver.
Los que dispongan del icono 🔓 en la columna OPCIONES **no se mostrarán**.

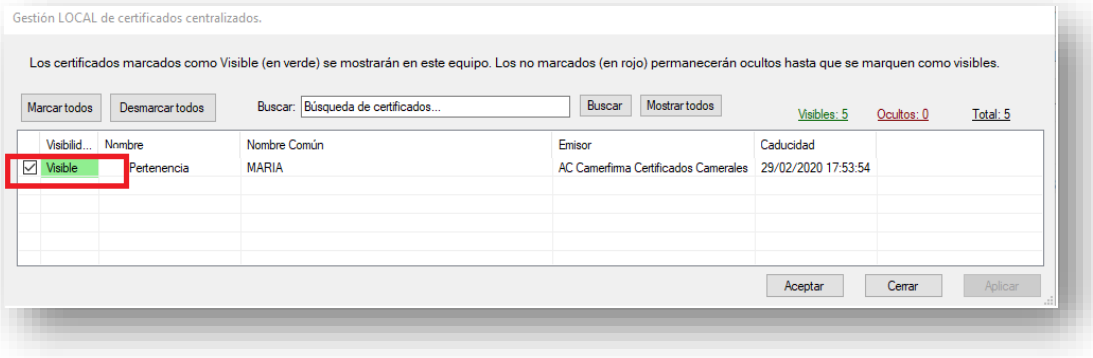


Estas acciones de habilitar o deshabilitar, sólo afectaran al equipo desde el que se está accediendo. Es decir, si existe un certificado delegado a otro usuario, los cambios de habilitar o deshabilitar, únicamente funcionarán en el equipo en el que se está haciendo. La persona que tenga ese certificado delegado deberá habilitar o deshabilitar los suyos en su equipo.

Para mostrar un certificado que esté oculto, se pulsará la casilla **OCULTO** de ese certificado.

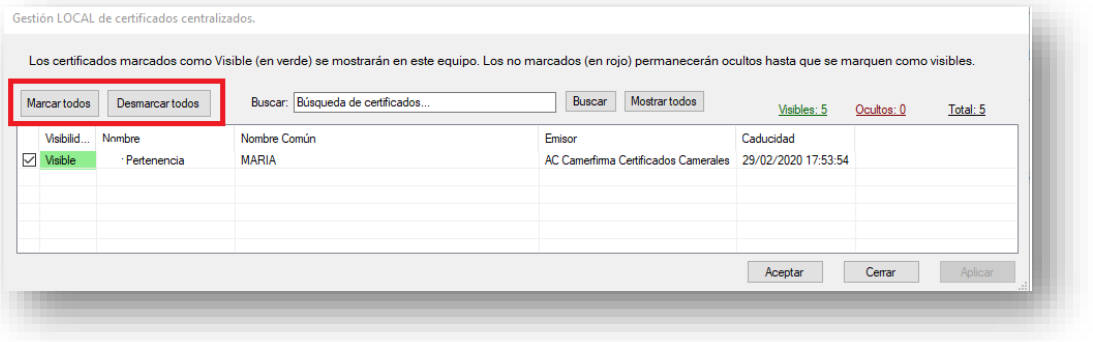


Para no mostrar un certificado que esté visible, se pulsará la casilla **VISIBLE** de ese certificado.

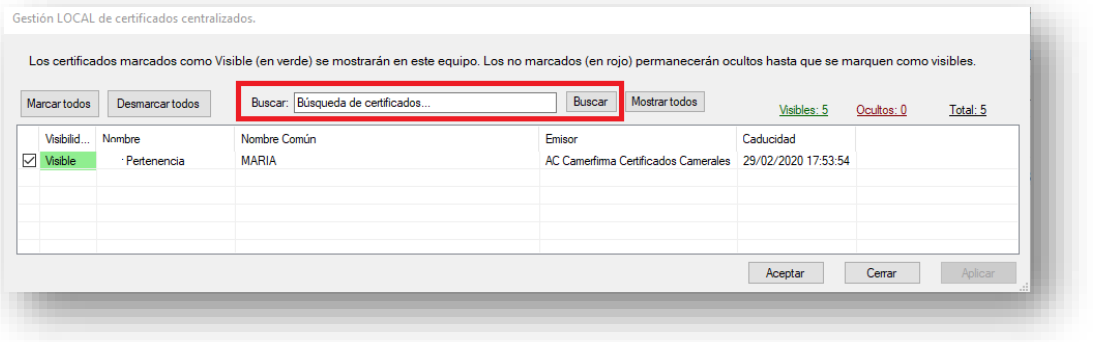


En ambos casos, la VISIBILIDAD cambiará automáticamente.

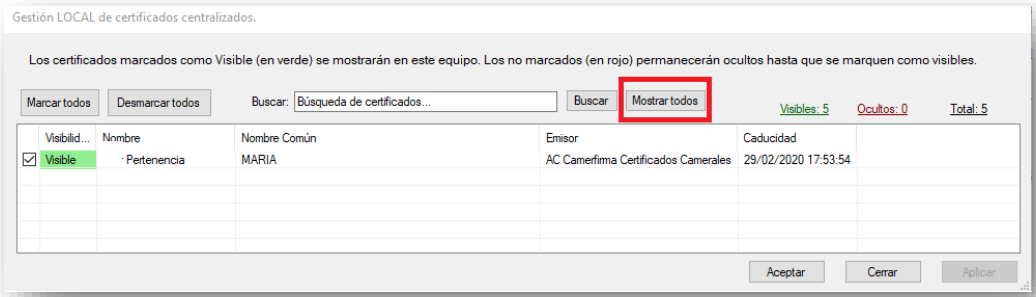
Estas acciones se podrán realizar de forma individual o de forma masiva pulsando **Marcar todos** o **Desmarcar todos**.



Se podrán filtrar los certificados por el contenido de todas las columnas (Visibilidad, Nombre, Nombre Común, Emisor o Caducidad) indicando el texto en el campo **Buscar** y pulsando INTRO o el botón **Buscar**. Se mostrarán todos los certificados que coincidan con el texto indicado.



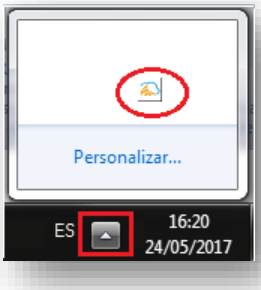
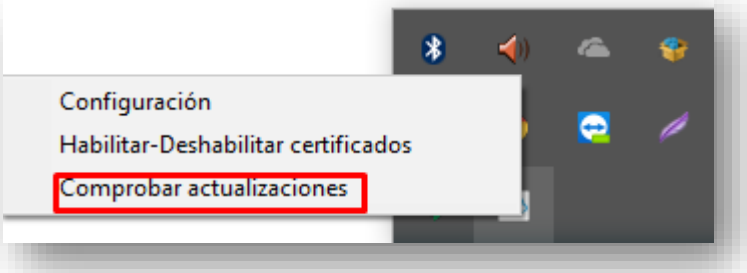
Para volver a mostrar todos los certificados de nuevo y poder realizar otro filtro, se pulsará **Mostrar todos**.


Gestión LOCAL de certificados centralizados.
Los certificados marcados como Visible (en verde) se mostrarán en este equipo. Los no marcados (en rojo) permanecerán ocultos hasta que se marquen como visibles.
Marcar todos
Desmarcar todos
Buscar:
Búsqueda de certificados...
Buscar
Mostrar todos
Visibles: 5
Ocultos: 0
Total: 5
Visibilid...
Nombre
Nombre Común
Emisor
Caducidad
Visible
Pertenencia
MARIA
AC Camerfirma Certificados Camerales
29/02/2020 17:53:54
Aceptar
Cerrar
Aplicar

5. Actualizaciones del driver criptográfico Driver KeyController

Periódicamente, el **Driver KeyController** informará de la última versión disponible, en una ventana de aviso en la barra de notificaciones.

Pulsando sobre el mensaje, se descargará el fichero que deberá **EJECUTAR** para que se apliquen las actualizaciones.

NOTA. Será imprescindible disponer de permisos de administrador en el equipo, para que se ejecute correctamente.

En caso de querer comprobar si está disponible alguna nueva versión sin esperar a la notificación automática, se podrá hacer la comprobación pulsando, sobre el icono situado en la barra de notificaciones, con el botón derecho del ratón, sobre la opción **Comprobar actualizaciones**.