Signe AC

Manual de Usuario de eToken

Documento:	SIGNE-ES-AC-MU-05
Versión:	1.3
Fecha:	05/09/2023
Tipo documento:	PÚBLICO

Registro de Versiones

Versión	Cambios	Fecha
1.0	Creación inicial del documento	14/05/2021
1.1	Se añade el punto notificación final	27/09/2022
1.2	Se sustituye el Viafirma Desktop por el RA Token Activation para la instalación de certificados en Token	31/01/2023
1.3	Nueva contraseña por defecto para los Token: "0000"	05/09/2023

Índice

1 Objetivo

El presente manual describe el modo de uso del dispositivo Token suministrado por la Autoridad de Registro de Signe.

2 Ámbito de aplicación

Este documento se aplica a los usuarios finales que han solicitado un certificado digital en Token a Signe AC.

3 Documentación relacionada

007-013559-007-_SafeNet Authentication Client_ 10.6_Windows_Post GA_Release Notes_Rev D
007-013560-005_SafeNet Authentication Client_10.6_Administrator_Guide_Windows_Rev B
700-013561-005-Safenet Authentication Client_10.6_GA_User_Guide_Rev B

4 Actividades

La generación del certificado en un token debe ser realizada en el navegador Internet Explorer. Puede hacer que este navegador sea el predeterminado o usar los enlaces en la ventana del navegador.
Los enlaces recibidos en los correos electrónicos se pueden copiar haciendo click con el botón derecho del ratón encima del enlace y eligiendo “Copiar Hipervínculo” para luego poder pegarlo en una ventana del navegador.

4.1 Instalación de drivers

Para poder hacer uso del certificado, deben instalarse los drivers del fabricante del token. El token suministrado es Safenet eToken 5110.

Los drivers y la documentación se pueden encontrar en la página web del fabricante www.gemalto.com, https://cpl.thalesgroup.com/access-management/authenticators/pki-usb-authentication/etoken-5110-usb-token, pero también los puede encontrar en la página web de Thomas Signe en el apartado de Certificación Electrónica/Soporte.

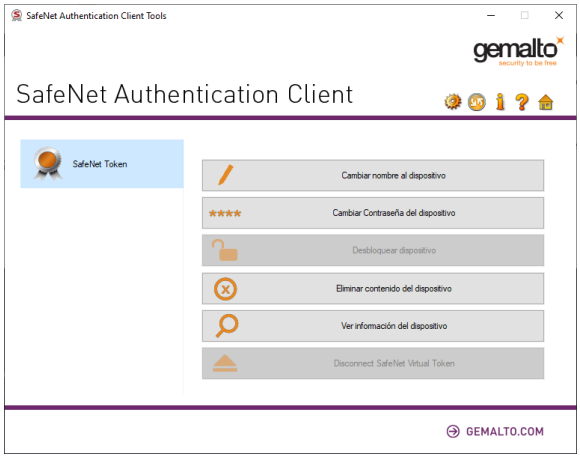
En la documentación del fabricante están incluidos los medios de contacto para cualquier problema en el dispositivo en el apartado “Support Contacts”.

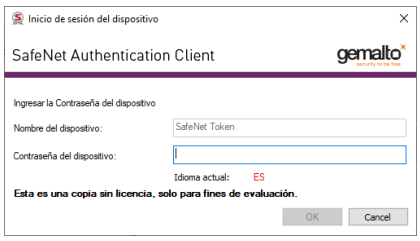
A continuación, indicamos los pasos a seguir para la correcta instalación de los drivers del fabricante del token:

1. Descargar el fichero comprimido "***DriversGemalto.rar***"
2. Guardarlo en una carpeta local y descomprimirlo.
3. Se habrán creado varias carpetas. Ir a la carpeta: ***CARPETA LOCAL*** *y* seleccionar la carpeta "*x32*" o "*x64*" dependiendo del sistema operativo de 32 o 64 bits del PC.
4. Ejecutar el programa incluido "*SafeNetAuthenticationClient-x32-10.6.msi*" o "*SafeNetAuthenticationClient-x64-10.6.msi*" y seguir las instrucciones del instalador.
5. Reiniciar el sistema.
6. Insertar el token en el conector USB del ordenador.
7. Si es la primera vez que se utiliza, pedirá el cambio de contraseña. Por defecto, la contraseña es "1234567890" o "0000".
8. Usar una contraseña segura y estará listo para instalar los certificados en el token.

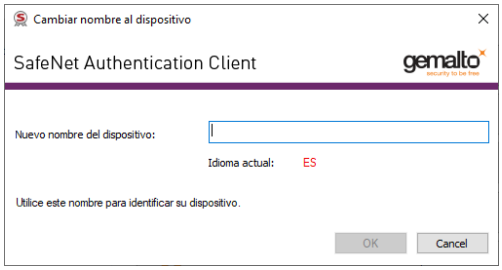
4.2 Gestión de Token

Para la gestión del token podemos utilizar el programa SafeNet Authentication Client Tools instalado en nuestro PC.



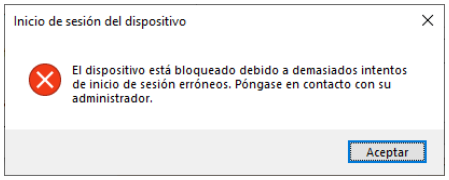


1. Cambiar nombre al dispositivo. Podemos otorgar un nombre al dispositivo para tenerlo fácilmente identificado.

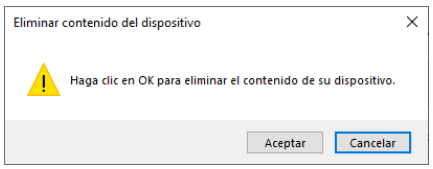


2. Cambiar contraseña del dispositivo. En cualquier momento puede modificarse la contraseña del dispositivo, para ello deberemos indicar primero la contraseña actual y después definir por duplicado la nueva contraseña. Esta contraseña debe cumplir los requisitos de seguridad definidos.

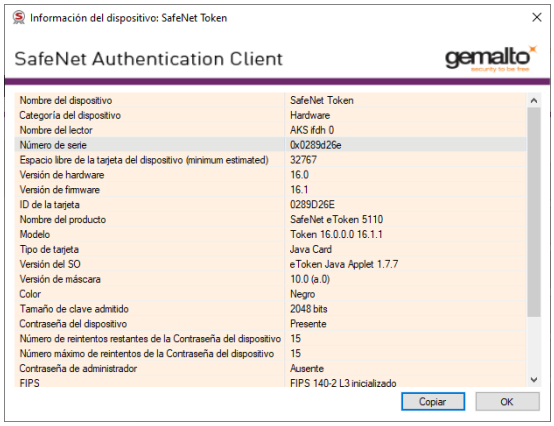
3. Desbloquear dispositivo. Si ha superado el máximo de intentos fallidos el dispositivo se bloqueará. Para desbloquearlo únicamente podrá hacerlo un Administrador. Otra opción es inicializar el dispositivo aunque con esta opción se perderá cualquier certificado que pueda contener el token.



4. Eliminar contenido del dispositivo. Esta opción elimina por completo, sin opción a volver a recuperarlo, cualquier certificado que tengamos instalado en el dispositivo.



5. Ver información del dispositivo. Accedemos a la información detallada del dispositivo conectado.



6. Opciones avanzadas.

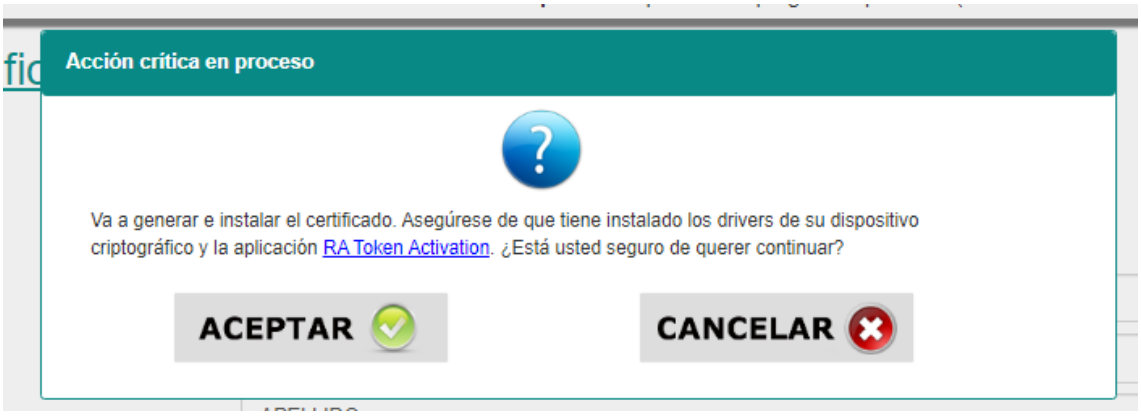
Desde la vista avanzada del dispositivo accedemos a otras funcionalidades, algunas son comunes desde la vista sencilla del dispositivo.

Desde esta vista avanzada podemos realizar las siguientes acciones:

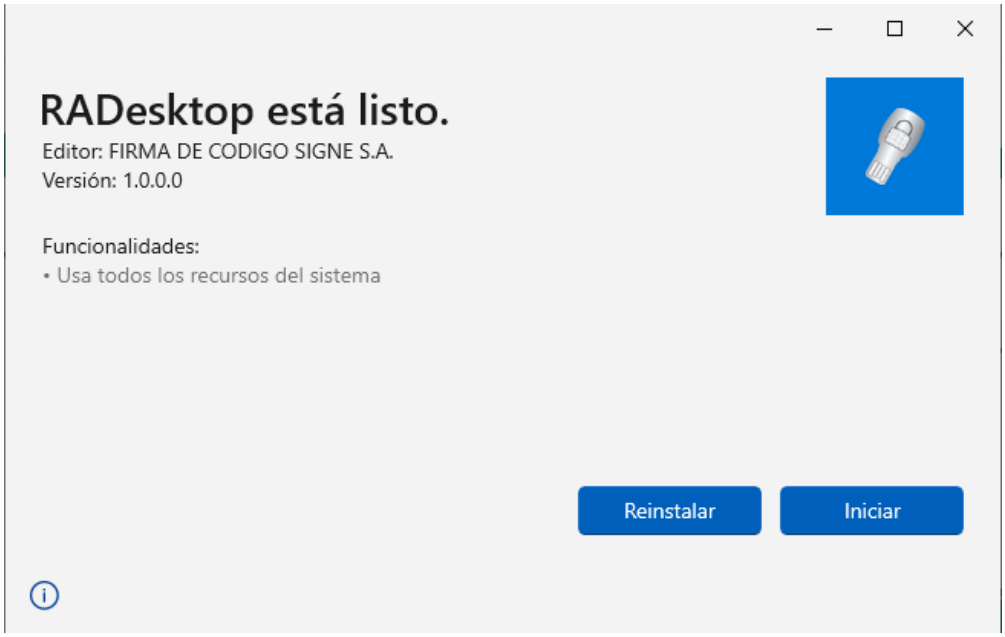
- Inicializar el dispositivo
- Iniciar sesión en el dispositivo
- Importar certificado
- Cambiar la contraseña
- Cambiar nombre al dispositivo
- Copiar al portapapeles
- Cerrar sesión en el dispositivo

4.3 Descarga e instalación RA Token Activation

Previamente a la descarga del certificado, es requisito necesario la instalación de la herramienta *RA Desktop.*
El software está disponible para su descarga desde la web, en la dirección RA Token Activation



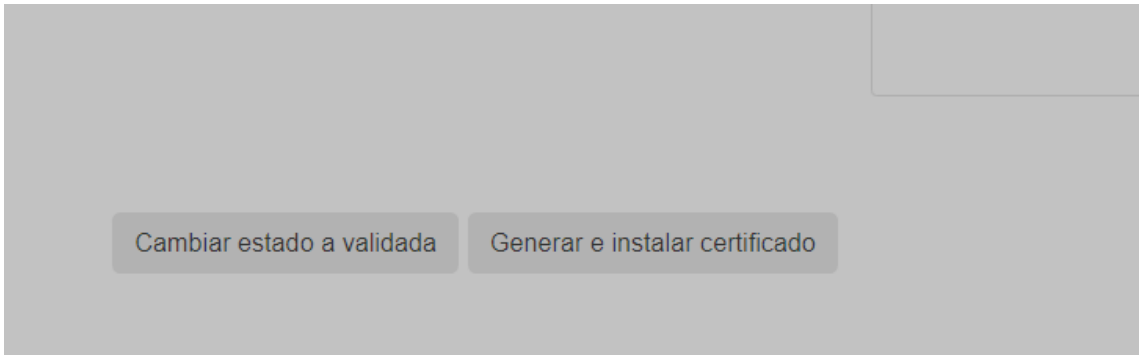
1- Tras su descarga, ejecutar el instalador, e instalar el software en el equipo.



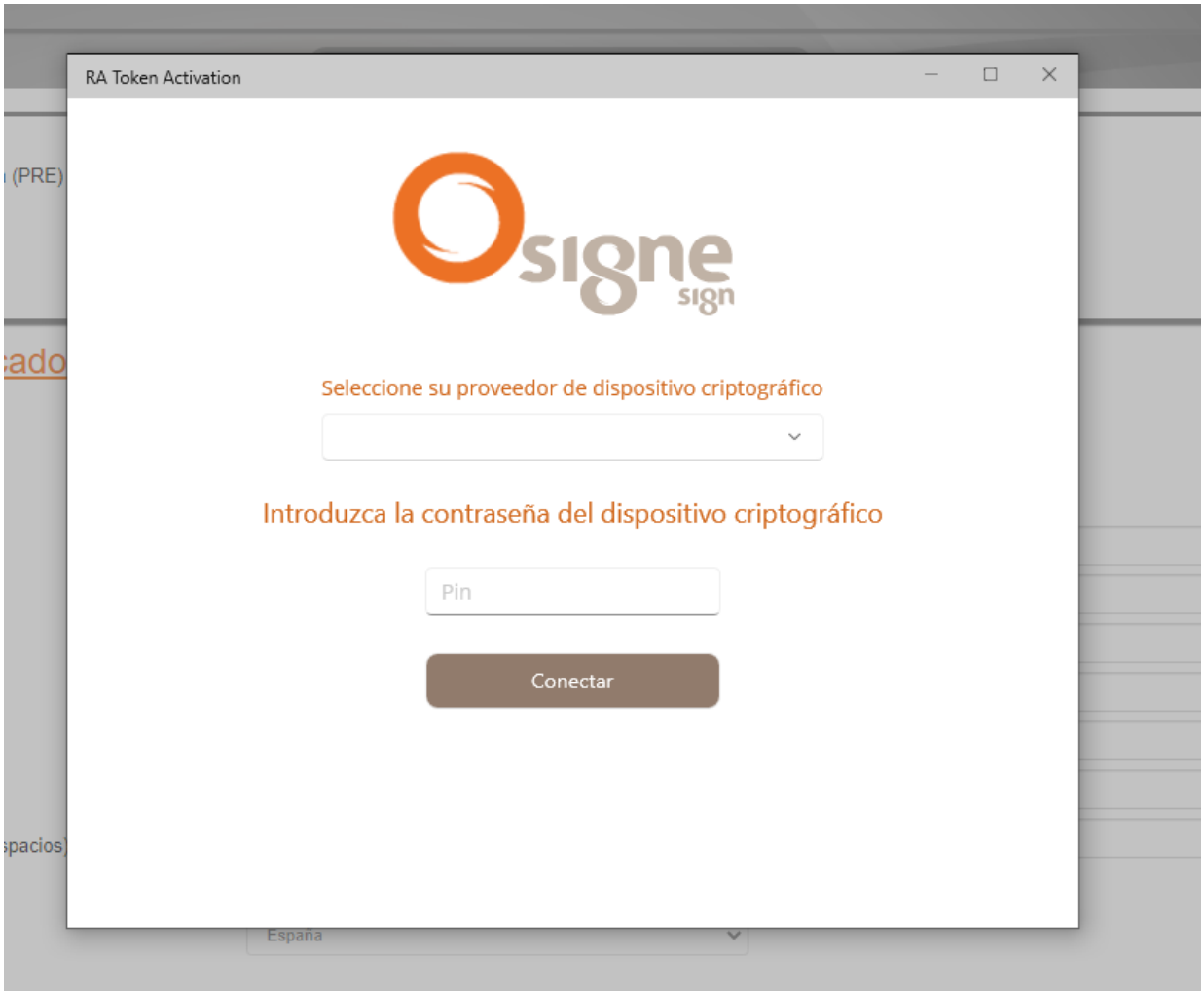
2- Cerrar el asistente una vez completadala instalación.

4.4 Generación del certificado

Para la generación del certificado se debe pinchar en Generar e instalar certificado



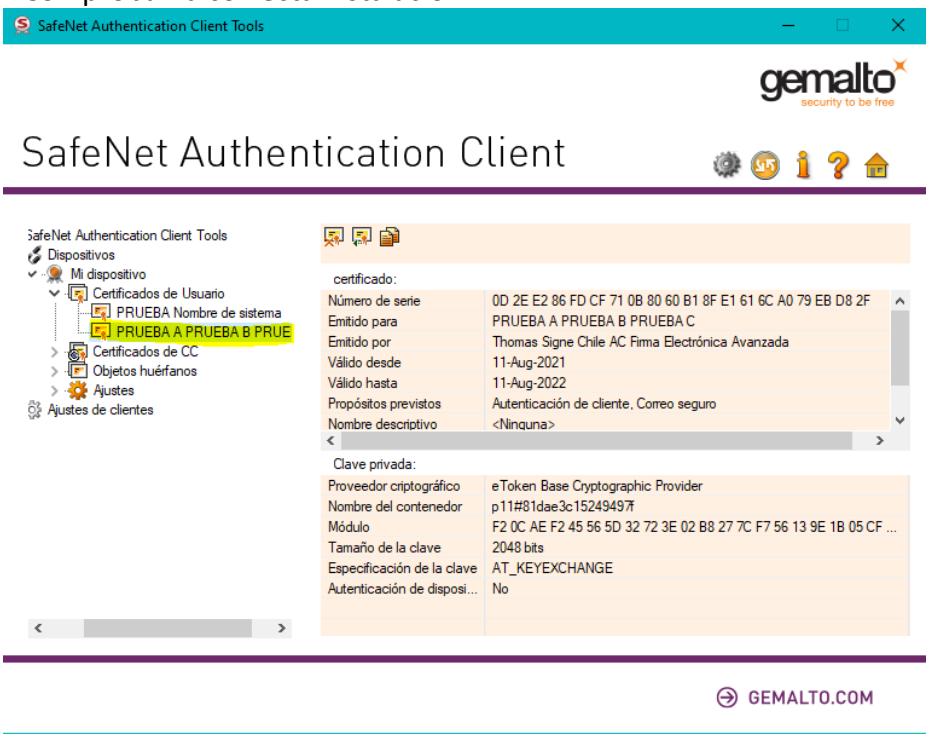
Se abrirá el RA Token Activation, seleccionar Safenet y teclear la contraseña del token



Indicará que se está conectando con el dispositivo y posteriormente generando claves

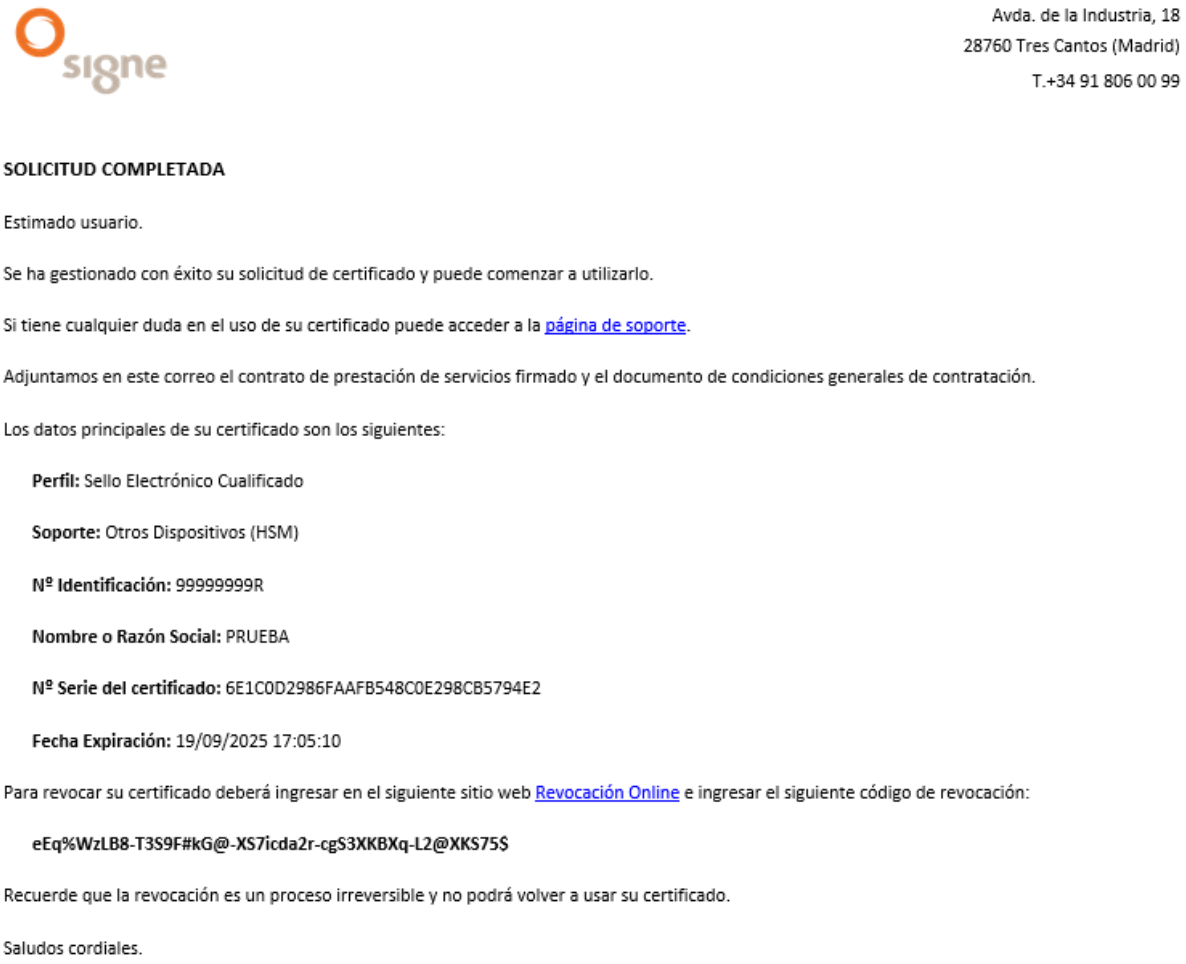
Finalmente indicará certificado descargado con éxito

Comprobar la correcta instalación



4.5 Notificación final

Tras la descarga del certificado el usuario recibirá una notificación final desde signe-ac@signe.com adjuntando la Solicitud y Aceptación del Servicio y las Condiciones Generales de Contratación, y los datos del certificado, así como un enlace a la página de soporte y los datos del certificado.



Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
T.+34 91 806 00 99

SOLICITUD COMPLETADA

Estimado usuario.

Se ha gestionado con éxito su solicitud de certificado y puede comenzar a utilizarlo.

Si tiene cualquier duda en el uso de su certificado puede acceder a la página de soporte.

Adjuntamos en este correo el contrato de prestación de servicios firmado y el documento de condiciones generales de contratación.

Los datos principales de su certificado son los siguientes:

Perfil: Sello Electrónico Cualificado

Soporte: Otros Dispositivos (HSM)

Nº Identificación: 99999999R

Nombre o Razón Social: PRUEBA

Nº Serie del certificado: 6E1C0D2986FAAFB548C0E298CB5794E2

Fecha Expiración: 19/09/2025 17:05:10

Para revocar su certificado deberá ingresar en el siguiente sitio web Revocación Online e ingresar el siguiente código de revocación:

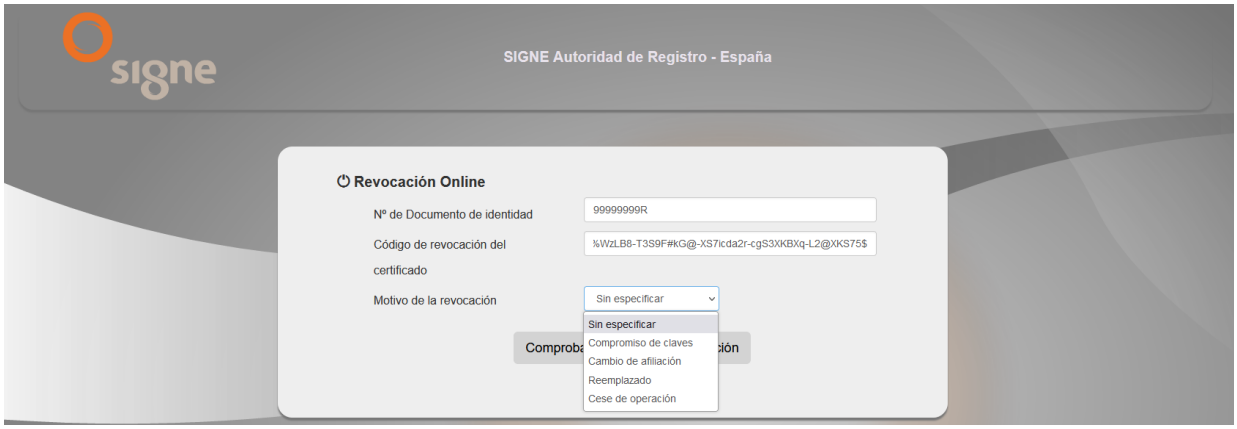
eEq%WzLB8-T3S9F#kG@-XS7icda2r-cgS3XKBXq-L2@XKS75$

Recuerde que la revocación es un proceso irreversible y no podrá volver a usar su certificado.

Saludos cordiales.

En el correo encontrará un enlace y un código para poder realizar la revocación del certificado.

El enlace llevará al usuario a la plataforma de revocación donde en caso de querer revocar el certificado, deberá indicar el número del documento de identidad, el código de revocación que se indica en el correo y seleccionar el motivo de revocación.



5 Datos de contacto

Si tiene algún problema con la gestión del certificado puede ponerse en contacto con nuestro servicio de soporte en los siguientes datos de contacto:

Signe
Correo electrónico de soporte: soporte@signe.com
Correo electrónico de información: comercial@signe.es

Una compañía de GRUPO signe

www.signe.es

Avda. de la Industria, 18
28760 Tres Cantos (Madrid)
España

Tel.: + 34 918 06 00 99
comercial@signe.es