



Signe AC

Manual de generación de certificados digitales en HSM Centralizado

Documento: SIGNE-ES-AC-MU-13
Versión: 1.3
Fecha: 30/09/2022
Tipo documento: PÚBLICO

Registro de Versiones

Versión	Cambios	Fecha
1.0	Creación inicial del documento	16/04/2019
1.1	Correcciones menores	14/05/2021
1.2	Se incluye apartado Notificación final	27/09/2022
1.3	Se incluye apartado Identificación del Firmante y pantalla login de Fortress	18/10/022

Índice

Índice.....	3
1 Objetivo	4
2 Ámbito de aplicación	4
3 Actividades.....	4
3.1 Identificación del Firmante	4
3.1.1 Personación.....	4
3.1.2 Video identificación	4
3.2 Activar su certificado.....	5
3.3 Notificación final	10

1 Objetivo

El presente manual describe el modo de generación de los certificados digitales en HSM Centralizado emitidos por Signe AC.

2 Ámbito de aplicación

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

3 Actividades

3.1 Identificación del Firmante

3.1.1 Personación

La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza regula en su artículo 7 la Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado:

La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

3.1.2 Video identificación

En la Orden ETD/465/2021, de 6 de mayo, se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

A tal efecto, Signe utiliza una herramienta que permite la identificación del firmante a través de medios telemáticos.

El usuario, tras haber proporcionado la documentación requerida para la gestión del certificado, recibirá un correo electrónico de la dirección de correo signe-ac@signe.com con un enlace para poder realizar la videoidentificación



ENLACE VIDEOIDENTIFICACIÓN

Le comunicamos que su solicitud de certificado digital ha sido aceptada y se está procesando en estos momentos.

Id solicitud: 2770

Suscriptor: fernando garcia

Nº Identificación: A99999999

Para continuar con el proceso es necesario validar su identidad mediante el proceso de videoidentificación automática.

Acceda al siguiente enlace y siga las instrucciones para llevar a cabo el proceso:

<https://pre-videoid.thesigne.com/video/E40A1515-D50E-4FE9-9F33-315F5C78B0BF>

Saludos cordiales.

El usuario deberá acceder al enlace y aceptar los términos y condiciones de la video identificación, en caso contrario será necesario realizar la personación ante un operador de registro de Signe para poder identificarse.

El usuario debe asegurándose de que esta en un lugar suficientemente iluminado para poder realizar la identificación.

La aplicación indica muy claramente los pasos a seguir:

- Enseñar el anverso del documento
- Enseñar el reverso (en su caso)
- Inclinar el documento para poder ver el holograma (en su caso)
- Acción a realizar por el usuario para tomar una grabación y fotografía

3.2 Activar su certificado

Tómate unos minutos para leer este manual y en 3 pasos podrás firmar todas las veces que quieras.

Activar usuario

NS No-reply Signe

Responder Responder a todos Reenviar

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.



En el correo haz clic en el botón activar usuario

Cuando acceda al enlace incluido en el mensaje, el usuario deberá configurar una contraseña para acceder al HSM Centralizado. La contraseña debe contener al menos una letra en minúscula, otra letra en mayúscula y algún número. Además, debe tener entre 8 y 15 caracteres. El usuario es el núm. de identificación.



Asignación de contraseña

Contraseña *

Confirme contraseña *

✓ Aceptar

Lo siguiente que debe hacer será activar el factor de autenticación **PASSWORD** para proteger el uso de su certificado digital.



Puede activar cualquiera de los siguientes factores de autenticación para proteger el uso de sus Certificados Digitales

••• Password

→ Aceptar

Tras realizar esta operación, la cuenta del usuario del HSM Centralizado quedará activada.



Info
La cuenta ha sido activada correctamente.

✓ Aceptar

Para acceder a la plataforma del HSM Centralizado (Fortress), el usuario debe identificarse en la plataforma mediante su usuario y posteriormente su contraseña. Para ello, tan solo tiene que acceder a la URL <https://fortress.signe.es/fortress/>



Usuario
|

Continuar

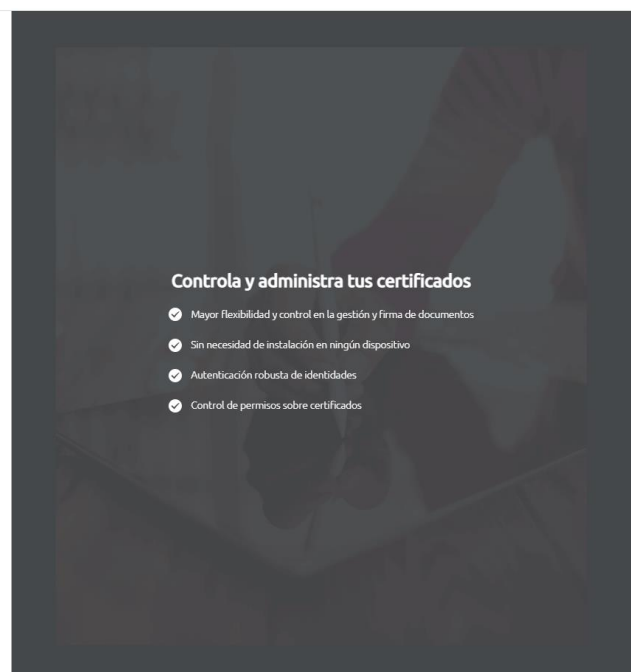
¿Olvidaste tu contraseña?

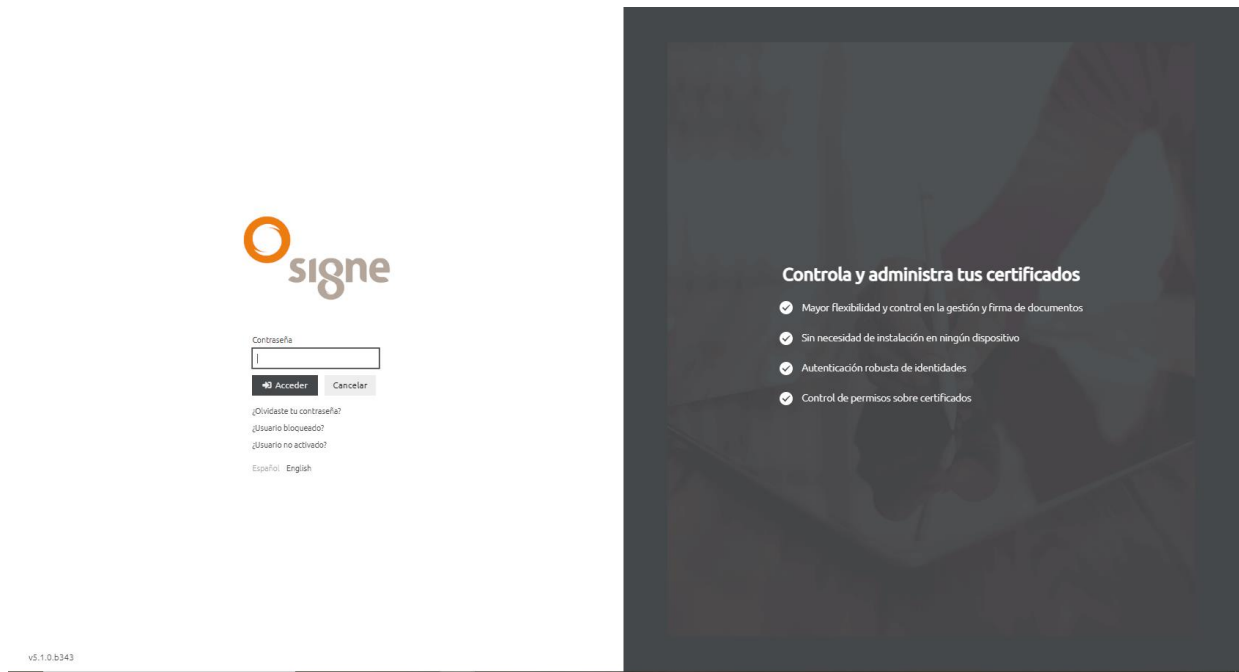
¿Usuario bloqueado?

¿Usuario no activado?

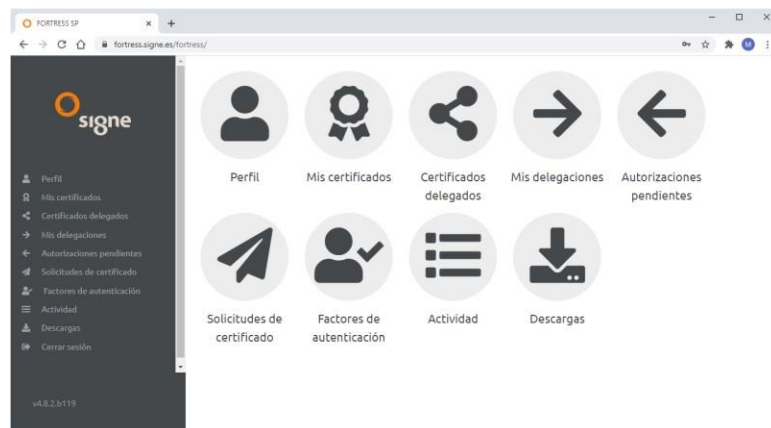
Español English

v5.1.0.b343





En la pantalla principal del sistema se muestran una serie de iconos para acceder a las diferentes secciones de la plataforma.



El usuario podrá utilizar su certificado digital en cualquier sitio web o aplicación que lo requiera, instalando en su PC con Windows el programa Signe HSM Centralizado Desktop, que podrá descargar directamente de su cuenta del HSM Centralizado, en el apartado “Descargas”.



Descargas

Una vez que el usuario haya instalado el ejecutable, deberá iniciar sesión en la aplicación. Recuerde que su usuario es su nº de identidad.



Cuando haya iniciado sesión podrá activar su certificado y poder utilizarlo de manera local en su PC.



3.3 Notificación final

Tras la activación 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: 6E1COD2986FAAFB548C0E298CB5794E2

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@XKS75S`

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.

The screenshot shows the 'Revocación Online' form in the SIGNE system. The form is titled 'Revocación Online' and contains the following fields and options:

- Nº de Documento de identidad:** 99999999R
- Código de revocación del certificado:** %WZLB8-T3S9F#kG@-X57icda2r-cgS3XKbXq-L2@XKS75\$
- Motivo de la revocación:** A dropdown menu with the following options:
 - Sin especificar (selected)
 - Sin especificar
 - Compromiso de claves
 - Cambio de afiliación
 - Reemplazado
 - Cese de operación

Below the form, there is a button labeled 'Comprobación'.

