



**Instalable módulo criptográfico Ceres**  
**Manual de usuario**



## TABLA DE CONTENIDO

<b>1.</b>	<b>INTRODUCCIÓN .....</b>	<b>1</b>
<b>2.</b>	<b>REQUISITOS .....</b>	<b>1</b>
<b>3.</b>	<b>INSTALACIÓN .....</b>	<b>2</b>
1.1.	Módulo CSP .....	6
1.2.	Módulo PKCS#11 .....	6
1.3.	Certificados raíz .....	7
1.4.	Herramientas de utilidades de la tarjeta Ceres .....	10
<b>4.</b>	<b>ACTUALIZACIÓN .....</b>	<b>10</b>
1.5.	Actualización menor .....	11
1.6.	Actualización mayor .....	13
<b>5.</b>	<b>MANTENIMIENTO .....</b>	<b>14</b>
1.7.	Desinstalación .....	16
1.8.	Reinstalación .....	18
1.9.	Modificación .....	20
<b>6.</b>	<b>VERSIÓN DESATENDIDA .....</b>	<b>20</b>

## 1. INTRODUCCIÓN

El objetivo del Instalable módulo criptográfico Ceres es proporcionar al usuario de la tarjeta Ceres un ejecutable que le permita la utilización de la misma desde un equipo con entorno Microsoft Windows.

Es un programa multilinguaje, que posibilita la instalación en castellano, catalán, gallego, euskera o inglés.

Hay dos versiones del instalable: una para sistemas con arquitectura de 32 bits y otra para 64 bits. En éste último caso, el instalable preparará el equipo para que el usuario pueda utilizar la tarjeta Ceres tanto para la versión de 64 bits de Internet Explorer como para la de 32 bits.

La instalación se realiza mediante un asistente, que va mostrando ventanas para guiar al usuario durante el proceso de instalación. No obstante, también existe la posibilidad de realizar una instalación desatendida del producto.

El ejecutable permite la instalación, actualización y mantenimiento del software. En este manual se documentan detalladamente los pasos de uso del instalable desde el punto de vista del usuario final.

El instalable permite que el usuario indique el directorio de instalación de la aplicación. Por defecto se instalará en *[directorio archivos de programa]\FNMT-RCM*, donde *[directorio archivos de programa]* es el directorio que el equipo tiene asignado para instalar las aplicaciones, usualmente *C:\Archivos de programa*. Cada vez que en este documento se tenga que hacer referencia a dicho directorio de instalación, se le nombrará como *[directorio instalación]*.

Adicionalmente, el instalable copia unas librerías en el directorio de sistema de Windows, usualmente *C:\Windows\system32*. En este documento se denominará este directorio como *[directorio sistema]*.

## 2. REQUISITOS

Para la instalación del Instalable módulo criptográfico Ceres el sistema debe cumplir los siguientes requisitos:

- Una resolución mínima de pantalla de 640×480 píxeles.
- Un procesador de 32 ó 64 bits, y que sea mínimo un 486.
- Una memoria RAM de almenos 16 MBytes.
- Un espacio de disco duro libre mínimo para la instalación.
- Que el sistema operativo sea uno de los siguientes:

- Windows 2000.
  - Windows XP.
  - Windows 2003.
  - Windows Vista.
  - Windows 7.
- Tener instalado al menos uno de los siguientes navegadores:
    - Internet Explorer 5.5 o posterior.
    - Firefox.
  - Que el usuario tenga permisos de administrador.

### 3. INSTALACIÓN

Para instalar la versión *x.y.z* del Instalable módulo criptográfico Ceres, basta con ejecutar el instalable *insmodcripc2vxyz.exe* (en la versión de 32 ó 64 bits, según corresponda), que se puede descargar en el siguiente enlace:

[http://www.cert.fnmt.es/content/pages\\_std/software/insmodcripc2vxyz.exe](http://www.cert.fnmt.es/content/pages_std/software/insmodcripc2vxyz.exe)

Lo primero que aparecerá, como podemos ver en la Ilustración 1, es una ventana en la que se solicita el idioma deseado para la instalación. Las posibles opciones son: castellano, catalán, euskera, gallego e inglés. El resto de las indicaciones de la instalación aparecerán en el idioma seleccionado.

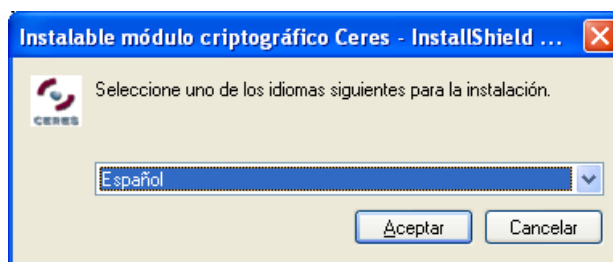


Ilustración 1. Elegir idioma de instalación

Una vez seleccionado el idioma, el instalable muestra una pantalla indicando que se está preparando el asistente para la instalación (Ilustración 2).

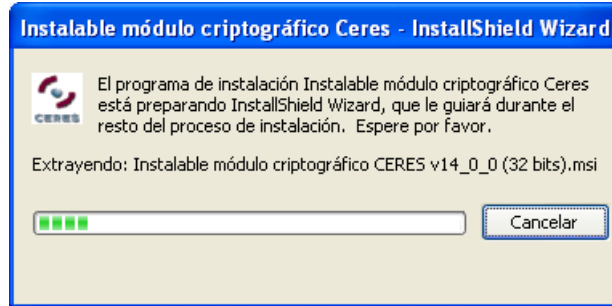


Ilustración 2. Preparando el asistente de instalación

A continuación, automáticamente se muestra una ventana dando la bienvenida al proceso de instalación (Ilustración 3).

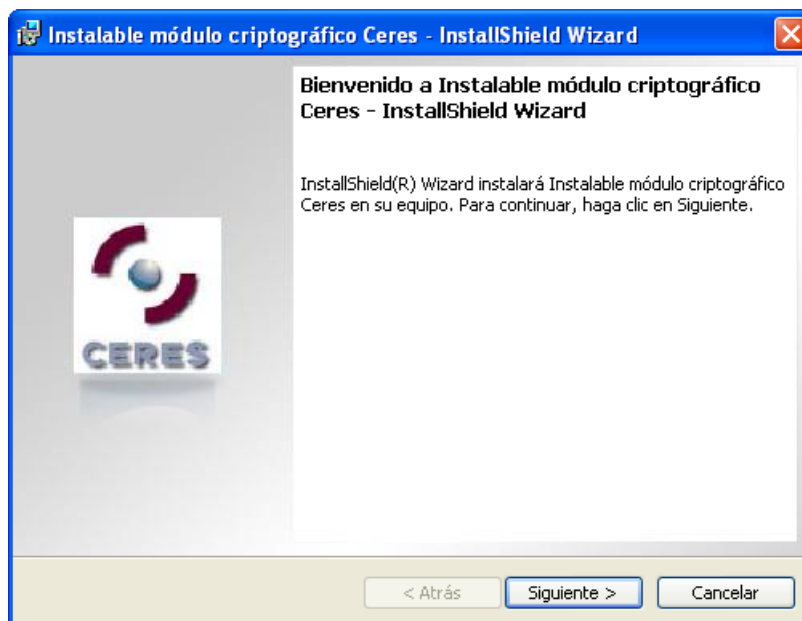


Ilustración 3. Bienvenido al proceso de instalación

Acto seguido, el instalable pedirá al usuario que indique el directorio donde se instalará la aplicación (Ilustración 4). Pulse *Siguiente*> para continuar con la instalación.

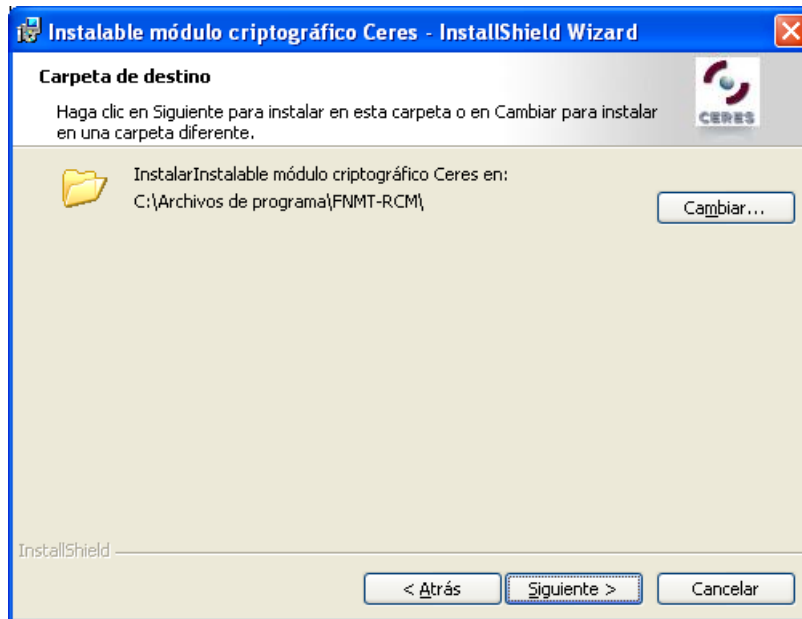


Ilustración 4. Selección del directorio de instalación

Seguidamente, aparece una ventana indicando que el asistente está preparado para comenzar la instalación (Ilustración 5). Pulse *Instalar* para comenzar la instalación.

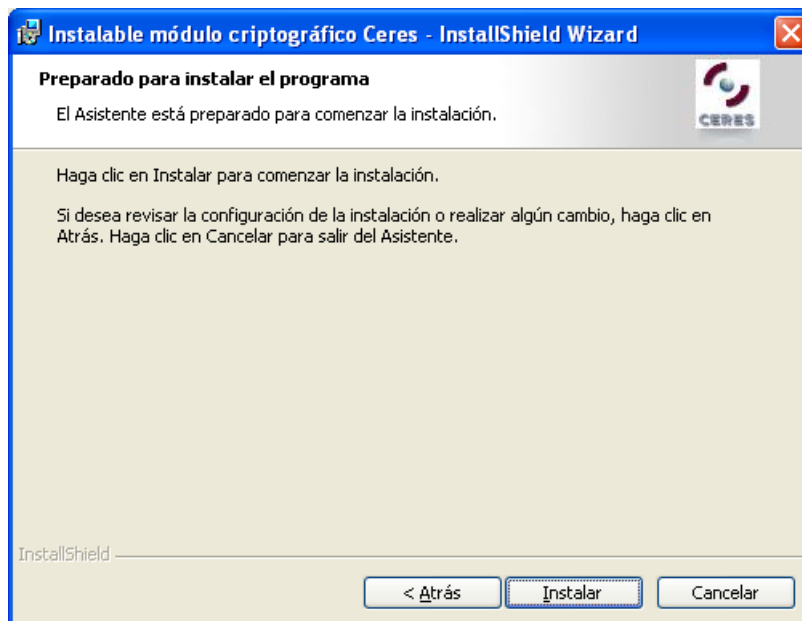


Ilustración 5. Preparado para instalar el programa

Durante el proceso de instalación, el asistente irá mostrando las acciones que se están realizando, así como una barra que indica el progreso de la misma (Ilustración 6).

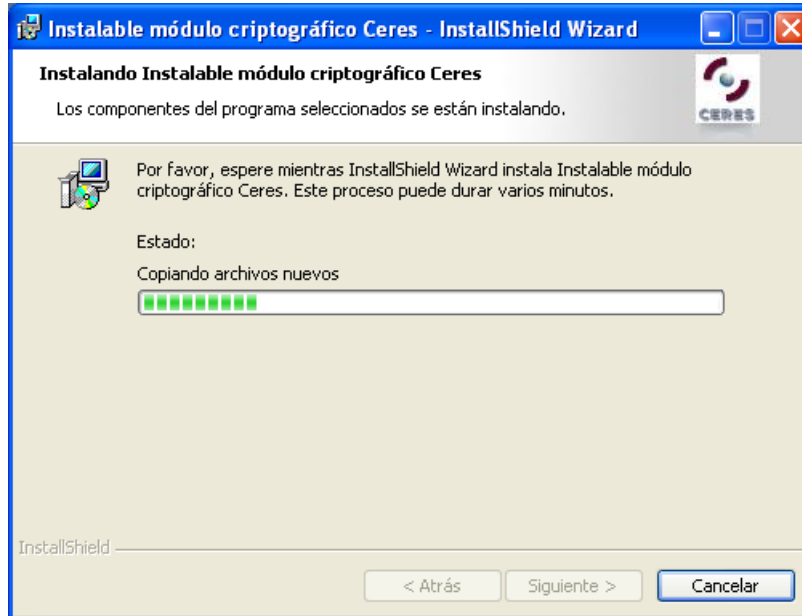


Ilustración 6. Estado de la instalación

Al finalizar, tal y como se muestra en la Ilustración 7, el instalable muestra una pantalla indicando que el proceso de instalación ha finalizado correctamente. Pulse *Finalizar* para salir del asistente

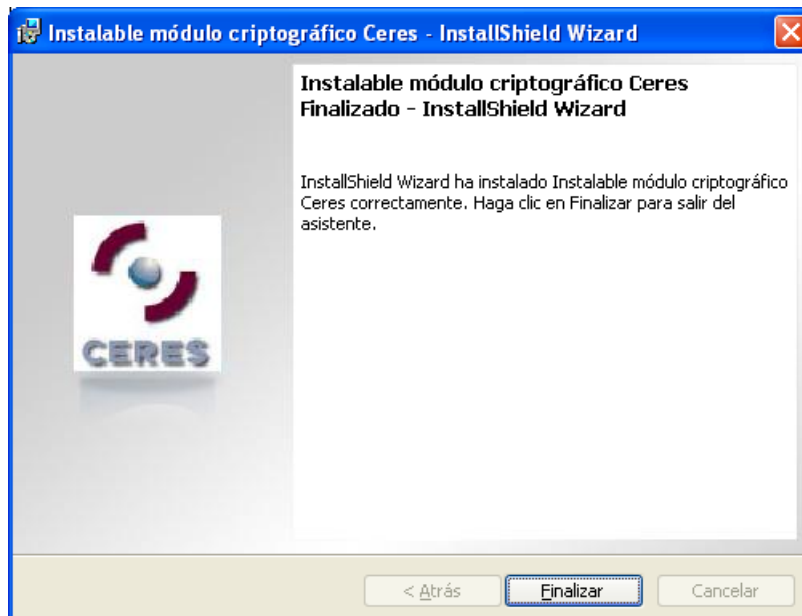


Ilustración 7. Fin de la instalación

Por último, se muestra un aviso indicando que debe reiniciar el sistema (Ilustración 8). Se da al usuario la opción de si desea reiniciar el equipo en ese momento o aplazarlo para más adelante. Hay que tener en cuenta que para completar la instalación es necesario reiniciar el equipo.

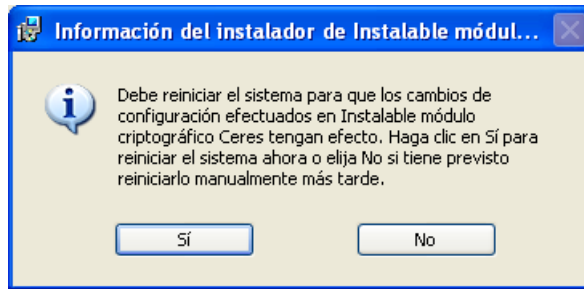


Ilustración 8. Reiniciar el sistema

Una vez finalizado correctamente todo el proceso, se habrán instalado en el equipo los componentes necesarios para el uso de la tarjeta Ceres. A continuación se detallan los más importantes.

## 1.1. Módulo CSP

Para permitir el empleo de la tarjeta Ceres mediante el navegador Internet Explorer, el ejecutable instala y registra las librerías del módulo CSP.

## 1.2. Módulo PKCS#11

El programa comprueba si el equipo tiene instalado el navegador Firefox e instala el módulo PKCS#11 para poder trabajar con la tarjeta Ceres. Para la correcta configuración debe tener cerrado el navegador durante la instalación.

También puede instalar el módulo PKCS#11 manualmente. Para ello, arranque el navegador y abra el menú *Herramientas – Opciones – Avanzado* y seleccione la pestaña *Cifrado* (Ilustración 9). Pulse *Dispositivos de seguridad* y compruebe si dentro de la lista se encuentra el de la FNMT (Ilustración 10). En caso negativo, pulse *Cargar*, dele un nombre al módulo (por ejemplo, *FNMT-RCM Modulo PKCS # 11*) y seleccione el archivo *[directorio sistema]\pkcsv2gk.dll*.

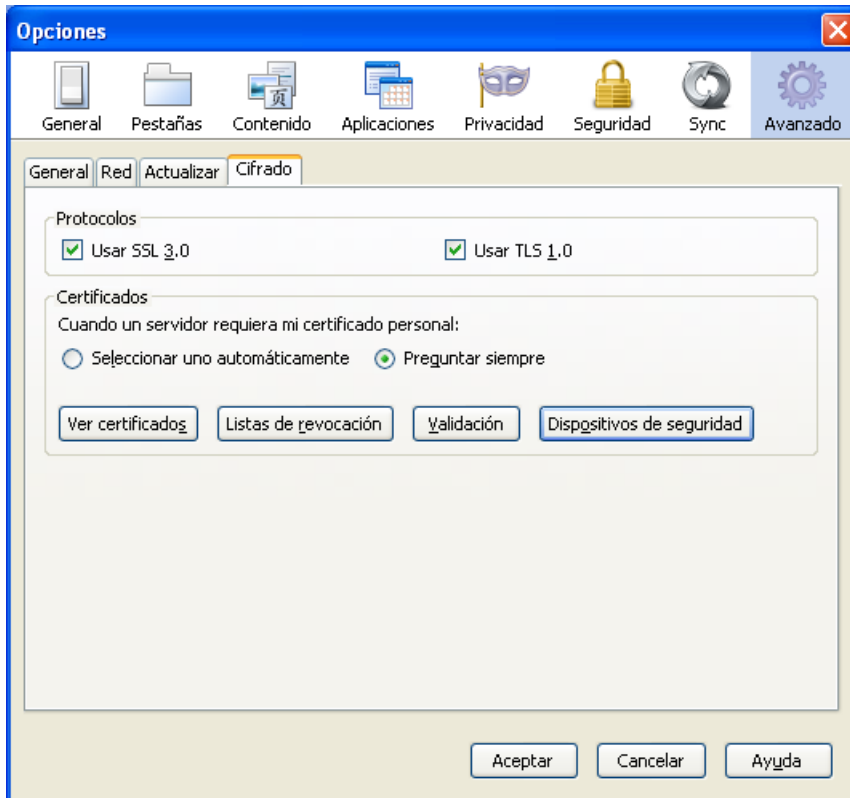


Ilustración 9. Configuración de opciones de cifrado en Firefox

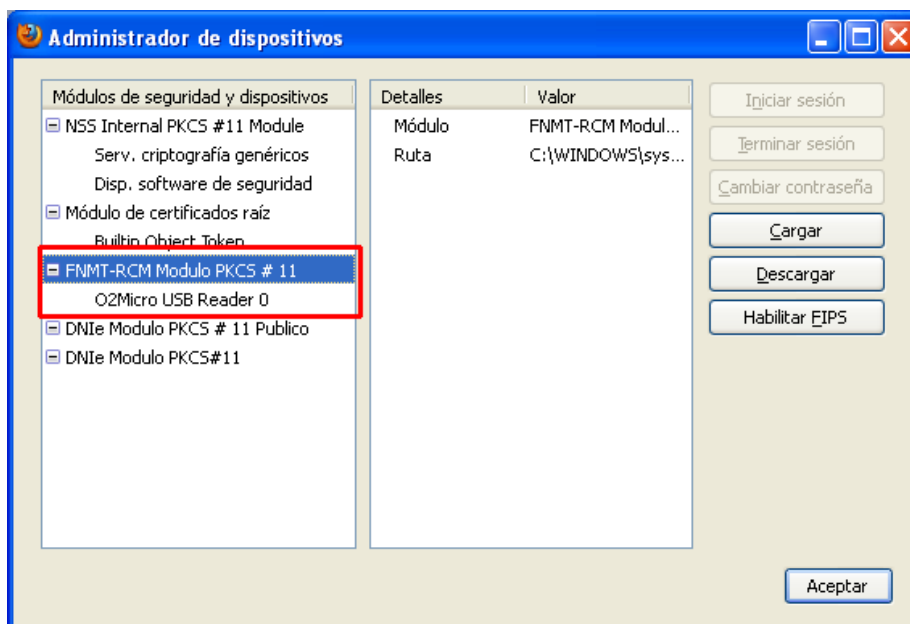


Ilustración 10. Administrador de dispositivos de seguridad en Firefox

### 1.3. Certificados raíz

Los certificados raíz se copian en *[directorio instalación]*.

La instalación de los certificados raíz en Internet Explorer se hace de forma automática durante la ejecución del instalable.

No obstante, la importación de los certificados raíz en Internet Explorer también puede hacerse de forma manual. Para ello, arranque el navegador Internet Explorer, y abra el menú *Herramientas – Opciones de Internet – Contenido*. Pulse el botón *Certificados* y seleccione la pestaña *Entidades emisoras raíz de confianza*. Compruebe si dentro de la lista de certificados se encuentra el de la FNMT (Ilustración 11).

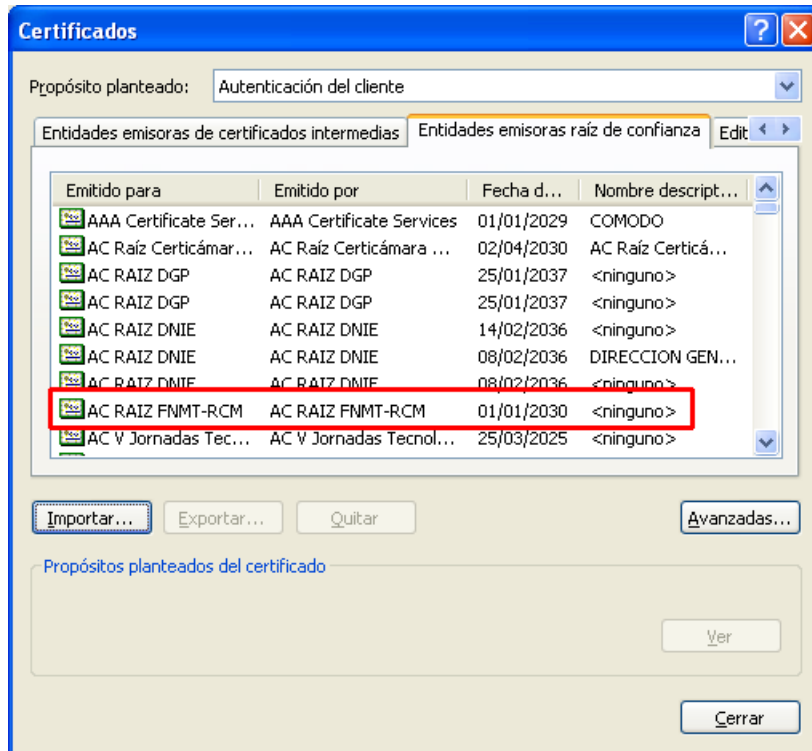


Ilustración 11. Administrador de certificados en Internet Explorer

En caso negativo, pulse *Importar...*, lo que hará que se inicialice el asistente para importación de certificados de Microsoft (Ilustración 12). Pulse *Siguiente>*, seleccione el archivo *[directorio instalación]\ACRAIZFNMT-RCM.cer* y acepte todos los pasos para su instalación. Repita este mismo proceso para cada certificado raíz.

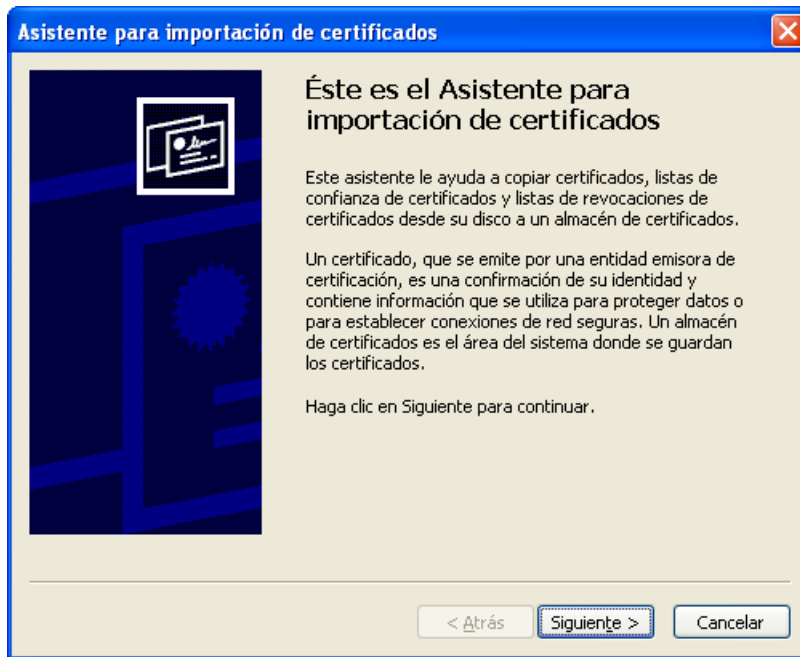


Ilustración 12. Asistente para la instalación de certificados en Internet Explorer

La instalación de los certificados raíz en Firefox también se realiza de forma automática.

No obstante, la importación de los certificados raíz en Firefox puede hacerse de forma manual. Para ello, arranque el navegador Firefox, y abra el menú *Herramientas – Opciones – Avanzado* y seleccione la pestaña *Cifrado* (Ilustración 9). Pulse *Ver certificados* y seleccione la pestaña *Autoridades*. Compruebe si dentro de la lista de certificados se encuentra el de la FNMT (Ilustración 13). En caso negativo, pulse *Importar* y seleccione el archivo `[directorio instalación]\ACRAIZFNMTRCM.cer`. Repita este mismo proceso para cada certificado raíz.

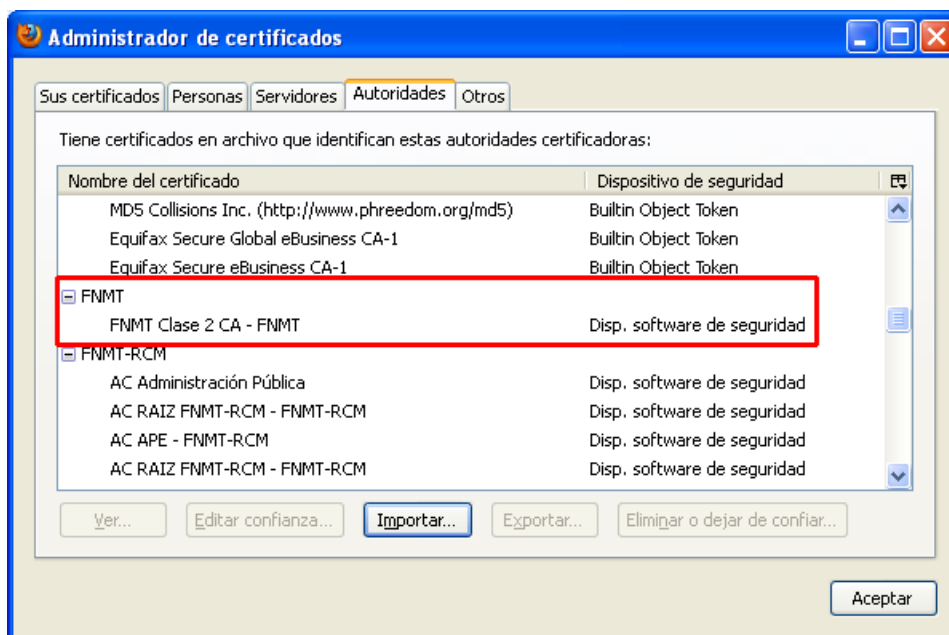


Ilustración 13. Administrador de certificados en Firefox

## 1.4. Herramientas de utilidades de la tarjeta Ceres

El Instalable módulo criptográfico Ceres contiene una herramienta para gestionar la tarjeta Ceres, la cual permite el desbloqueo de la misma, la importación de certificados, seleccionar el modo de generación de números aleatorios, configurar la caché de PIN y habilitar o deshabilitar el mecanismo SHA1. Se puede acceder a ella mediante *Panel de control – Aplicaciones FNMT-RCM* (Ilustración 14).

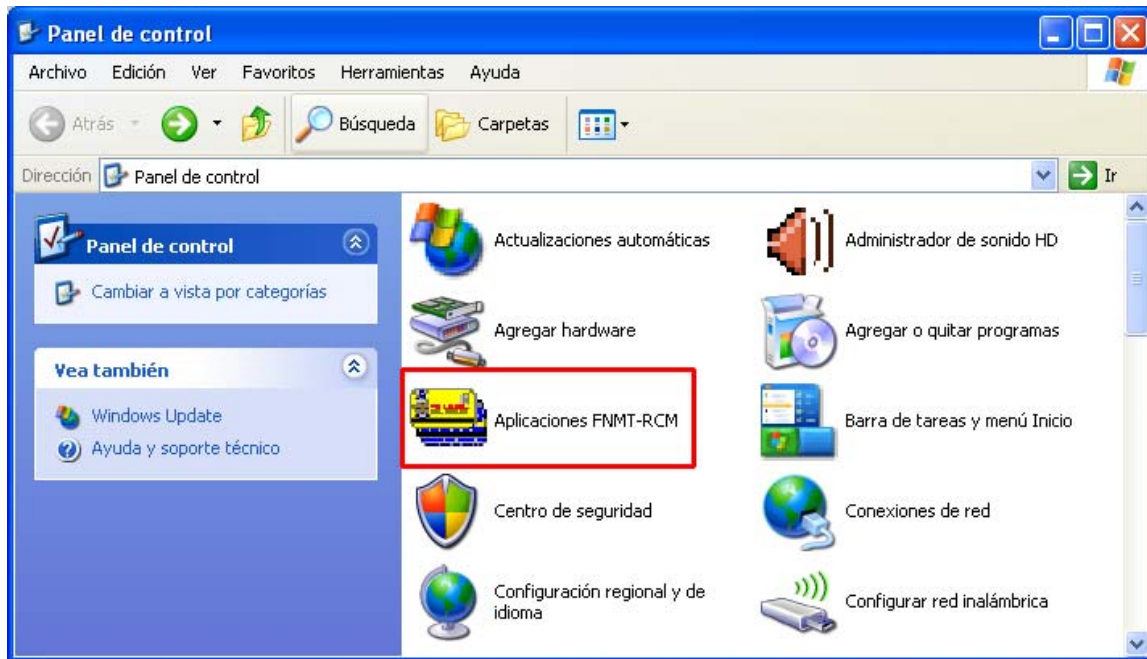


Ilustración 14. Acceso a la herramienta de gestión de aplicaciones de la FNMT-RCM

Además, desde el menú *Inicio – Programas – FNMT-RCM*, también se puede acceder a otras utilidades de la tarjeta Ceres (*Cambio de PIN*, *Importador de Certificados*, *Desbloqueo de Tarjeta* y *Ordena Certificados*), así como consultar documentación sobre la misma.

## 4. ACTUALIZACIÓN

Cuando se ejecuta el Instalable módulo criptográfico Ceres versión *x.y.z*, éste comprueba si ya está instalada en el equipo una versión previa de la aplicación. En este caso, lo que se hace es una actualización de la misma.

Podemos distinguir dos tipos de actualizaciones: actualizaciones menores y actualizaciones mayores.

## 1.5. Actualización menor

Una actualización menor es un pequeño cambio del producto, como, por ejemplo una nueva versión de las librerías que instala.

En este caso, si al ejecutar el Instalable módulo criptográfico Ceres versión *x.y.z* ya está instalada en el equipo la versión previa *x.a.b* del producto, se procede a una actualización menor del software. Lo que hace el instalable es actualizar los pequeños cambios del producto sobre la instalación que ya hay hecha.

Al ejecutar el instalable, en primer lugar se muestra una pantalla pidiendo permiso para realizar una actualización del Instalable módulo criptográfico Ceres (Ilustración 15).

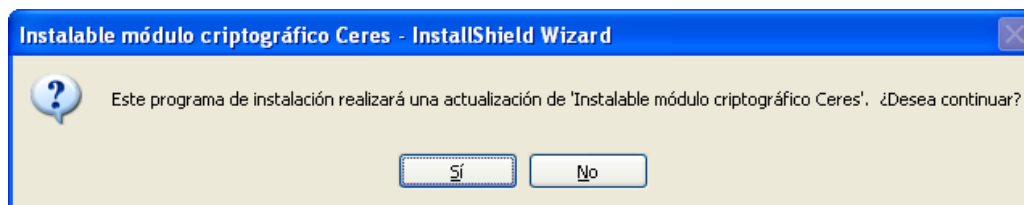


Ilustración 15. Confirmación de la actualización

Tras aceptar continuar con la actualización, el instalable muestra una pantalla indicando que se está preparando el asistente para la instalación (Ilustración 16).

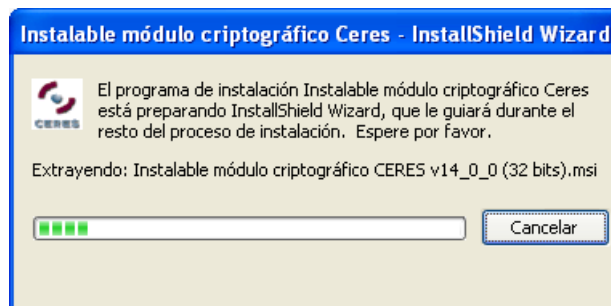


Ilustración 16. Preparando el asistente de instalación

Acto seguido indica que se va a continuar con la instalación del programa, es decir, se va a actualizar (Ilustración 17).

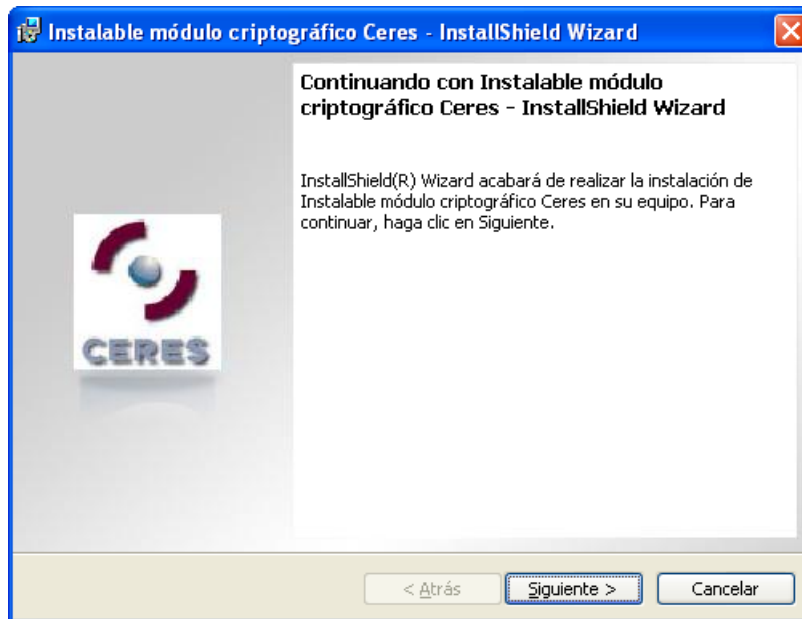


Ilustración 17. Continuación de la instalación

Durante el proceso de instalación, el asistente irá mostrando las acciones que se están realizando, así como una barra que indica el progreso de la misma (Ilustración 18).

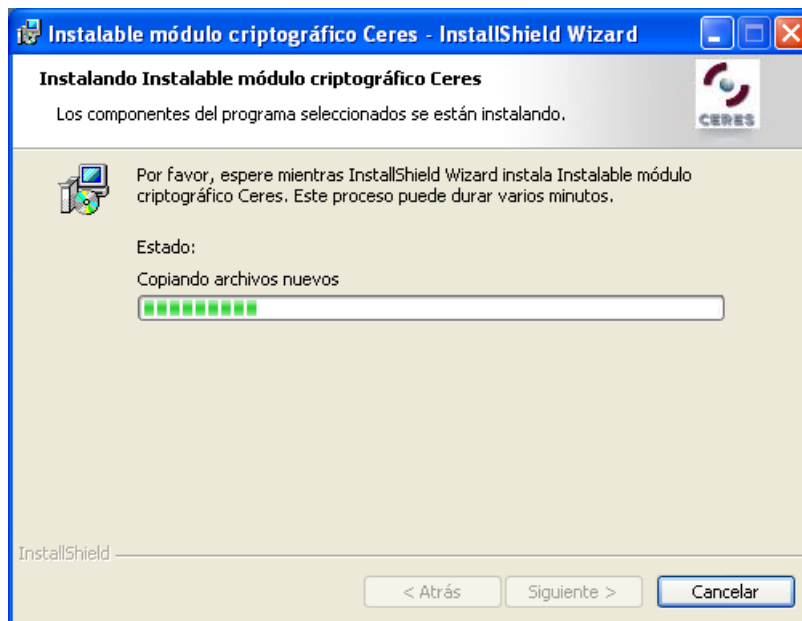


Ilustración 18. Estado de la instalación

Al finalizar, tal y como se muestra en la Ilustración 19, el instalable muestra una pantalla indicando que el proceso de instalación ha finalizado correctamente. Pulse *Finalizar* para salir del asistente.

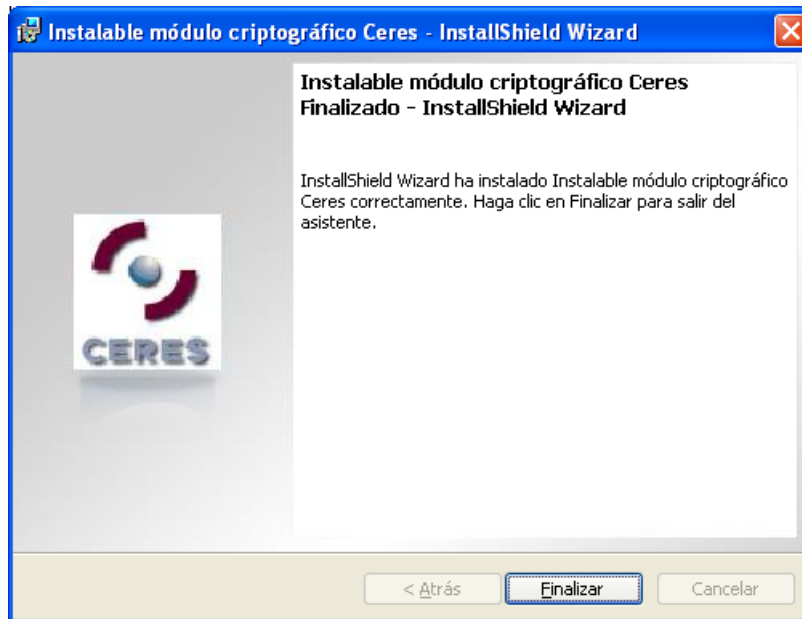


Ilustración 19. Fin de la instalación

Por último, se muestra un aviso indicando que debe reiniciar el sistema (Ilustración 20). Se da al usuario la opción de si desea reiniciar el equipo en ese momento o aplazarlo para más adelante. Hay que tener en cuenta que para completar la actualización es necesario reiniciar el equipo.

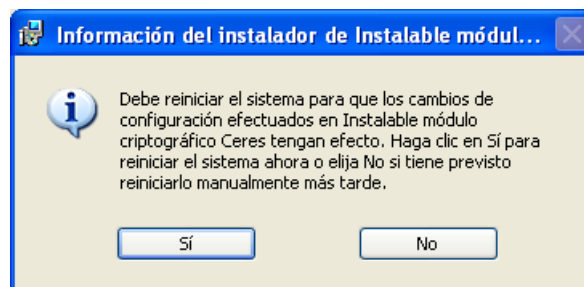


Ilustración 20. Reiniciar el sistema

## 1.6. Actualización mayor

Una actualización mayor se da cuando se produce un cambio considerable en el producto.

En este caso, si al ejecutar el Instalable módulo criptográfico Ceres versión *x.y.z* ya está instalada en el equipo una versión del producto previa a la *x.0.0*, se procede a una actualización mayor del software. Lo que hace el instalable es desinstalar previamente la versión instalada antes de proceder automáticamente a la nueva instalación.

Al ejecutar el instalable, lo primero que aparecerá, como podemos ver en la Ilustración 21, es una ventana en la que se solicita el idioma deseado para la instalación. El resto de las indicaciones de la instalación aparecerán en el idioma seleccionado.

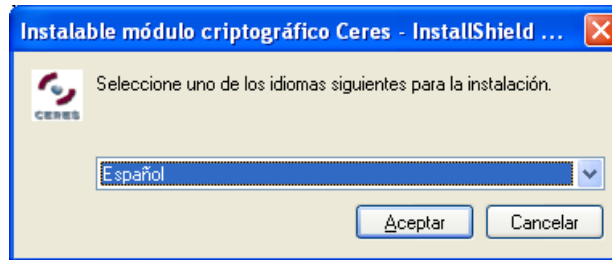


Ilustración 21. Elegir idioma de instalación

Una vez seleccionado el idioma, el instalable muestra una pantalla indicando que se está preparando el asistente para la instalación (Ilustración 22).

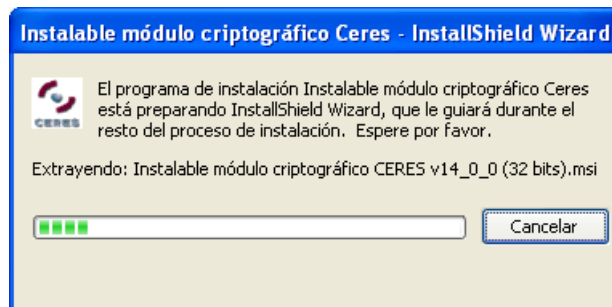


Ilustración 22. Preparando el asistente de instalación

Acto seguido, automáticamente se muestra un mensaje advirtiendo que se ha encontrado una versión anterior y pidiendo confirmación para proceder a su desinstalación (Ilustración 23).

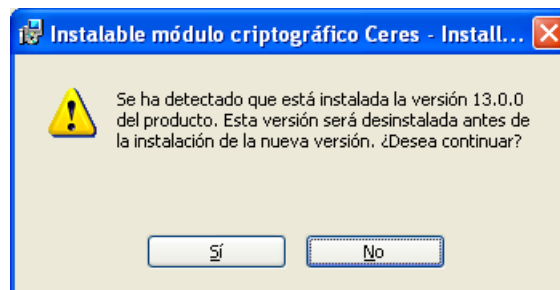


Ilustración 23. Confirmación de la desinstalación de la versión anterior

Una vez que se acepta continuar con la actualización, se seguirán los mismos pasos que para una nueva instalación.

Si la versión previamente instalada es anterior a la 12.0.0, al estar implementadas con un enfoque diferente, la desinstalación de la versión anterior no se podrá realizar automáticamente, por lo que se deberá realizar su desinstalación desde el Panel de Control antes de instalar la nueva versión.

## 5. MANTENIMIENTO

Si se ejecuta el Instalable módulo criptográfico Ceres en un equipo en el que ya está instalada esta misma versión, se arranca el mantenimiento de la instalación. Lo

primero que se muestra es una pantalla indicando que se está preparando el asistente para la instalación (Ilustración 24).

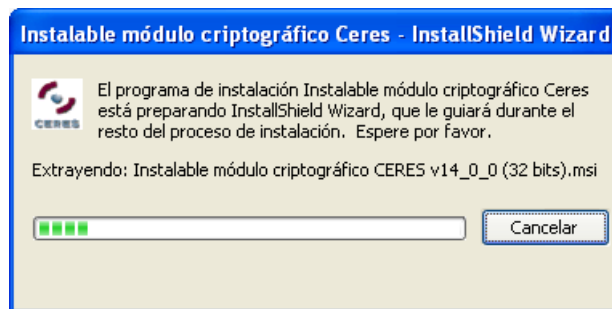


Ilustración 24. Preparando el asistente de instalación

Después, automáticamente se muestra una ventana dando la bienvenida al proceso de instalación (Ilustración 25).

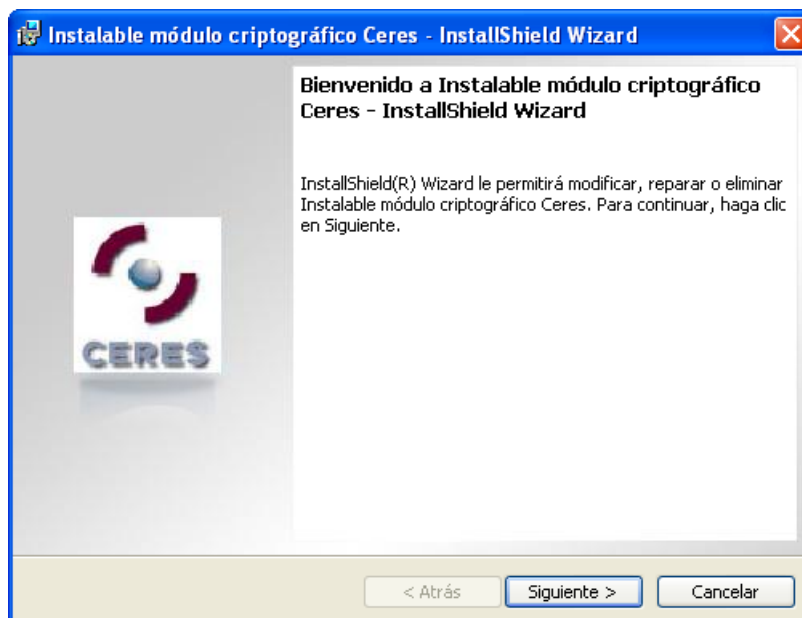


Ilustración 25. Bienvenido al proceso de instalación

A continuación aparece un menú con las distintas opciones de mantenimiento de la instalación (Ilustración 26):

- **Modificar:** Modificación de los componentes de la aplicación instalados.
- **Reparar:** Reinstalación de la aplicación.
- **Eliminar:** Desinstalación de la aplicación.

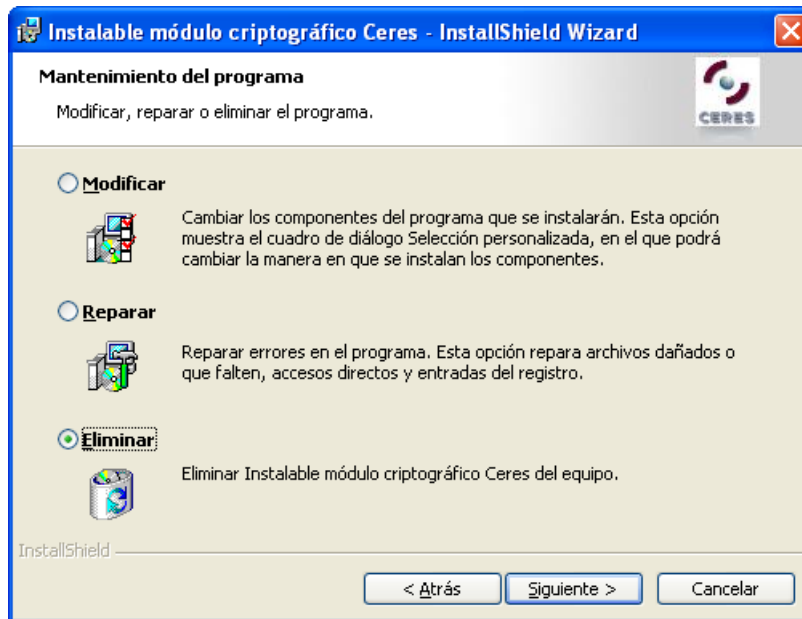


Ilustración 26. Opciones de mantenimiento de la instalación

## 1.7. Desinstalación

Al solicitar la desinstalación de la aplicación, lo primero que aparece es un mensaje solicitando confirmación (Ilustración 27).

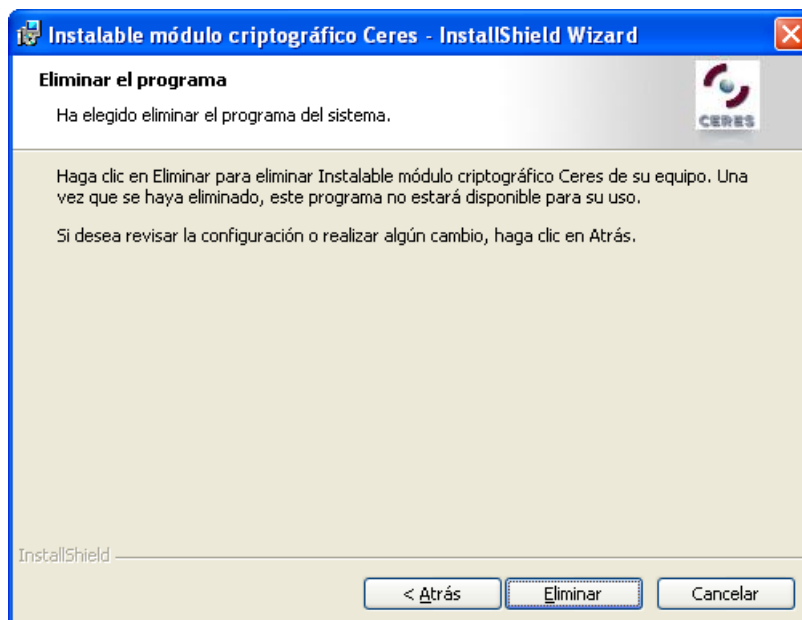


Ilustración 27. Confirmación de la desinstalación

Durante el proceso de desinstalación, el asistente irá mostrando las acciones que se están realizando, así como una barra que indica el progreso de la misma (Ilustración 28).

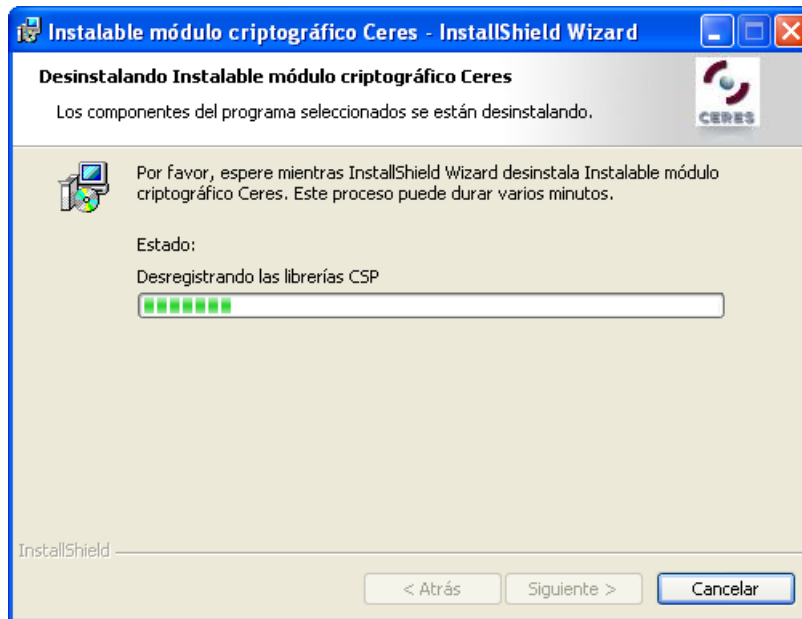


Ilustración 28. Estado de la desinstalación

Al finalizar, tal y como se muestra en la Ilustración 29, el instalable muestra una pantalla indicando que el proceso de desinstalación ha finalizado correctamente. Pulse *Finalizar* para salir del asistente

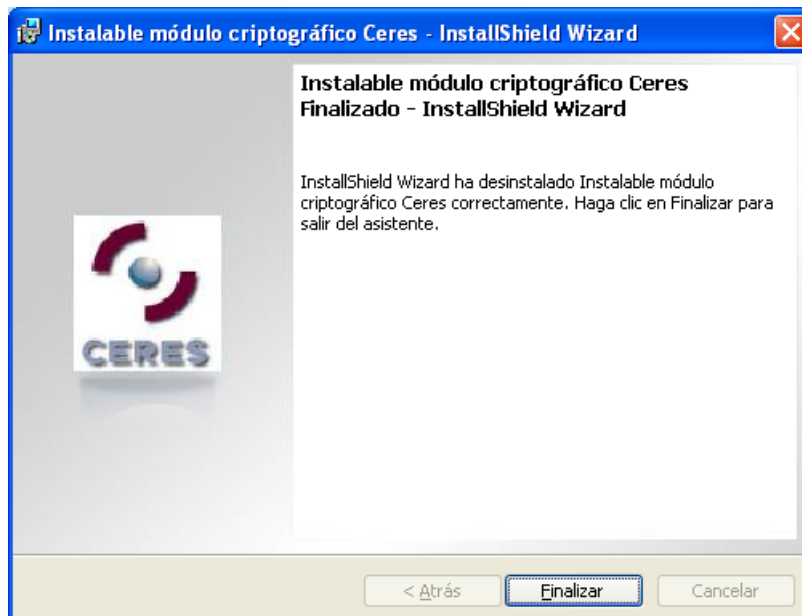


Ilustración 29. Fin de la desinstalación

Por último, se muestra un aviso indicando que debe reiniciar el sistema (Ilustración 30). Se da al usuario la opción de si desea reiniciar el equipo en ese momento o aplazarlo para más adelante. Hay que tener en cuenta que para completar la desinstalación es necesario reiniciar el equipo.

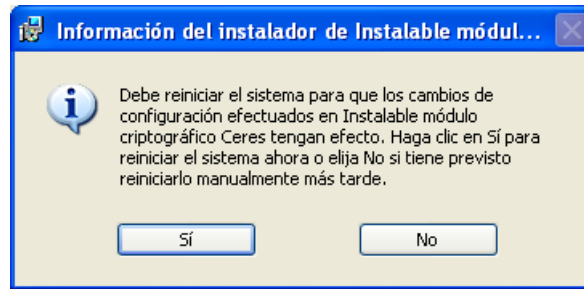


Ilustración 30. Reiniciar el sistema

## 1.8. Reinstalación

Al solicitar la reinstalación de la aplicación, el instalable mostrará una ventana indicando que está preparado para reparar el programa (Ilustración 31).

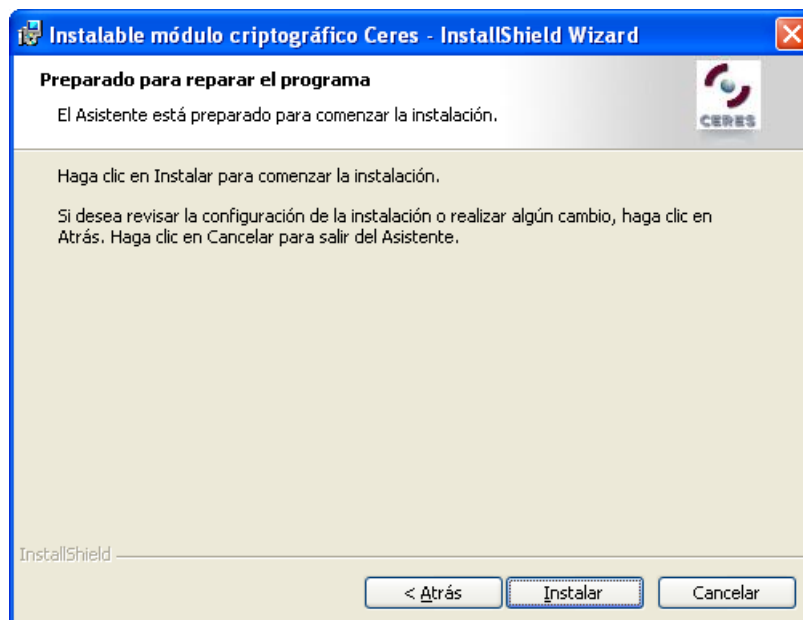


Ilustración 31. Preparado para reparar el programa

A continuación, el asistente irá mostrando las acciones que se están realizando, así como una barra que indica el progreso de la misma (Ilustración 32).

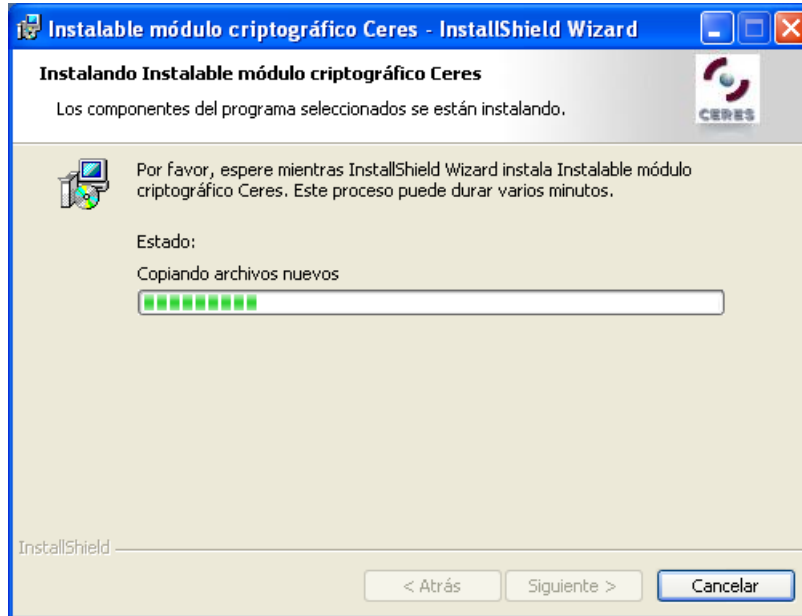


Ilustración 32. Estado de la instalación

Al finalizar, tal y como se muestra en la Ilustración 33, el instalable muestra una pantalla indicando que el proceso de instalación ha finalizado correctamente. Pulse *Finalizar* para salir del asistente

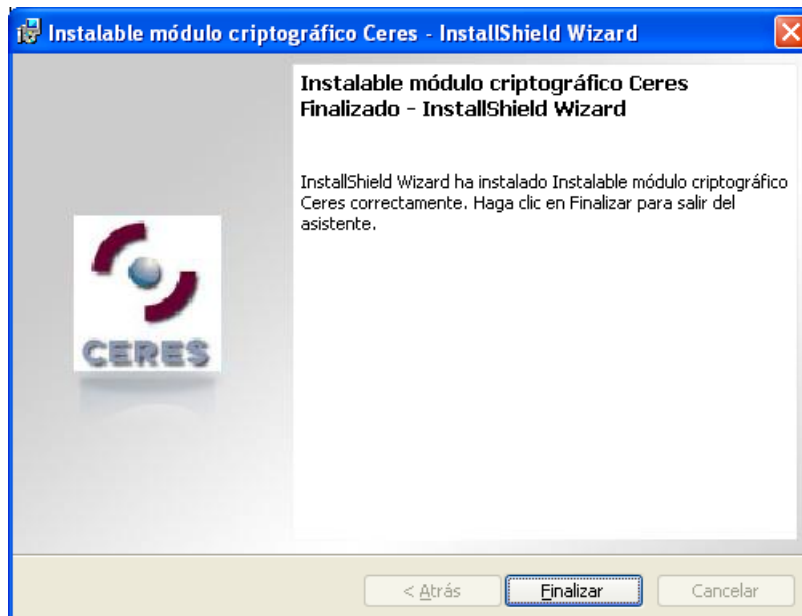


Ilustración 33. Fin de la instalación

Por último, se muestra un aviso indicando que debe reiniciar el sistema (Ilustración 34). Se da al usuario la opción de si desea reiniciar el equipo en ese momento o aplazarlo para más adelante. Hay que tener en cuenta que para completar la instalación es necesario reiniciar el equipo.

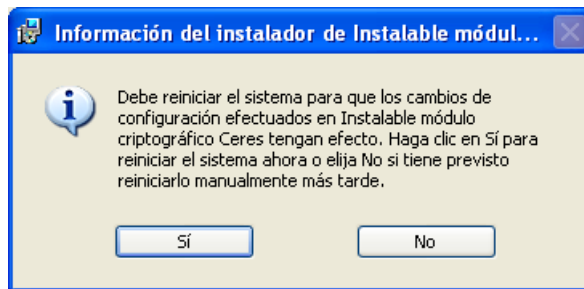


Ilustración 34. Reiniciar el sistema

## 1.9. Modificación

Al solicitar la modificación de la aplicación, el instalable muestra una lista con los componentes de la misma para poder modificar cuáles se quiere tener instalados (Ilustración 35). Como el Instalable módulo criptográfico Ceres tiene un único componente, tan sólo se podrá desinstalar la aplicación completa.

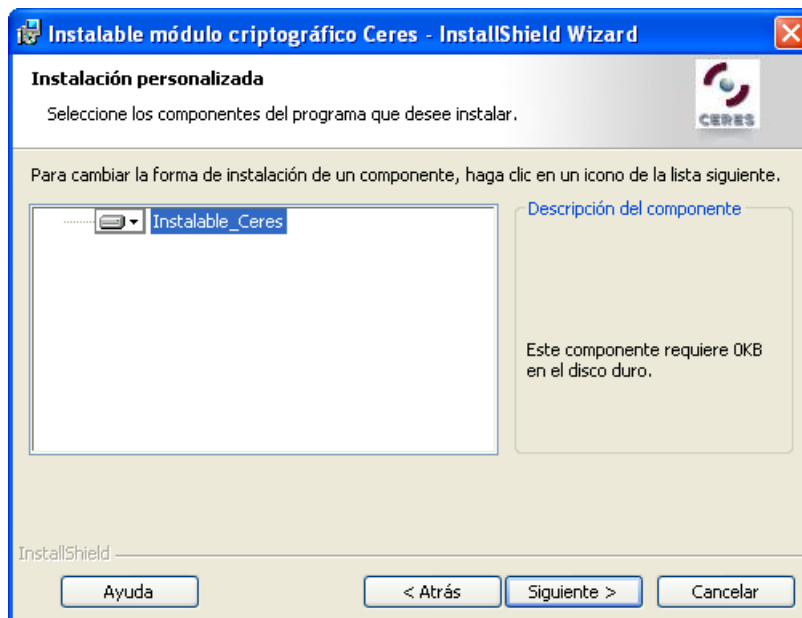


Ilustración 35. Selección de componentes instalados

## 6. VERSIÓN DESATENDIDA

Por defecto, la instalación del programa se facilita mediante una serie de ventanas que van guiando al usuario durante el proceso de instalación. No obstante, también se puede lanzar el instalable en modo desatendido, de forma que se realiza una instalación automática del producto. Para ello, hay que ejecutar la siguiente instrucción por línea de comandos:

```
insmodcripc2vxyz.exe /la /v"/qn TIME=b"
```

Donde *a* es el idioma de instalación (1034 para castellano, 1027 para catalán, 1110 para gallego, 1069 para euskera y 1033 para inglés) y *b* es el número de segundos

de espera antes de reiniciar el equipo automáticamente tras la instalación (10 por defecto si no se indica nada).

Al invocar la versión desatendida del instalable, lo primero que se muestra es una pantalla indicando que se está preparando la instalación (Ilustración 36).

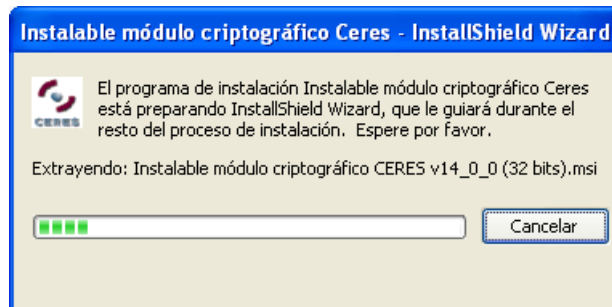


Ilustración 36. Preparando el asistente de instalación

Al finalizar la instalación provoca el reinicio automático del sistema, informando previamente en una ventana de los segundos restantes (Ilustración 37).

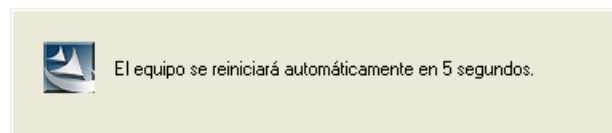


Ilustración 37. Aviso del reinicio automático del sistema

Si al invocar el instalable en modo desatendido detectara que ya hay instalada una versión anterior, realizaría una actualización del producto; si ya estuviera instalada esta misma versión, la reinstalaría.

También es posible realizar una desinstalación desatendida de la aplicación. Para ello, hay que ejecutar la siguiente instrucción por línea de comandos:

```
insmodcripc2vxyz.exe /x /v"/qn TIME=b"
```

Donde *b* es el número de segundos de espera antes de reiniciar el equipo automáticamente tras la instalación (10 por defecto si no se indica nada).