Instalable módulo criptográfico CERES Clase 2

Manual de usuario

Versión 3.0

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Tabla de contenido

1. INTRODUCCIÓN 1
2. REQUISITOS 2
3. INSTALACIÓN 3
3.1. Módulo CSP 6
3.2. Módulo PKCS#11 6
3.3. Certificado raíz de la FNMT 8
3.4. Herramientas de utilidades de la tarjeta CERES 9
4. ACTUALIZACIÓN 11
4.1. Actualización menor 11
4.2. Actualización mayor 13
5. MANTENIMIENTO 17
5.1. Desinstalación 18
5.2. Reinstalación 19
5.3. Modificación 20
6. VERSIÓN DESATENDIDA 22

1. Introducción

El objetivo del Instalable módulo criptográfico CERES Clase 2 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 multilenguaje, que posibilita la instalación en castellano, catalán, gallego o euskera.

Además está preparado para soportar sistemas con arquitectura de 64 bits. En estos casos, 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 Clase 2 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 98.
    - Windows Me.
    - Windows NT 4.0 (mínimo con el Service Pack 3).
    - 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.
- Netscape 4.73 o posterior.
- Mozilla.
- Que el usuario tenga permisos de administrador.

3. Instalación

Para instalar la versión *x.y.z* del Instalable módulo criptográfico CERES Clase 2, basta con ejecutar el instalable *insmodcripc2vx.y.z.exe*, que se puede descargar en el siguiente enlace:

http://www.cert.fnmt.es/content/pages_std/software/insmodcripc2vx.y.z.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, gallego y euskera. El resto de las indicaciones de la instalación aparecerán en el idioma seleccionado.

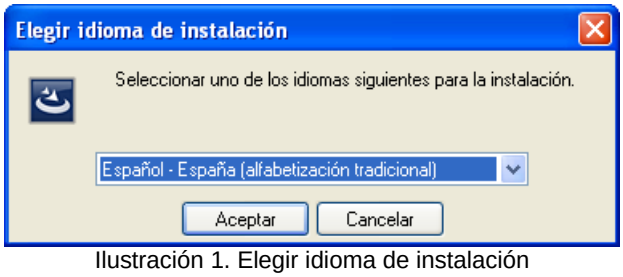

Ilustración 1. Elegir idioma de instalación

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

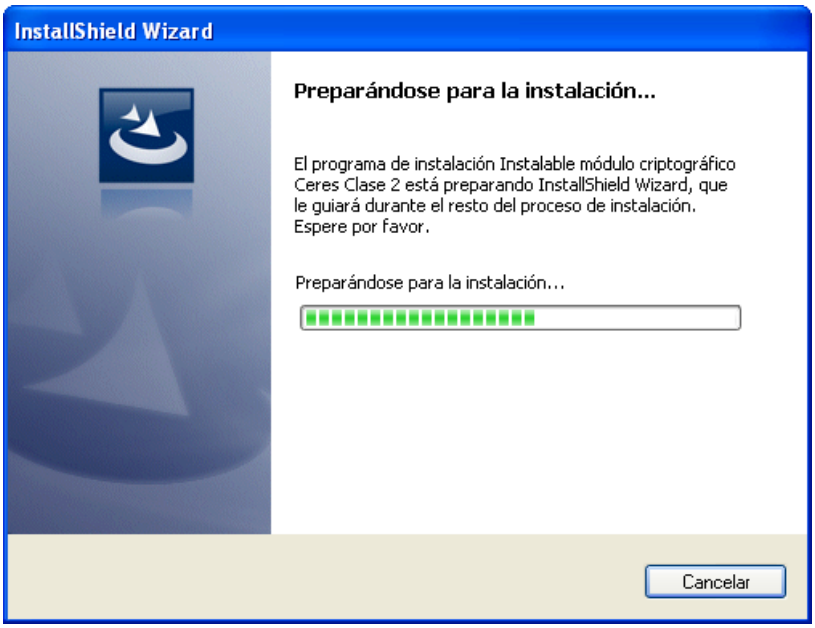

Ilustración 2. Preparando el asistente de instalación

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

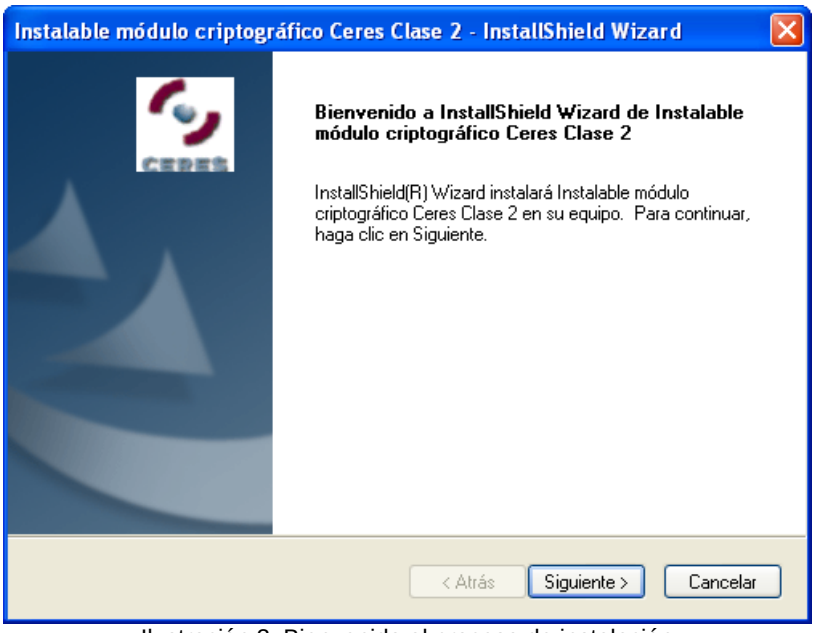

Ilustración 3. Bienvenido al proceso de instalación

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.

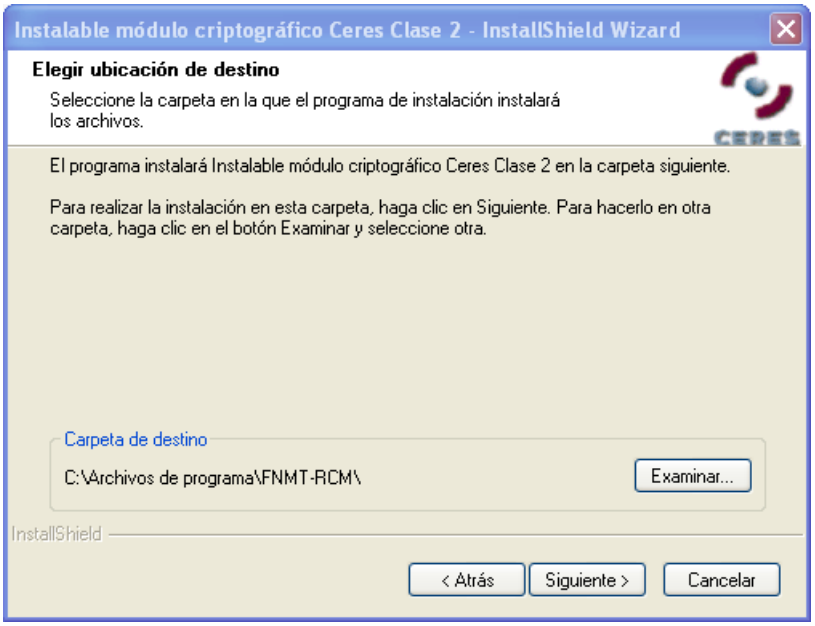

Ilustración 4. Selección del directorio de instalación

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 5).

Ilustración 5. Estado de la instalación

Por último, tal y como se muestra en la Ilustración 6, el instalable muestra una pantalla indicando que el proceso de instalación ha finalizado correctamente y que se debe reiniciar el equipo. 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 6. Fin de la instalación

Una vez finalizado correctamente todo el proceso, se habrán instalado en el equipo los componentes necesarios para el uso de la tarjeta CERES Clase 2. A continuación se detallan los más importantes.

3.1. Módulo CSP

Para permitir el empleo de la tarjeta CERES Clase 2 mediante el navegador Internet Explorer, el ejecutable instala y registra las librerías del módulo CSP.

3.2. Módulo PKCS#11

El programa comprueba si el equipo tiene instalados los navegadores Firefox, Netscape o Mozilla, e instala para cada uno de ellos el módulo PKCS#11. Al reiniciar el equipo tras la instalación, se arrancarán cada uno de esos navegadores con una página con los pasos para la instalación del módulo criptográfico CERES, y aparecerá una ventana pidiendo autorización (Ilustración 7). Para su correcto funcionamiento, debe aceptar la instalación.

Ilustración 7. Confirmar instalación módulo PKCS#11 en navegadores Firefox, Netscape y Mozilla

Una vez aceptada la instalación, el navegador mostrará un mensaje informando de ello (Ilustración 8).

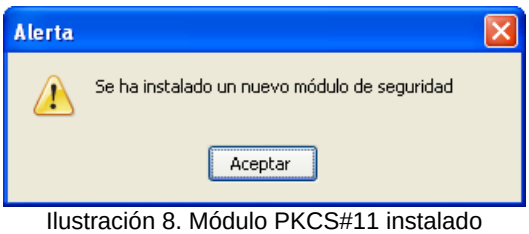

Ilustración 8. Módulo PKCS#11 instalado

A partir de la versión 3.5 del navegador Firefox, se pedirá permiso para la ejecución del script de configuración (Ilustración 9). Debe permitir su ejecución para que se pueda instalar correctamente el módulo PKCS#11.

Ilustración 9. Permitir ejecución de script para instalación módulo PKCS#11 en navegadores Firefox 3.5 y posteriores

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 10). Pulse *Dispositivos de seguridad* y compruebe si dentro de la lista se encuentra el de la FNMT (Ilustración 11). 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*.

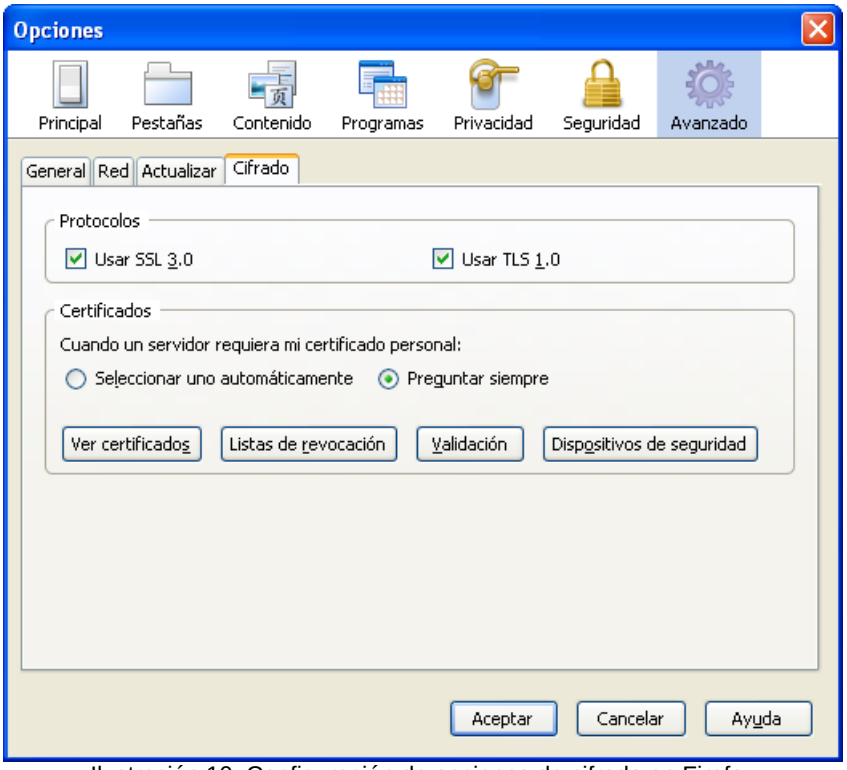

Ilustración 10. Configuración de opciones de cifrado en Firefox

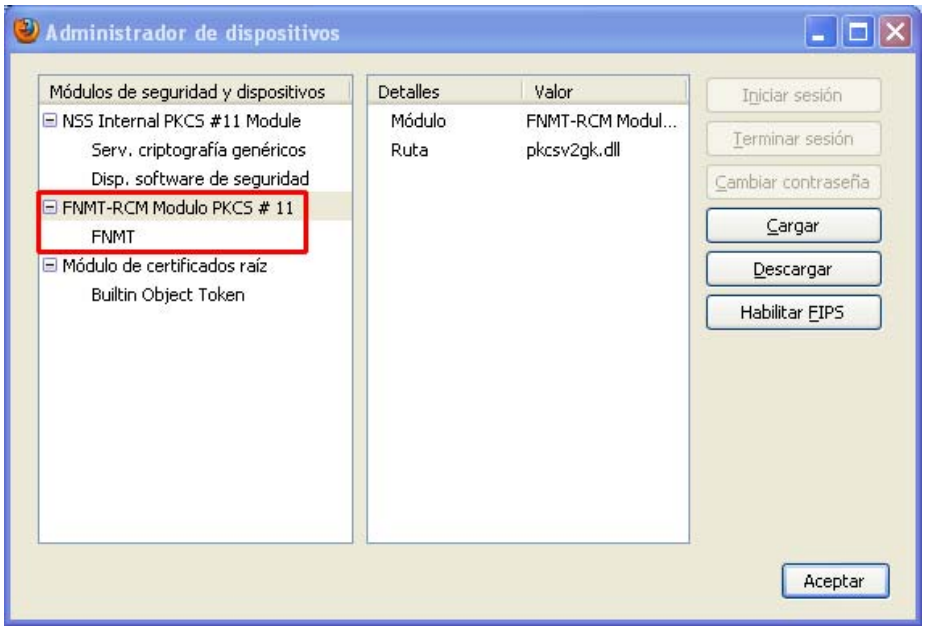

Ilustración 11. Administrador de dispositivos de seguridad en Firefox

3.3. Certificado raíz de la FNMT

El certificado raíz de la FNMT se copia en *[directorio instalación]\FNMTClase2CA.der*. En el navegador Internet Explorer este certificado ya viene instalado por defecto. Para el caso de los navegadores Firefox, Netscape y Mozilla, al reiniciar el equipo tras la instalación, y después de instalar el módulo PKCS#11, se volverá a abrir el navegador con una ventana en la que se solicita que establezca la confianza para el certificado raíz (Ilustración 12). Deberá marcar las tres casillas de confianza y aceptar la descarga.

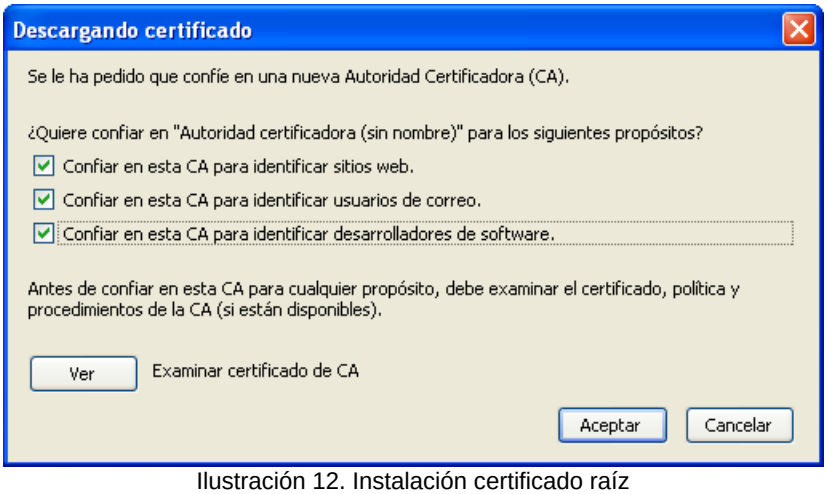

Ilustración 12. Instalación certificado raíz

A partir de la versión 3.0 del navegador Firefox, éste no carga automáticamente el certificado raíz. En este caso, habrá que instalarlo manualmente. Para ello, arranque el navegador Firefox, y abra el menú *Herramientas – Opciones – Avanzado* y seleccione la pestaña *Cifrado* (Ilustración 10). 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]\FNMTClase2CA.der*.

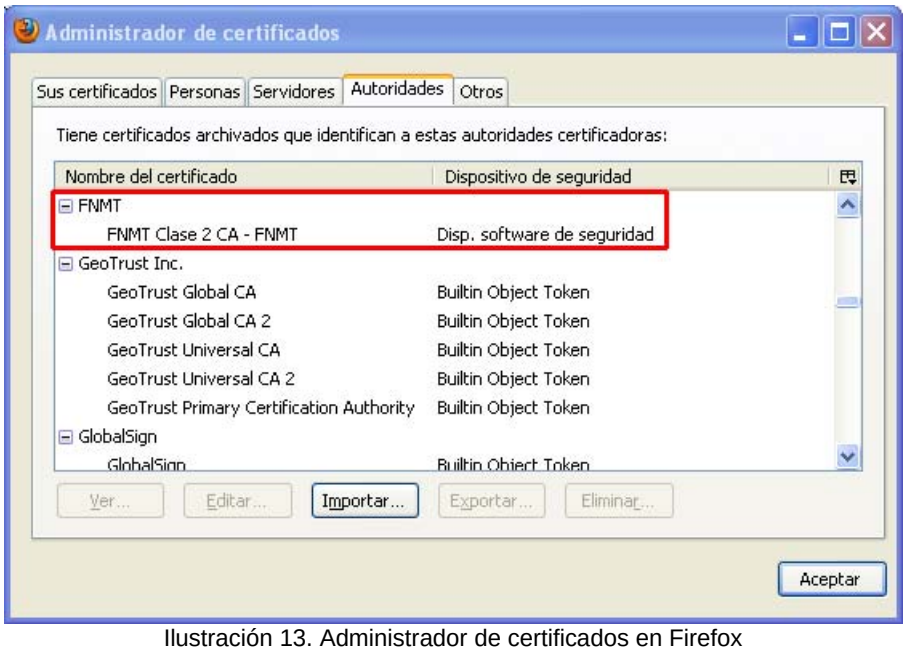

Ilustración 13. Administrador de certificados en Firefox

3.4. Herramientas de utilidades de la tarjeta CERES

El Instalable módulo criptográfico CERES Clase 2 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 datos y habilitar o deshabilitar el mecanismo SHA1. Se puede acceder a ella mediante *Panel de control – Aplicaciones FNMT-RCM* (Ilustración 14).

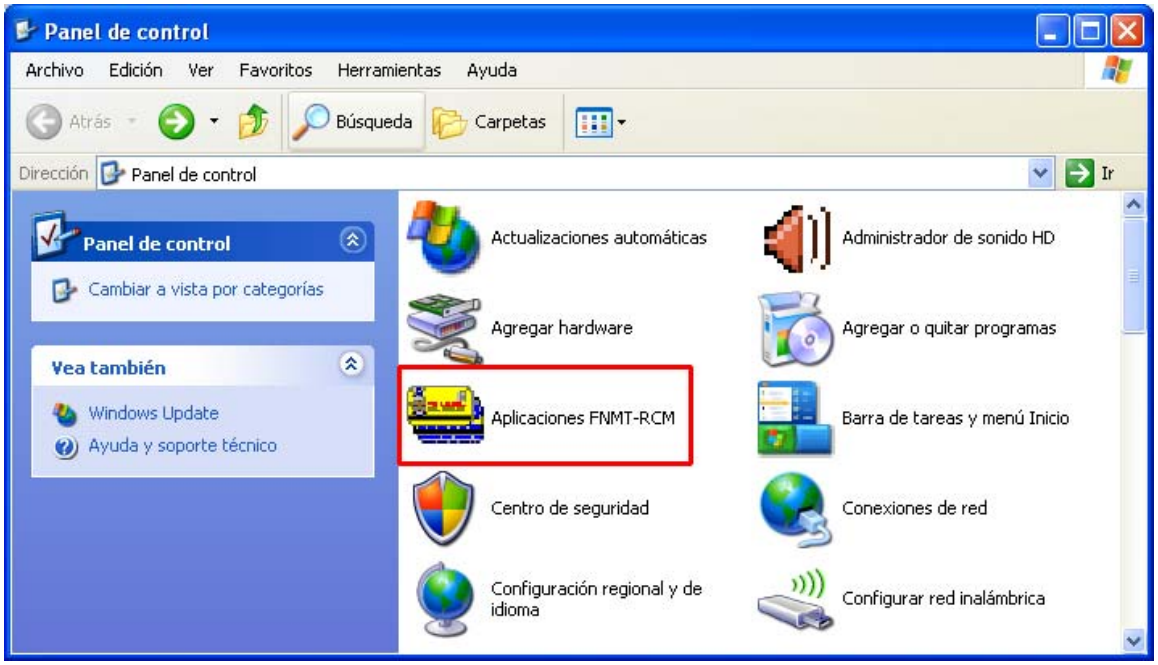

Ilustración 14. Acceso a la herramienta de gestión de aplicaciones de la FNMT-RCM

Además, desde el menú *Inicio – Programas – FNMT-RCM*, también se puede acceder a otras utilidades de la tarjeta CERES (cambiar el PIN, desbloquear la tarjeta, ordenar los certificados e importar nuevos certificados), así como documentación sobre la misma.

4. Actualización

Cuando se ejecuta el Instalable módulo criptográfico CERES Clase 2 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.

4.1. 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 Clase 2 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 indicando que se está preparando el asistente para la instalación (Ilustración 15).

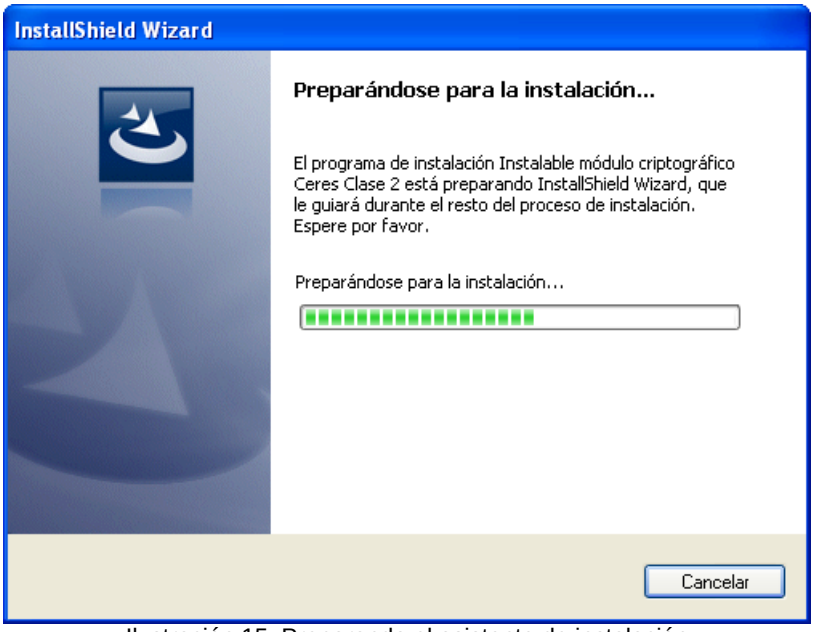

Ilustración 15. Preparando el asistente de instalación

Acto seguido indica que se va a continuar con la instalación del programa, es decir, se va a actualizar (Ilustración 16).

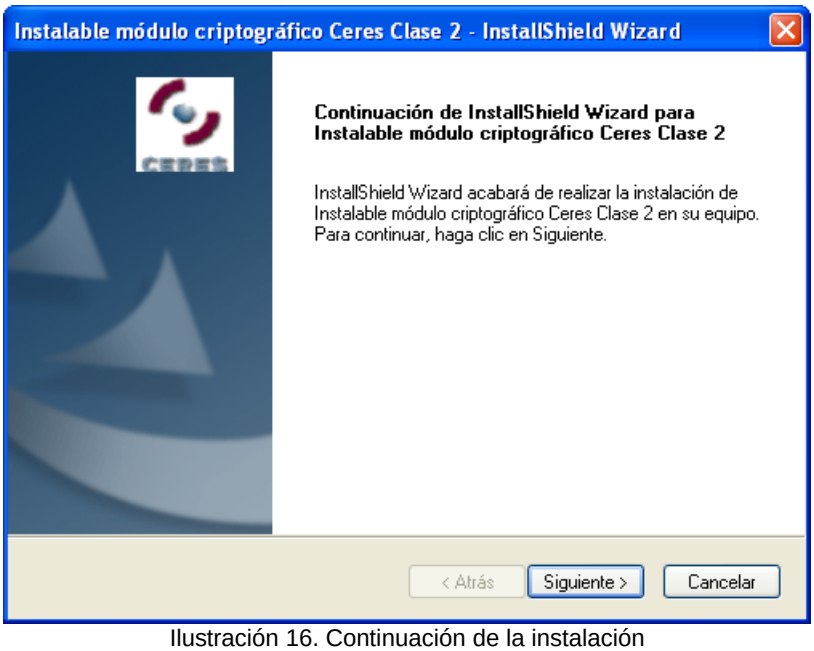

Ilustración 16. Continuación de la instalación

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 17).

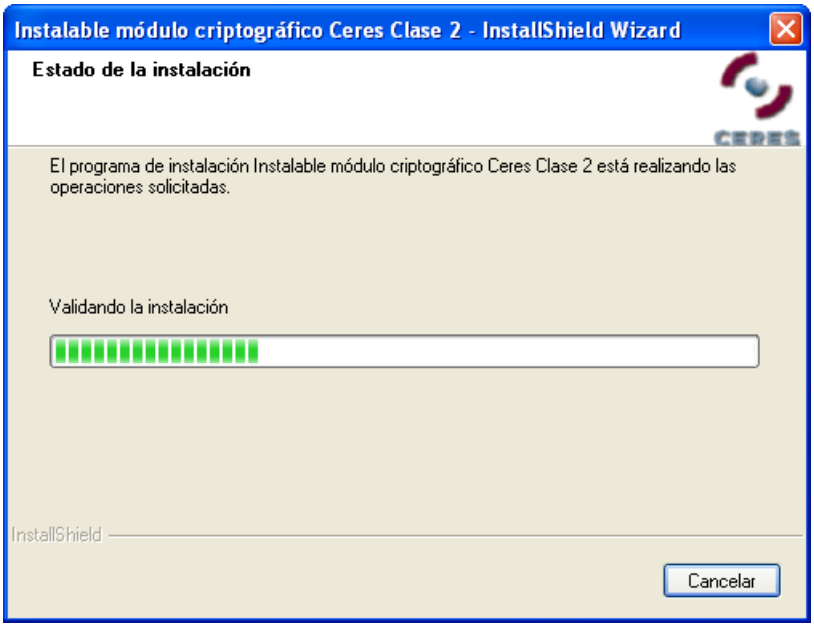

Ilustración 17. Estado de la instalación

Por último, tal y como se muestra en la Ilustración 18, el instalable muestra una pantalla indicando que el proceso de instalación ha finalizado correctamente y que se debe reiniciar el equipo. 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 18. Fin de la instalación

4.2. 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 Clase 2 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 19, 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.

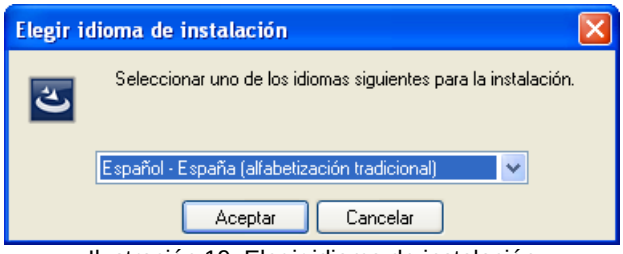

Ilustración 19. Elegir idioma de instalación

Una vez seleccionado el idioma, el instalable muestra una pantalla indicando que se está preparando el asistente para la instalación (Ilustración 20).

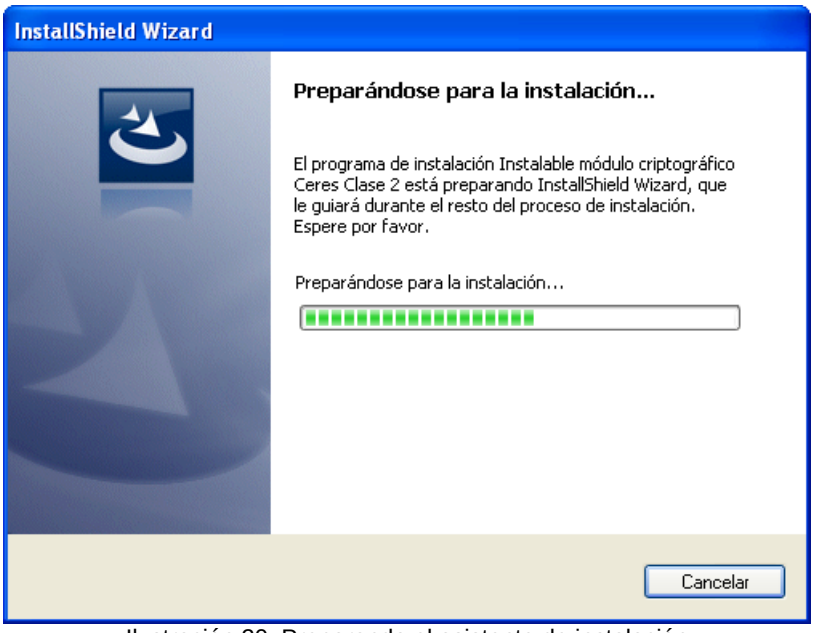

Ilustración 20. Preparando el asistente de instalación

Acto seguido, automáticamente se muestra un mensaje advirtiendo que se ha encontrado una versión anterior y pidiendo confirmación para proceder a su desinstalación (Ilustración 21).

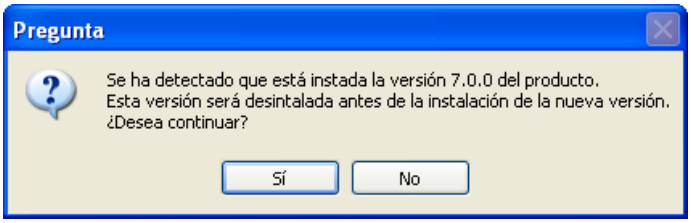

Ilustración 21. Confirmación de la desinstalación de la versión anterior

A continuación, automáticamente se muestra una ventana dando la bienvenida al proceso de instalación (Ilustración 22).

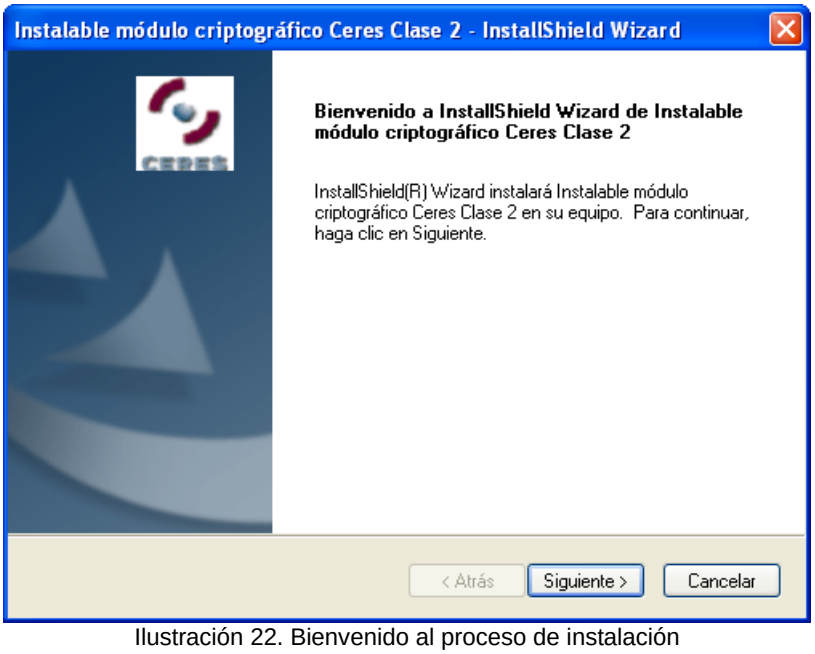

Ilustración 22. Bienvenido al proceso de instalación

El asistente irá mostrando las acciones que se están realizando, así como una barra que indica el progreso de la misma, tanto para el proceso de desinstalación de la versión anterior (Ilustración 23) como para el de instalación de la nueva versión (Ilustración 24).

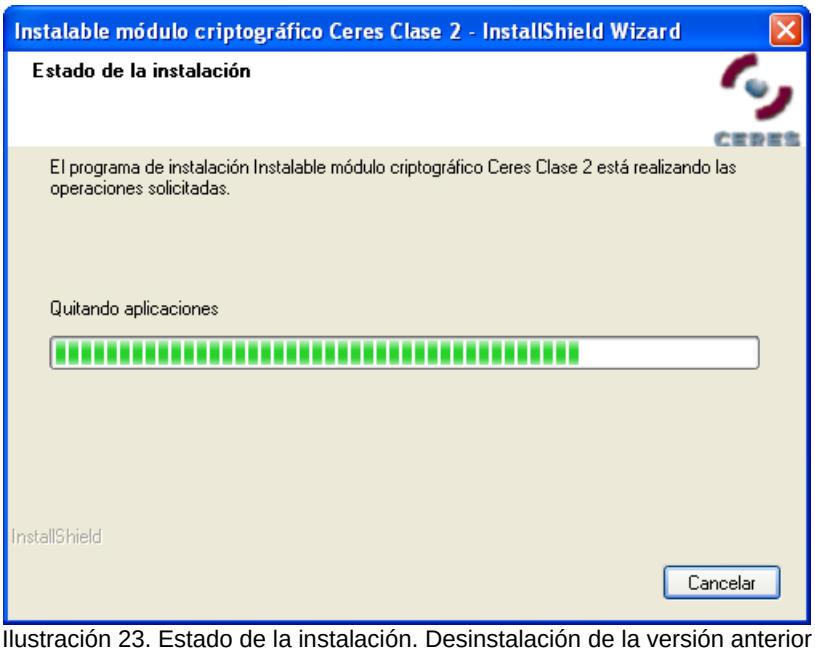

Ilustración 23. Estado de la instalación. Desinstalación de la versión anterior

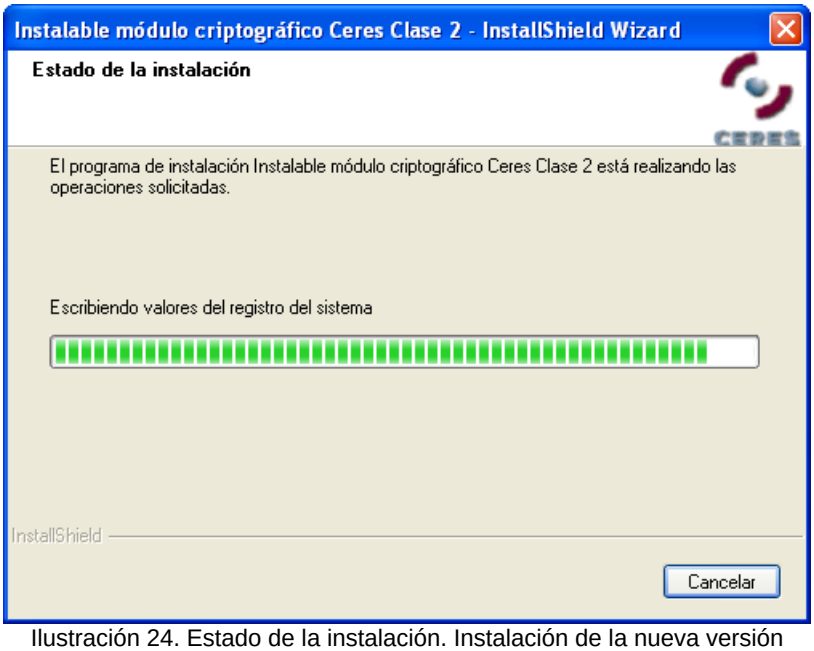

Ilustración 24. Estado de la instalación. Instalación de la nueva versión

Por último, tal y como se muestra en la Ilustración 25, el instalable muestra una pantalla indicando que el proceso de instalación ha finalizado correctamente y que se debe reiniciar el equipo. 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 25. Fin de la instalación

Si la versión previamente instalada es anterior a la 7.0.0, al estar implementadas con otro software de desarrollo, lo que hace es invocar al instalable antiguo para su eliminación, requiriendo una nueva ejecución del Instalable módulo criptográfico CERES Clase 2 versión *x.y.z* para su instalación.

5. Mantenimiento

Si se ejecuta el Instalable módulo criptográfico CERES Clase 2 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 26).

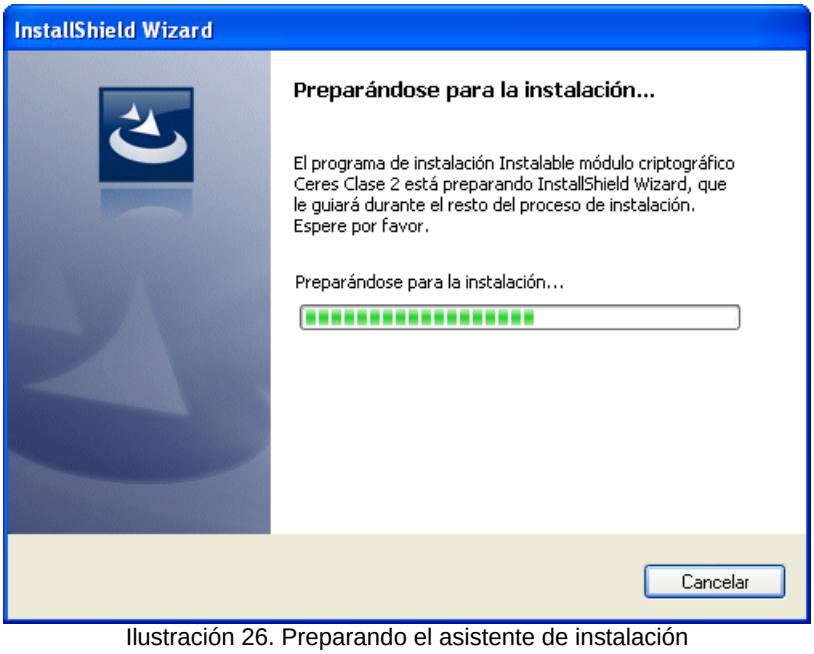

Ilustración 26. Preparando el asistente de instalación

A continuación aparece un menú con las distintas opciones de mantenimiento de la instalación (Ilustración 27):

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

Ilustración 27. Opciones de mantenimiento de la instalación

5.1. Desinstalación

Al solicituar la desinstalación de la aplicación, lo primero que aparece es un mensaje solicitando confirmación (Ilustración 28).

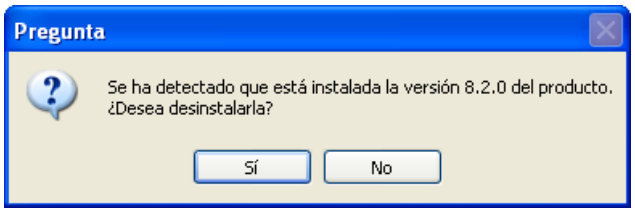

Ilustración 28. Confirmación de la desinstalación

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 29).

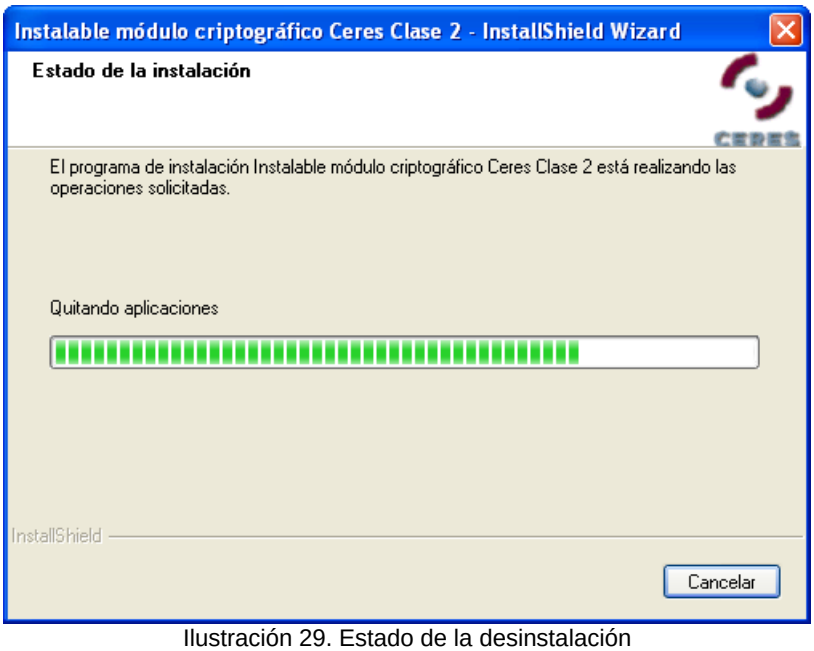

Ilustración 29. Estado de la desinstalación

Por último, tal y como se muestra en la Ilustración 30, el instalable muestra una pantalla indicando que el proceso de desinstalación ha finalizado correctamente y que se debe reiniciar el equipo. 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. Fin de la desinstalación

5.2. Reinstalación

Al solicitar la reinstalación de la aplicación, el instalable irá mostrando las acciones que se están realizando, así como una barra que indica el progreso de la misma (Ilustración 31).

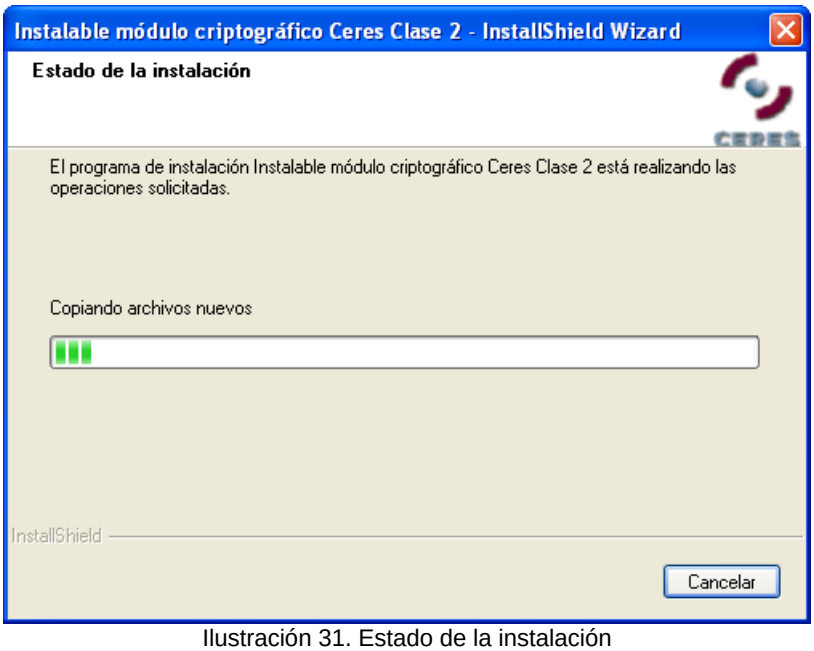

Ilustración 31. Estado de la instalación

Por último, tal y como se muestra en la Ilustración 32, el instalable muestra una pantalla indicando que el proceso de reinstalación ha finalizado correctamente y que se debe reiniciar el equipo. 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.

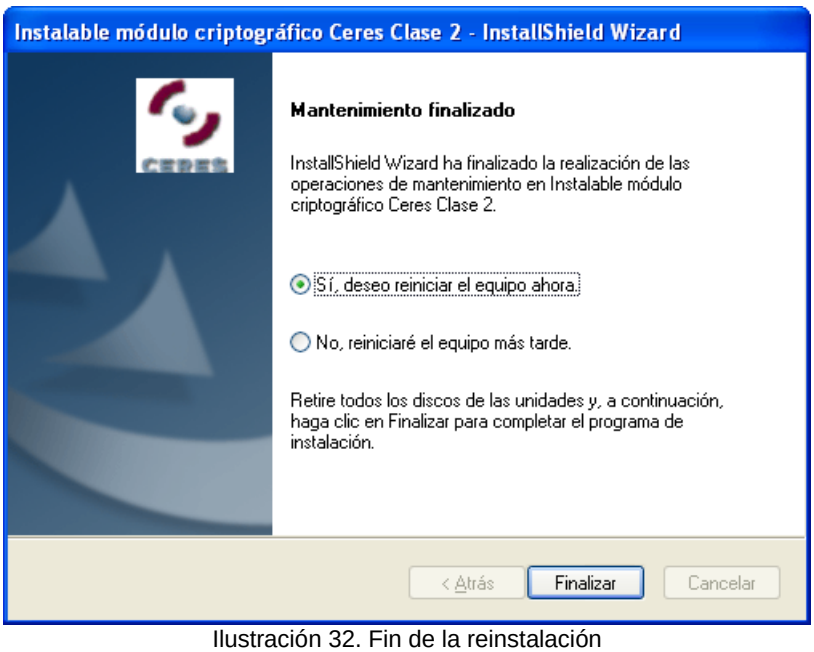

Ilustración 32. Fin de la reinstalación

5.3. 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 33). Como el Instalable módulo criptográfico CERES Clase 2 tiene un único componente, tan sólo se podrá desinstalar la aplicación completa.

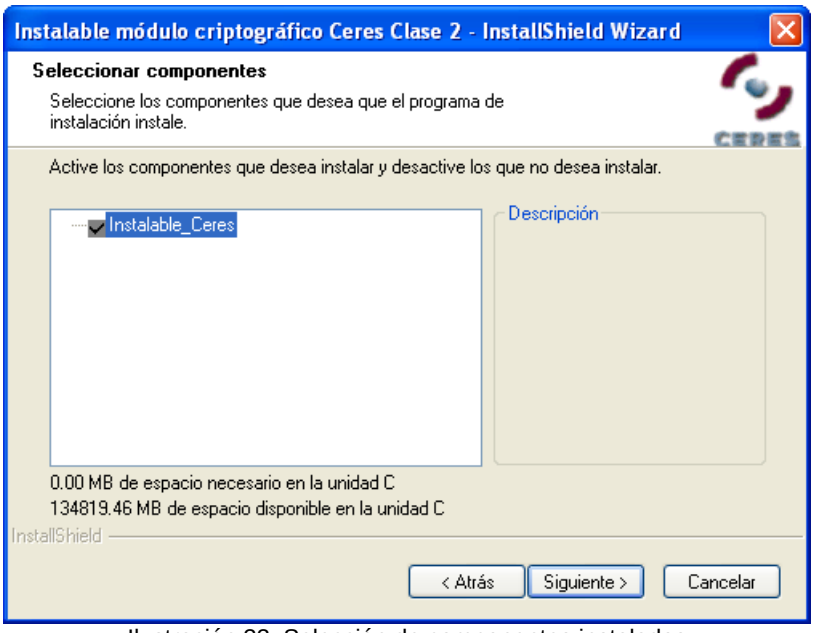

Ilustración 33. Selección de componentes instalados

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:

insmodcripc2v802.exe /zsx /Ly

Donde *x* es el número de segundos de espera antes de reiniciar el equipo automáticamente tras la instalación (10 por defecto si no se indica nada), e *y* el idioma de instalación (1034 para castellano, 1027 para catalán, 1110 para gallego y 1069 para euskera).

Al invocar la versión desatendida del instalable, lo primero que se muestra es una pantalla indicando que se está preparando la instalación (Ilustración 34).

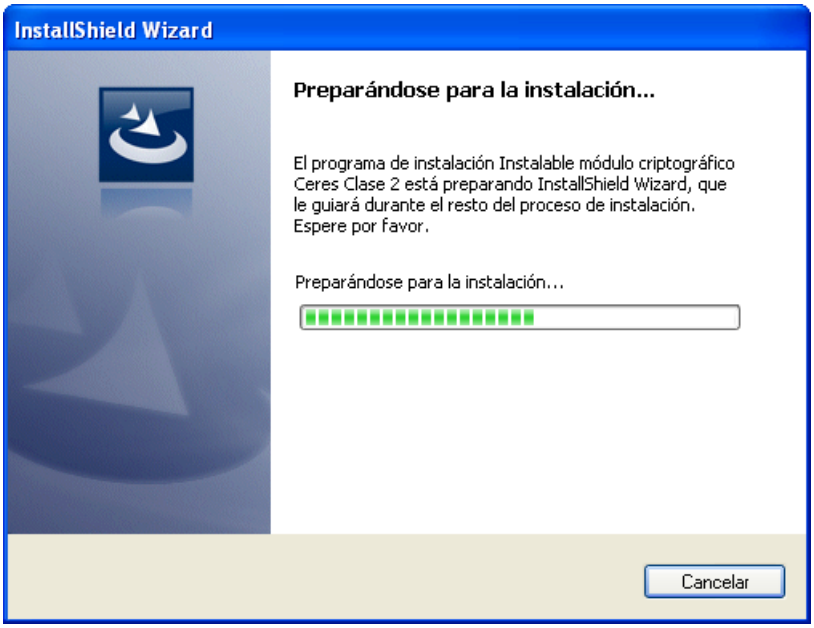

Ilustración 34. Preparando la instalación

Al finalizar la instalación provoca el reinicio automático del sistema, informando previamente en una ventana de los segundos restantes (Ilustración 35).

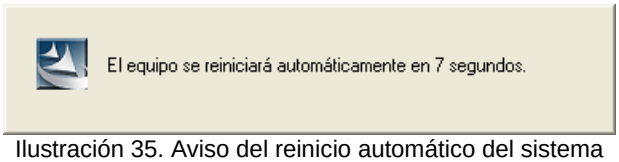

Ilustración 35. Aviso del reinicio automático del sistema

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.