



Signe AC

Manual de Usuario de eToken

Documento: SIGNE-ES-AC-MU-05
Versión: 1.0
Fecha: 14/05/2021
Tipo documento: PÚBLICO

Registro de Versiones

Versión	Cambios	Fecha
1.0	Creación inicial del documento	14/05/2021

Índice

Índice	3
Objetivo	4
Ámbito de aplicación	4
Documentación relacionada	4
Actividades	4
Instalación de drivers	4
Gestión de Token	5
DATOS DE CONTACTO.....	7

Objetivo

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

Ámbito de aplicación

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

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

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.

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.

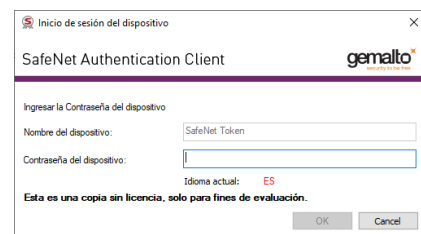
En la documentación del fabricante están incluidos los medios de contacto para cualquier problema en el dispositivo en el apartado “Support Contacts”.

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

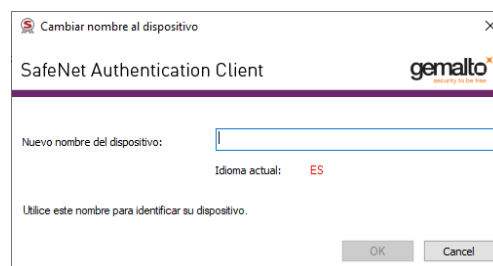
1. Descargar el fichero comprimido “**DriversGemalto.rar**”
2. Guardarlo en una carpeta local y descomprimirlo.
3. Se habrán creado varias carpetas. Ir a la carpeta: **CARPETA LOCAL** y seleccionar la carpeta “x32” o “x64” dependiendo del sistema operativo de 32 o 64 bits del PC.
4. Ejecutar el programa 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”.
8. Usar una contraseña segura y estará listo para instalar los certificados en el token.

Gestión de Token

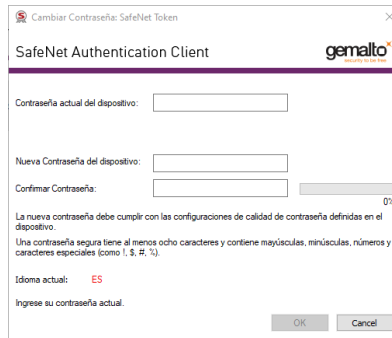
Para la gestión del token podemos utilizar el programa SafeNet Authentication Client Tools instalado en nuestro PC.



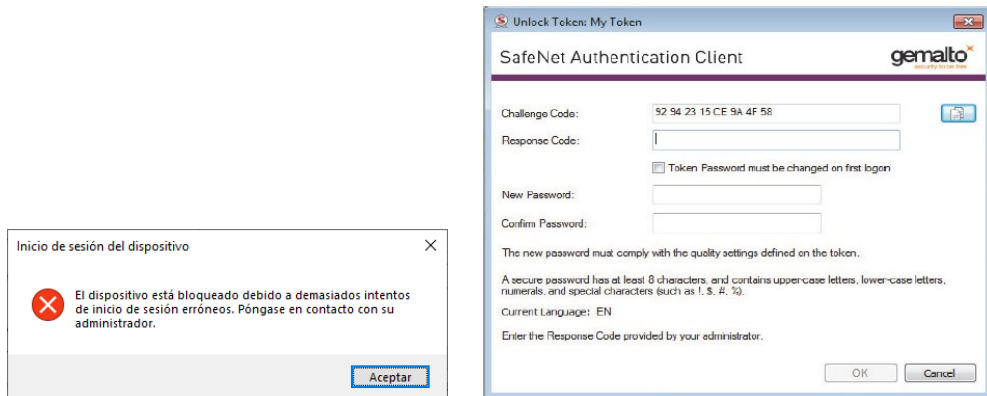
1. Cambiar nombre al dispositivo. Podemos otorgar un nombre al dispositivo para tenerlo fácilmente identificado.



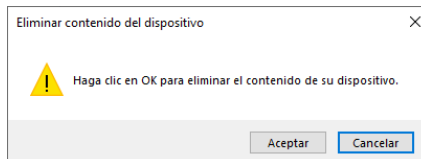
2. Cambiar contraseña del dispositivo. En cualquier momento puede modificarse la contraseña del dispositivo, para ello deberemos indicar primero la contraseña actual y después definir por duplicado la nueva contraseña. Esta contraseña debe cumplir los requisitos de seguridad definidos.



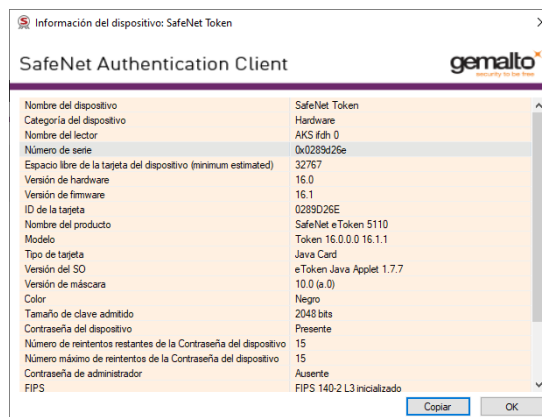
1. Desbloquear dispositivo. Si ha superado el máximo de intentos fallidos el dispositivo se bloqueará. Para desbloquearlo únicamente podrá hacerlo un Administrador. Otra opción es inicializar el dispositivo aunque con esta opción se perderá cualquier certificado que pueda contener el token.



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



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



4. 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

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

